



TIBCO BusinessConnect™

Trading Partner Administration

Version 7.4.0
May 2023



Contents

Contents	2
Participants	11
Participants Overview	11
Hosts and Partners	11
Managing Participants	12
Creating a New Participant	12
Exporting Participant Data	13
Importing Participant Data	14
Copying a Participant	15
Deleting a Participant	15
Searching for a Participant	16
Editing Participant Data	17
General Tab for Participants	18
Business Locations Tab for Participants	18
Credentials Tab for Participants	20
PKI (Public Key Infrastructure)	20
PGP (Pretty Good Privacy)	21
Managing Host Credentials	21
Managing Partner Credentials	26
Exporting PGP Keys	29
Protocols Tab for Participants	33
Enabling a Protocol	33
Disabling a Protocol	34
Configuring a Protocol	34
Managing Transports for Participants	35
Proxy Settings Tab for Partners	35
User Access Tab for Participants	37

All Authorized Users	37
Adding Users with Access Rights	38
Adding Groups with Access Rights	38
Visibility Tab for Partners	39
Configuring Participant Visibility Settings for tibbr	39
Configuring Participant Visibility Settings for TIBCO BusinessEvents	40
Business Agreements	42
Business Agreements Overview	42
Identifying the Participants for a New Business Agreement	43
Selecting Participants	43
General Tab for Business Agreements	43
Adding a Protocol Binding	44
.....	44
Configuring a Protocol	45
User Access Tab for Business Agreements	51
All Authorized Users	52
Adding Internal Users	52
Adding Groups	53
Operations Editor	54
Operations Editor Overview	54
Importing and Exporting Operations	55
Importing an Operation	55
Exporting an Operation	56
File Specification Dialog	57
System Settings	59
General	59
Certificate Store	60
.....	60
Credentials Tab	60

New Identities Tab	61
Server Identities and Certificates Tab	66
Inbound Public Transport Types	67
Inbound Mail POP3 Servers	68
Outbound HTTP/FTP Proxy and Mail SMTP Servers	70
Adding a Proxy for a Host	71
Selecting the Default Proxy for a Host	73
Audit, Non-Repudiation and Runtime Database Configuration	74
User Authentication Configuration	75
Adding an Authentication Source	75
Activated Protocol Plug-ins and Properties	78
Metadata Type Configuration	102
Adding and Removing Metadata	103
Private Process Smart Routing	103
Creating Business Rules for Private Process Smart Routing	104
Managing Business Rules for Private Process Smart Routing	106
Credential Expiry Alerter	107
Configuring the Credential Alerter	108
User Access Audit Trail	109
Grouping Search Results	111
Utilities	112
Exporting Schemas	112
Visibility	112
Configuring tibbr Settings	112
Configuring TIBCO BusinessEvents Settings	115
Configuring Application Monitoring and Management Settings	117
User Access Management	123
Overview	123
TIBCO Administrator User Categories	123
User Management	124
Using TIBCO Administrator User Management	124

Setting TIBCO BusinessConnect Access Rights for a User	125
Managing Users with TIBCO BusinessConnect User Management	126
Adding Users	128
Editing Users	133
Authenticating External Users	140
Editing LDAP Connection	140
Removing Users	141
Searching for Users	141
Managing Groups with TIBCO BusinessConnect User Management	141
Adding a Group	141
Log Viewer	148
Overview	148
Audit Logs	148
Non-Repudiation Logs	148
Resend Logs	149
Performing Log Searches	149
Setting Preferences	150
Performing a Log Search	153
Viewing Search Results	155
Summary View	156
Transaction Details View	156
State Details View	156
Canceling Transactions	157
Saving and Reusing Queries	158
Saving a Query	158
Reusing a Query	159
Resending Transactions	159
Resendable Transactions	159
Viewing Resend History	160
Reporting	162

Overview	162
Generating Reports	162
Inbound Transaction Per Protocol	163
Outbound Transaction Per Protocol	163
External Reporting	164
Email Transport	165
Email Overview	165
Configuring POP3 and SMTP for Email	168
Configuring the POP3 Server Polling Service	168
Configuring an SMTP Server for a Host	168
Configuring an SMTP Server for a Partner	168
Setting Up Email for a Trading Host	169
Selecting Email for the Trading Host	169
Setting the Host's Email Address for a Protocol	169
Setting Up Email for a Trading Partner	169
Configuring Email for a Trading Partner	170
Setting the Partner's Email Address for a Protocol	173
Configuring Email for a Business Agreement	174
FTP and FTPS Transports	175
FTP Transport Overview	175
FTP/S Inbound	177
FTP/S Outbound	178
Setting Up FTP/S for a Trading Host	179
Enabling FTP/S Inbound	179
Selecting and Configuring FTP/S Inbound	179
Setting Up FTP/S for a Trading Partner	183
Configuring FTP/S Outbound	184
Setting Up FTP Proxies	187
SSHFTP Transport	188

SSHFTP Transport Overview	188
Setting Up SSHFTP for a Trading Host	188
Enabling SSHFTP Inbound	189
Selecting and Configuring SSHFTP Inbound	189
Setting Up SSHFTP for a Trading Partner	198
Configuring SSHFTP Outbound	198
HTTP, HTTPS, and HTTPSCA Transports	202
Overview	202
Setting Up HTTP/S for a Trading Partner	203
Configuring HTTP/S for a Trading Partner	203
Setting Up HTTP Proxies	206
FIPS Mode Support	207
Configuring Internal Key and Certificates for FIPS	208
AS2 Transport	210
AS2 Transport Overview	210
AS2 Transport	210
AS2 Identifiers	214
Setting Up AS2-HTTP/S for a Trading Host	215
Setting the Host's AS2 Identifier for a Protocol	215
Setting Up AS2-HTTP/S for a Trading Partner	216
Configuring AS2-HTTP/S for a Trading Partner	216
Synchronous and Asynchronous Receipts	221
AS1 Transport	223
AS1 Transport Overview	223
AS1 Transport	223
Configuring POP3 and SMTP Servers for AS1 Email	227
Configuring the POP3 AS1 Email Server	227
Configuring an SMTP Server for a Host	227
Configuring an SMTP Server for a Partner	227

Setting Up AS1 Email for a Trading Host	228
Selecting AS1 Email for the Trading Host	228
Setting the Host's Email Address for a Protocol	228
Setting Up AS1 Email for a Trading Partner	228
Configuring AS1 Email for a Trading Partner	229
Setting Up the Partner's Email for a Protocol	232
Configuring AS1 Email for a Business Agreement	233
File Transport	234
File Transport Overview	234
Outbound File Transport	234
Configuring Outbound File Transport for a Partner	235
Outbound File Pollers	237
Inbound File Pollers	237
Enabling and Configuring Inbound File Poller	237
Selecting File Inbound in the Business Agreement	238
Inbox Transport	239
Inbox Transport Overview	239
Outbound Inbox Transport	239
Configuring Outbound Inbox Transport for a Partner	239
Message Disposition Notification Receipts	242
Overview	242
Configuring MDN Receipts	243
MDN Receipts and Business Acknowledgments	244
MDN Messages Sent to Private Processes	244
Troubleshooting	246
Troubleshooting Transport Problems	246
All Transports	246
FTP Transport	247
Email Transport	247

Troubleshooting Database Problems	248
Scripts	250
Overview	250
FTP Scripts	250
Document Security through PGP	251
File Scripts	252
FTP Inbound	252
FTP and File Outbound	253
Supported FTP Commands	255
File Outbound	256
Managing Errors	257
Retrying Document Posting	257
Returning Errors from Scripts	257
Audit Logging in Scripts	258
Remote Client Service Audit Log	260
Overview	260
TIBCO BusinessConnect Remote Audit Log Viewer	260
Application Monitoring and Management by Processing Rulebases	262
Overview	262
Creating a Rulebase	262
Building a Rule	262
Specifying a Data Source	264
Defining Tests	265
Creating a New Test	266
Building a Test Expression	267
Building Compound Tests	267
Using Advanced Test Features	269
Defining Actions	269
Using Advanced Action Features	271

Saving a Rulebase	272
Working with Rulebase Files	272
TIBCO Documentation and Support Services	273
Legal and Third-Party Notices	275

Participants

This section provides both conceptual and procedural information to help you configure participants for TIBCO BusinessConnect hosts and trading partners.

For general information about this product and its architecture, components, and various usage and deployment scenarios, see *TIBCO BusinessConnect™ Concepts*.

To install and configure the BusinessConnect server, see *TIBCO BusinessConnect™ Installation and Configuration*.

Participants Overview

Participants store a variety of information about trading partners, from the very general (for example the location of the company headquarters) to the detailed (for example, security credentials and available protocols).

Hosts and Partners

TIBCO BusinessConnect defines two types of participants that can exchange electronic documents:

- **Hosts** A host is a participant in a business agreement and an organizational entity within your company. Hosts participate in the electronic documents exchange using the TIBCO BusinessConnect B2B gateway. One host or multiple hosts might exist, of which private keys are stored by TIBCO BusinessConnect.
- **Partners** A partner participant is outside of your company and typically has its own B2B gateway, either TIBCO BusinessConnect or some other solution. Your BusinessConnect installation stores public keys for your partners.

There is little difference between hosts and partners because much of the same information is required to configure both types of participants. An agreement has to be established between a host and a partner.

Managing Participants

You can manage participants as follows:

- **Create a new participant** Create a new participant as explained in [Creating a New Participant](#).
- **Export or import a participant** Export an existing participant's data for use in another BusinessConnect installation and/or import a participant from another BusinessConnect installation, as explained in [Exporting Participant Data](#).
- **Copy an existing participant** Copy the participant's data. See [Copying a Participant](#) for more information.
- **Delete a participant** Remove the participant from your system. See [Deleting a Participant](#) for more information.
- **Edit participants data** After the participants are created, their data can be changed. See [Editing Participant Data](#).
- **Search for a participant** Use the Search function to search for participant. See [Searching for a Participant](#) for more information.

Creating a New Participant

**Note**

Before you start creating any participants, you must have at least one protocol installed.

To create a new participant:

1. Click **BusinessConnect > Participants**.
2. Click **New**.
3. Type the name in the **Participant Name** field.
4. Select **Host** or **Partner** from the list.

Select **Host** if this participant is internal to your enterprise; select **Partner** if this participant is external to your enterprise.

**Note**

Default Host: 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 in **System Settings > General**. You cannot delete the default host; therefore, if you have only one host participant, you cannot delete it. To delete a default host, first assign a different host participant as the default host, creating a new host participant if necessary.

5. Click **OK**.

A new dialog is displayed allowing you to provide detailed information about the participant.

6. Select the **Active** checkbox if you want to activate this participant right away. Otherwise, you can activate this participant later.

**Note**

If the participant is activated, all grammar rules associated with this participant are validated. No validation is performed for an inactive participant. This allows the user to provide only a partial information while the participant is still inactive, and then add the remaining required information when activating the participant.

7. Provide as much information as you require about the address and contact information for the company headquarters.

**Note**

To select legal and support contacts, you must first add these contacts to the system. Add contacts to a business location. See [Business Locations Tab for Participants](#) for more information.

Exporting Participant Data

To export participant data from one BusinessConnect installation to another, perform these steps:

1. Expand **BusinessConnect > Participants**.
2. Select the checkbox next to the participant(s) that you want to export.
3. Click **Export**.

4. In the Export Participants dialog, set the password if needed.
5. Click **Export Configuration Data**.

This creates the .csx file with the compressed data of the exported participant.

6. Save the file to the desired location.

Import this .csx file into another BusinessConnect installation.

7. Click **Done**.

**Note**

When a participant is exported, the associated business agreements and the host/partner with which the agreement exists, are also exported automatically. If a host is exported, all partners with which the host has business agreements are also exported, along with those business agreements. If a partner is exported, all hosts with which the partner has business agreements are also exported, along with those business agreements. In configurations where a large number of partners exist, to accomplish a delta export of just one or few partners, it is advisable to select only those partners. Selecting the host(s) is redundant and can also slow down the export by exporting all other partners, which are associated with those hosts.

Importing Participant Data

**Note**

Before importing participant data into a BusinessConnect installation, first install and activate all protocols associated with the participants and import all operations associated with the participants.

To import participant data, perform the following steps:

1. Expand **BusinessConnect > Participants**.
2. Click **Import** and then click the link **change** to identify the .csx file that contains the participants for import.
3. Click **Browse** to navigate to and select the .csx file that was created during the export of participant data.
4. Enter the password, if it was used to secure the data during the export.

5. Click **Import Participants**.
6. Click **Done**.

Copying a Participant

To copy a participant, perform these steps:

1. Expand **BusinessConnect > Participants**.
2. Select the checkbox next to the participant you want to copy.
3. Click **Copy**.
4. In the next dialog, enter the name for the new participant.

If you open the new participant, you will see that most of its general, business, credentials, protocols, and proxy data has been transferred from the participant it was copied from.



Note

When you create a new participant by using the Copy function, any unique constraints such as domain IDs, AS transport IDs, and name of the trading partner will not be copied. This data must be later entered for the new trading partner using the steps as explained in [Editing Participant Data](#).

Deleting a Participant

Deleting a Host




Note

Default Host: 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 in **System Settings > General**.

You cannot delete the default host; therefore, if you have only one host participant, you cannot delete it unless you add a replacement host.

You must first add at least one new host following the steps described in [Creating a New Participant](#), and then remove the host you do not need any more.

1. Expand **BusinessConnect > System Settings > General**.
2. Make sure that the host selected in the **Default Host** list is not the one you wish to delete.

 **Note:** You cannot select **None** as the default host. Select an actual host for the default.

3. Click **Save**.
4. Expand **BusinessConnect > Participants**.
5. Select the checkbox next to the host you want to delete.
6. Click **Delete**.

Deleting a Partner

To delete a partner, perform these steps:

1. Expand **BusinessConnect > Participants**.
2. Select the checkbox next to the participant you wish to delete.
3. Click **Delete**.

Searching for a Participant

In addition to entering the participant's name or selecting it from the list, you can use the Search function to find a specific participant. This allows you to use a wildcard and search for a participant's name when you do not know the exact (full) name.

1. Enter the search string by using the wild card to substitute any characters before, after, or before and after the string you are entering.
2. Click **Search**.

3. The participant name(s) that correspond to the search criteria will be displayed in the Name list, while the others will be removed
4. To view all participants, click the **Show All** link.

Editing Participant Data

To edit participant's data, click the participant whose information you wish to edit. The Edit Participant dialog is displayed.

Figure 1: Editing a Participant

The screenshot shows the 'Edit Partner Participant: Company2' dialog box. At the top, there are buttons for 'Save', 'Cancel', and 'Apply'. Below these are tabs for 'General', 'Business Locations', 'Credentials', 'Protocols', 'Proxy Settings', 'User Access', and 'Visibility'. The 'General' tab is selected. It contains the following fields:

- Participant Name: Company2
- Active: ☒
- Type: Partner
- Headquarters Business Location section:
 - Address 1st Line: [text box]
 - Address 2nd Line: [text box]
 - Address 3rd Line: [text box]
 - City/State/Zip Code: [text box] [text box] [text box]
 - Country: [text box]
 - Phone: [text box]
 - Fax: [text box]
 - Email: [text box]
 - Web URL: [text box]
 - Primary Legal Contact: [dropdown menu]
 - Primary Support Contact: [dropdown menu]

The following tabs are available for managing participants:

- [General Tab for Participants](#)
- [Business Locations Tab for Participants](#)
- [Credentials Tab for Participants](#)
- [Protocols Tab for Participants](#)
- [Proxy Settings Tab for Partners](#) (only for partner participants)

- [User Access Tab for Participants](#)
- [Visibility Tab for Partners](#) (only for partner participants)

General Tab for Participants

The General tab allows you to add or change the participant's data such as address and email.

Most of these fields are optional, except for the following:

- Participant Name
- Active checkbox (select to activate the participant)

For the following fields, you have to pay attention while entering data:

- **Primary Legal Contact** and
- **Primary Support Contact** These contacts can also be entered using the Business Location tab.

Once you enter all contacts using the Business Location tab, you will come back to the General tab and select the appropriate contacts from the lists that will have the contact entries.

Business Locations Tab for Participants

A business location is simply the address and other identifying information for a participant. One participant often has multiple departments or other distinct groups at various locations. You can set up multiple locations for one participant to simplify shipping and billing procedures.

A business location can include contacts. A contact is the name, phone number, and email address of a person associated with a particular location of a participant. Each business location can have multiple contacts.

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

1. Expand **BusinessConnect > Participants** and then click the name of the participant you are editing.
2. Select the **Business Locations** tab.

3. Click **New**.

The New dialog is displayed.

Provide values for each of the appropriate text fields as explained in [Business Location, New Dialog](#).

Business Location, New Dialog

Field	Enter
Name	(Required) Only the Name field is required as it identifies the participant. You cannot leave “unnamed” in this field.
Address 1st Line Address 2nd Line Address 3rd Line	Enter the participant’s address.
City/State/Zip Code	Enter the participant’s data.
Country	Enter country name.
Phone/Fax/Email/Web URL	Enter the participant’s data.
Primary Legal Contact	Select an item from the list.
Primary Support Contact	Select an item from the list.

4. To assign primary legal and/or support contacts to this business location, or if you want to add contacts to this participant, create these contacts as follows:

Click **New**.

The New Contact screen is displayed:

Business Location, New Contact

Field	Enter
First Name, Last Name	Enter the participant's data.
Contact Type	Select a contact type from the list. Only contacts designated as type Legal or Support will be available from the Primary Legal Contact and Primary Support Contact lists in the business location.
Email, Phone, Fax, Pager	Enter the participant's data.

After you finish entering data and click **Save**, your contact is displayed in the section Contacts.

To delete this contact at any time, select the checkbox next to the contact's name and click **Delete**.

5. Click **Save**.

Credentials Tab for Participants

BusinessConnect uses two methods of public key cryptography:

PKI (Public Key Infrastructure)

This method uses a hierarchical key management system that includes a certification authority (CA). The CA issues digital certificates by binding the identity of a user or a system to a public key with a digital signature. The host can use the trading partner's public key to authenticate a sender, enable non-repudiation, encrypt a transport, or encrypt a message.

PGP (Pretty Good Privacy)

PGP does not use Certificate Authorities and instead each public key is bound to a username and/or an e-mail address. A "web of trust" is used to establish the authenticity of the binding between a public key and its owner. In BusinessConnect, PGP keys are used for message signatures and encryption on the FTP, FTPS, SSHFTP transports.

**Note**

To learn how to work with keys, you can use the samples provided with this program in the directory `BC_HOME/samples/keys`. Keep in mind that the chosen password is `Password1`.

Managing Host Credentials

There are several credentials available for a host that can be uploaded using the Credentials tab:

- [New Private Key](#)
- [New SSH Private Key](#)
- [Generating New PGP Key Pairs](#)
- [Assigning a Shadow Key for the Host](#)
- [Exporting PGP Keys](#)

New Private Key

To upload a private key for the host, perform these steps:

1. Expand **BusinessConnect > Participants > host > Credentials** tab.
2. Click **New Private Key**.
3. Type the name of the key in the **Alias** field.
4. In the Current Credential line click **change**.
Browse and navigate to the file containing the private key and click **OK**.
5. Click **set** next to **Password**.
Type the password (required for private keys) in the **Enter Password** and **Enter**

Password Again fields.

If you are using any of the sample keys provided in the directory *BC_HOME\samples\keys*, the password is "Password1".

6. Click **OK and Save**.

The new private key for the host is now listed in the Credential Name list.

New SSH Private Key

SSH keys are used to support the SSHFTP transport in BusinessConnect.

To upload a SSH private key, perform these steps:

1. Expand **BusinessConnect > Participants > host > Credentials** tab.
2. Click **New SSH Private Key**.
Type the name of the key in the Alias field.
3. In the Current Credential line click **change**.
Browse and navigate to the file containing the SSH private key and click **OK**.
4. Click **set** next to Password.
Type the password (required for private keys) in the Enter Password and Enter Password Again fields.
5. Click **OK and Save**.
The new SSH key for the host is now listed in the Credential Name list.

Generating New PGP Key Pairs

TIBCO BusinessConnect can create new PGP key pairs for users and store them in the certificate store. These key pairs contain a private and a public key and can have a key size of 1024 or 2048 bytes. The key types are DSA and ElGamal or RSA and allows both for encryption and signing. These key pairs also contain the name of the private key owner, as well as an email address of that owner.

The new PGP key are automatically imported into the TIBCO BusinessConnect configuration store and associated with the host.

1. Expand **BusinessConnect > Participants > host > Credentials** tab.
2. Click **New PGP Private Key**.
3. Select the mode by which the new key will be generated and click **OK**:

- [Generating a New Key Pair](#)
- [Uploading from a File](#)
- [Importing from ASCII Armor](#)

Generating a New Key Pair

This option generates both a private and a public key. When a key pair generated this way is exported either in form of binary files or in the ASCII Armor format, both keys will be exported at the same time.

Generating a New PGP Key Pair

Field	Description
Alias	Name for the new PGP key pair
Password	Password associated with the private key
Expiry Date	A date by which the key pair will be valid
Key Size	Size of the new key in bytes: 1024 or 2048
Key Type	For the new PGP key pairs there are two selections available: <ul style="list-style-type: none">• DSA and ElGamal Both created keys, private and public, support signing using the DSA algorithm and encryption using the ElGamal algorithm.• RSA Key Pair Both created keys, private and public, support signing and encryption using the RSA algorithm.
Real Name	A user supplied name to be used in conjunction with the email address in constructing the PGP User ID of the key pair.
Email Address	Email address to be associated with the generated key pair.

Uploading from a File

When exporting an uploaded private key for the host, it will only have the option of exporting this private key, without the public part.

Uploading a Private PGP Key from a File

Field	Description
Alias	Name of the uploaded key.
Current Credential	Browse to the location where a PGP private key that you want to use is located and upload a PGP private key.
Password	Supply a password that corresponds to the key.

Importing from ASCII Armor

Users can import a PGP key pair for the host partner in two ways:

- Import a set of files, with one file for each key part. Content of the file for a key part can be in binary or in ASCII armor format
- Import by pasting the ASCII armor private and public key parts into a screen
Uploading from a file supports only the private PGP key for the host.

Importing from the ASCII armor allows you to import both the private and public PGP key. In the Import from ASCII Armor window, enter data as explained in [Importing a PGP Key Pair from the ASCII Armor](#).

Importing a PGP Key Pair from the ASCII Armor

Field	Description
Alias	Name of the imported key pair.
Password	Supply a password that corresponds to the private PGP key.
ASCII Formatted Text (Private)	<p>Paste the text in ASCII armor format, where the private key is base64 encoded and wrapped with a PGP specific header and footer such as:</p> <pre>-----BEGIN PGP PRIVATE KEY BLOCK----- Version: BCPG v1.46 lQ00BE2cttgDCAC04PRiKPLFNheitPoyNvnuNTghwjNNmSB7BMprzQ3vMeV1X MUg aAW7/qH3YxT3UbHdXkyP9oH/A47pFNoMCvsIgae9mqZoKKWoKCWHRpishTtv5</pre>

Field	Description
	<pre> rXV ... 0hRVJ7VW6Eu3h8dKH/TCC8yzvPrKbLTh2vzm+Y2q1oo5CBZazw== =2IyA -----END PGP PRIVATE KEY BLOCK----- </pre>
ASCII Formatted Text (Public)	<p>Paste the text in ASCII armor format, where the public key is base64 encoded and wrapped with a PGP specific header and footer such as:</p> <pre> -----BEGIN PGP PUBLIC KEY BLOCK----- Version: BCPG v1.46 mQENBE2cttgDCAC0PRiKPLFNheitPoyNvnuNTghwjNNmSB7BMprzQ3vMeV1X MUg aAW7/qH3YxT3UbHdXkyP9oH/A47pFNoMCvsIgae9mqZoKKWoKCWHRpishTtv5 rXV P20/KhUqjgBCd3HZ1qjnDJEVHwOm37H6Iqyd66tRTsW57Wztxy9hRdftM77aa KJl ... AwKMfdaQnd1ntV6BXM6GXdl5HJhjjY/HVJtRb498Rjba9IUVSe1VuhLt4fHS h/0 wgVms7z6ymy04dr85vmNqtaKOQgWws8= =Fd6T -----END PGP PUBLIC KEY BLOCK----- </pre>

- Click Save.

All PGP keys, generated or uploaded/imported, will be available in the Edit Host Participant window.

Assigning a Shadow Key for the Host



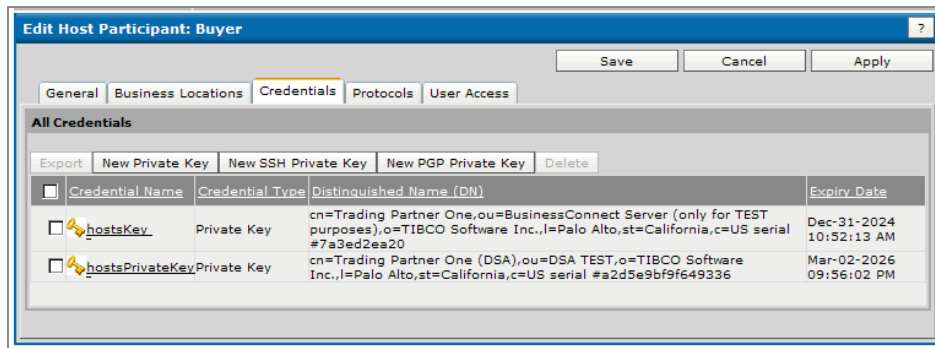
Note

Shadow PGP keys are currently not supported.

To assign a shadow key, follow these steps:

1. Expand **BusinessConnect > Participants > host > Credentials** tab.

Figure 2: Editing Host Participant: Credentials Tab



- Click the private key that will expire first, such as **hostsKey**.
The Edit Private Key dialog is displayed.
- In the Shadow Settings area, select the **Activation date for shadow key** using the three menus. This date has to be chosen *before* the first key is about to expire. From the Shadow Key list, select the key you would like to use as replacement, such as **hostsPrivateKey**.
- Click **Save**.
After the shadow key takes effect, it is still a shadow key. You have to remove or update the original credential and remove or promote the shadow key.

Managing Partner Credentials

There are several credentials available for a partners that can be uploaded using the Credentials tab:

- [New Certificate](#)
- [New SSH Public Key](#)
- [New PGP Public Key](#)
- [Assigning a Shadow Certificate for the Partner](#)
- [Exporting PGP Keys](#)

New Certificate

To upload a new certificate key for the partner, perform these steps:

1. Expand **BusinessConnect > Participants > *partner* > Credentials** tab.
2. Click **New Certificate**.
Type the name of the key in the Alias field.
3. In the Current Credential line click **change**.
Browse and navigate to the file containing the certificate and click **OK**.
4. Click **Save**.
The new certificate for the partner is now listed in the Credential Name list.

New SSH Public Key

SSH keys are used to support the SSHFTP transport in BusinessConnect.

To upload a SSH public key, perform these steps:

1. Expand **BusinessConnect > Participants > *partner* > Credentials** tab.
2. Click **New SSH Public Key**.
Type the name of the key in the Alias field.
3. In the Current Credential line click **change**.
Browse and navigate to the file containing the SSH private key and click **OK**.
4. Click **Save**.
The new SSH key for the partner is now listed in the Credential Name list.

New PGP Public Key

When a user creates a PGP key pair for a host, it is automatically imported into the TIBCO BusinessConnect configuration store as a Server PGP key pair and is associated with the host. For the partner, users can only upload or import the public portion of a PGP key pair, which is normally received from the trading partner.

1. Expand **BusinessConnect > Participants > *partner* > Credentials** tab.
2. Click **New PGP Public Key**.
The New PGP Public Key dialog opens.
3. Select the mode by which the key will be uploaded or imported and click **OK**.
 - [Uploading from File](#)
 - [Importing from ASCII Armor](#)

Uploading from File

Field	Description
Alias	Name of the uploaded key
Current Credential	Browse to the location where a PGP public key that you want to use is located.

Importing from ASCII Armor

Field	Description
Alias	Name of the imported key
ASCII Formatted Text	<p>Paste the text of a PGP public key in ASCII Armor format, where the key is base64 encoded and wrapped with a PGP specific header and footer such as:</p> <pre> -----BEGIN PGP PUBLIC KEY BLOCK----- Version: BCPG v1.46 mQENBE2cttgDCAC04PRiKPLFNheitPoyNvnuNTghwjNNmSB7BMprzQ3vMeV1X MUg aAW7/qH3YxT3UbHdXkyP9oH/A47pFNoMCvsIgae9mqZoKKWoKCWHRpishTtv5 rXV P20/KhUqjgBCd3HZ1qjnDJEVHwOm37H6Iqyd66tRTsW57Wztxy9hRdftM77aa KJl ... AwKMfdaQnd1ntV6BXM6GXdl5HJhjY/HVJtRb498Rjba9IUVSe1VuhLt4fHS h/0 wgVms7z6ymy04dr85vmNqtaK0QgWws8= =Fd6T -----END PGP PUBLIC KEY BLOCK----- </pre>

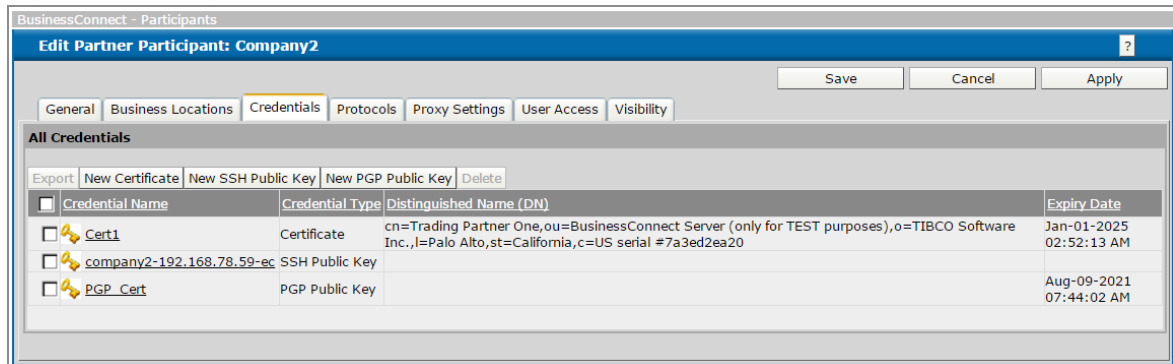
Assigning a Shadow Certificate for the Partner**Note**

Shadow PGP certificates are currently not supported.

To assign a shadow certificate:

1. Expand **BusinessConnect > Participants > partner > Credentials** tab.

Figure 3: Editing Partner Participant, Credentials Tab



2. Click the certificate that is about to expire first.
The Edit Certificate dialog is displayed.
3. In the Shadow Settings area, select **Activation date for shadow Certificate** using the three menus. This date has to be chosen *before* the first certificate is about to expire.
4. From the Shadow Certificate list, select the certificate you would like to use as replacement.
5. Click **Save**.
After the shadow certificate takes effect, it is still a shadow certificate. You have to remove or update the original certificate and remove or promote the shadow certificate.

Exporting PGP Keys

PGP keys can be exported in two formats:

- **Binary** With this format, the key content will be saved directly into a file.
- **ASCII Armor** With this format, both the private and the public keys will be base64 encoded and wrapped with a PGP specific header and footer. The text boxes that contain the ASCII Armor encoded key parts are editable.

Users can export either the public or private portions of the PGP key pair, but these two portions of a key pair are always exported separately. When users also have an option to copy the contents of the public key in ASCII armor format from a screen.

**Note**

If a PGP private key was generated, or imported from ASCII Armor format where both the private key part and the public key part are available, then both the private key and the public key can be exported; otherwise, if the PGP private key was uploaded from a file where only the private key part is available, then only the private key can be exported.

Exporting the Host's PGP Key Pair in a Binary Format

To export a PGP key pair in a binary format:

1. In the **BusinessConnect > Participants > Host > Credentials** tab, select the checkbox next to the PGP private key you want to export.
2. Click **Export**.
3. In the Export PGP Private Key window:
Click **set** next to the Private Key Password.
Enter the new password for export two times.
4. In the Private Key section, click **Export Binary File**.
5. Save the file `key_name_pgp.priv` on a desired location.
6. In the Public Key section, click **Export Binary File**.
7. Save the file `key_name_pgp.pub` on a desired location.

Exporting the Partner's PGP Public Key in a Binary Format

To export an uploaded public PGP Key in a binary format:

1. In the **BusinessConnect > Participants > Partner > Credentials** tab, select the checkbox next to the PGP public key you want to export.
2. Click **Export**.
3. In the Export PGP Public Key window, click **Export Binary File**.
4. Save the file `key_name_pgp.pub` on a desired location.

Exporting the Host's PGP Key Pair in the ASCII Armor Format

To export the host's PGP key pair in the ASCII Armor format:

1. In the **BusinessConnect > Participants > Host > Credentials** tab, click the link for the PGP private key you want to export.
2. In the Edit PGP Private Key window, copy the text block for ASCII Armor formatted text (private), and ASCII Armor formatted text (public).

These text blocks can be pasted to export the key pair to another location. Users can copy the public key from the PGP Public Key text box, copy it into an email message, and send to their trading partners.

The text boxes that contain key parts are editable. An example of the private PGP key exported in the ASCII Armor format looks as follows:

```
-----BEGIN PGP PRIVATE KEY BLOCK-----
Version: BCPG v1.46
lQH0BE6Djw4DBADAW6JewR3W60WZXfqjo5zKb2I+FYMFOUFsQ4P0kXM2/iorTX0h
RZm2uVGq6hi5YwxaCiNOFv+KZV1MhPXVlhq3j/yWQ6ylzE/SRvtTQmFsSw3uzLDS
BU+UsIREVbZ0uXl/8Hl1eVLwS6iL+T06RMeCtzf7tJvGM9mynNcn0vs68QARAQAB
/wkDArjX6KnITRqiYPPjbsIZhhxTWb0YnBSEXRhSpk3bPVBhFcC+BTWnq4vtRd0
qchQWnQAYuvq94zJhI69tT+L15PTj4geixZvID/ZxCUoBzGyw0JC4SEaZYGEPrV+
nIzN2zYZvf266ZApjNv+gWYhvCRI7r8YPCQo2rD2sx2IRl7/bnHcn6W9UgVAN4Vl
VESIbKvrODd0+XUZbqVZl5Jg9lQZFNv0/fnmdvx6tBZXuw6WT20IJFTe0oLl6S/z
h0MvB20jMgqMofhhw80ji2zqmr/Py4gMKSVOblLD7YvTGKL1TX8/YtmjoTTFo6Qk
53mwQrQNh+CC01TIEd86dsT5ZbFRZByWcPfmEfU5yWKRVSxHxHbueeySNLevXARbe
px5yQHFkbW5lKorfEE5BUoMwnRUvqe9XZ47GU3L4PDmT7+IOXWReCbeL7TPn7lu
69mfJ7azHQsMfe4VBJCLTzZcu8/Qkxq0GEpvaG4gRG9lIDxqb2huQGFjbWUuY29t
Poi3BBMDAgAhBQJ0g480BQkB49Z/BwsJCACAwQDFgECBRUCAQMFAoQBAAoJEBt2
dzrZM3bEtVQD/2mJadc79xdkrJteQBGiipitEnpsiTvbGJk4V8pPX5jH5rBls/Q3
axcL7jmkAddSrlKGNZh0EZ2d2UYBiGIztLH6iednTKH5K+S0+DVJfJp9CkFRQzyX
/4ZsQK8Lva20v/QrVNCtkRGtMPOS+WteEle5Atj0z8G+pX+KfSMI2QkOnQH0BE6D
jw4CBACaRqi7rKuEnyQcHbZ+Kx0RWS5uyFUyHLhZWV4xizU7HXgdUwdB8vIKLJwF
pT1ayC2mHDveJl1RDqv/iN8GmUW5SX5rzz7XdCz03ZECLJDwryqV83lVW0GKc3bU
ujtIxVQUcNY7uJXbS/EAQrJjzPTT11vqCXkqbBWfkyJ9WmGU6wARAQAB/wkDAhvZ
cI9XQ3aqYFxFmsgyWIwDxypGugz7U/f4ioRXn4i1EnPm5Q9YoMh7nhzIZxJU1CAHS
uqpB5W/tsp2RGMmhn0+j6Zo0/QB5htiNuLi5/eu1qDIjHLtEVFhylvV4cwET2lVZ
r6H0VV94B1hqDS3kgHSwGHmGZoMpd7cTAYjTJ8g4BXz6xIrLUJFwAnyKUCZ7uMl0
t607Q07yPrckA3UmzYNKrfFZwRzXoOaeNy3uc24XLngxVIYTaeM7VShwOyHK0TD/
o4ZBU48XEEmmW/VWhHz3RJadABjHqwkWd1h0YG3gCr7byTY+mIoab2Be+i2nXXxz
60Zv8tAqqERUj51T011CRpIeskjBJKAlvLW2WmCyb+Ma+FXu53eihmB0w078oaR1
bajn4Tqo85ewTHUlX1IjYD7IGzKGjVZ4JeU67yMRhKGhEhqsCGu9YUH5HQJ2+Og
Gi/S4aOPJdsueSRbrbAMaQ+ItwQYAwIAIQUCToOPDgUJAePWfwcLCQgHAgMEAxYB
AgUVAgEDBQKEAQAKCRAbdnc62TN2xK8sBACb7knDY1HTZUw4dzr0K5JPAkylzSS
3G6ml7/cmQyJb0WPmGXNLO9AE565FAQ7/6jFpMrH9C9SuoayjDD57Z7qTKqdDDZr
aSpuU9vTEbS0ku55BZN0/goSZn1ML2XSNVbnWgoXbINGY3J2WIwQcVZc5eZp8DBA
BAB8xKvrAwvAsA==
=EsBt
-----END PGP PRIVATE KEY BLOCK-----
```

An example of the public PGP key exported in the ASCII Armor format looks as follows:

```
-----BEGIN PGP PUBLIC KEY BLOCK-----
Version: BCPG v1.46
mI0ET0OPDgMEAMBbol7BHdbrRZld+q0jnMpvYj4VgwU5QWxDg/SRczb+KitNfSFF
mba5UarqGLljDFoKI04W/4pLXUyE9dWWGreP/JZDrKXMT9JG+1NCYWxLDe7MsNIF
T5SwhERVtk65eX/weXV5UvBLqIv5PTpEx4K3N/u0m8Yz2bKc1w3S+zrxABEBAAG0
GEpvaG4gRG9lIDxqb2huQGFjbWUuY29tPoi3BBMDAgAhBQJ0g480BQkB49Z/BwsJ
CAcCAwQDFgECBRUCAQMFAoQBAAoJEBt2dzrZM3bEtVQD/2mJadc79xdkrJteQBGi
ipitEnpsiTvbGJk4V8pPX5jH5rBlS/Q3axcL7jmkADdSrLKGnZh0EZ2d2UYBiGIZ
tLH6iednTKH5K+S0+DVJfJp9CkFRQzyX/4ZsQK8Lva20v/QrVNcTKRGtMPOS+Wte
Ele5Atj0z8G+pX+KfSMI2Qk0uI0ET0OPDgIEAJpGqLusq4SfJBwdtn4rHRFZLm7I
VTIcuFLZXjGLNTsdeB1TB0Hy8gosnAWLPvrILaYc094mXVE0q/+I3waZRblJfmvP
Ptd0LPTdkRwskPCvKpXzeVVbQYpzdts600jFVBRw1ju4ldtL8QBCsmPM9NPXW+oJ
eSpsFZ+Rgn1aYZTrABEBAAGItwQYAwIAIQUCT0OPDgUJAePWfwcLCQgHAgMEAxYB
AgUVAgEDBQKEAQAACRAbdnc62TN2xK8sBACb7knDY1HTZUw4dzr0K5JPAkylyzSS
3G6ml7/cmgyJb0WPmGXNL09AE565FAQ7/6jFpMrH9C9SuoayjDD57Z7qTKqdDDzr
aSpU9vTEbS0ku55BZN0/goSZn1Ml2XSNVbnWgoXbINGY3J2WIwQcVZc5eZp8DBA
BAb8xKvrAwvAsA==
=QoV7
-----END PGP PUBLIC KEY BLOCK-----
```

Exporting the Partner's PGP Public Key in the ASCII Armor Format

To export the partner's PGP public key in the ASCII Armor format:

1. In the **BusinessConnect > Participants > Partner > Credentials** tab, click the link for the PGP public key you want to export.
2. In the Edit PGP Public Key window, copy the text block for ASCII Armor formatted text (public).

Users can copy the public key from the PGP Public Key text box, copy it into an email message, and send to their trading partners.

The text boxes that contain key parts are editable. An example of the public PGP key exported in the ASCII Armor format looks as follows:

```
-----BEGIN PGP PUBLIC KEY BLOCK-----
Version: BCPG v1.46
mI0ET0OPDgMEAMBbol7BHdbrRZld+q0jnMpvYj4VgwU5QWxDg/SRczb+KitNfSFF
mba5UarqGLljDFoKI04W/4pLXUyE9dWWGreP/JZDrKXMT9JG+1NCYWxLDe7MsNIF
T5SwhERVtk65eX/weXV5UvBLqIv5PTpEx4K3N/u0m8Yz2bKc1w3S+zrxABEBAAG0
GEpvaG4gRG9lIDxqb2huQGFjbWUuY29tPoi3BBMDAgAhBQJ0g480BQkB49Z/BwsJ
CAcCAwQDFgECBRUCAQMFAoQBAAoJEBt2dzrZM3bEtVQD/2mJadc79xdkrJteQBGi
ipitEnpsiTvbGJk4V8pPX5jH5rBlS/Q3axcL7jmkADdSrLKGnZh0EZ2d2UYBiGIZ
```



```
tLH6iednTKH5K+S0+DVJfJp9CkFRQzyX/4ZsQK8Lva20v/QrVNcTKRGtMPOS+Wte
Ele5Atj0z8G+pX+KfSMI2Qk0uI0ET0OPDgIEAJpGqLusq4SfJBwdtn4rHRFZLm7I
VTIcuFLZXjGLNTsdeB1TB0Hy8gosnAWlPvRILaYc094mXVE0q/+I3waZRblJfmvP
Ptd0LPTdkRwskPCvKpXzeVVbQYpzdts600jFVBRw1ju4ldtL8QBCsmPM9NPXW+oJ
eSpsFZ+Rgn1aYZTrABEBAAGItwQYAwIAIQUCTo0PDgUJAePWfwcLCQgHAgMEAxYB
AgUVAgEDBQKEAQAKCRABdnc62TN2xK8sBACb7knDY1HTZUw4dzr0K5JPAkylyzSS
3G6ml7/cmqyJb0WPmGXNL09AE565FAQ7/6jFpMrH9C9SuoayjDD57Z7qTKqdDDzr
aSpU9vTEbS0ku55BZN0/goSZn1Ml2XSNVbnWgoXbINGY3J2WIwQcVZc5eZp8DBA
BAb8xKvrAwvAsA==
=QoV7
-----END PGP PUBLIC KEY BLOCK-----
```

Protocols Tab for Participants

All protocols need to be installed following the appropriate installation instructions provided for each of the protocols.

To learn more, see *TIBCO BusinessConnect™ Concepts*, "Protocols."

Enabling a Protocol

To enable a protocol for a participant, perform these steps:

1. Expand **BusinessConnect > Participants** and click the participant's name.
2. In the window Edit Host (or Partner) Participant, select the **Protocols** tab.
3. To enable a protocol a protocol that's not present in the Protocol Name list, click **Enable**.

In the Enable dialog, select the appropriate available protocol.

4. Click **OK**.

Back in the Edit Participant dialog, you will see the list of protocols. Each of these enabled protocols must be edited before it can be used for transactions.

5. Proceed with steps described in [Configuring a Protocol](#).

Disabling a Protocol

To disable a business protocol for a participant, perform these steps:

1. Expand **BusinessConnect > Participants** and then click the participant's name.
2. In the window Edit Host (or Partner) Participant, select the **Protocols** tab
3. Select the checkbox next to each protocol you want to disable.
4. Click **Disable**.

**Notes**

You cannot disable a protocol that is used by a current business agreement. You first need to delete the business agreement using the protocol, and then to remove the protocol itself. To remove a business agreement, see [Deleting a Business Agreement](#).

5. Click **Save**.

Configuring a Protocol

Each protocol and participant type provides a unique set of configuration tabs.

All protocols and participant types have the General tab, which allows you to configure identity information for the participant, among other properties.

Protocols that support the AS1 and AS2 transports provide the AS2 Identifier and Valid Email Address List properties on the General tab.

**Note**

Email addresses entered in the Valid Email Address List box must be separated either by a semicolon or by a comma.

A General tab for the installed TIBCO BusinessConnect™ Services Plug-in is presented in [Add New HTTP/S Transport](#).

To learn how to configure different protocols, see the appropriate documentation for the specific protocol.

Managing Transports for Participants

To make an outbound public transport available for a participant, you have to perform the following tasks:

Configure an appropriate transport for the participant

Each of the public transports is covered in a separate section in this manual, and the appropriate sections that are explaining transports for participants are as follows:

- [Setting Up HTTP/S for a Trading Partner](#)
- [Setting Up AS2-HTTP/S for a Trading Partner](#)
- [Setting Up AS1 Email for a Trading Partner](#)
- [Setting Up Email for a Trading Partner](#)
- [Setting Up FTP/S for a Trading Partner](#)
- [Setting Up SSHFTP for a Trading Partner](#)
- [Configuring Outbound File Transport for a Partner](#)
- [Configuring Outbound Inbox Transport for a Partner](#)

Select the participant's transport in the business agreement

To select the configured participant's transport in the specific business agreement, use the protocol binding dialog as explained in [Editing Protocol Bindings: Transports Tab](#).

Proxy Settings Tab for Partners

This tab is available only if you are configuring a partner participant. It is used to activate the proxy that BusinessConnect will use as a default connection for any outgoing traffic with a specific trading partner.

1. Expand **BusinessConnect > Participants > *partner_participant***.
2. Click the **Proxy Settings** tab.

The Edit Partner Participant: Proxy Settings dialog is displayed.

3. Select proxies using the information from [Selecting Proxy Settings for the Partner](#).

Selecting Proxy Settings for the Partner

Field	Description
Proxy Alias	This section shows the proxies that were previously configured.

Connection Defaults

Use Proxies

- If the checkbox **Use Proxies** is cleared, no proxy will be used regardless of any selections in the proxy list or in the **BusinessConnect > System Settings > Outbound HTTP/FTP Proxy and Mail SMTP Servers**.
- If the checkbox **Use Proxies** is selected and a proxy is selected from the list, the selected proxies for this partner will be used: the default system settings will be overridden.

Using the Default Name from the list means that BusinessConnect will use the proxy defined under **BusinessConnect > System Settings > Outbound HTTP/FTP Proxy and Mail SMTP Servers**. Therefore, if the proxy is not specified on the partner level, the TIBCO BusinessConnect user is indicating that there is no preference, and whatever is defined on the system level should be used for this trading partner.

HTTP Proxy

Select 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.

See [Adding a Proxy for a Host](#).

FTP Proxy

Select the previously configured FTP proxy.

Available FTP and SOCKS4/SOCKS5 proxy servers are displayed for selection.

See [Adding a Proxy for a Host](#).

SMTP Server

Select the previously configured SMTP server.

Field	Description
	Available SMTP proxy servers are displayed for selection. See Adding a Proxy for a Host .

4. Click **Done**.

User Access Tab for Participants

The access rights of users can be restricted by participant and business agreement. For participants (host or partner), users can be assigned access rights to all participants or to particular participants: access rights can be fine tuned with respect to trading partner access. To read more about user access management in TIBCO BusinessConnect, see *TIBCO BusinessConnect™ Concepts*, TIBCO BusinessConnect User Management.





You can define the access rights of specific users to the TIBCO BusinessConnect partners also using the User Management option by expanding **BusinessConnect > User Management > Users**. See [Permissions Tab for Administrative and Super Users](#) for more details. You can also define user access rights to certain participants in the TIBCO BusinessConnect installation using the User Access tab in the Edit Partner dialog.

All Authorized Users

Find out who are the authorized users for which you can edit access rights.

- Click View All Authorized Users link to see the list.

Figure 4: All Authorized Users

All Authorized Users				
Name	Read	Update	Delete	Logs and Reports
 admin	[X]	[X]	[X]	[X]
 BCadmin1	[X]	[X]	[X]	[X]
 BCuserA	[X]	[X]	[X]	[X]
 BCuserB	[X]	[X]	[X]	[X]

Using **Add Users** and **Add Groups**, you can fine tune these access rights.

Adding Users with Access Rights

To add the users who have access rights to the selected participant, perform the following steps:

1. Click **Add Users**.
2. Check the checkbox next to the user you wish to grant access rights to the participant. These users have to be previously added through the User Management interface at **BusinessConnect > User Management > Users > Admin**.

The added user is displayed on the user list.

3. You can add or remove the permissions that this user has for the selected participant.

You cannot remove permissions of a super user, since these were granted using TIBCO Administrator User Management.



Note

To add Internal and External users for TIBCO BusinessConnect, see [Adding Users](#).

Adding Groups with Access Rights

To add the groups with defined access rights to the selected participant, perform the following steps:

1. Click **Add Groups**.
2. Check the checkbox next to the group you want to grant access rights to the participant.
The added group is displayed on the user list.
3. You can add or remove the permissions that this group has for the selected participant.

Visibility Tab for Partners

TIBCO BusinessConnect can publish error messages to tibbr and message events to TIBCO BusinessEvents. This functionality must be enabled and configured at a global level in **BusinessConnect > System Settings > Visibility** before it is configured for a partner. See [Visibility](#) for more information about how to configure error message posting to tibbr and publishing message events to TIBCO BusinessEvents on a global level. For more conceptual information about this functionality, see *TIBCO BusinessConnect™ Concepts, System Settings*.

Configuring Participant Visibility Settings for tibbr

You can enable TIBCO BusinessConnect to post error messages generated by transactions for any protocol and partner to tibbr by going to **BusinessConnect > System Settings > Visibility > tibbr**. You can also enable specific trading partners to post error messages generated by transactions for protocols used by that partner. By enabling error message posting at both a global and trading partner level, you can view and filter error messages by subject on tibbr. For example, you might want to see all error messages generated by X12 transactions as well as all error messages generated by transactions involving a trading partner named Acme, who also uses the X12 protocol. For more information about this functionality, see [Configuring tibbr Settings](#) and *TIBCO BusinessConnect Concepts, System Settings*.



Note

Subject names in tibbr must be unique. Once a subject has been created in tibbr it cannot be recreated, even if you have deleted it. Subjects are retained internally by tibbr to preserve old messages posted to that subject. For example, if you create the subject BCX12 and then delete it,

you cannot recreate the subject BCX12.

If you have created and deleted a subject that you want to use again, you must create another subject with a different prefix for messages to be posted to tibbr. For example, you could create the subject BC-X12 or BC_X12 if you have created and deleted the subject BCX12.

To configure error posting for a trading partner, enter information according to [Participant Visibility Settings for tibbr](#).

Participant Visibility Settings for tibbr

Field	Description
Enable Partner Related Error Posting	Check this checkbox to enable error message posting for the selected trading partner.
Subject Prefix	The subject prefix to be used for posting to tibbr. For example, bc.acme.X12 Default: bc.participantname
List of Protocols to Enable Error Posting (Example: X12;EZComm;ebXML)	The protocols for which you want error messages posted to tibbr. If you enter multiple protocols, they must be separated by a ; (semi-colon). Note: Protocols must be enabled at a global level in BusinessConnect > System Settings > Visibility > tibbr .

Configuring Participant Visibility Settings for TIBCO BusinessEvents

TIBCO BusinessConnect can publish messages to TIBCO BusinessEvents as events. This functionality must be enabled at a global level, in **BusinessConnect > System Settings > Visibility > BusinessEvents**.

To enable a trading partner's messages to be published to TIBCO BusinessEvents as events, check the **Enable Publishing to BusinessEvents for this Partner** check box.

For more information about this functionality, see [Configuring TIBCO BusinessEvents Settings](#) and *TIBCO BusinessConnect Concepts*, System Settings.

Business Agreements

This section describes how to create business agreements.

Business Agreements 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

This section provides an overview of the basic tasks required to create a valid business agreement.



Note

Much of the information required to create a business agreement is protocol specific.

The procedures in this section assume that you have fully configured both parties to the agreement.

These are the basic tasks required to create a valid business agreement:

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

Identifying the Participants for a New Business Agreement

Before you configure a business agreement, you need first to identify the participants: a host and a trading partner (or partners). You can define the agreement period as indefinite by using the Valid checkbox or you can define the agreement using specific start and end dates. The period can be set to indefinite by checking the valid checkbox and setting start and end date blank.

Selecting Participants

To select the participants:

1. Expand **BusinessConnect > Business Agreements**.
2. In the Business Agreements dialog, click **New**.
3. To find a participants, you can perform the following steps:
 - Type names of the participants into the Host Party and Partner Party fields
 - Use the Search function, or click Show All to display all available participants.
4. Once the proper participants are displayed, select the button next to the partners name.
5. Click **OK**.

The new business agreement is displayed.

There are two tabs for managing a business agreement:

- [General Tab for Business Agreements](#)
- [User Access Tab for Business Agreements](#)

General Tab for Business Agreements

To define the agreement period, perform these steps:

1. Select the **Valid** checkbox if you want this agreement to be valid immediately and for an indefinite period of time.

2. To define a specific time frame, use the **Start Date** and **End Date** lists to define the exact period during which the agreement will be valid.

**Note**

If the business agreement is validated, all grammar rules associated with this agreement are validated too. No validation is performed for an inactive agreement. This allows the user to provide only a partial information while the business agreement is still inactive, and then add the remaining required information when validating the agreement. A non-validated business agreement is listed in the Agreement Name as “Inactive”.

3. Click **Save**.

The Business Agreements dialog is displayed, showing the new active agreement.

4. To configure more business agreements, click **New** and repeat steps described in [Selecting Participants](#), steps 3 and 4, and [General Tab for Business Agreements](#).

After the agreement period is defined, you can move on to configuring protocols bindings as explained in [Adding a Protocol Binding](#).

Adding a Protocol Binding

**Note**

Both parties to the business agreement must have protocols enabled before you can add protocol bindings to a business agreement.

To add a protocol, perform these steps.

1. Expand **BusinessConnect > Business Agreements**.
2. Click the name of the agreement to which you want to add a protocol.
3. In the Edit Agreement dialog, click **Add Protocol Bindings**.
4. In the Select Protocol dialog, select the desired protocol from the list.

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

5. Click **OK**.

Configuring a Protocol

To edit a protocol:

1. Expand **BusinessConnect > Business Agreements**.
2. Click the name of the specific agreement you want to configure.
3. Click the protocol you want to edit.
4. There are three tabs available in the standard view and five tabs available in the advanced view for configuring protocol bindings. The first three tabs —Operation Bindings, Document Security, and Transports — are configured in the same way for all protocols, while the two tabs in the advanced view are configured in a protocol-specific way.
To edit Host's and Partner's Configuration tabs, see the other appropriate protocol specific documents.

Business Agreement: Operation Bindings Tab

Use this tab to bind operation that have been already defined so that they can be used for a particular business agreement.



Note

The desired protocol must have operations defined before you can configure an operation binding. Some protocols include pre-configured operations.

1. Expand **BusinessConnect > Business Agreements > business_agreement > protocol > Operation Bindings**.
2. Configure operation bindings using the information provided in the following table.

Editing Protocol Bindings: Operation Binding Tab

Field	Select
Allow All Operations	Select this checkbox to allow all operations that are found under BusinessConnect > Operations Editor > Protocol for any business transaction. Note: This function also applies to all operations that are specifically

Field	Select
	<p>listed under Initiating Operations or Responding Operations.</p> <p>Clear this checkbox to allow only the restricted set of operations listed under Initiating Operations or Responding Operations for a particular business transaction.</p>
Non-Repudiation Logging	The non-repudiation log is used to provide proof of the delivery of messages. For more details, see Non-Repudiation Logs .
Initiating Operations	<p>Add operation bindings for initiating operations.</p> <ul style="list-style-type: none"> Click Add Operation Binding, and in the Select Operation window select one of the available operations. Click OK.
Responding Operations	<p>Add operation bindings for responding operations.</p> <ul style="list-style-type: none"> Click Add Operation Binding, and in the Select Operation window select one of the available operations. Click OK.

3. Click **Save**.

Business Agreement: Document Security Tab

The Document Security tab is used to specify security settings for the business transaction that is being exchanged. See the content about Security in *TIBCO BusinessConnect™ Concepts* for more details.



Note

Before using the Document Security tab to select any keys or certificates, you must first configure these keys or certificates as explained in the sections: [New Private Key](#) and [New Certificate](#).

1. Configure document security using the information provided in the following table:

Editing Protocol Bindings: Document Security Tab

Field	Enter/Select
<h2>Outbound Doc Exchange</h2> <p>For each selection, you need either one of supported key types for the PKI method, or a PGP private or public key.</p>	
<h2>Signing Info Settings</h2>	
Signing Key	Select the private key of the host from the list.
Digest Algorithm	Select the hash algorithm from the list: SHA1, SHA256, SHA384, or SHA512.
PGP Signing Private Key (FTP only)	Select the private PGP key of the host from the list.
PGP Hash Algorithm (FTP only)	Select the PGP hash algorithm from the list: SHA1, RIPEMD160.
<h2>Encryption Info Settings</h2>	
Encryption Certificate	Select the partner's certificate from the list.
Encryption Algorithm	<p>Select the algorithm from the list: DES3, AES-128, AES-192, or AES-256, AES-128-GCM, AES-192-GCM, or AES-256-GCM.</p> <p>Galois/Counter Mode (GCM) is a block cipher mode of operation that uses universal hashing over a binary Galois field to provide authenticated encryption.</p> <p>The AES-128-GCM, AES-192-GCM, and AES-256-GCM algorithms to support Advanced Encryption Standard (AES) in GCM mode. These algorithms only apply to the two business protocols: TIBCO BusinessConnect™ SOAP Protocol and TIBCO BusinessConnect™ ebXML Protocol.</p>

Field	Enter/Select
PGP Encryption Public Key (FTP only)	Select the partner's PGP public key from the list.
PGP Encryption Algorithm (FTP only)	Select the PGP encryption algorithm from the list: DES3, CAST5, AES-128, AES-192, AES-256, or BLOWFISH.

Inbound Doc Exchange

Signing Info Settings: Verification Certificate

Verification Certificate	Select the partners' certificate. For more details about certificates, see <i>TIBCO BusinessConnect™ Concepts</i> , "Security."
PGP Signing Verification Public Key (FTP only)	Select the partners' certificate. For more details about this certificate, see <i>TIBCO BusinessConnect™ Concepts</i> , "Security."

Encryption Info Settings: Decryption Key

Decryption Key	Select the host's private key. For more details about host's private key, see <i>TIBCO BusinessConnect™ Concepts</i> , Security.
PGP Decryption Private Key (FTP only)	Select the host's private PGP key. For more details about host's private key, see <i>TIBCO BusinessConnect™ Concepts</i> , Security.

2. Click **Save** to save the selected keys and certificates.

Business Agreement: Transports Tab

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

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

Editing Protocol Bindings: Transports Tab

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

Field	Enter/Select
Identity for HTTPS, FTPS, HTTPSCA	
Client Authentication Identity for SSHFTP	Select the host's SSH private key from the list.

Allowed Inbound Transports for Partner

HTTP, HTTPS, HTTPSCA, FTP, FTPS, SSHFTP, FILE

Only the checkboxes for the previously configured and enabled transports will be visible. Select the appropriate checkbox to allow an inbound transport for the trading partner to communicate with the host.

If the transports HTTP, HTTPS, HTTPSCA, FTP, FTPS, or SSHFTP have been enabled and show on this list, they will be accompanied with an additional link called Edit Settings.

To edit settings of an enabled transport:

1. Click **Edit Settings** next to the transport you want to edit. A dialog for the appropriate transport is displayed.
2. Continue by entering data as follows:

- For HTTP, HTTPS, and HTTPSCA, select the **Require HTTP Basic Authentication** checkbox to do the basic authentication for inbound messages. Click **OK**.

The user and password available in the incoming HTTP message are authenticated against the External User information configured in TIBCO BusinessConnect. The user information can also be set in LDAP server. The password is passed in plain text across the network.

See [Authentication Source Defaults](#) for more information about the authentication source.

Refer to RFC 2617, HTTP Authentication for more

Field	Enter/Select
	information.
	<ul style="list-style-type: none"> — For HTTPSCA only, select the Client Authentication Identity from the list and click OK. — For FTP and FTPS, use the configuration data as explained in Inbound FTP/S Settings. — For SSHFTP, use the configuration data as explained in Inbound SSH Settings.

2. Click **Save**.

Show Advanced

By using **Show Advanced**, you can configure additional settings for either a host or a partner in a business agreement using Host's Configuration and Partner's Configuration. For more information, see the specific protocol's documentation.

Deleting a Business Agreement

To delete a business agreement:

1. Expand **BusinessConnect > Business Agreements**.
2. Select the checkbox next to the agreement you want to delete and click **Delete**.

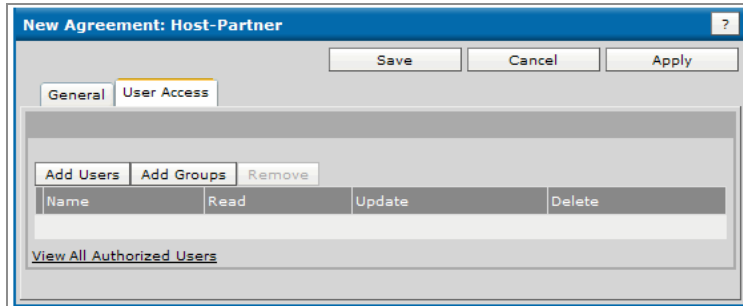
User Access Tab for Business Agreements

The access rights of users can be restricted by participant and business agreement. For business agreements, users can be assigned access rights to all agreements or to particular agreements: access rights can be fine tuned with respect to business agreement access. To read more about user access management in TIBCO BusinessConnect, see *TIBCO BusinessConnect™ Concepts*, TIBCO BusinessConnect User Management.

To define the access rights of specific users to the TIBCO BusinessConnect partners using the User Management option, expand **BusinessConnect > User Management > Groups**. See [Permissions Tab for Groups](#) for more details. You can also define user access rights to

business agreements in the TIBCO BusinessConnect installation using the User Access tab in the New Agreement dialog.

Figure 5: Editing Business Agreement: User Access Tab



All Authorized Users

To find out who are the authorized users for which you can edit access rights, click the link **View All Authorized Users**. A list of users with defined access rights for this participant is displayed.

Figure 6: All Authorized Users

Name	Read	Update	Delete	Logs and Reports
admin	[X]	[X]	[X]	[X]
BCadmin1	[X]	[X]	[X]	[X]
BCUserA	[X]	[X]	[X]	[X]
BCUserB	[X]	[X]	[X]	[X]

To fine tune the access rights, use **Add Users** and **Add Groups**.

Adding Internal Users

To add internal users who have access rights to the selected business agreement, perform the following steps:

1. Click **Add Users**.
2. Check the checkbox next to the user you wish to grant access rights to the business agreement.

The added user is displayed on the user list.

3. You can add or remove the permissions that this user has for the selected business agreement.

Adding Groups

To add the groups with defined access rights to the selected business agreement, perform the following steps:

1. Click **Add Groups**.
2. Check the checkbox next to the group you wish to grant access rights to the business agreement.
The added group is displayed on the user list.
3. You can add or remove the permissions that this group has for the selected business agreement.

Operations Editor

This section explains how to configure operations for protocols and how to specify files for uploading or referencing.

Operations Editor Overview

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. In discussing the operations editor we are using the term in the latter sense.

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

- Name of the operation
- Document (an XML file that clearly defines the electronic document that partners will exchange as part of this operation)
- Root XML element name (the top-level XML element in the document. See [Importing and Exporting Operations Protocol-Specific Terminology](#).)

**Note**

Only schemas that are in the operations editor will be loaded down by the BusinessConnect palette. The BusinessConnect palette does not evaluate partner-level overrides.

For more information about schemas, see the content about implementing custom schemas in *TIBCO BusinessConnect™ Palette Reference*, and *TIBCO BusinessConnect™ Concepts*, "Schemas."

-

Protocol-Specific Terminology

Protocol	Term for Operation
RosettaNet	Activity
TEXT	Message type
X12	Transaction
EDIFACT	Message
Gateway	Transmission
EZComm	Operation
SOAP	Operation
CMI	Transaction
cXML	Operation
ebMS3	Transaction
ebXML	Transaction
EIBCS	Operation
TRADACOMS	Transmission

Importing and Exporting Operations

Using the operations editor you can import and export operations. To manage operations, see documentation provided for a specific protocol.

Importing an Operation

To import an operation, perform the following steps:

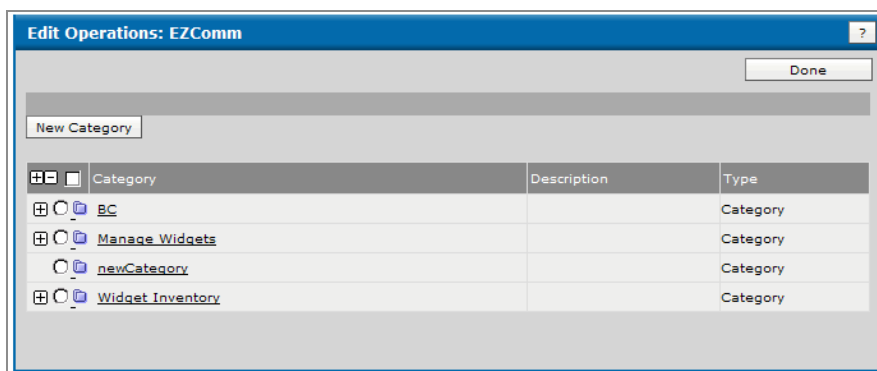
1. In the Operations Editor window, click **Import**.
2. In the Import Operations dialog, click **change**.
3. Click **Browse** and go to the location where you have saved the operations.
4. Select the saved .csx file and click **Open**.
5. Click **OK** to upload the file.

The uploaded file is displayed in the Import Operations dialog.

6. Set the password if the exported file was saved with one.
7. Click **Import**.
8. Click **Done** to finish the import.
9. Click the link for the protocol for which the operation has been imported.

The imported operations are listed.

Figure 7: Imported Operations Listed



Note

If an operation with the same name is already present, the operation will not imported and will be skipped instead.

Exporting an Operation

To export an operation, perform the following steps:

1. Select the button next to one of the activated protocols.
2. Click **Export**.

In the Export Operation dialog, set password if desired. If a password is set for the exported file, it must be used when importing this file.

3. Click **Export Data**.

Click **Save** to save the file (such as `operations.csx`) on the desired location.

4. Click **Done** to finish the export.

File Specification Dialog

There are two ways to specify the file: file reference and uploaded file. With a file reference, a reference to the file is maintained in the configuration store, whereas with the uploaded file, the entire file is maintained in the configuration store.

A file reference takes less space, but the reference can become invalid if the file that the reference points to is moved. With an uploaded file, a schema (DTD), a guideline, or a script file is always available.

However, if a file that you have uploaded changes, you have to re-upload file. With a file reference, all changes to the referenced file are dynamically loaded by TIBCO BusinessConnect.

Specifying a File Reference or a File to Upload

To specify a file reference or to designate a file for uploading, such as a schema for validation, perform the following steps:

1. Click the **change** link in the field where the file is specified.
2. Select **File Reference** or **Uploaded File** from the Type list.
 - File Reference:
In the File Reference field, enter the path to the file.
 - Uploaded File:
Click **Browse** in the Upload File field.
Navigate to the file.
Click **Open**.
3. Click **OK**.

If you upload the file, you can later download it by clicking the file name.

System Settings

This section provides information about the parameters you can access from the System Settings screen.

General

General Settings allow you to modify the installation name, installation prefix, and description of the installation.

Server Settings Fields

Field	Description
Installation Name	<p>The name of the BusinessConnect installation. BusinessConnect names the installation automatically as <i>BC-domain_name</i>. You can change the name as desired.</p> <p>Note: TIBCO BusinessConnect uses the installation name within TIBCO Rendezvous and JMS subjects. If you rename the installation after deploying the BusinessConnect server, subject names will be out of synch. Therefore, if you modify the installation name, undeploy and then redeploy the server.</p> <p>For more information, see <i>TIBCO BusinessConnect™ Concepts</i>, "TIBCO Rendezvous Subject Names" and "JMS Message Format."</p>
Installation Prefix	<p>The prefix BusinessConnect appends to the subject of every message. The default value is <i>AX.BC</i>.</p> <p>Note: If you change the installation prefix after deploying the BusinessConnect server, subject names will be out of synch. Therefore, if you modify the prefix, undeploy and then redeploy the server.</p>
Description	<p>An optional text description of this BusinessConnect installation.</p>

Field	Description
Default Host	<p>The default host for the BusinessConnect installation. The first host participant that you add to the installation is automatically set as the default host.</p> <p>A user can modify the default host when required, and this change does not require redeployment or restarting of the BusinessConnect server.</p>

Certificate Store

**Note**

The CA (Certificate Authority) is not used with PGP keys. CA certificates are used only with the PKI validation method.

The certificate store allows you to manage all credentials (certificates and private keys) in one location. These credentials are owned by participants, the BusinessConnect server, and by the trusted CAs (Certificate Authorities). You can add and remove CA certificates, and you can create new identity (leaf) certificates, which you can send to a certificate authority for signing using Certificate Signing Request (CSR). For information about certificates and security in general, see [Credentials Tab for Participants](#) and *TIBCO BusinessConnect Concepts, Security*.

**Note**

To learn how to work with keys, you can use the samples provided with this program in the directory `BC_HOME/samples/keys`. Keep in mind that the chosen password is `Password1`.

Credentials Tab

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.

Adding Certificate Authority

1. Expand **BusinessConnect > System Settings > Certificate Store**.
2. Click **Add Certificate Authority**.
3. In the Import CA Certificate window, click the link **change**.
4. Click **Browse** to upload the CA certificate file that should be already available on your machine. If not, make sure to acquire a root certificate before proceeding with this configuration.
5. Click **OK** twice.

Removing Certificate Authority

1. Expand **BusinessConnect > System Settings > Certificate Store**.
2. Select the checkbox associated with the certificate you wish to remove.
3. Click **Remove Certificate Authority**.
4. In the new dialog that doesn't show the CA you just removed, click **Done**.

New Identities Tab

This tab allows you to 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 will be 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 will be attached to the corresponding private key and this new identity becomes usable for decryption/verification, representing itself as stated in the certificate.

Creating New Identity

1. Expand **BusinessConnect > System Settings > Certificate Store > New Identities**.
2. Click **Create New Identity**.

Certificate Signing Request Wizard

A six-step Certificate Signing Request wizard is displayed that will allow you to generate a CSR.

Step 1. General Information

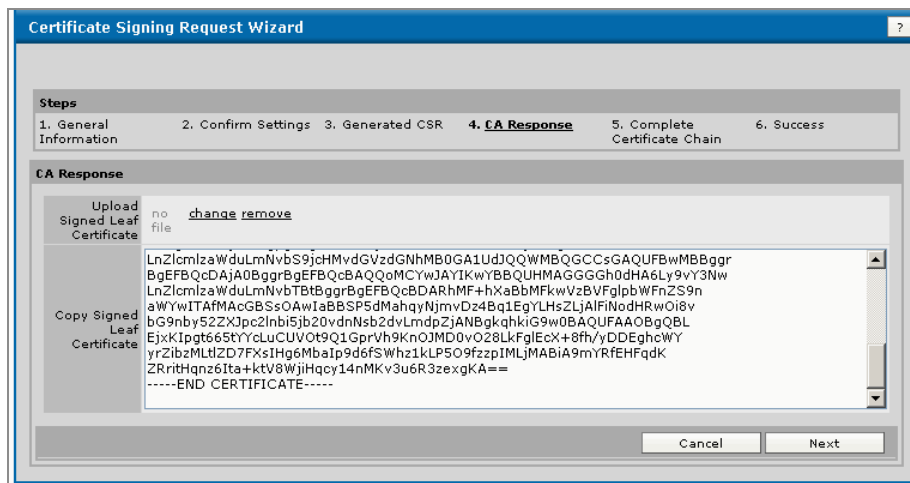
1. Supply the required information using [CSR Wizard, General Information](#).

CSR Wizard, General Information

Field	Enter Information:
Identity Alias	(Required) 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	(Required) Only two digit entries are allowed, due to the restrictions posed by X.500. Example: US
State	(Required) Enter the state where the host is located. Example: California
Organization	(Required) Enter your company's name. Example: Widgets Inc.
Organization Unit	Enter your organization unit's name. Example: HR
Locality	(Required) Enter your locality. Example: San Jose
Common Name	(Required) Fully qualified domain name (FQDN) of the server where the host is located. Example: widgets.com
Key Length (bits)	(Required) Key length of the private key. Choose among 512, 1024, and 2048 bits. Example: 512

- paste the certificate text into the dialog window

Figure 9: CSR Wizard Step 4, CA Response



2. Click **Next** to proceed.

Step 5. Complete Certificate Chain

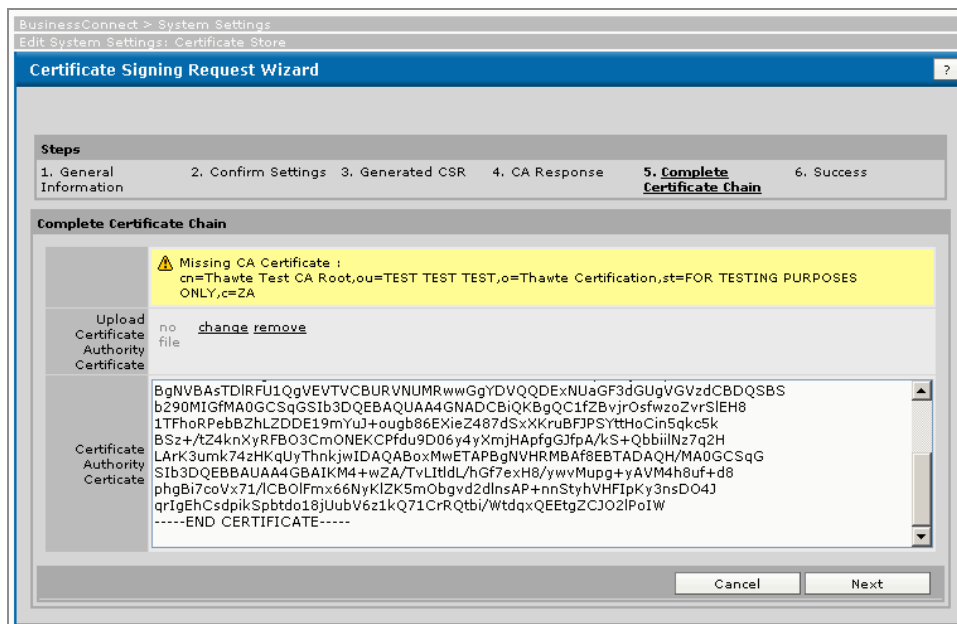
In this step, you can upload the CA root certificate to complete the certificate chain.

The dialog is displayed with an error message Missing CA Certificate. Certificates are only operable if both trading partners trust the CA that signed the other's root certificate.

Upload the CA (root) certificate from a location on your machine by clicking on the link **change**, or

Paste the certificate text into the dialog window

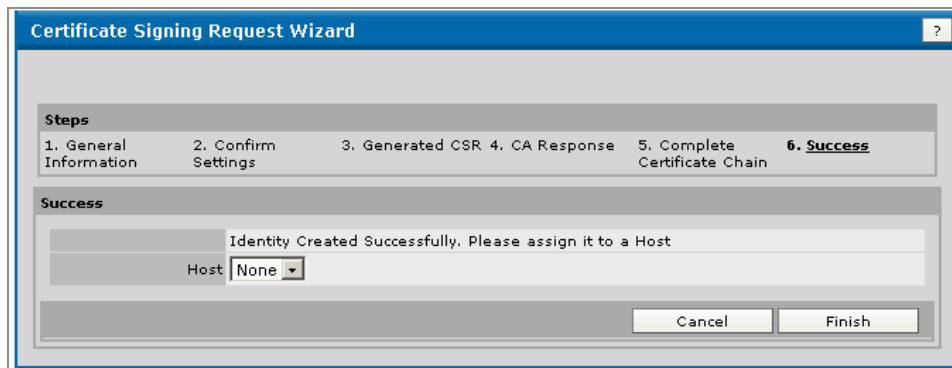
Figure 10: CSR Wizard Step 5, Complete Certificate Chain



Step 6. Success

After successfully uploading the verified certificate, you arrive to step 6, Success.

Figure 11: CSR Wizard Step 6, Success



Your new leaf certificate, verified by the CA, is available for you to use. You have to assign the new leaf certificate to your server by selecting the server from the list next to the label Host.

Click **Finish**.

Server Identities and Certificates Tab

In the **Server Identities and Certificates** tab, you can add an LDAP, a JMS, or an Email server certificate to use with the main system.



Note

To learn how to work with keys, you can use the samples provided in the directory `BC_HOME/samples/keys`.

Keep in mind that the chosen password is Password1.

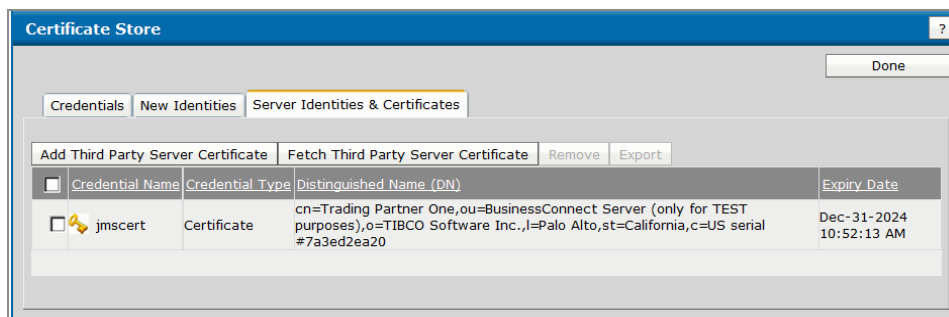
Adding LDAP/JMS/Email Server Certificates

The JMS certificate is a credential of the JMS server, which is expected to be configured according to the corresponding guidelines. Before the BusinessConnect palette can verify the identity of a JMS server, this certificate has to be added and the checkbox Verify JMS Server has to be selected.

A server certificate is stored in the certificate store and must be created before it is assigned to a transport. To create it, perform the following steps:

1. Expand **BusinessConnect > System Settings > Certificate Store > Server Identities & Certificates**.
2. Click **Add Third Party Server Certificate**.
3. In the New Certificate dialog, enter an alias name for this certificate.
4. Upload the certificate file.
The imported certificate will appear in the Credential Name list.

Figure 12: Imported Server Certificate



5. Click **Done**.

Fetching a 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:

1. Expand **BusinessConnect > System Settings > Certificate Store > Server Identities & Certificates**.
2. Click **Fetch Third Party Server Certificate**.
3. In the Fetch Certificate dialog:
Enter the host in **Host** field. For example: `smtp.gmail.com`.
Enter the port number in **Port** field. For example: 465.
4. Click **OK** to save the certificate.
5. Click **Done**.

Inbound Public Transport Types

The inbound transport types available for TIBCO BusinessConnect are:

- **Email**
 - Mail POP3 Server Polling Service - Mailbox #1
 - Mail POP3 Server Polling Service - Mailbox #2
 - Mail POP3 Server Polling Service - Mailbox #3
- **FTP** Plain FTP Get Client
- **FTPS** Secure FTP Get SSL Client
- **SSHFTP** Secure FTP Get SSH Client
- **HTTP** Gateway Plain HTTP Service
- **HTTPS** Gateway Secure HTTP SSL Service
- **HTTPSCA** Gateway Secure HTTP SSL Service with Client Authentication
- **File** Gateway File Polling Service

Each of the public transports can be selected and enabled or disabled by selecting the appropriate checkbox associated with a specific transport and clicking on **Enable** or **Disable**.

These transports are described separately in the following sections:

- [Inbound Mail POP3 Servers](#)
- [Email Transport](#)
- [FTP and FTPS Transports](#)
- [SSHFTP Transport](#)
- [HTTP, HTTPS, and HTTPSCA Transports](#)
- [AS2 Transport](#)
- [AS1 Transport](#)
- [File Transport](#)

Inbound Mail POP3 Servers

You can use this part of the section to 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**.

[Inbound Mail POP3 Servers](#) lists the fields configured on inbound mail POP3 servers.

Inbound Mail POP3 Servers

Field	Description
Mailbox #1, #2, or #3	

Field	Description
Mail POP3 Server	<p>Name of the POP3 server.</p> <p>Note: If the SSL checkbox is selected, the port number is required in this field. For example: pop.gmail.com:995.</p>
User Name	Name of the user for this mailbox.
Password	Password of the user for this mailbox.
Polling Interval (seconds)	<p>Sets the polling interval to specify the frequency which the credential alerter keeps tracking and publishing alerts on expiring credentials.</p> <p>The default value is 180 seconds.</p>
SSL	<p>Secure Sockets Layer (SSL) configuration.</p> <p>For inbound messages, when this checkbox is selected, SSL/TLS protocols are used to ensure secure communication.</p>
Trusted Certificates	<p>Uploads an X.509 certificate file encoded in Privacy-enhanced Electronic Mail (PEM) format.</p> <p>This PEM encoded file contains the server X.509 certificate along with all the CAs in the certificate path.</p> <p>Note: Only the PEM encoded X.509 files are supported. If the certificate expires, download the latest certificate.</p>
Verify Host Name	<p>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.</p> <p>This is optional.</p>
Strong Cipher Suites Only	Only cipher suites with strong encryption can be used, if they are available on the host you are connecting to.

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

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

Outbound HTTP/FTP Proxy and Mail SMTP Servers



Use of proxy servers is optional.

Note

The Outbound Proxy Settings link adds proxy servers for use by BusinessConnect. Different proxy server types are supported to provide for different types of outbound transports protocols:

- **HTTP Proxy and SOCKS4/ SOCKS5 Proxy Servers** For outbound HTTP transport protocols
- **SMTP Server** For outbound Email transport protocols

- **FTP Proxy and SOCKS4 / SOCKS5 Proxy Servers** For outbound FTP transport protocols

To select a proxy for a partner participant, see [Select the Default Proxy for a Trading Partner](#) and [Configuring an SMTP Server for a Partner](#).

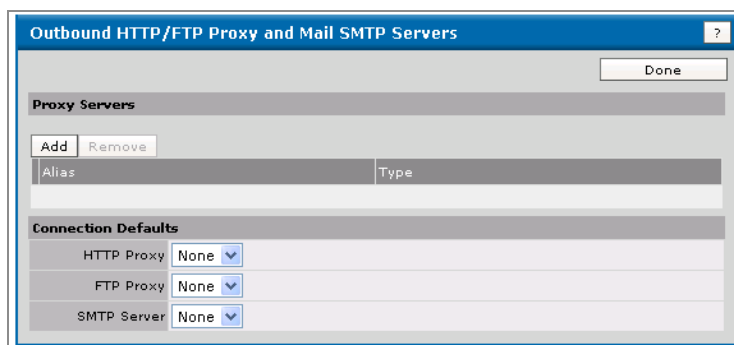
To learn about proxy servers, see *TIBCO BusinessConnect™ Concepts*, "Proxy Servers."

Adding a Proxy for a Host

Using the Outbound HTTP/FTP Proxy and Mail SMTP Servers window, you are allowed to add a proxy server for a host.

1. Expand **BusinessConnect > System Settings**.
2. Click **Outbound HTTP/FTP Proxy and Mail SMTP Servers**.

Figure 13: Outbound HTTP/FTP Proxy Settings



3. Click **Add** to add a proxy server.
4. In the Name field, enter a meaningful Proxy Name
5. From the **Type** list, select the server: **HTTP**, **SOCKS4**, **SOCKS5**, **FTP**, or **SMTP**.



Note

FTP and FTPS support for mput/mget is available through either SOCKS4, SOCKS5, or FTP Gateway.

The FTP Gateway is an FTP server emulator application, which routes both ways between an FTP client (BusinessConnect) and an FTP server using either passive or active mode.

**Note**

SSHFTP can only use SOCKS4 or SOCKS5 and the methods listed in the SSHFTPClient interface.

6. When you configure a proxy for a participant, you will have only three options to select from: HTTP, FTP, and SMTP. The SOCKS4 and SOCKS5 proxies are available for users who use such proxies.
7. Click **OK**.

In the New Proxy Connection dialog, enter the information using [New Proxy Connection](#):

New Proxy Connection

Field	Enter
Alias	Type an identifier for these proxy settings.
Host Name	Type the name of the host on which the proxy server is installed.
Port Number	Type the number of the port that the proxy server is using.
Proxy User Name	Type a valid username for the proxy server, if applicable.
Proxy Password	Type the password associated with the user name, if applicable.
For SMTP only:	
SMTP Server Name	<p>An SMTP server name with port number. For example: <code>smtp.gmail.com:587</code>.</p> <p>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.</p> <p>For the SMTPS transport, if port number is not given, the default port number 25 is used.</p>
Server Certificate	Server certificate of this SMTPS used for the STARTTLS, SSL, and TLS protocols.

Field	Enter
	<p>Certificate Authorities can be added under BusinessConnect > System Settings > Certificate Store > Credentials.</p> <p>You have to add server certificates according to your own needs. Server certificates can be added under BusinessConnect > System Settings > Certificate Store > Server Identities & Certificates > Add Third Party Server Certificate.</p> <p>The sample certificates are in the <i>TIBCO_HOME/bc/version/samples/keys/email_ssl</i> directory.</p> <p>Note: 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.</p>
Secure Transport Mode	<p>The secure protocol employed in the transport layer. The STARTTLS, SSL, and TLS protocols are listed in the list.</p> <p>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.</p>

8. Click **change** to set the proxy password.

9. Click **Save**.

The new proxy is displayed in the Proxy Alias list. You can now select this proxy server in the list for the appropriate server type (HTTP, FTP, or SMTP) in the Connection Defaults area.

10. Click **Done** to accept the new proxy.

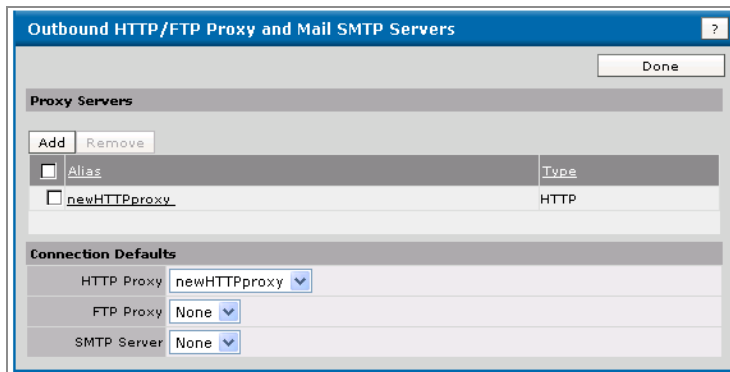
Selecting the Default Proxy for a Host

In the section Connection Defaults of the Edit System Settings: Outbound Proxy Settings dialog, you can select which proxy server to use with a host.

1. Expand **BusinessConnect > System Settings**.
2. Click **Outbound HTTP/FTP Proxy and Mail SMTP Servers**.

The Edit System Settings dialog is displayed.

Figure 14: Selecting Outbound Proxy Settings for a Host



3. In the section Connection Defaults, select a Proxy (HTTP or FTP) from the list.
You can choose any of the added proxies or None. If you choose None, no proxies will be used for this host.
4. Select an SMTP Server from the list.
You can choose any of the added SMTP servers or None. If you choose None, no SMTP server will be used for this host.
5. Click **Done**.

Audit, Non-Repudiation and Runtime Database Configuration

Configuration of database connections, connection settings, as well as export DDL for the database table schemas and creation of database tables are described in *TIBCO BusinessConnect Installation and Configuration*, "Audit, Non-Repudiation and Runtime Database Configuration."

See also *TIBCO BusinessConnect™ Interior Server Administration*, "section A, Database Schema Definition."

User Authentication Configuration

This system settings window is used to add or remove the user authentication source for TIBCO BusinessConnect. These source types are:

- LDAP server, which is used only for external users.
Supported LDAP servers include Open LDAP, IBM Tivoli Directory Server LDAP, Microsoft Directory LDAP, Sun ONE LDAP.
- TIBCO BusinessConnect database, which is used both for internal or external users.

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

Adding an Authentication Source

1. Click **Add** to add an authentication source.
2. Two options are available:
 - [LDAP Server](#)
 - [BC Database](#)

After the LDAP server or a BC Database are configured, they are displayed in the Source Alias list.

LDAP Server

When LDAP is selected, a window opens with the configuration fields described in [LDAP Server Settings](#):

LDAP Server Settings

Field	Description
Alias	Alias name for the LDAP server.

Field	Description
Host Name	The IP address or name of the machine on which the LDAP server resides.
Port Number	The port number on the LDAP machine to use for connecting to LDAP.
Bind DN and Bind Password	<p>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</p> <p>The Bind DN provided can be an LDAP user that has both read and write permissions to LDAP. The user needs permission to:</p> <ul style="list-style-type: none"> — Read and write LDAP user objects — Read and write LDAP group objects <p>Authenticate other users to LDAP (that is, call the LDAP authenticate API or have read access to password/credentials of LDAP user objects).</p>
Base DN	Gets prepended to Bind DN when searching for users. This is the starting point in the LDAP hierarchy at which the search begins.
User Search Filter	<p>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:</p> <ul style="list-style-type: none"> • Base DN: dc=na,dc=tibco,dc=com • User Search Filter: objectclass=person
username Attribute	<p>Provide the LDAP attribute name that represents the username in the LDAP directory server.</p> <p>It is good practice to use the value of cn for all the supported LDAP servers.</p>
User to Group or Role Membership Attribute	<p>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.</p> <p>Note: Different LDAP servers have different User to Group or Role</p>

Field	Description
	membership attributes. For example, specify the value of <code>memberOf</code> for the Open LDAP server or Microsoft Active Directory LDAP server, <code>nsroledn</code> for the Sun ONE LDAP server, and <code>ibm-allGroups</code> for the IBM Tivoli Directory Server.
isSecure	Used to check whether this is a secure LDAP URL.
isEnabled	Used to check whether the LDAP connection is enabled. No operations are permitted for disabled connections.
isReadOnly	Used to check whether the LDAP 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 Test Connection 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.

See [LDAP Configuration](#) for more information about the LDAP Role BaseDN Attribute.

BC Database

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

Authentication Source Defaults

The added and configured authentication sources are displayed in the **Source Alias** list. The Priority column indicates the order in which TIBCO BusinessConnect will use the sources to authenticate external users. For example, if you add BC Database and then LDAP as authentication sources, BCDB (the BC Database alias) will be listed first in the Source Alias list with a Priority of 1; LDAP will be listed second in the Source Alias list with a Priority of 2. When authenticating external users, TIBCO BusinessConnect will use BCDB, the source with a Priority of 1, first. If authentication fails with that source, TIBCO BusinessConnect will retry the authentication using LDAP, the source with a Priority of 2.

You can use **Move Up** and **Move Down** in **User Authentication Configuration** to adjust the priority of an authentication source.

Removing the Configured LDAP Server or the BC Database

Click **Remove** to remove the configured LDAP server or a BC Database.

Activated Protocol Plug-ins and Properties

This section explains management of the BusinessConnect plug-in properties. The Activated Protocol Plug-ins and Properties window displays any installed and activated protocol. From this window, you can perform the following steps:

- Verify the installed protocols and their versions.
- Add, change, or remove TIBCO BusinessConnect or protocol specific properties.

Activated Protocol Plug-ins and Properties

Plug-in	Title	Protocols
BC	BusinessConnect Interior Server	TIBCO BusinessConnect AS1 Transport
	Note: The pre-defined (default) properties for TIBCO BusinessConnect cannot be deleted by a user. This applies also to the internal (hidden) TIBCO BusinessConnect properties.	TIBCO BusinessConnect AS2 Transport

Plug-in	Title	Protocols
	In the Edit Plug-in Properties, enter or select data as described in the table below.	
BCRemote	BusinessConnect Remote Client Service Currently there are no default properties specific to the TIBCO BusinessConnect Remote Client Server.	PartnerSelfService
BE	BE	BE Service
CMI	BusinessConnect ConfigStore Management Interface Protocol	CMI
ebXML	BusinessConnect ebXML Protocol	ebMS3 ebXML
EZComm	BusinessConnect Services Plug-in	EZComm
GS-FILE	BusinessConnect Plug-in for FILE	FILE Gateway Service
GS-FTPS	BusinessConnect Plug-in for FTP Server	FILE Gateway Server
GS-HTTP	BusinessConnect Plug-in for HTTP	HTTP Gateway Service
GS-MGMT	BusinessConnect Gateway Management	Gateway Service Instance Gateway Service Session Lost and Found
GS-PX	BusinessConnect Plug-in for PartnerExpress	PartnerExpress Gateway Service
GS-SFTP	BusinessConnect Plug-in for SSH Server	SSH Server
GS-TCM	BusinessConnect Plug-in for Trading Community Management	PartnerSelfService Gateway Service

Plug-in	Title	Protocols
		PartnerSelfService
		PartnerSelfService Queue
RosettaNet	BusinessConnect RosettaNet Protocol	RosettaNet
SOAP	BusinessConnect SOAP Protocol	SOAP
Tibbr	Tibbr	Tibbr service
tibEDI	BusinessConnect EDI Protocol powered by Instream	EDIFACT
		Gateway
		Service
		TEXT
		TRADACOMS
		X12

This screen will contain any other activated protocols. Refer to the documentation for each of the protocols for details.

Adding, Deleting, and Editing Plug-in Properties for the TIBCO BusinessConnect Server

The following table lists plug-in properties for the TIBCO BusinessConnect server:

TIBCO BusinessConnect Server Properties Overview

Table Section	Field	Explanation / Enter
BC (BusinessConnect Interior Server)		
Database Settings	bc.db.maxretry	The maximum number of retries for a database connection in case of

Table Section	Field	Explanation / Enter
		failures. The default value is 3.
	bc.db.sleep.between.retry	The time interval between retries, in milliseconds. The default value is 1000.
	bc.db.auditlog.style	<p>How audit and non-repudiation data is stored: Uncompressed or Compressed.</p> <p>Messages are compressed to save disk space, which also triggers the overhead of compressing the messages. Therefore, choosing whether messages will be stored in compressed or in uncompressed format depends on the priorities for a specific server: saving disk space or keeping better performance.</p> <p>Note: This property cannot be changed dynamically: the TIBCO BusinessConnect server has to be restarted for this property to take effect.</p>
HTTP Settings	bc.http.threadPool.maximum	Maximum number of threads used for Outbound HTTP (or HTTPS) requests. The default value is 32.
SSL Caching Setting	bc.ssl.disableSessionCache	<p>Disable session cache for outbound HTTPS and FTPS.</p> <p>HTTPS (SSL) transport endpoints (HTTPS, AS2-HTTPS) and FTPS use an internal SSL transport cache to significantly improve the performance of negotiating security parameters</p>

Table Section	Field	Explanation / Enter
		<p>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 hasn't changed during any cached session.</p> <p>The cache usually holds successfully negotiated 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.</p> <p>In order for TIBCO BusinessConnect to enforce the renegotiation of the peer's credentials, the Disable Session Cache checkbox can be selected for any individual outgoing transport. If selected, each time TIBCO BusinessConnect has business data to be delivered to the corresponding trading partner, the peer's credentials are requested and re-verified.</p> <p>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</p>

Table Section	Field	Explanation / Enter
		problems with the involved third party server application's handling of SSL session caching.
IPFilter Settings	bc.ipfilter.enabled	Enable and disable Gateway Service Network filtering.
	bc.ipfilter.default.noMatchPolicy	<p>Default IP Filter Policy when no matching rules are evaluated on an inbound Gateway Service request where applicable. Valid values are Accept or Deny.</p> <p>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 will be evaluated to either Accept or Deny the request.</p> <p>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.</p>
Scheduler Poller	bc.task.scheduler.polling.interval	Scheduler Polling Interval (secs). The default value is 60.
Queue Poller	bc.queue.poller.enabled	Turns the message queue poller on or off. The Queue Poller monitors the message queue table to schedule sets of transactions to be sent as batches.

Table Section	Field	Explanation / Enter
		By default, this property is enabled.
	bc.queue.poller.pollingInterval	Queue Poller Polling Interval (secs). The default value is 60.
MDN Poller	bc.mdn.poller.enabled	Turns the MDN timeout poller on or off. The MDN poller should be enabled when asynchronous MDNs (receipts) are used with the standard Email, AS1 Email or AS2 HTTP/S transports. The MDN poller checks for expired receipt requests. The default option is on .
	bc.mdn.poller.pollingInterval	MDN Poller Interval (secs) The polling interval specified determines how often TIBCO BusinessConnect will check for expired receipt (MDN) requests for the standard Email, AS1 Email and AS2 transports. A shorter polling interval will allow MDN timeouts to be detected closer to the timeout period configured in the Receipt Timeout field of the Email, AS1, and AS2 transports. However, the polling interval should be long enough so that MDN timeout polling does not bog down the system. If possible, 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.

Table Section	Field	Explanation / Enter
Cancel Poller	bc.tx.terminator.enabled	<p>Cancel Poller enabled</p> <p>The Cancel Poller is used to monitor the Poller table for any pending transactions that have been marked for cancel by a user.</p> <p>By default, this property is enabled.</p>
	bc.tx.terminator.pollingInterval	<p>Cancel Polling Interval (secs). Specifies the polling interval of the cancel poller, which is responsible for terminating transactions that were marked for canceling from the GUI.</p> <p>The default value is 60.</p>
Resend Poller	bc.tx.resend.enabled	<p>Turns the resend poller on or off. The resend poller is used to monitor the Resend table for any transactions that have been marked for resending by a user.</p> <p>By default, this property is enabled.</p>
	bc.tx.resend.pollingInterval	<p>Resend polling interval, in seconds. Transactions can be selected to be resent from the GUI. BusinessConnect keeps polling for such transactions at a regular interval so it can collect them and send them as requested. The polling interval specifies the lookup frequency for the transactions that are sent.</p> <p>The default value is 120.</p>
	bc.tx.resend.messagesPerPoll	<p>This property specifies the maximum</p>

Table Section	Field	Explanation / Enter
Hibernation Poller	bc.hibernation.pollingInterval	<p>number of messages that BusinessConnect resends during one polling cycle. If there are many messages that need to be resent, memory might be 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 resent.</p>
		<p>This property along with the property <code>bc.tx.resend.pollingInterval</code> makes it possible to fine tune resend behavior by limiting the maximum number of messages to be processed in one polling cycle.</p> <p>The default value is 500.</p>
		<p>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.</p> <p>The request message from a receipt request for the standard Email, AS1 Email or AS2 HTTP/S transports will be put into hibernation until the receipt is received or the receipt timeout is exceeded. The Hibernation poller is</p>

Table Section	Field	Explanation / Enter
		<p>also used for the FTPGet transport with TEXT.</p> <p>The Hibernation Polling interval specifies how long TIBCO BusinessConnect will sleep between each polling cycle for expired hibernated messages.</p> <p>The default value is 75.</p>
	bc.hibernation.mode	<p>The hibernation mode.</p> <p>Two modes are available:</p> <ul style="list-style-type: none"> • db • ascache
FTP Poller	bc.ftpget.poller.enabled	<p>This property indicates that the poller is enabled.</p> <p>By default, this property is enabled.</p>
	bc.ftpget.poller.pollingInterval	<p>FTP polling interval, in seconds. The polling interval specifies how long TIBCO BusinessConnect sleeps between each cycle of retrieving files from the trading partners FTP sites.</p> <p>The default value is 120.</p>
	bc.ftpget.timeout	<p>FTP timeout, in seconds.</p> <p>The value specified is used to set the socket timeout for an FTP get command.</p> <p>The FTP get command terminates if it does not complete within the timeout</p>

Table Section	Field	Explanation / Enter
		period. The default value is 300.
	bc.ftpget.workers	<p>Max FTP/SSHFTP Workers per Poll.</p> <p>The FTP Poller is now multithreaded. This means that each polling cycle can utilize one or more workers. The default value is 5.</p> <p>Each worker can process an FTP/S or SSHFTP poll at a time and they are executed concurrently. One polling cycle completes if every participant's transport (that wanted to use the poller) has completed the poll.</p> <p>For example, if there are 10 participants that have set up FTP GET (or SSHFTP GET) and you specified 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 start in a similar fashion as required by the polling interval.</p> <p>The default value is 5.</p>
	bc.ftp.enablecmd.passive	<p>Enable the FTP Passive mode.</p> <p>In the FTP Passive mode, the FTP client initiates both data and command connections to the remote FTP server.</p> <p>By default, this property is enabled.</p>

Table Section	Field	Explanation / Enter
	bc.honorThreshold	<p>Honor Inbound Threshold for FTP Large Files. When selected, this checkbox directs TIBCO BusinessConnect to honor the preset inbound threshold for the large file sizes using FTP.</p> <p>If you change this setting, be sure to restart the BusinessConnect engine for the changes to take effect.</p> <p>By default, this property is enabled.</p>
SSHFTP Settings	bc.sshftp.cache.tunnel	<p>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 will destroy the tunnel and create a new one the next time the BusinessConnect engine needs to send or receive messages. If the tunnel is destroyed earlier because of other problems, such as the trading partner closed it or a disconnection occurred, BusinessConnect will try to create a new tunnel automatically and fall back to that if possible.</p> <p>The default value is 120.</p>
EDIINT	bc.ediint.streamSize	<p>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</p>

Table Section	Field	Explanation / Enter
		<p>memory. Consider setting this property to a low value when processing large messages, since it will help to conserve system memory.</p> <p>The default value is 50000000.</p>
	bc.ediint.suppress.foldedheader	<p>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).</p> <p>The resulting content-type header will be all on one line. This property can be set for a specific trading partner by creating a Boolean property with the following name format: <code>bc.ediint.suppress.foldedheader.<tpName></code></p> <p>Any spaces in the trading partner name should be replaced with underscores (_) when specifying the name of the property.</p> <p>By default, this property is enabled.</p>
	bc.ediint.as2.inbound.filename.preservation	<p>Enable file name preservation for the inbound AS2 Messages. When set to true, all inbound AS2 messages with a content disposition type of “attachment” will be stored on the file system after unpackaging. Files are stored in the shared directory for BusinessConnect, under a subdirectory for the trading partner, and by date in</p>

Table Section	Field	Explanation / Enter
		<p>the following way: If a file name has been specified in the content disposition header, it will be used when storing the message.</p> <p>If the filename already exists for that trading partner and date, it will be generated based upon the filename specified in the content disposition header and will have the following form:</p> <pre><specified filename base>_ <TP name>_<GUID>_<inbound file number>.<specified filename extension></pre> <p>If a file name extension is not specified, none is used.</p> <p>Note: Various operating systems restrict the characters used in filenames. Therefore, TIBCO BusinessConnect does not allow use of the following characters in filenames: embedded quotes, <, >, ?, :</p>
	bc.ediint.as2.outbound.filename.preservation	<p>Enable file name preservation for the outbound AS2 Messages. When set to true, BusinessConnect will try to package all outbound AS2 messages as attachments with file names by including a content disposition header of the following form:</p> <pre>Content Disposition: attachment; filename=<i>specified_filename</i></pre> <p>The value of <i>specified_filename</i> is taken from the file name specified in the</p>

Table Section	Field	Explanation / Enter
		<p>content disposition field of the message INITIATOR.REQUEST.</p> <p>If the outbound File poller is used to pass messages from the private process to BusinessConnect, the name of the file containing the message from the outbound File poller is used as the value of <i>specified_filename</i> in the content disposition header.</p> <p>Note: Various operating systems restrict the characters used in file names. Therefore, TIBCO BusinessConnect does not support the use of the following characters in file names: embedded quotes, <, >, ?, :</p>
	bc.ediint.digestAlgorithmEnabled	<p>Determines whether the AS1 and AS2 transports default to using the SHA1 message digest algorithm or pick up the digest algorithm setting from the Business Agreements/Document Security/Outbound Document Exchange/ Signing Info Settings/Digest Algorithm.</p> <p>By default, bc.ediint.digestAlgorithmEnabled is false and the AS1 and AS2 handlers will always use SHA1 for the message digest algorithm as recommended by their respective specifications.</p>
DDTP Settings	bc.ib.channel.force.plain	TIBCO BusinessConnect Gateway Server and TIBCO BusinessConnect Interior Server can use plain HTTP

Table Section	Field	Explanation / Enter
		<p>connections for DMZ Data Transfer Protocol (DDTP) data transferring after you enable this property in TIBCO Administrator GUI and set the value of the</p> <p><code>java.property.bc.ib.channel.force.plain</code> property in all <code>gsengine.tra</code> files to <code>true</code> separately. This implementation can reduce the communication time consumption between Gateway Server and Interior Server when highly performance is required and the data transfer security across the inner firewall is not a big concern.</p> <p>By default, this property is disabled.</p> <p>This property is also added to the <code>gsengine.tra</code> file located in the <code>BC_HOME/bin</code> directory in each Gateway Server.</p>
	bc.ib.channel.maxProcessor	<p>This property applies to 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 PartnerExpress, SSHFTP or FTPS service.</p>

Table Section	Field	Explanation / Enter
		<p>The default value of this property is 5. You can increase this value when high volumes or large payloads are processed.</p> <p>When you set a value for this property, it is good practice that the total value of this property in all Interior Servers is close to the total value of the <code>java.property.gs.webengine.ddtp.maxProcessor</code> property in all Gateway Servers.</p>
Others	bc.useFlock	<p>Two options are available in the list: File and Database.</p> <p>In TIBCO BusinessConnect, some functions use locks to achieve synchronization among TIBCO BusinessConnect Servers.</p> <p>If you install TIBCO BusinessConnect 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.</p> <p>Note: If you deploy TIBCO BusinessConnect in load balancing mode, you must set this property to the database-based lock.</p>
	bc.securityLevel	<p>Security Level when connecting to an HTTPS server. Select from menu: HIGH or LOW. All leaf certificates need to be checked and this value dictates how this will be done. This property is checked only on the client side and</p>

Table Section	Field	Explanation / Enter
		<p>has the following values:</p> <ul style="list-style-type: none"> • LOW Used when testing with sample certificates. When the value is LOW, the host name authentication is not done. • HIGH Default setting. BusinessConnect preforms a very strict validation on the remote server certificate to ensure that the host registered with that certificate is the same 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.restrictVersion	Security level restrict to the specified version or later. Select All, SSLv3, TLSv1, TLSv1.1, TLSv1.2, or TLSv1.3.
	bc.security.sslv2hello.enabled	Select this checkbox to enable SSL agreement authentication between trading partners.
	bc.maxAuditLog.EntriesPerView	<p>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.</p> <p>Note: If this value is set too high, it might consume all the available</p>

Table Section	Field	Explanation / Enter
		memory and put the system at risk. The default value is 300.
	bc.repo.fetch.limit	<p>This property is used to limit how many configuration items are 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.</p> <p>The default value of this property is 500.</p> <p>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 outside of 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.</p>
External Reporting Settings	bc.external.reporting.poller.enabled	This property is used to enable the external reporting poller.
	bc.external.reporting.poller.pollingInterval	This property is used to control the external reporting poller interval.
Inbox Transport Settings	bc.inbox.sendEmail	Send an Email to the Partner on successful Inbox storage when using Inbox Transport as the primary transport.

Table Section	Field	Explanation / Enter
	bc.inbox.notify.payload.Timeout	<p>Default time for the Notify transaction payload to reside in Inbox before it is purged (in minutes).</p> <p>BusinessConnect honors Asynchronous Request timeout when uploading a request to Inbox TIBCO BusinessConnect storage to be retrieved by TIBCO PartnerExpress.</p> <p>For Notify operations uploaded into the Inbox TIBCO BusinessConnect storage, the timeout value specified here will be used.</p> <p>The default value of this property is 1440.</p>
	bc.inbox.response.payload.Timeout	<p>Default time for the Response transaction payload to reside in Inbox before it is purged (in minutes).</p> <p>BusinessConnect honors Asynchronous Request timeout when uploading a request to Inbox TIBCO BusinessConnect storage to be retrieved by TIBCO PartnerExpress™.</p> <p>For Response operations uploaded into the Inbox TIBCO BusinessConnect storage, the timeout value specified here will be used.</p> <p>The default value of this property is 1440.</p>
LDAP Configuration	bc.ldap.rolebasedn.attribute	<p>The distinguished name of an LDAP entry that contains role entries. For example, the following information</p>

Table Section	Field	Explanation / Enter
		<p>can be a roleBaseDN:</p> <p>CN=Users,DC=adldap,DC=com</p> <p>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.</p> <p>See Adding an Authentication Source for more information about User Authentication and LDAP server configuration.</p> <p>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.</p>
JMS Configuration	bc.jms.destination.cache	<p>A JMS destination cache is created after you enable this property.</p> <p>By using the cache, TIBCO BusinessConnect 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</p>

Table Section	Field	Explanation / Enter
		<p>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.</p> <p>By default, this property is enabled.</p>
Audit Log	bc.auditlog.messageInAsync	<p>This property specifies whether to save transaction messages in audit log asynchronously.</p> <p>By default, this property is disabled.</p> <p>Note: With the properties of <code>bc.auditlog.messageInAsync</code>, <code>bc.auditlog.messageInAsync.maxMessages</code>, <code>bc.auditlog.messageInAsync.maxTotalSize</code>, and <code>bc.auditlog.messageInAsync.threadPool.size</code>, 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.</p>
	bc.auditlog.messageInAsync.maxMessages	<p>This property specifies the maximum number of messages in asynchronous message audit log queue.</p>

Table Section	Field	Explanation / Enter
		The default value of this property is 2000.
	bc.auditlog.messageInAsync.maxTotalSize	<p>This property specifies the maximum size of memory in MB that can be used for asynchronous message audit log.</p> <p>The default value of this property is 128.</p> <p>The limit for messages is controlled by both the <code>maxMessage</code> and <code>maxTotalSize</code> properties, the property that first reaches the limit condition takes effect.</p>
	bc.auditlog.messageInAsync.threadpool.size	<p>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.</p> <p>The default value of this property is 10. You can increase this value if the memory occupied by the messages grows up, however more database writing bandwidth is available.</p>
SSO Settings	auth.oauth.enabled	Select this checkbox to enable the SSO functionality.
	auth.oauth.authorizationURI	Enter the authorization URI of an SSO provider. It is the URI where the delegated authentication occurs.
	auth.oauth.tokenURI	Enter the token URI of an SSO provider. The token URI specifies the

Table Section	Field	Explanation / Enter
		endpoint at which the application exchanges the intermediate authorization code (JWT) with the actual access token (user information).
	auth.oauth.logouturl	Enter the SSO logout URI. This URI specifies the endpoint at which the application is logged out of the OAuth session.
	auth.oauth.tokenype	Enter ID_token, access_token, or other key ID, which holds the external user ID. During authentication, it is used to fetch the authorization permissions after retrieving the external user ID.
	auth.oauth.useridkeyattribute	Enter the key to retrieve the external user ID (for example, sub).
	OAuth Client ID	<p>Enter a unique ID for your application. It is a public key that is used to authenticate your application enabled with SSO.</p> <p>Note: This field is applicable only for TCM and PX.</p>
	OAuth Client Secret	<p>Enter a secret key for your application. It is a private key for your, which is used to authenticate the application to the authorization server.</p> <p>Note: This field is applicable only for TCM and PX.</p>

Add a Property

To add a property to any of the listed protocol plug-ins:

1. In the Edit Plug-in Properties: *plug-in_name* dialog, click **Add**.
2. In the **Property Name** field, enter the name for the new property.
3. Enter or select information as explained in the following table:

Adding New Property

Field	Description
Property Name	Type a name for the property (required)
Property Type	Select a data type from the list: boolean, string, or integer
Description	Type a description of the new property in the Description field

Delete a Property

To remove a property:

1. In the screen Edit Plug-in Properties: *plug-in_name*, click **Delete**.
2. In the Delete Property dialog, enter the name of the property to be deleted.
3. Click **OK**.



Note

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

Metadata Type Configuration

The functionality in this area is protocol-specific:

- **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™ RosettaNet Protocol User Guide*.

- **Domains** Supported by TIBCO BusinessConnect Services Plug-in, TIBCO BusinessConnect™ RosettaNet Protocol, and TIBCO BusinessConnect™ EDI Protocol powered by Instream®.

Each trading partner involved in the exchange of documents has a domain. Look in the User Guides for each of these protocols for more information.

- **Partner Classification Codes** Supported by RosettaNet. Example: Buyer.
Partner Classification Codes are explained in *TIBCO BusinessConnect™ RosettaNet Protocol User Guide*.
- **Supply Chain Codes** Supported by RosettaNet. Example: Electronic Components.
Supply Chain Codes are explained in *TIBCO BusinessConnect™ RosettaNet Protocol User Guide*.

Adding and Removing Metadata

You use the TIBCO BusinessConnect console 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 console. You can then use the new values in setting up the host or a trading partner.

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

1. Expand **BusinessConnect > System Settings > Metadata Type Configuration**.
2. Click the type of metadata to which you want to add, and click **New**.
3. To remove a value, select the checkbox next to it and click **Delete**.

Private Process Smart Routing

BusinessConnect allows you to define business rules to route messages to specific private processes. For more details, see *TIBCO BusinessConnect™ Concepts*, "Private Process Smart Routing."

Creating Business Rules for Private Process Smart Routing

A Smart Routing business rule defines a smart ID and a set of conditions to which BusinessConnect compares all messages. For example, a business rule might define a smart ID of ezacme and these conditions: protocol is TIBCO BusinessConnect Services Plug-in and messages are sent to Acme. Whenever BusinessConnect receives messages that match these conditions, it adds the smart ID ezacme to the message. This is the first step in the Smart Routing process.

**Note**

BusinessConnect does not assign multiple smart IDs to a single message; it assigns a maximum of one. If multiple business rules identify the same set of messages or overlapping sets, BusinessConnect assigns the ID associated with the first matching rule. BusinessConnect processes the rules as listed in the Smart Routing Configuration dialog, starting from the top.

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

1. Expand **BusinessConnect > System Settings > Private Process Smart Routing**.

The Edit System Settings:Private Process Smart Routing dialog is displayed.

2. Click **Add**.

The New Entry dialog is displayed.

3. Define the condition for the rule using the following table:

New Rule for the Private Process Smart Routing

Field	Description
Enabled	If selected, the new Smart Routing rule will be enabled.
Protocol	(Required) Choose the protocol for the message from the list. Use the asterisk character (*) to match all protocols.
From	(Required) The name of the trading partner that sends the original message. If Host (your company) sends a request to Partner and Partner

Field	Description
	<p>sends a response, you might want to use Smart Routing for the response. In this case, the from field is matched by Host because Host is the originator of the business transaction.</p> <p>Use the asterisk character (*) to match all hosts and partners, but <i>do not</i> use the asterisk character with a string. For example, <i>do not</i> use TIB*.</p>
To	<p>(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, the To field is matched by Host because Host is the recipient of the request.</p> <p>Use the asterisk character (*) to match all hosts and partners, but <i>do not</i> use the asterisk character with a string. For example, <i>do not</i> use TIB*.</p>
Direction	<p>(Required) The <i>business</i> direction of the message:</p> <ul style="list-style-type: none"> 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 Partner sends a response, the <i>message</i> direction of the response is inbound, but the <i>business</i> direction of the response is outbound because the original message was outbound. * The asterisk character matches both directions.
Operation ID	<p>(Required) The location and identifier of the operation. This takes the form of a series of nodes, for example: BC/1.0/Notify.</p> <p>Use one asterisk character (*) to match all operations directly under a specific node. For example:</p> <p>BC/*/ matches BC/MyNotify/Test but not BC/MyNotify/Test/notify1</p> <p>Use two asterisk characters (**) to match operations recursively. Use double asterisks alone or use them as the last node. For example:</p> <p>BC/MyNotify/** matches BC/MyNotify/1.3/Test</p> <p>BC/MyNotify/**/notify1 is the same as BC/MyNotify/**. The software</p>

Field	Description
	<p>ignores any nodes after a double asterisk.</p> <p>You can use both a single asterisk and a double asterisk, for example:</p> <p>BC/*/1.0/** matches BC/Test-01/1.0/A/B</p>
CMName	<p>The name of the listening CM (certified messaging) transport for the private process. This is optional.</p> <p>If you provide the CM name for the listening CM transport, BusinessConnect pre-registers the CM name, assuring creation of a ledger and persistence of messages in the event that the listening transport is down.</p> <p>If the CM name is not pre-registered, and BusinessConnect has not yet had an opportunity to create a ledger, and the listening CM transport is down, messages do not persist.</p> <p>Note: Do not use the asterisk character (*) in this field.</p> <p>Verify the accuracy of the CM name before deploying the rule. If the CM name you provide does not exist, the ledger will grow indefinitely.</p> <p>For more information about CM listeners and CM names, see <i>TIBCO Rendezvous Concepts</i>.</p>
Smart ID	<p>An identifier that indicates which smart routine rules the message satisfied. Any combination of alphanumeric characters, with a minimum of one character and a recommended maximum of 25 characters.</p>

4. Click **Save** and then **Done**.

The rules you have created will appear in the dialog Edit System Settings: Private Process Smart Routing, with a serial number associated to each rule.

Managing Business Rules for Private Process Smart Routing

Once the rules for Private Process Smart Routing are added, they appear on the list with their serial numbers.

You can manage the rules placement, or edit any of the rules.

Managing Business Rules Placement

You can manage the placement of the business rules on the list by using the following tabs:

- **Move Up** Select the button next to the rule's serial number and click this tab to move it up in the list.
- **Move Down** Select the button next to the rule's serial number and click this tab to move it down in the list.
- **Insert After** Select the button next to the rule's serial number and click this tab. The dialog New Entry will appear to allow you to add a new rule following the procedure explained in [Creating Business Rules for Private Process Smart Routing](#).
- **Remove** Select the button next to the rule's serial number and click this tab to remove it from the list.

Editing a Business Rule

To edit any of the configured business rules, perform the following steps:

1. Click the serial number of the rule you want to edit (not on the button next to it).
The Edit Entry dialog is displayed.
2. Edit any of the data using the [New Rule for the Private Process Smart Routing](#) table as a reference.
3. Click **Done**.

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 these steps:

1. Expand **BusinessConnect > System Settings > Credential Expiry Alerter**.
2. Enter data based on the information in [Credential Alerter](#).

Credential Alerter

Field	Enter/Select
Enable	
Polling Interval (hours)	The polling interval specifies the frequency by which the credential alerter keeps tracking and publishing alerts on expiring credentials. The default value is 24 hours.
Days Before Leaf Certificate Expiry	Specify how many days before the leaf certificate expires.
Days Before Key Expiry	Specify how many days before the key expires.
Days Before CSR Expiry	Specify how many days before the CSR expires.
Days Before CA Certificate Expiry	Specify how many days before the CA certificate expires.
Notify Email Addresses	<p>Provide one or more comma-separated email addresses for notification.</p> <p>Note: The email addresses must be different from the email addresses that you entered for the inbound mail POP3 servers.</p> <p>See Inbound Mail POP3 Servers for more details.</p>

Field	Enter/Select
From Email Address	Specify the initiating email address.

3. Click **Save**.

User Access Audit Trail

The User Access Audit Trail function provides an audit trail of all the activities that users perform on trading partners, business agreements, and operations.



Note

The User Access Audit Trail function will not audit user actions when you perform exports of one of the following:

- Participants
- Keys
- Operations

1. Expand **BusinessConnect > System Settings > User Access Audit Trail**.

The Search panel will appear as shown in [User Access Audit Trail](#).

User Access Audit Trail

Field	Description
Filters	
System Audit Trail	Select YES for the system audit trails. Selecting YES from the System Audit Trail list shows additional internal information as a part of Audit Trail information.
User Type	Choose whether the TIBCO Administrator User or ANY user is used to filter the results.
Connection	Select the database where user access audit data is saved.

Field	Description
	The default value is bc-db .
Date Range	Set the range as predefined to One Day, One Week, One Month, or Year . You can also set a custom time frame.
Add	<p>To add an advanced filter for looking at the audit trails, click Add.</p> <p>If you choose to add a filter, you will configure it as follows:</p> <p>Save as Query: enter the query name</p> <p>Username: is, contains, is not, is not like</p> <p>Action: is Create, Update, Delete ANY</p> <p>Entity Type: is Participant, Business Agreement, Operation, ANY</p> <p>Entity Name: is, contains, is not, is not like</p> <p>For more details, see Advanced.</p>

2. After you configure the query, click **Search**.

Figure 15: Result of the Audit Trail Search

BusinessConnect > System Settings

User Access Audit Trail

Search Done

Filters

System Audit Trail: YES

User Type: TIBCO Administrator User

Connection: bc-db

Date Range: One Week

Start: December 05, 2015 13:37

End: December 12, 2015 13:37

Advanced None Edit


Username: admin

Action: create

Summary Results Group by: User Name

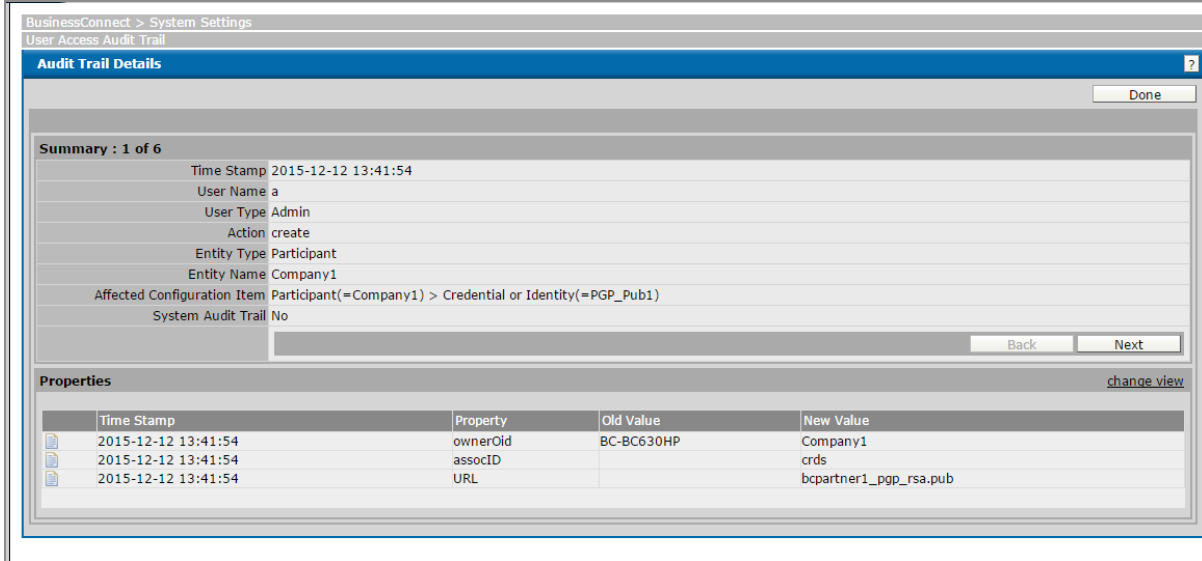
Hide Header

User Name	Date Group	Time Stamp	Action	Entity Type	Entity Name	Affected Configuration Item	System Audit Trail
a : TIBCO Administrator User 5 item(s)							
TODAY	Dec-12-2015	10:41:28 AM	update	Participant	Buyer	Participant(=Buyer) > Credential or Identity(=hostKey)	No
TODAY	Dec-12-2015	10:41:27 AM	delete	Participant	Buyer	Participant(=Buyer) > Credential or Identity(=d)	No
TODAY	Dec-12-2015	10:41:23 AM	delete	Participant	Buyer	Participant(=Buyer) > Credential or Identity(=pgp2)	No
TODAY	Dec-12-2015	10:41:23 AM	delete	Participant	Buyer	Participant(=Buyer) > Credential or Identity(=PGPPrv1)	No
TODAY	Dec-12-2015	10:41:11 AM	update	Participant	Buyer	Participant(=Buyer)	No

3. Click  to see the details.

The Audit Trail Details screen is displayed.

Figure 16: Audit Trail Details



BusinessConnect > System Settings
User Access Audit Trail

Audit Trail Details ?

Done

Summary : 1 of 6

Time Stamp	2015-12-12 13:41:54
User Name	a
User Type	Admin
Action	create
Entity Type	Participant
Entity Name	Company1
Affected Configuration Item	Participant(=Company1) > Credential or Identity(=PGP_Pub1)
System Audit Trail	No

Back Next

Properties [change view](#)

Time Stamp	Property	Old Value	New Value
2015-12-12 13:41:54	ownerOld	BC-BC630HP	Company1
2015-12-12 13:41:54	assocID		crds
2015-12-12 13:41:54	URL		bcpartner1_pgp_rsa.pub

The Details screen shows all information about the specific audited event.

The Affected Configuration Item gives the affected configurations that have been changed with respect to the GUI names and values. The values are noted within braces as a part of this audit.

By clicking **Next**, you can browse through the events that were found with this search.

Grouping Search Results

To easier read the User Access Audit Trail search results, grouping the results by using the Group By list:

- **None** Audit query results are listed starting with the latest activity.
- **Date Group** Results are grouped by days the activities have occurred.
- **User Name** Results are grouped by the user who initiated the activities.
- **Entity Name** Results are grouped by the partner for whom the activities have been initiated.

Utilities

BusinessConnect allows you to export the protocol AE schemas. This function can be used to obtain the current AE schemas for the installed business protocols, which helps understand the structure of a valid AE message for various business message types.

The Utilities function exports schemas for the protocols that are installed at a given time.

Exporting Schemas

To use this option, perform the following steps:

1. Expand **BusinessConnect > System Settings > Utilities**.
2. Click **Export**.
3. The File Download dialog will offer to open or to save the file `AESchemas.zip`.
4. You can save this file on a desired location in the compressed format, or open the file with your decompressing utility.
5. Press **Done** when finished.

Visibility

Visibility settings allow you to integrate TIBCO BusinessConnect with several other TIBCO applications: tibbr, TIBCO BusinessEvents, and TIBCO Hawk. This integration provides near real-time visibility of the overall TIBCO BusinessConnect implementation. For more conceptual information about these TIBCO BusinessConnect visibility, see *TIBCO BusinessConnect™ Concepts*, TIBCO BusinessConnect Architecture.

Configuring tibbr Settings

TIBCO BusinessConnect can post error messages to a specified tibbr subject. You can define one global tibbr subject to which TIBCO BusinessConnect will post error messages generated by transactions involving any installed and enabled protocol for all partners. You can also define a tibbr subject for error messages generated by each trading partner. For

more information on how to configure error message posting for trading partners, see [Visibility Tab for Partners](#).

All tibbr subjects created by TIBCO BusinessConnect are public. If TIBCO BusinessConnect posts to a private subject that already exists on the tibbr host, an error message in the trace log will be generated.



Note

Subject names in tibbr must be unique. Once a subject has been created in tibbr it cannot be recreated, even if you have deleted it. Subjects are retained internally by tibbr to preserve old messages posted to that subject. For example, if you create the subject BCX12 and then delete it, you cannot recreate the subject BCX12.

If you have created and deleted a subject that you want to use again, you must create another subject with a different prefix for messages to be posted to tibbr. For example, you could create the subject BC-X12 or BC_X12 if you have created and deleted the subject BCX12.

To post TIBCO BusinessConnect error messages to tibbr on a global level, follow the steps below.

1. Go to **BusinessConnect > System Settings > Visibility > tibbr**.
The tibbr Settings dialog is displayed.
2. Enter information according to [tibbr Settings](#), and click **Save**.

tibbr Settings

Field	Description
Enable Global Error Posting to tibbr	<p>Check this checkbox to enable TIBCO BusinessConnect to post error messages to the specified tibbr instance and subjects.</p> <p>Note: To enable error posting for trading partners, see Configuring Participant Visibility Settings for tibbr.</p>
tibbr Host	<p>The hostname of the server hosting tibbr. The hostname must include the protocol prefix, either <code>http://</code> or <code>https://</code>. If the hostname is secure (that is, preceded by <code>https</code>), you must provide a tibbr certificate, as explained below.</p> <p>Example: <code>https://acme.tibbr.com</code></p>

Field	Description
tibbr Port	<p>Port number of the tibbr host. The default value is 80.</p> <p>If you are using HTTPS, you must change this to the port number used by your secure tibbr instance. In most cases, 443.</p>
tibbr Certificate	<p>If the tibbr instance is a secure one (that is, if the hostname you entered was preceded by https), you must provide a certificate. If the tibbr instance is not a secure one (that is, if the hostname is preceded by http), select None from the list (this is the default).</p> <p>To obtain the certificate, follow these steps:</p> <ol style="list-style-type: none"> 1. Expand BusinessConnect > System Settings > Certificate Store. 2. In the Certificate Store dialog, click the Server Identities & Certificates > Fetch Third Party Server Certificate tab. 3. Enter the hostname — without the protocol prefix — of the tibbr instance in the Host field. For example, acme.tibbr.com. 4. Enter the port number of the tibbr instance in the Port field. This field is pre-populated with 443. You can change it if your secure tibbr instance uses another port. 5. Click OK. <p>TIBCO BusinessConnect fetches the certificate and adds it to the list Server Identities and Certificates.</p> <p>Once the certificate has been fetched, you can select it from the list.</p>
tibbr User	<p>The name of the tibbr user who will post the error messages. You can create a user specifically for this purpose.</p> <p>Example: bcadmin</p>
tibbr Password	<p>The password of the tibbr user who will post error messages.</p>
Subject Prefix	<p>The prefix of all the error messages posted to tibbr. The default value is bc. You can also define a subject prefix for each trading partner.</p>

Field	Description
(default: bc)	Example: bcX12
List of Protocols to Enable Error Posting	Any installed protocols are listed in this section. Check each protocol for which you want to enable error posting.

Configuring TIBCO BusinessEvents Settings

To enable TIBCO BusinessConnect to send messages to TIBCO BusinessEvents, follow these steps:



Note

You must also enable TIBCO BusinessEvents integration for each partner to publish messages to TIBCO BusinessEvents. See [Configuring Participant Visibility Settings for TIBCO BusinessEvents](#) for more information about how to configure publishing to TIBCO BusinessEvents for trading partners.

1. Expand **BusinessConnect > System Settings > Visibility > BusinessEvents**.

The BE Settings dialog is displayed.

2. Check the **Enable BE Integration** checkbox.

TIBCO BusinessConnect can send six types of messages to TIBCO BusinessEvents: Initiator Request, Initiator Response, Responder Request, Responder Response, Inbound Message, and Error Advisory. These message types are listed in the Message Types area of the BE Settings dialog.

Figure 17: BE Setting

BE Settings

Done

Interior Server must be redeployed for new changes to apply.

Enable BE Integration ☒

Message Type	Destination name	Enabled	JMS Channel Type
Initiator Request	AX.BC.BE.BC-ryoung.INITIATOR.REQUEST	true	Topic
Initiator Response	AX.BC.BE.BC-ryoung.INITIATOR.RESPONSE	true	Queue
Responder Request	AX.BC.BE.BC-ryoung.RESPONDER.REQUEST	true	Queue
Responder Response	AX.BC.BE.BC-ryoung.RESPONDER.RESPONSE	true	Queue
Inbound Message	AX.BC.BE.BC-ryoung.INBOUND.MESSAGE	true	Queue
Error Advisory	AX.BC.BE.BC-ryoung.ERROR.ADVISORY	true	Queue

You must enable each message type that you want sent to TIBCO BusinessEvents. You must also specify the destination name and JMS channel type (that is, Topic or Queue) for each message type.

The destination name serves as the TIBCO Rendezvous subject name or the JMS topic or queue name, depending on which private process transport type you selected in **Application Management > BusinessConnect > Configuration > BusinessConnect > Private Process Configuration**. See *TIBCO BusinessConnect™ Interior Server Administration*, Private Process Configuration for more information about private process configuration.

To make changes to any of these settings:

3. Click a message type.

The Edit Entry dialog is displayed.

Figure 18: Message Type Configuration

Edit Entry: Initiator Request

Save Cancel

Destination name AX.BC.BE.BC-ryoung.INITIATOR.REQUEST

Enabled ☒

JMS Channel Type Queue ▼

4. Enter the destination name you want to use in the **Destination name** field. This field is pre-populated according to the following form:

`AX.BC.BE.installation_name.MESSAGE.TYPE`

5. Check the **Enabled** checkbox to enable messages of this type to be sent to TIBCO BusinessEvents.
6. Select either **Queue** or **Topic** from the **JMS Channel Type** list.

Configuring Application Monitoring and Management Settings

The health and statistical information of TIBCO BusinessConnect Interior Server Instances and Gateway Instances can be exposed to TIBCO Hawk. The health and statistical information of Interior Server Instances and Gateway Instances are also available in TIBCO Administrator through TIBCO Hawk.

TIBCO BusinessConnect Interior Server Instances play the bridge role between the Gateway Instances and TIBCO Hawk Agent. TIBCO Hawk Agent and Display do not have to run within the same DMZ or subnet where the Gateway Instances run.

Rulebases can be used to manage Gateway Instances as other applications.

**Note**

Before monitoring and managing TIBCO BusinessConnect Interior Server Instances and Gateway Instances by TIBCO Hawk, you are required to install the full version of TIBCO Hawk first, and then install TIBCO Hawk® JMX Plug-in.

You do not have to install the TIBCO Hawk Agent component, because this component is contained in TIBCO Runtime Agent.

See the readme file for the supported versions.

You have two deployment modes for TIBCO Hawk, one is installing and configuring on one local machine, and the other is using a remote machine to monitor and manage TIBCO BusinessConnect Interior Server Instances and Gateway Instances of your local machine. See [Deployment Modes for Application Monitoring and Management](#).

After installing TIBCO Hawk and TIBCO Hawk JMX Plug-in, the following configuration tasks are required for enabling application monitoring and management:

Selecting an internal user that TIBCO Hawk uses for authentication.

See [Selecting an Internal User for Application Monitoring and Management](#) for more details.

1. Enabling application monitoring and management for each Interior Server Instance you want to monitor.
See [Enabling Application Monitoring and Management for Service Instances](#) for more details.

2. Editing the JMX configuration file, `JMXPluginConfig.xml`.
You must define an MBean Server section for each Interior Server Instance you want to monitor. See [Editing the JMX Configuration File for Application Monitoring and Management](#) for more details.
3. Configuring TIBCO Hawk for application monitoring and management. See [Configuring TIBCO Hawk for Application Monitoring and Management on Windows](#) and [Configuring TIBCO Hawk for Application Monitoring and Management on UNIX](#) for more details.

After performing the preceding tasks, see [Monitoring and Management with TIBCO Hawk](#) for how to track the status of TIBCO BusinessConnect Interior Server Instances and Gateway Instances.

The rulebases have to be set for monitoring. See [Application Monitoring and Management by Processing Rulebases](#) for more details. For more information on how to build a rule, see [Building a Rule](#).

Deployment Modes for Application Monitoring and Management

You have two deployment modes for TIBCO Hawk, one is installing and configuring on one local machine, and the other is using a remote machine to monitor and manage TIBCO BusinessConnect Interior Server Instances and Gateway Instances of your local machine.

- Install, configure, monitor, and manage on one local machine:

To install the required software, see Software Requirements in *TIBCO BusinessConnect™ Installation and Configuration*.

To configure TIBCO Hawk for application monitoring and management, you have to perform all the tasks on [After installing TIBCO Hawk and TIBCO Hawk JMX Plug-in, the following configuration tasks are required for enabling application monitoring and management:](#).

- Use a remote machine to monitor and manage the application of the local machine:

This deployment mode is suitable for the local machine that TIBCO BusinessConnect is installed, but the full version of TIBCO Hawk and TIBCO Hawk JMX Plug-in are not installed. You can set a remote machine to install the full version of TIBCO Hawk and TIBCO Hawk JMX Plug-in.

To install the required software on a remote machine, you have to install TIBCO Rendezvous, TIBCO Runtime Agent, TIBCO Administrator, full version of TIBCO Hawk, and then install TIBCO Hawk JMX Plug-in. You do not need to install TIBCO Hawk Agent component, because this component is contained in TIBCO Runtime Agent.

**Note**

You have to create a domain for configuration on your local machine which TIBCO BusinessConnect is installed. You also need to create another unique domain on the remote machine for configuration.

Selecting an Internal User for Application Monitoring and Management

1. Go to **BusinessConnect > System Settings > Visibility > Application Monitoring & Management**.

2. Select a user from the **Administrator User** list.

The TIBCO Hawk Agent authenticates against this user to connect to TIBCO BusinessConnect to monitor and manage the service instances.

Internal users can be viewed and created by going to **BusinessConnect > User Management > Users** and clicking the **Internal** tab. The credentials created for this user are used when editing the JMX configuration, as described in [Editing the JMX Configuration File for Application Monitoring and Management](#).

3. Click **Save**.

**Note**

If you change the credentials for this user, you must restart the Interior Server Instance for the changes to take effect. You must also update the TIBCO Hawk Agent's JMX configuration file with the new credentials to ensure successful connection to the Interior Server Instances, and restart TIBCO Hawk Agent.

See [Managing Users with TIBCO BusinessConnect User Management](#) for more information.

Enabling Application Monitoring and Management for Service Instances

You must enable application monitoring and management in each Interior Server Instance you want to monitor and manage:

1. Go to **Application Management > BusinessConnect > Configuration**.
2. Select a service instance.
3. In the Edit Service Instance page, select the **Process Configuration** tab.

4. In the **Application Monitoring & Management** area, select the **Enable** check box.
5. In the **Monitoring Port** field, enter the port number to be used by TIBCO Hawk. The default value is 11010.

Note: The port number must be unique and cannot be used by other processes.

6. Click **Save**.
7. Redeploy TIBCO BusinessConnect by clicking **Deploy**, and click **OK**.

Editing the JMX Configuration File for Application Monitoring and Management

The username and password of the Administrator user selected at [Select a user from the Administrator User list](#) in [Selecting an Internal User for Application Monitoring and Management](#) must also be specified in the MBean Server section of the JMX configuration file. To edit the file, follow these steps:

1. Edit the JMXPluginConfig.xml file in the *TIBCO_HOME\hawk\version\plugin* directory.
2. In the MBeanServerList section of the JMXPluginConfig.xml file, add an MBeanServer entry and define values for each parameter. The values should correspond to the Interior Server Instance you want to monitor. Each of these instances must be enabled in TIBCO Administrator GUI, as described in [Enabling Application Monitoring and Management for Service Instances](#).

```
<MBeanServer name="BusinessConnect InteriorServer1" type="JSR160">
  <JMXClassPath>D:/tibco/tibcojre64/1.8.0/lib/rt.jar</JMXClassPath>
  <ParameterList>
    <param name = "JMXServiceURL" value =
"service:jmx:rmi:///jndi/rmi://127.0.0.1:11010/jmxrmi"/>
    <!-- login/password to connect to the connector server. -->
    <param name = "login" value = "username"/>
    <param name = "password" value = "secure_password"/>
  </ParameterList>
</MBeanServer>
```

The value for the **JMXServiceURL** parameter is the service instance you want to monitor. The IP address can be the same as the local server or another, remote server. In either case, the port number must be the same one entered in [In the](#)

[Monitoring Port](#) field, enter the port number to be used by TIBCO Hawk. The default value is 11010. of [Enabling Application Monitoring and Management for Service Instances](#).

The values for the **login** and **password** parameters must be same as those defined for the Internal User selected in [Select a user from the Administrator User list](#). of [Selecting an Internal User for Application Monitoring and Management](#). If a user and password are not defined, application monitoring and management are disabled.

You must create an MBeanServer entry for each Interior Server Instance. Different MBeanServer entry has different names, but the same type. For example, the **JMXClassPath** parameter is *TIBCO_HOME/tibcojre64/version/lib/rt.jar*. Each additional section must be under the same MBeanServerList.

Configuring TIBCO Hawk for Application Monitoring and Management on Windows

Using TIBCO Hawk for application monitoring and management on Windows requires some additional configuration. After editing the JMX configuration file, perform the following steps:

1. Run `tibhawkconfig.exe`.
2. Enter your TIBCO Hawk domain, TIBCO Rendezvous settings, and your TIBCO Hawk Agent name.
3. Go to the *TIBCO_HOME/tra/domain/domain_name* directory.
4. In the `hawkagent.cfg` file, ensure that the property **hma_plugin_dir** is defined as the *TIBCO_HOME/hawk/version/plugin* directory.

For more detailed information about configuring TIBCO Hawk, see the appropriate TIBCO Hawk documentation.

Configuring TIBCO Hawk for Application Monitoring and Management on UNIX

Using TIBCO Hawk for application monitoring and management on UNIX requires some additional configuration. After editing the JMX configuration file, perform the following steps:

1. Ensure that the `hawkagent_domain_name.tra` file correctly references the

hawkagent.cfg file. Both of these files are located in the *TIBCO_HOME/tra/domain/domain_name* directory.

2. Ensure that the following properties are correctly defined in the hawkagent.cfg file. For example, the **auto_config_dir** property should be defined as the *TIBCO_HOME/hawk/version/autoconfig* directory.

The properties that must be defined correctly are:

- **domain** Your domain name.
- **agent_name** Your computer name.
- **rvd_session** Your TIBCO Rendezvous parameters for TIBCO Hawk. The default value is 7474;tcp:7474. If you are going to use the TIBCO Hawk display to add rulebases for TIBCO BusinessConnect, see [auto_config_dir](#) Your auto configuration directory. For example, *TIBCO_HOME/hawk/version/autoconfig*. If you are going to use the TIBCO Hawk display to add rulebases for TIBCO BusinessConnect, configure the **rvd_session** property in the hawkdisplay.cfg file in the *TIBCO_HOME/hawk/version/bin* directory..
- **hma_plugin_dir** Your TIBCO Hawk plugin directory. For example, *TIBCO_HOME/hawk/version/plugin*.
- **auto_config_dir** Your auto configuration directory. For example, *TIBCO_HOME/hawk/version/autoconfig*.
If you are going to use the TIBCO Hawk display to add rulebases for TIBCO BusinessConnect, configure the **rvd_session** property in the hawkdisplay.cfg file in the *TIBCO_HOME/hawk/version/bin* directory.

For more detailed information about configuring TIBCO Hawk, see the appropriate TIBCO Hawk documentation.

Monitoring and Management with TIBCO Hawk

Log in to TIBCO Administrator, **All Alerts**, **Hawk Console**, and **Monitoring Console** is under **Monitoring Management**. See *TIBCO Hawk Plug-in For TIBCO Administrator* for more information.

The rulebases are need to be set for monitoring, see [Application Monitoring and Management by Processing Rulebases](#) for more details.

User Access Management

User management allows you to define different access privileges for users or groups of users as required by your business needs.

Overview

With TIBCO Administrator User Management, you can create users and roles and assign them access rights to resources available in the administration domain. It provides the ability to manage access restrictions on users of the TIBCO BusinessConnect administration console.

TIBCO BusinessConnect User Management works in conjunction with TIBCO Administrator User Management. The access rights defined for a user with TIBCO Administrator User Management can be further restricted using TIBCO BusinessConnect User Management.

TIBCO Administrator User Categories

Users and roles are first created by using TIBCO Administrator User Management.

The user categories that are created are:

- TIBCO Administrator User
- TIBCO BusinessConnect Super User
- TIBCO BusinessConnect User (internal and external)

For more details about the different categories of users, see also:

- *TIBCO Administrator™ User Guide*, "Managing Users and Roles."
- *TIBCO BusinessConnect Concepts*, "TIBCO BusinessConnect User Management."

User Management

TIBCO BusinessConnect User Management provides the ability to reduce access for the users of the TIBCO BusinessConnect administration console.

Using TIBCO BusinessConnect User Management, the access rights of users can be further restricted by participant and business agreement. For participants (Host or Trading Partner), users can be assigned access rights to all participants or to particular participants.

To read general information about user management, see *TIBCO BusinessConnect™ Concepts*, "TIBCO BusinessConnect User Management."

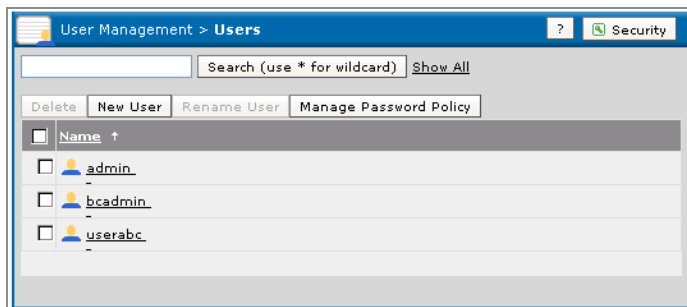
To learn how to proceed with managing groups and users, see:

- [Managing Users with TIBCO BusinessConnect User Management](#)
- [Managing Groups with TIBCO BusinessConnect User Management](#)

Using TIBCO Administrator User Management

TIBCO Administrator User Management allows you to create users and roles and assign them access rights to resources available in the administration domain; you can give users Read, Write or Administer access to the TIBCO BusinessConnect components. After creating users with TIBCO Administrator User Management, you will obtain a list of users with different access rights (see [List of Users Created by TIBCO Administrator User Management](#)).

Figure 19: List of Users Created by TIBCO Administrator User Management



The created user categories are:

- **TIBCO Administrator User** (with various levels or privileges). The domain administrator user has Super User privileges in TIBCO Administrator and can assign other users to the Super User role. To learn more, see *TIBCO Administrator™ User Guide*, Granting Security Access to Objects.

The TIBCO Administrator Super User will always have full access to the configuration information of TIBCO BusinessConnect. However, this user will not be automatically assigned as a TIBCO BusinessConnect Super User unless it is the user who created the TIBCO BusinessConnect installation.

- **TIBCO BusinessConnect Super User** In addition to the TIBCO Administrator Super User, a TIBCO BusinessConnect Super User can use TIBCO BusinessConnect User Management to add other TIBCO Administrator Users to TIBCO BusinessConnect and manage the access rights of those users. There must always be at least one TIBCO BusinessConnect Super User.

The TIBCO Administrator user who creates the TIBCO BusinessConnect installation is automatically a TIBCO BusinessConnect Super User. For more details, see *TIBCO BusinessConnect™ Concepts*, "TIBCO BusinessConnect Super User."

- **TIBCO BusinessConnect Internal User** (with various levels or privileges).

Setting TIBCO BusinessConnect Access Rights for a User

To set TIBCO BusinessConnect access rights for a user under TIBCO Administrator User Management, log in as a user that has Administer access to the resources of TIBCO BusinessConnect to which you wish to allow access for that user and do this:

1. Expand **User Management > Users**.
2. Double click the user needing access rights, such as bcsuper (TIBCO BusinessConnect Super User).
3. Select the **Permissions** tab.
4. Expand the resource list under 'TIBCO Administrator' by clicking on the '+' next to the item **TIBCO Administrator**.
5. Expand the resource list under BusinessConnect by clicking on the '+' next to the item **BusinessConnect**.
6. Click the appropriate box for the BusinessConnect component to allow Read, Write or Administer permissions.

Figure 20: Allow Permissions for TIBCO BusinessConnect Components

Authorization for: bcsuperuser				
		Read	Write	Administer
[-] TIBCO Administrator		<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
[-] Users		<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
[+] Roles		<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
[-] Machines		<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
[+] Application Management		<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
[-] Application Domains		<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
[-] BwManualWork		<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
[-] BusinessConnect		<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
[-] Participants		<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
[-] Business Agreements		<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
[-] Operations Editor		<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
[+] Partner Management		<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
[-] Log Viewer		<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
[-] Gateway		<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
[-] Reporting		<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
[-] Dashboard		<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
[-] System Settings		<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
[+] User Management		<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
[-] UDDI Servers		<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
[+] Data Access				

**Note**

When users log in, they will not be able to see the TIBCO BusinessConnect components they were given access to unless they are also given read access to the top-most TIBCO BusinessConnect component.

In the example on [Three Types of Users](#), the user has been given Read/Write/Administer access to all TIBCO BusinessConnect components.

Managing Users with TIBCO BusinessConnect User Management

TIBCO BusinessConnect User Management is integrated with the user management capabilities of TIBCO Administrator.

First you have to add users and give them access rights to one or more components of TIBCO BusinessConnect using TIBCO Administrator User Management.

After that, you will add these users to TIBCO BusinessConnect User Management and give them access rights fine tuned with respect to trading partner access, business agreement access, log viewer access, and reports access. See [Adding Users](#) for more information.

Finally, you can add groups and join users to these groups to facilitate management of user permissions.

**Note**

The process of adding or deleting users through TIBCO BusinessConnect User Management does not actually add or remove users from the application: it only changes their permissions and access rights with respect to TIBCO BusinessConnect.

Super Users

As explained in [TIBCO Administrator User Categories](#), there are two types of super users:

- The TIBCO Administrator Super User has the full access to the configuration information of TIBCO BusinessConnect, but is not automatically assigned to be a TIBCO BusinessConnect Super User unless it is the user who created the TIBCO BusinessConnect installation.
- The TIBCO BusinessConnect Super User is the only user who can use TIBCO BusinessConnect User Management to add other TIBCO Administrator Users and manage the access rights of those users. There must always be one TIBCO BusinessConnect Super User.

Internal Users

Internal Users in TIBCO BusinessConnect are used for authentication from requests sent by Interior private process applications, such as the CMI protocol, to manage participant, business agreement as well as operation level information for business protocols such as TIBCO BusinessConnect EDI Protocol powered by Instream, TIBCO BusinessConnect RosettaNet Protocol, TIBCO BusinessConnect ebXML Protocol, TIBCO BusinessConnect SOAP Protocol, TIBCO BusinessConnect Services Plug-in, amongst others. Internal users are also used by TIBCO Hawk to authenticate its connection to TIBCO BusinessConnect to monitor and manage the application.

To add an internal user, see [Adding Internal Users](#).

For more details, see:

- [User Access Tab for Participants](#)
- [User Access Tab for Business Agreements](#)
- [Configuring Application Monitoring and Management Settings](#)

External Users

TIBCO BusinessConnect External users are specified only in the TIBCO BusinessConnect administrative GUI and they are associated with a trading partner, not with a specific protocol.

The same administrative GUI is used to assign the Server (PartnerExpress, TCM, SSH, or FTPS) with which these external users will communicate.



Note

The **External** tab under **BusinessConnect > User Management > Users** only displays the external users configured in the authentication source, which is listed at the top on the User Authentication Configuration page. You have to move an authentication source to the top to display the users configured in this source.

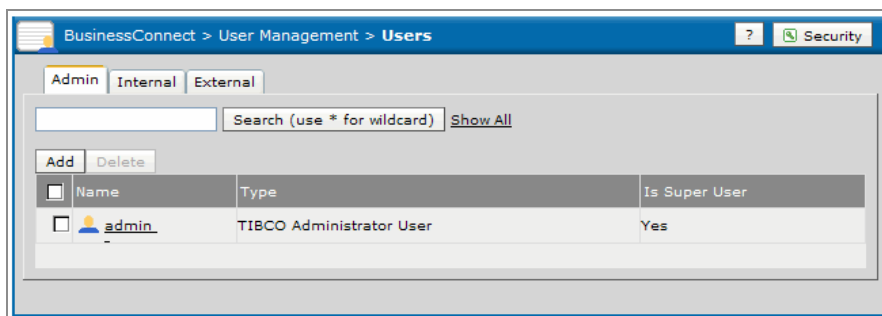
To add an external user, see [Adding External Users](#).

Adding Users

Expand **BusinessConnect > User Management > Users** in the TIBCO Administrator console.

Three types of users are available: Admin, Internal, and External.

Figure 21: Three Types of Users



You can now add other users who were granted permission to access TIBCO BusinessConnect using TIBCO Administrator.

Adding Administrative Users

To add a TIBCO BusinessConnect administrative user:

1. Expand **BusinessConnect > User Management > Users > Admin.**

2. Click **Add**.

Select the TIBCO BusinessConnect administrator user to add.

A list will appear showing users who have been added using TIBCO Administrator and granted permissions to access TIBCO BusinessConnect (as explained in [Setting TIBCO BusinessConnect Access Rights for a User](#)).

3. Check the checkbox next to the user names.
4. Click **OK**.

Continue editing this administrative user as explained in the section [Editing Users](#).

The list shows whether the TIBCO Administrator user is a TIBCO BusinessConnect Super User. There are two types of super users:

- The TIBCO Administrator Super User has the full access to the configuration information of TIBCO BusinessConnect, but is not automatically assigned to be a TIBCO BusinessConnect Super User unless it is the user who created the TIBCO BusinessConnect installation.
- The TIBCO BusinessConnect Super User is the only user who can use TIBCO BusinessConnect User Management to add other TIBCO Administrator Users and manage the access rights of those users. There must always be one TIBCO BusinessConnect Super User.

Adding Internal Users

To add a TIBCO BusinessConnect internal user:

1. Expand **BusinessConnect > User Management > Users > Internal.**
2. Click **Add**.
3. Set a username and click OK.

Continue editing this internal user as explained in the section [Editing Users](#).

Adding External Users

External users are specified in the TIBCO BusinessConnect administrative GUI and associated with a trading partner, not with a specific protocol. The same administrative GUI is used to assign the Gateway Services, which these external users can communicate with.

TIBCO BusinessConnect supports using the TIBCO Administrator GUI to directly add, delete, and update external users to BCDB and LDAP servers, such as the Microsoft Active Directory LDAP, Sun ONE LDAP, and IBM Tivoli Directory Server LDAP, Open LDAP servers.

When adding external users to LDAP servers, ensure that you configure a valid value for the `bc.ldap.rolebasedn.attribute` property that is located in TIBCO Administrator GUI under **BusinessConnect > System Settings > Activated Protocol Plug-ins and Properties > BC**.

To add external users, perform the following steps:

1. On the User Authentication Configuration page, move the authentication source where you want to add the users, to the top of the **Authentication Source** list. This authentication source is the target authentication source of your user management activities.
2. To add an external user, expand **BusinessConnect > User Management > Users > External**.
3. Click **Add**.
In the Set Email dialog, enter the following information:
 - **Email** Enter the Email address for the new external user.
 - **Belongs to Partner** From the list, select the name of the partner with which this external user will be associated.
4. Click **OK**.
5. In the Edit New User window, enter information as explained in [Editing External User](#).

Editing External User

Field	Description
General	
Email	This field initially contains user's name. Enter the email of the new

Field	Description
	external user.
Password	Click Set to enter the password that will be used to authenticate the user.
First Name	First name of the user you are creating.
Last Name	Last name of the user you are creating.
Belongs to Partner	The previously selected Partner is displayed. This information cannot be changed using the external user's settings.

Access: GatewayServerPX

(available only if PartnerExpress is installed and activated)

ReadWrite	<p>Select whether this external user has read and write permissions for the PartnerExpress Server.</p> <p>If this checkbox is checked, the external user can log into the PartnerExpress Server; otherwise, the external user has no permission to log in. You can also update its permissions by using the TCM user management function. For more details, see <i>TIBCO BusinessConnect™ Trading Community Management User Guide</i>.</p>
------------------	--

Access: GatewayServerFTPS

(available only if FTP Server is installed and activated)

ReadWrite	<p>Select whether this external user has read and write permissions for the FTPS Server.</p> <p>If this checkbox is checked, the external user can log into the FTP Server; otherwise, the external user has no permission to log in. You can also update its permissions by using the TCM user management function. For more details, see <i>TIBCO BusinessConnect™ Trading Community Management User Guide</i>.</p>
------------------	---

Field	Description
Access: GatewayServerSFTP	
(available only if SSH Server is installed and activated)	
ReadWrite	<p>Select whether this external user has read and write permissions for the SSH Server.</p> <p>If this checkbox is checked, the external user can log into the SSH Server; otherwise, the external user has no permission to log in. You can also update its permissions by using the TCM user management function. For more details, see <i>TIBCO BusinessConnect™ Trading Community Management User Guide</i>.</p>
Access: GatewayServerTCM	
(available only if TCM Server is installed and activated)	
Read Only	<p>Select whether this external user has read permissions for the TCM Server.</p> <p>If this checkbox is checked, the external user can log into the TCM Server; otherwise, the external user has no permission to log in. You can also update its permissions by using the TCM user management function. For more details, see <i>TIBCO BusinessConnect™ Trading Community Management User Guide</i>.</p>
ReadWrite	<p>Select whether this external user has read and write permissions for the TCM Server.</p> <p>If this checkbox is checked, the external user can log into the TCM Server; otherwise, the external user has no permission to log in. You can also update its permissions by using the TCM user management function. For more details, see <i>TIBCO BusinessConnect™ Trading Community Management User Guide</i>.</p>
Super User	<p>Select whether this external user has read and write permissions for the TCM Server.</p> <p>If this checkbox is checked, the external user is granted the permissions to act as a TIBCO BusinessConnect Super User for the TCM Server. You can</p>

Field	Description
	also update its permissions by using the TCM user management function. For more details, see <i>TIBCO BusinessConnect™ Trading Community Management User Guide</i> .

Editing Users

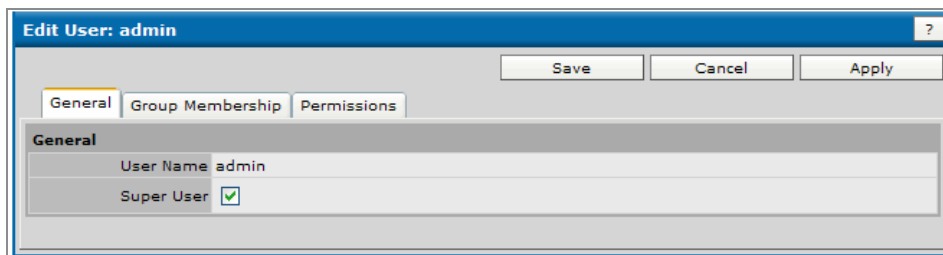
To edit any of the listed administrative users, perform the following steps:

1. Expand **BusinessConnect > User Management > Users > Admin|Internal|External**.
2. Select the username link.
The Edit User dialog is displayed with three tabs: General, Group Membership, and Permissions.

General Tab for Administrative Users

The General tab has a non-editable field for User Name. This name was created using the TIBCO Administrator User Management function and cannot be changed by the TIBCO BusinessConnect User Management.

Figure 22: Editing Administrative Users: General Tab



1. When the Super User checkbox is checked, the user is granted the permissions to act as a TIBCO BusinessConnect Super User for this TIBCO BusinessConnect installation. See *TIBCO BusinessConnect™ Concepts*, TIBCO BusinessConnect Super User for more information.

Change of user roles (promoting users to super users or removing the super user role) can be done by the following users:

TIBCO BusinessConnect Super User

TIBCO Administrator Super User

The administrative user who has created the installation.

Note: The role of the last TIBCO BusinessConnect™ Super User is locked with the system and cannot be changed.

2. Click **Apply** to continue editing other two tabs, or **Save** if you have finished with editing this user.

General Tab for Internal Users

The General tab for non-administrative users has only two fields that are both editable: username and password.

Figure 23: Editing Non-Administrative Users: General Tab

The screenshot shows a window titled "Edit User: BCadmin1". At the top right are buttons for "Save", "Cancel", and "Apply". Below these are three tabs: "General", "Group Membership", and "Permissions". The "General" tab is selected and shows two input fields: "User Name" with the value "BCadmin1" and "Password" with masked characters "*****" and a "change..." link next to it.

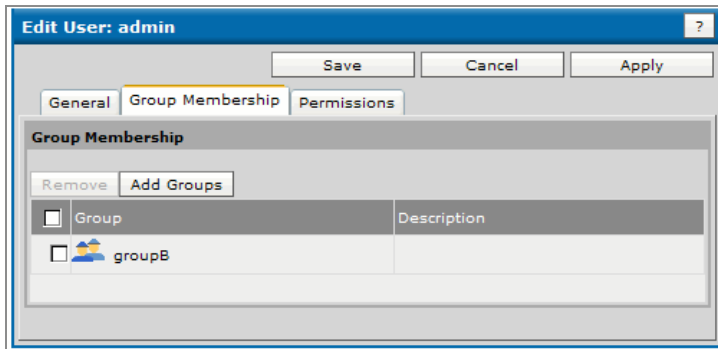
1. If needed, edit the name or password of this user.
2. Click **Apply** to continue editing other two tabs, or **Save** if you have finished with editing.

Group Membership Tab for Administrative and Internal Users

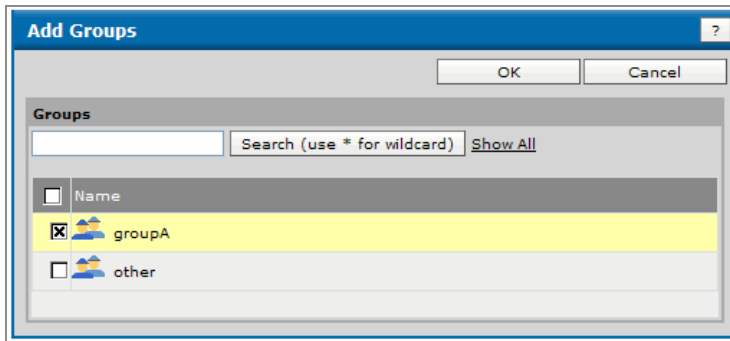
This tab verifies user's group membership and adds or removes the user from groups.

Add a Group

1. Select the **Group Membership** tab.
The Group Membership window shows the (list of) groups that this user belongs to.

Figure 24: Group Membership Tab

2. To add this user to a group, click **Add Groups**.
The Add Groups dialog is displayed.

Figure 25: Adding Groups

3. Check the checkbox next to the group to which you want to add the user.
4. Click **OK**.

Remove a Group

1. Check the checkbox next to the group.
2. Click **Remove**.
3. Click **Apply** to continue editing other two tabs, or **Save** if you have finished with editing this user.

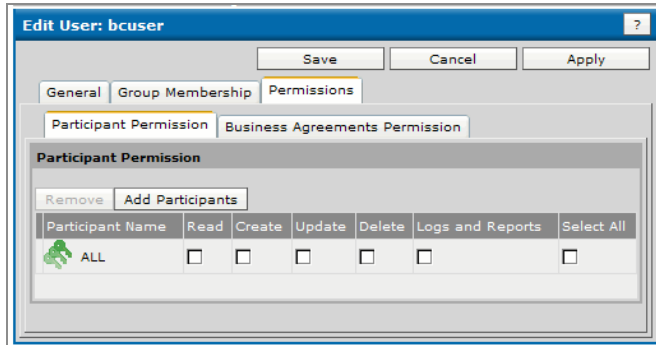
Permissions Tab for Administrative and Super Users

Currently, all added internal users by default are super users and have all permissions. The permissions of super users cannot be edited.

The access rights of users can be further restricted by participant and business agreement. For participants (Host or Trading Partner), users can be assigned access rights to all participants or to particular participants: access rights can be fine tuned with respect to trading partner access and business agreement access.

When you select this tab, the two sub tabs appear: Participant Permission and Business Agreements Permission.

Figure 26: Editing User Permissions



Participant Permissions Tab for Administrative and Internal Users

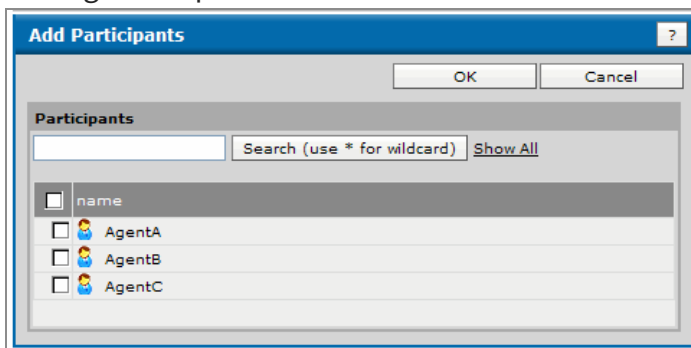
In the Participant Permissions sub tab, you can add or remove participants (host or trading partners), as well as change the permission that a particular user has regarding its access to these participants.

Add Participants

1. Click **Add Participants**.

The list of trading partners configured for the current TIBCO BusinessConnect installation is displayed.

Adding Participants

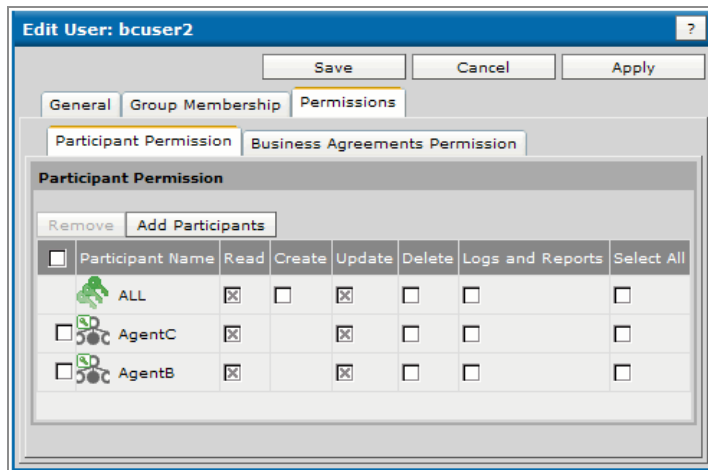


2. Check the checkbox next to the trading partners for which you want to change user's access rights.
3. Click **OK**.

Change Permissions

The list of trading partners is displayed, with the user access rights for dealing with these participants.

Figure 27: Participant Permissions for Users



1. Select or clear check boxes for any permissions that you want to fine tune: Read, Create, Update, Delete, Logs and Reports, or Select All.
For an overview of user access rights, see *TIBCO BusinessConnect™ Concepts*, "Participants Access Rights."
Again, you can only reduce the level of access rights that the specific user has in dealing with the selected trading partners.
When you select the checkbox Select All in the category ALL, all permissions will be checked.

Remove Participants

1. Select the checkbox next to any participant name.
2. Click **Remove**.
The participant is removed.

**Note**

The participant is not removed from the installation; it only means that the user you are editing has no configured permissions to deal with this trading partner.

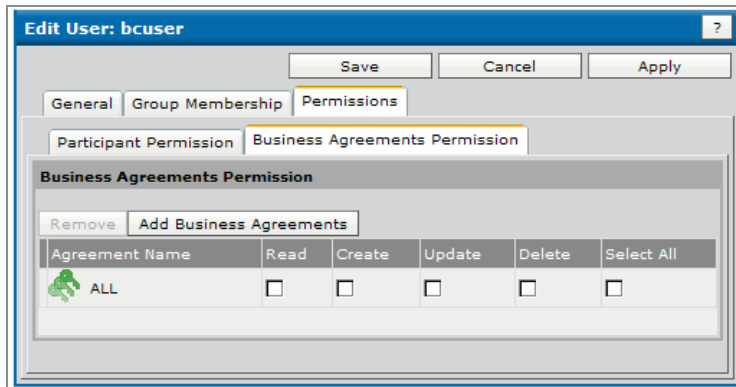
Business Agreements Permission Tab for Administrative and Internal Users

For Business Agreements, users can be assigned access rights to all Business Agreements or to particular Business Agreements.

This tab allows you to add and/or remove business agreements, as well as to change access rights that the specific user has regarding these agreements.

This window shows the list of business agreements to which the edited user has access rights, as well as the level of these access rights: Read, Create, Update, Delete, and Select All.

Figure 28: Business Agreement Permissions



Add Business Agreements

1. Click **Add Business Agreements**.

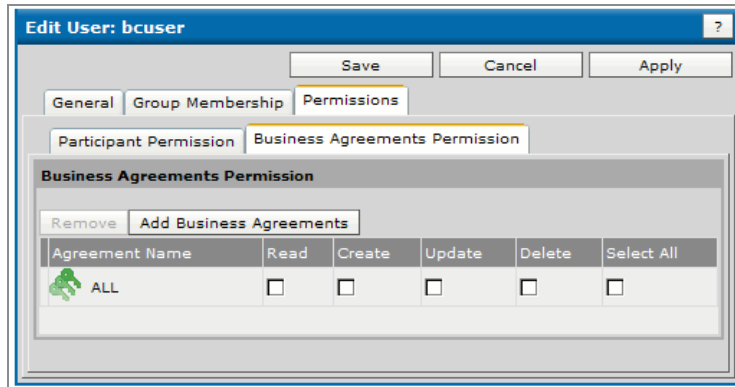
The list of configured business agreements for the current TIBCO BusinessConnect installation is displayed.

2. Check the check boxes next to the business agreements for which you want to change user's access rights.
3. Click **OK**.

Change Permissions

The list of business agreements is displayed, with the user access rights for dealing with these agreements.

Figure 29: Business Agreements Permissions for Users



1. Select or unselect check boxes for any agreements that you want to fine tune: Read, Create, Update, Delete, or Select All.
For an overview of user access rights, see *TIBCO BusinessConnect™ Concepts*, "Business Agreements Access Rights."
Again, you can only reduce the level of access rights that the specific user has in dealing with the selected business agreements.
When you select the checkbox Select All in the category ALL, all permissions will be checked.

Remove a Business Agreement

1. Select the checkbox next to any business agreement.
2. Click **Remove**.
The business agreement is removed.



Note

The business agreement is not removed from the installation; it only means that the user you are editing has no configured permissions to deal with this business agreement.

Authenticating External Users

To add an authentication source for external users:

1. Expand **BusinessConnect > System Settings > User Authentication Configuration**.
2. In the **External** tab, configure settings as explained in [Configuring the Authentication Source for the External User](#).

Configuring the Authentication Source for the External User

Field	Description
Add	<p>To add the authentication source:</p> <ol style="list-style-type: none">1. Click Add.2. In the type list, select the source type with which the external user will be authenticated: LDAP If the LDAP server is selected, proceed with configuring its settings as described in Editing LDAP Connection. BC Database This is the internal TIBCO BusinessConnect database.3. Click OK. The added type, LDAP or BC Database, will now be available as the Authentication Source.4. In the Edit LDAP Connection screen, click Test Connection. If the test is not successful, review the configuration steps. <p>The LDAP or BC Database that you added is displayed in the list of source aliases in the User Authentication Configuration dialog. If you added more than one source alias, you can adjust the priority of each one by using Move Up and Move Down.</p>

Editing LDAP Connection

If you select the LDAP server for authentication source, enter information as described in [LDAP Server Settings](#).

Removing Users

You can remove any of the users from this list by checking the user checkbox and then clicking **Delete**.

Searching for Users

Use the **Search (use * for wildcard)** function to search for the users that are not displayed on the list.

Managing Groups with TIBCO BusinessConnect User Management

In TIBCO BusinessConnect 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 groups are the equivalent of TIBCO Administrator roles and behave similarly but use the access rights which are specific to TIBCO BusinessConnect.

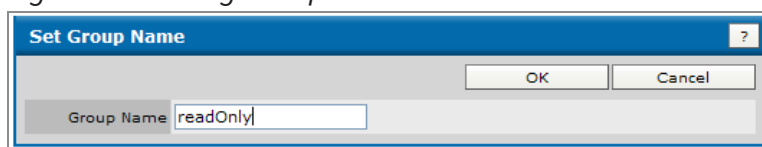
For an overview of the TIBCO BusinessConnect User Management feature for managing groups, see *TIBCO BusinessConnect™ Concepts*, "TIBCO BusinessConnect Group Management."

Adding a Group

To add user groups in TIBCO BusinessConnect, perform the following steps:

1. Expand **BusinessConnect > User Management > Groups**.
No pre-assigned groups are available for this installation.
2. In the User Management: Groups dialog click **Add**.

Figure 30: Setting Group Name



3. In the Set Group Name dialog, enter the new group name and click **OK**.
The New Group window is displayed with three tabs: General, Members, and Permissions.

General Tab for Groups

The General tab is used to edit information such as group name or description.

Figure 31: New Group Dialog

The screenshot shows a dialog box titled "New Group: readOnly" with a help icon (?) in the top right corner. At the top, there are three buttons: "Save", "Cancel", and "Apply". Below these are three tabs: "General", "Members", and "Permissions". The "General" tab is selected and highlighted. Inside the "General" tab, there is a section labeled "General" containing two input fields: "Group Name" with the text "readOnly" and "Description" which is empty. The "Description" field has a small blue arrow icon on its right side.

1. Enter the name in the window Group Name.
2. Enter the group description (optional)
3. Click **Apply** to continue editing other two tabs, or **Save** if you have finished with editing this group.

Members Tab for Groups

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

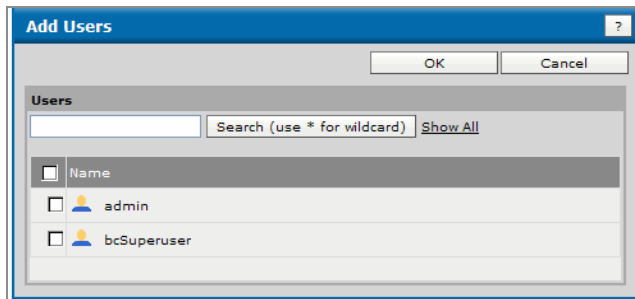
Figure 32: Members Tab for Groups

The screenshot shows a dialog box titled "Edit Group: readOnly" with a help icon (?) in the top right corner. At the top, there are three buttons: "Save", "Cancel", and "Apply". Below these are three tabs: "General", "Members", and "Permissions". The "Members" tab is selected and highlighted. Inside the "Members" tab, there is a section labeled "Members" containing two buttons: "Remove" and "Add Users". Below these buttons is a table with two columns: "User" and "Category". The table is currently empty.

Using this tab, you actually only add or remove associations between users and their groups; this option does not create or remove users from the TIBCO BusinessConnect application.

1. Click **Add Users**.

Figure 33: Adding Users to Groups



Check the boxes next to the users you want to join this group. These users have been previously generated, as described in [Using TIBCO Administrator User Management](#).

Permissions Tab for Groups

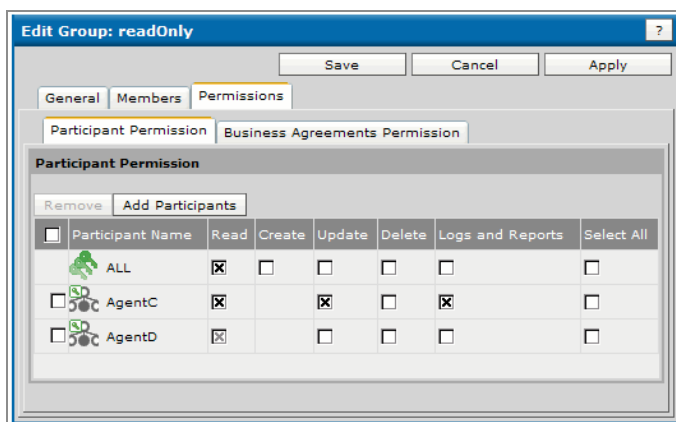
The access rights defined in groups can be further restricted by participant and business agreement.

When you select this tab, the two subtabs appear: Participant Permission and Business Agreements Permission.

Participant Permissions Tab for Groups

In the Participant Permissions subtab, you can add or remove participants (host or trading partners), as well as change the permission that they have in the group.

Figure 34: Participants Permissions for Groups

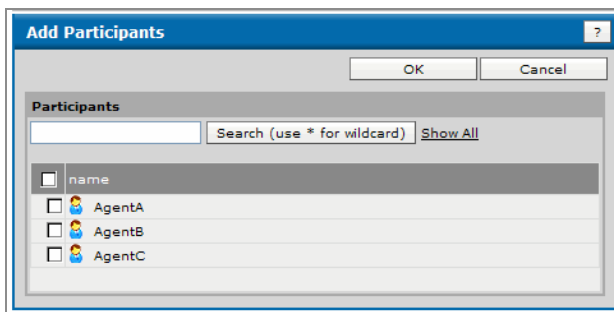


Add Participants

1. Click **Add Participants**.

The list of trading partners configured for the current TIBCO BusinessConnect installation is displayed.

Figure 35: Adding Participants

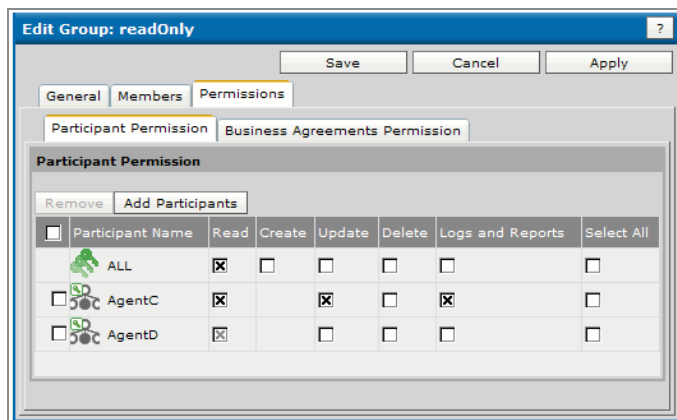


2. Check the checkboxes next to the participants you want to add to this group.
3. Click **OK**.

Change Permissions

The list of participants is displayed, with the user access rights that these participants have been granted.

Figure 36: Participant Permissions for Groups



1. Select or unselect checkboxes for any permissions that you want to fine tune: Read, Create, Update, Delete, Logs and Reports, or Select All.
For an overview of user access rights, see *TIBCO BusinessConnect™ Concepts*,

"Participants Access Rights."

You can only reduce the level of access rights that a specific participant within the group will be granted. When you select the checkbox **Select All** in the category **ALL**, all permissions will be checked.

Remove Participants

1. Select the checkbox next to any participant name.
2. Click **Remove**.

The participant is removed.



Note

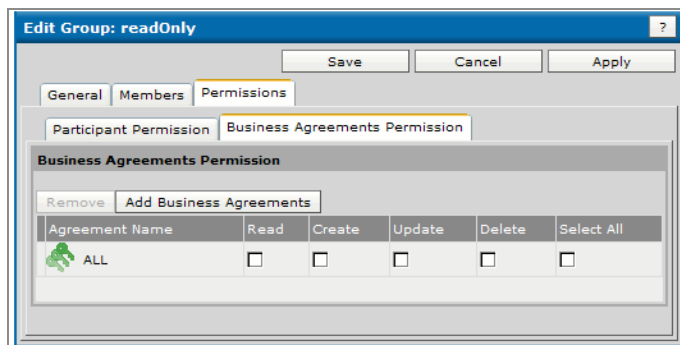
The participant is not removed from the installation; it only means that the user you are editing has no configured permissions within this group.

Business Agreements Permission Tab for Groups

Groups can be assigned access rights to all Business Agreements or to particular Business Agreements.

This tab allows you to add and/or remove business agreements, as well as to change access rights that the specific group has regarding these agreements. It shows the list of business agreements to which the group has access rights, as well as the level of these access rights: Read, Create, Update, Delete, and Select All.

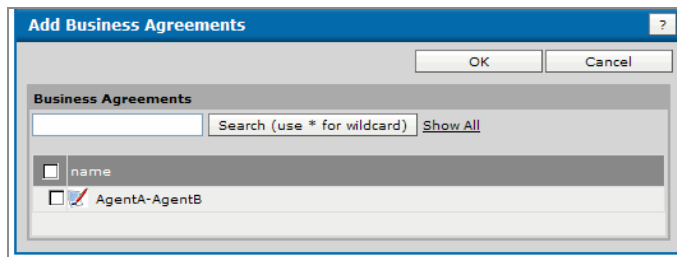
Figure 37: Business Agreements Permissions for Groups



Add Business Agreements

1. Click **Add Business Agreements**.
2. The list of configured business agreements for the current TIBCO BusinessConnect installation is displayed.

Figure 38:
Adding BusinessAgreements for Groups

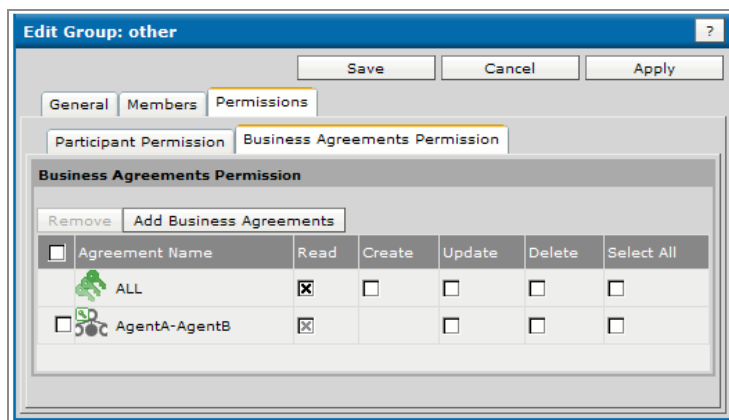


3. Check the checkboxes next to the business agreements for which you want to change the group's access rights.
4. Click **OK**.

Change Permissions

The list of business agreements is displayed, with the group access rights for dealing with these agreements.

Figure 39: Business Agreements Permissions for Groups



1. Select or unselect check boxes for any agreements that you want to fine tune: Read, Create, Update, Delete, or Select All.
For an overview of user access rights, see *TIBCO BusinessConnect™ Concepts*,

"Business Agreements Access Rights."

You can only reduce the level of access rights that the specific group has in dealing with the selected business agreements. When you select the checkbox Select All in the category ALL, all permissions will be checked.

Remove Business Agreements

1. Select the checkbox next to any business agreement.
2. Click **Remove**.
3. The business agreement is removed.



Note

The business agreement is not removed from the installation; it only means that the group you are editing has no configured permissions to deal with this business agreement.

Log Viewer

This section describes the types of logs provided by TIBCO BusinessConnect, how to search and view logs, and operations that you can perform on log entries.

Overview

The log viewer allows you to search and view information from the following system logs, which is collected during transaction processing:

Audit Logs

Audit logs are used to store information about the messages and documents processed by TIBCO BusinessConnect.

You can use an audit log to follow the processing states of inbound or outbound documents. Some of the types of information stored in the audit log include:

- Sent and received documents
- Document originator
- Trading partner name
- Processing status
- Validation errors

Non-Repudiation Logs

Non-repudiation logs are used to provide proof of the delivery of messages. Non-repudiation depends on authentication using digital signatures. Incoming messages which have been digitally signed are authenticated and stored in the non-repudiation database. Outbound messages that have been digitally signed are also stored in the database. The non-repudiation logs are intended for long-term storage. Only the minimum information

necessary to prove the delivery of messages is stored. Therefore only a subset of the information available in the audit log can be viewed in the non-repudiation log.

For more information on non-repudiation, see *TIBCO BusinessConnect™ Concepts*, "Non-Repudiation."

Resend Logs

Resend logs provide two views into an audit log:

- **Resendable transactions** Allows you to resend a transaction.
- **Resend history** Allows you to view messages that have been resent.

For information on resend logs, see [Resending Transactions](#).

Performing Log Searches

In each log you can search for specific log entries using either the basic or advanced query interface, and you can save and reuse queries.

The basic search allows you to search all logs based on the following criteria:

- Protocol
- Status
- Date Range Criteria

The advanced query interface allows you to search on protocol-specific criteria



Note

When doing searches, keep in mind that the character “*” is not considered to work as a wild card, but it represents a part of a name instead.

Figure 40: Log Viewer

Plug-in	Protocol	Transactions Today	Transactions Last 7 days
BCRremote	BusinessConnect Remote Client Service		1 item(s)
	PartnerSelfService	0	0
EZComm	BusinessConnect EZComm Protocol		1 item(s)
	EZComm	0	0
GGS-MGMT	BusinessConnect Gateway Management		3 item(s)
	Gateway Service Instance	0	1
	Gateway Service Session	0	0
	Lost and Found	0	0

Setting Preferences

Preferences for All Protocols

The Preference dialogs allows you to maintain the log viewer settings that are specific to the current BusinessConnect installation and apply to all users of that installation.



Only Administrator User can access the **Preferences** function.

Note

To set the preferences applicable for all protocols, perform the following steps:

1. Expand **BusinessConnect > Log Viewer**.
2. Click **Preferences** when no protocols are selected.

The Preference options for the log viewer are explained in [Log Viewer Preferences: All Protocols](#).

Log Viewer Preferences: All Protocols

Field	Description
Show Protocols in List	<p>All enabled protocols will be listed.</p> <p>Select or unselect the check boxes next to the protocols that you want to show in the list as accessible from the main log viewer table. Only the selected protocols will be listed in the log viewer.</p> <p>These protocols or services are always visible on the screen:</p> <ul style="list-style-type: none"> • PartnerSelfService • Gateway Service Instances (see <i>BusinessConnect Gateway Server Administration</i> for more details) • Gateway Service Session (see <i>BusinessConnect Gateway Server Administration</i> for more details) • Lost and Found
Database Connections	<p>Select the default database connection for each of the log search types: Audit, Non-Repudiation, and Resend History.</p> <p>The chosen connection will be used as a default choice when opening the corresponding log viewer dialog.</p>
Show Start Time in Summary	<p>Select to show or hide the Start Time column in the Summary View applicable to the Audit, Resendable Transactions and Resend History. Note that Start Time is not applicable for the Non-Repudiation Log Viewer. The Message Queue Log Viewer will always display the Start and End Time columns.</p>
Date Range	<p>Select the Date Range basic search criterion from the list.</p>

Preferences for a Selected Protocol**Note**

The log viewer preferences will vary depending on the selected protocol.

To set the preferences for a specific protocol, perform the following steps:

1. Expand **BusinessConnect > Log Viewer**.
2. Select a protocol.
3. Click **Preference**.

The preference options for the selected Protocol, in this case TIBCO BusinessConnect Services Plug-in, are explained in table [Log Viewer Preferences: Selected Protocol TIBCO BusinessConnect Services Plug-in](#).

Log Viewer Preferences: Selected Protocol TIBCO BusinessConnect Services Plug-in

Field	Description
Protocol	Name of the selected protocol.
Show Protocol in List	Select or unselect the checkbox to display the selected protocol in the list.
Defaults	
Host	Select the default host name from the list.
Status	Select the protocol status that will be used to display the logs: CANCELED, COMPLETED, ERROR, ERROR SECURITY, PENDING, RECEIPT PENDING, ANY
Resendable States	Choose the resendable status from the list: <ul style="list-style-type: none"> • RECEIVED_FROM_PP • SEND_TO_PP (This option is available only for the protocols that support resendable transactions, such as TIBCO BusinessConnect Services Plug-in)
Group By Column	
Audit	Columns available for grouping the audit logs depend on the protocol. For example, for the TIBCO BusinessConnect Services Plug-in, these groups are: None, Date group, Host, Trading Partner,

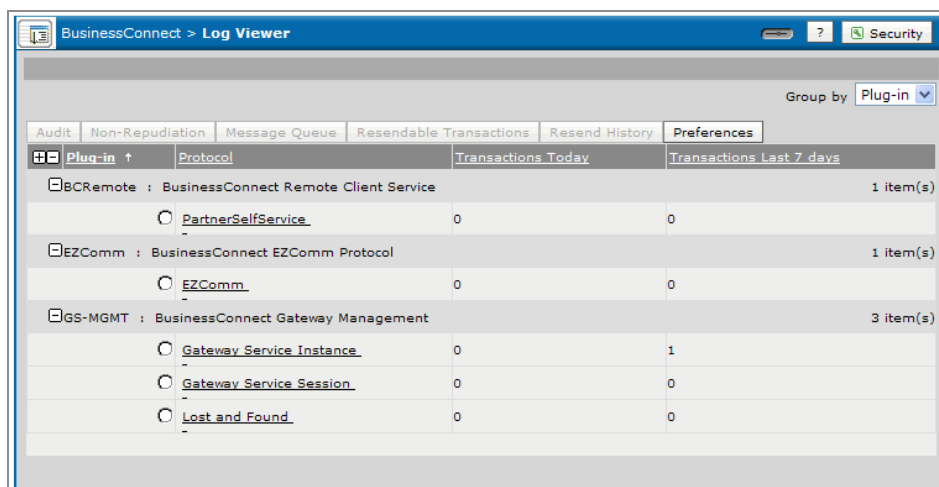
Field	Description
	Operation ID, Document ID, Host Initiates, User TranID, and Transaction Type.
Non-Repudiation	<p>Columns available for grouping the non-repudiation logs depend on the protocol.</p> <p>For example, for the TIBCO BusinessConnect Services Plug-in, these groups are: None, Date group, Trading Partner, Operation ID, Document ID, User TranID, and Transaction Type.</p>
Resend	<p>Columns available for grouping the resendable transactions depend on the protocol.</p> <p>For example, for the TIBCO BusinessConnect Services Plug-in, these groups are: None, Date group, Trading Partner, Operation ID, Document ID, User TranID, Transaction Type, and Host Initiates.</p>

Performing a Log Search

To perform a log search:

1. Expand **BusinessConnect > Log Viewer**.

Figure 41: Log Viewer II



There are five different log searches you can perform: Audit Logs, Non Repudiation Logs, Message Queue, Resendable Transactions, and Resend History.

2. Click **Log Viewer** for the type of log you want to search, such as **Audit**.

The available search options will be displayed, while the ones that are not available will be grayed out:

3. Configure the search using the information from [Configuring Log Search](#).

Configuring Log Search

Field	Description
Filters	
Status	<p>Find log entries for transactions that terminated with a specific status.</p> <p>Options depend on the selected protocol. For example, for TIBCO BusinessConnect Services Plug-in, the options are Select the protocol status that will be used to display the logs: CANCELED, COMPLETED, ERROR, ERROR SECURITY, PENDING, RECEIPT PENDING, and ANY.</p> <p>The default status that is displayed in the dialog is the one that was configured in the field Status for the corresponding protocol preference.</p>
Connection	<p>The database that you connect to.</p> <p>Allows you to switch among multiple Audit Log databases in this list.</p>
Date Range	<p>The Custom option allows you to specify a range with a specific Start and End Date Time.</p> <p>The option is predefined to allow you to specify a range with as follows: One Day, One Week, One Month and One Year.</p>
Advanced	
Add	<p>Add advanced filters to define the criteria such as: AS2 Message ID, Gateway Instance Information, Host, Trading Partner, Operation ID, Document ID, Host Initiates, Transaction, User TranID, and Transaction Type.</p>

Field	Description
	<p>Each of these variables can be searched by choosing one of the following options from the list: is, contains, is not, is not like.</p> <p>While you can perform a search without adding a query, it will save you time in the future if you set up queries. Keep in mind that a query can be used again <i>only</i> if it is saved under a specific name; if you fill all required query details and click Save without providing a query name, such query will be performed as an advanced query but cannot be re-used.</p> <p>Once the filter is specified, select it in the list for executing the search, or click Edit to change the filter criteria.</p> <p>Note: Fields are protocol and log type specific.</p>

Summary Results

Use this section to:

- Search through existing results
- Group the results on the criteria as they are added using the **Add** function.

Group by	Use this list to group the search results by the following criteria: Date group, Host, Trading Partner, Operation ID, Document ID, Host Initiates, User TranID, Transaction Type.
-----------------	---

4. Click **Search**. Only the log entries that meet all of the criteria you specify will be returned.
5. Save the advanced filters as a query by specifying a name for the query in the editing dialog and click **OK**.

Viewing Search Results

Several views are accessible from the search results.

Summary View

Searches in any log will return the results in a table. The table columns are protocol specific and each table entry represents a transaction.

Transaction Details View

To view the details of a transaction, click the active document icon in the left-most column of a transaction in the Summary View. The Log Viewer first displays the general information for this entry, then a table with available information for each state in that transaction. The table columns are protocol specific. Only certain logs support the transaction details view. To move between various transactions, use **Back** and **Next**.

State Details View

To view the details of a state, click the active document icon in the left-most column of an entry in the Transaction Details View. Only certain logs support the state details view. By selecting the Change View link, you can view all transaction detail states in a table form.

Figure 42: State Details View

BusinessConnect > Log Viewer
Audit Logs > E2Comm > Connection > bcddb

Transaction Details

Filters > Status: ANY > Dec-08-2015 15:44 ~ Dec-09-2015 15:44

Summary: 3 of 16

Outbound AS2 Message ID	
Inbound AS2 Message ID	
Gateway Instance Information	
Host	Company1
Trading Partner	Company2
Operation ID	BC/1.0/Notify
Document ID	eK9ozfaEU9A7SUc-T0SKfy7kAgQ
Host Initiates	true
User TranID	eK9ozfaEU9A7SUc-T0SKfy7kAgQ
Transaction Type	EZComm-Notify

Back Next

States

Time Stamp	Status	State	Description
Dec-09-2015 09:27:28 AM	PENDING	RECEIVED_FROM_PP	Received request from private process over RV transport
Dec-09-2015 09:27:30 AM	PENDING	PACKAGE_MSG	Email message packaged for Company2. The message was not signed, not encrypted and not compressed.
Dec-09-2015 09:27:30 AM	PENDING	REQUEST_TO_TP	Sending Request to trading partner.
Dec-09-2015 09:27:31 AM	PENDING	ACK_FROM_TP	Received acknowledgement from Trading Partner: Status: Email has been sent.
Dec-09-2015 09:27:31 AM	COMPLETED	SEND_TO_PP	Acknowledgement sent to private process.

change view

To move between various states, use **Back** and **Next**.

Enable Detailed View

You can see the detailed log view by selecting the **Change View** hyperlink.

From the state details view you can save the message associated with the processing state entry to a file. If there is a message associated with the processing state entry, the State Detail panel will also display a character count greater than 0 next to **Save Message**; for example, [290 bytes].

Save Message

Click **Save Message** to save the message associated with this processing state to a file on your local file system.

Resend

Click **Resend** to resend the private process message associated with this transaction, if available. Depending on the state, the private process message is resent either to the TIBCO BusinessConnect server or to the back office application for reprocessing.

Canceling Transactions

**Note**

This feature is protocol specific and is not supported for all protocols.

TIBCO BusinessConnect Services Plug-in does not support the canceling transactions feature.

In the audit log you can cancel a transaction if the transaction has not completed (that is, the transaction status is not COMPLETED).

To cancel a transaction, perform the following steps:

1. Ensure that the TIBCO BusinessConnect engine is running.
2. In the audit log Summary View, check the checkbox in the left-most column of the transaction entry. If there is no checkbox in the left-most column of the transaction entry, the transaction is not in a state that is cancelable.
3. Click **Cancel Transaction**.

When you click Cancel Transaction, the transaction is terminated and the transaction status is logged as CANCELED with a state of CANCELED.

**Note**

The TIBCO BusinessConnect engine checks for the cancel action only at certain points during the processing of a transaction. If the TIBCO BusinessConnect engine requires time to process the transaction between those points, it might not act on the cancel message immediately and you will observe a delay between clicking **Cancel Transaction** and the change in the transaction status.

Also, it is not guaranteed that the transaction *will be canceled* after **Cancel Transaction** is clicked since the transaction could be completed before TIBCO BusinessConnect could cancel the transaction.

Saving and Reusing Queries

In the context of the BusinessConnect log viewer, a *search* is a one-time occurrence and a *query* is a search that one has saved for reuse. Upon saving a search, it becomes a named query and is available from the Queries list.

Saving a Query

To save a query, perform these steps:

1. Click **Add** to define the search criteria under the Advanced Filters section.
2. Define the search criteria in the Advance Filers dialog.
3. Specify a name for the optional field **Save As Query**.
4. Click **Save**.

**Note**

The saved query does not include the settings for the database connection and the date range criteria.

Reusing a Query

To reuse a query, perform these steps:

1. Select the desired query in the Queries list. The Advanced Filters are restored from the selected saved query.
2. Click **Search**.

Resending Transactions

The resend log provides two views into the audit log:

- **Resendable Transactions** Search for resendable and resend transactions.
- **Resend History** View transactions that have been resent.

Resendable Transactions

Resendable transactions can be re-transmitted from TIBCO BusinessConnect to a trading partner or from TIBCO BusinessConnect to a private process. Each protocol defines the set of resendable states, which you can determine by looking at the State list on the Resendable Transactions tab.

**Note**

The entire AESchema is stored in the fields REQUEST_FROM_PP and SEND_TO_PP fields in the audit log, since this is required for the resend.

**Note**

Only transactions for the current transport will be listed under resendable transactions: if JMS is the current transport, only JMS transactions will be listed.

When resending messages to the private process, such as the messages RESPONDER.REQUEST and INITIATOR.RESPONSE that were previously smart-routed, the smart route ID will be re-evaluated upon the re-transmission. This allows a different back office process to handle the re-transmission of the message to the private process.

Enabling Transaction Resend

To enable the resend feature, you must enable the inclusion of message contents in log entries. See *TIBCO BusinessConnect™ Installation and Configuration*, "Audit, Non-Repudiation and Runtime Database Configuration."

Resending a Transaction

To resend a transaction, perform following steps:

1. Expand **BusinessConnect > Log Viewer > Resendable Transactions** for the selected protocol.
2. Configure the options explained in [Performing a Log Search](#).
3. Select the resendable state in the **State** list.
4. Click **Search** and select the checkbox of the transaction to resend.
5. Resending a message could be identical to making a new message request, depending on the state that was chosen, and can result in multiple transactions of the same request.
6. Click **Resend**. For outbound documents, clicking Resend retransmits the document to the trading partner. For inbound documents, clicking Resend will resend the message to the private process.



Warning

Use with caution. If the resend request is activated before the current transaction completes or returns an error, the outcome is beyond control of the protocol.

Viewing Resend History

To view the resend history of a transaction:

1. Expand **BusinessConnect > Log Viewer > Resend History**.
2. Configure the options as explained in [Performing a Log Search](#).
3. Click **Search**.
4. Any resent transactions satisfying the options configured in [Configure the options as explained in Performing a Log Search](#) are listed.

5. If you resend a transaction multiple times you can click the timestamp of the transaction in the Search results to see a list of all child transactions of the original transaction.
6. View the administrator who did the resend for a particular entry by looking at Resend User Name. This feature is available for all protocols.

Figure 43: Resend History Details

Date Group	Time Stamp (PDT)	Host	Trading Partner	Operation ID	Document ID	Host Initiates	User TranID	Transaction Type	Resend User Name
TWO WEEKS AGO 1 item(s)									
	Sep-16-2011 02:49:34 PM	nabooJUNO	BC/1.0/Notify	P90508-B7Z866-0007KU-false B2NFLR-0305				EZComm-Notify	admin

Reporting

This section explains how to generate various reports for the TIBCO BusinessConnect installation.

Overview

TIBCO BusinessConnect generates data reports for inbound transactions per protocol and outbound transactions per protocol on audit log data:

**Note**

Audit log reports cannot be generated for the protocol TIBCO BusinessConnect Remote.

Reports are in the form of data values representing the number of transactions that BusinessConnect has processed per day, per protocol.

Generating Reports

To generate a report, perform these steps:

1. Expand **BusinessConnect > Reporting**.
2. Click the link associated with the type of data report that you want to generate:
 - [Inbound Transaction Per Protocol](#)
 - [Outbound Transaction Per Protocol](#)

Both data reports (for Inbound and for Outbound transaction per protocol) use the same dialog to select criteria for the report generation.

**Note**

When exporting Inbound or Outbound transactions, the Resend transaction data is also exported as a part of reporting. This is true for all TIBCO BusinessConnect protocols.

Inbound Transaction Per Protocol

To obtain the report, select parameters as explained in [Data Reports](#).

Data Reports

Field	Enter or Select Data
Protocol	Select any of the installed protocols for which the report is done. The report will only include the transactions that used the selected protocols.
Date Range Criteria	You can use Custom Date Range to specify the range with a specific start date and time and a specific end date and time. Predefined Date Range allows you to specify the range using the additional field Previous.
Previous	Field Previous allows you to specify the Predefined Date Range.
Status	<p>Click Add to select the transaction status for which the report is done:</p> <p>The options are: CANCELED, COMPLETED, ERROR, ERROR SECURITY, PENDING, RECEIPT PENDING.</p> <p>You can also remove any of the status choices by clicking Delete.</p>
Display Fields	<p>Click Add to specify which fields will appear in the generated report.</p> <p>The options are: Document ID, Host, Host Initiates, Operation ID, Start Time, Status, Time Stamp, Trading Partner, Transaction Type, User TranID.</p>

- Once the query is defined, click **Execute Query** to generate report.
- To save the defined query, click **Save Current Query**.
- To export the report, click **Export CSV Report**.
- When the query is defined, click **Generate Report**.

Outbound Transaction Per Protocol

To obtain the report, select parameters as explained in [Data Reports](#).

External Reporting

You can also build the reports externally by using BusinessConnect data. This can include both the audit data and the configuration data. The configuration data that is stored in opaque BLOB columns are denormalized through an external reporting poller. This poller runs inside the interior server engine.

To configure this poller, navigate to System Settings > External Reporting > Activated Protocol Plug-ins and Properties > BC in the administrator UI.

For more details about database schema, see TIBCO BusinessConnect™ Interior Server Administration, Database Schema Definition.

Email Transport

This section describes how to use Email transport for document exchange.

Email Overview

TIBCO BusinessConnect provides the ability to communicate with trading partners using email.

The TIBCO BusinessConnect Email transport can be used to send or receive messages from email clients.

The TIBCO BusinessConnect 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 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.



Note

When an inbound or outbound message arrives but the protocol cannot be determined, the message is written to the audit log under the special protocol name `LostandFound`, which is a substitute name for an unidentified protocol.

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 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 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 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 protocol to verify whether it supports sending attachments with the Email transport.

Content Disposition Filename

Some TIBCO BusinessConnect 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 Email transport. The filename can be specified for the Content Disposition header associated with the main document and/or any attachments.

The TIBCO BusinessConnect 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 Guide of the respective TIBCO BusinessConnect 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 does not support receipts from Microsoft Outlook email clients. This could happen when TIBCO BusinessConnect 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, 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.

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

Identifying the Sender and Receiver

TIBCO BusinessConnect 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 the **BusinessConnect > Participants > Participant_Name > Protocols > Protocol_Name > 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 for Email

Configuring the POP3 Server Polling Service

TIBCO BusinessConnect allows you to configure up to three POP3 Email servers, so that email messages from all these servers can be received. All POP3 servers are configured in the same way as follows:

1. In TIBCO Administrator, expand **BusinessConnect > System Settings > Inbound Mail POP3 Servers**.
2. Configure the fields using the information in [Inbound Mail POP3 Servers](#).
3. Redeploy BusinessConnect.

Configuring an SMTP Server for a Host

To enable communication for a host through an SMTP server, see

- [Adding a Proxy for a Host](#)
- [Selecting the Default Proxy for a Host](#)

Configuring an SMTP Server for a Partner

To enable use of an SMTP server for a partner, see

- [Proxy Settings Tab for Partners](#).

Setting Up Email for a Trading Host

Selecting Email for the Trading Host

1. In TIBCO Administrator, expand **BusinessConnect > Business Agreements**.
2. Click a business agreement link.
3. Click the protocol link.
4. In the Edit Protocol Binding dialog, click the **Transports** tab.
5. Check the **Email** checkbox in the Allowed Inbound Transports area.
6. Click **Save** twice.

Setting the Host's Email Address for a Protocol

1. In TIBCO Administrator, expand **BusinessConnect > Participants**.
2. Click a host participant link.
3. Click the **Protocols** tab.
4. Click a protocol link.
5. Add the host's email address to the Valid Email Address List field.

**Note**

Email addresses entered in the Valid Email Address List box must be separated either by a semicolon or by a comma.

6. Click **Save** twice.

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 a specific business agreement using the Edit Protocol Binding dialog. See [Business Agreement: Transports Tab](#) for more details.

Configuring Email for a Trading Partner

1. In TIBCO Administrator, expand **BusinessConnect > Participants**.
2. Click a partner participant link.
3. Click the **Protocols** tab.
4. Click the protocol link.
The General tab is selected by default.
5. Click the **Transports** tab.
6. Click **Add**.
7. Enter the transport name.
8. Select **Email** from the list.

Select or enter data as described in the following table:

Email Transport Settings

Field	Description
Transport Name	An identifier for these transport settings.
URL (required)	(Required) The URL for the trading partner is: mailto: e-mailID@domain.com.
Subject	<p>A short string identifying the topic of the email message; for example, "Purchase Order from ABC Company".</p> <p>For more information on the Subject Header field for MIME messages, refer to RFC C2822, Internet Message Format.</p>
Base64	Base64 encode plain outbound email messages. Plain messages are those

Field	Description
Encode Clear Text Messages	messages which are not signed, not encrypted, and not compressed.
Non Repudiation of Receipt	<p>Enable logging of receipts in the non-repudiation table.</p> <p>If you check this option, you must also check the Sign checkbox 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.</p> <p>For more information, see <i>TIBCO BusinessConnect™ Concepts</i>, "Non-Repudiation."</p>
Sign	<p>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.</p> <p>TIBCO BusinessConnect can <i>process</i> messages which contain message digests computed using the SHA1 hash algorithm. However, TIBCO BusinessConnect will compute its message digests using the digest algorithm setting specified for the business agreement in the Document Security tab.</p> <p>Whether an outbound receipt is signed or not is controlled by the setup in the requesting partner's Request Receipt list.</p>
Signature Scheme	<p>Select the desired signature algorithm from the list of options: RSA, RSA-PSS.</p> <p>The default option is RSA.</p> <p>Note: Ensure to enable the Sign checkbox to apply the signature scheme.</p>
Encrypt	<p>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 will be used to encrypt the email messages.</p>

Field	Description
Encryption Scheme	<p>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.</p> <p>The default option is RSA-PKCS1-v1_5.</p> <p>Note: Ensure to enable the Encrypt checkbox to apply the encryption scheme.</p>
Compress	<p>If selected, each outgoing message is compressed in GZIP file format.</p> <p>File compression is always performed before message signing.</p>
Send Data as Attachment	<p>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.</p>
Use Attachment Filename as Subject	<p>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.</p> <p>Note: This feature is introduced for TIBCO BusinessConnect EDI Protocol powered by Instream, EDIFACT Protocol, and cannot be used by other protocols.</p> <p>If both the Subject and Use Attachment Filename as Subject check boxes are selected, the Use Attachment Filename as Subject checkbox takes precedence.</p>
Request Receipt	<p>The type of receipt returned from the trading partner. The following options are available:</p> <ul style="list-style-type: none"> • 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

Field	Description
	<p>partner for each message.</p> <p>If you choose to request a receipt of any kind, you must have a valid email address set for the trading host.</p> <p>If you checked Non Repudiation of Receipt, you should select Signed. For computing the message digest, BusinessConnect uses the digest algorithm that was configured for the business agreement in the Document Security screen.</p> <p>For more information on receipts, see Message Disposition Notification Receipts.</p>
Receipt Timeout (minutes)	<p>The amount of time within which a receipt should be returned by the trading partner.</p> <p>Example: 5</p>

9. Click **Save** two times.

Setting the Partner's Email Address for a Protocol

1. In TIBCO Administrator, expand **BusinessConnect > Participants**.
2. Click the partner participant link.
3. Click the **Protocols** tab.
4. Click a protocol link.
5. Add the partner's email address to the Valid Email Address List field.



Note

Email addresses entered in the Valid Email Address List box must be separated either by a semicolon or by a comma.

6. Click **Save** two times.

Configuring Email for a Business Agreement

To configure the Email transport for a business agreement, see [Business Agreement: Transports Tab](#).

FTP and FTPS Transports

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

FTP Transport Overview

TIBCO BusinessConnect 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 happen securely so that the integrity of the transmission is not compromised. To accommodate this, TIBCO BusinessConnect provides different ways of sending files through FTP transport.

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

- 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 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.

**Note**

When an inbound or outbound message arrives but the protocol cannot be determined, the message is written to the audit log under the special protocol name `LostandFound`, which is a substitute name for an unidentified protocol.

Explicit and Implicit FTPS Connections

TIBCO BusinessConnect supports FTPS in explicit mode, which means that the BusinessConnect 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 specificationRFC2228). 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 Uses
TpName	
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)

User Provides	TIBCO BusinessConnect Uses
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
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-2013-Apr-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, such as *BC_HOME\tmp\protocol\tpName*.

The files in the temporary directory are either moved to a permanent storage directory or are removed from the local file system after TIBCO BusinessConnect processes the file contents.

The permanent storage location is determined by the value set in the Shared Temporary Location field, which you can locate using TIBCO Administrator as follows:

1. Expand **Application Management > BusinessConnect > Configuration**.
2. Click the **BusinessConnect** link in the right panel.
3. The Shared Temporary Location field is located in the Advanced area at the bottom of the Public Process Configuration tab.

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 TIBCO BusinessConnect, 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.

For information about how FTP interacts with EDI-Gateway, see *TIBCO BusinessConnect™ EDI Protocol powered by Instream Gateway Configuration*.

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

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

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. In TIBCO Administrator, expand **BusinessConnect > System Settings > Inbound Public Transport Types**.
2. Check the **FTP** or **FTPS** check box.
3. Click **Enable**.

The enabled protocol(s) will now appear with a red checkmark in the Enabled column.

Selecting and Configuring FTP/S Inbound

1. In TIBCO Administrator, expand **BusinessConnect > Business Agreements**.
2. Click the business agreement link.
3. Click a protocol link.
4. In the Edit Protocol Binding dialog, click the **Transports** tab.
5. Check the **FTP** or **FTPS** checkbox in the Allowed Inbound Transports area.
6. Click **Edit Settings** next to the selected transport.
7. Configure the options listed in the following table:

Inbound FTP/S Settings

Field	Description
URL	<p>The URL for the directory on the FTP server, which is <code>ftp://host_name:port/path_name/</code>, where</p> <ul style="list-style-type: none"> <i>host_name</i> is the name of the machine (server) where the FTP server is running <i>port</i> is the port on the machine to which the FTP server is listening to <i>path_name</i> 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 username for authenticating the host on the partner FTPS service.
Password	The password for authenticating the host on the partner FTPS service.
File Processing	<p>The mechanism for deciding which files to retrieve. There are two choices:</p> <ul style="list-style-type: none"> 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 (*), BusinessConnect searches for all files in the specified FTP directory. To prevent the retrieval of files that have already been retrieved, there are two options:

Field	Description
	<ul style="list-style-type: none"> • 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. <p>See Supported File Mask Options for more information.</p> <p>See <i>TIBCO BusinessConnect™ EDI Protocol powered by Instream User Guide</i> for information on pre-defined and user-defined options for input file masks for EDI.</p>
Include Full File Path	<p>The complete file path is enabled to distinguish this file from other files.</p> <p>If the complete file path is required, select this checkbox to send the getting request by FTP/FTPS poller file full path to the original file field of the Business Connect ReceiveRequest palette.</p>
Scripts	Specify an FTP script. See Scripts for information on how to write scripts, and File Specification Dialog for information on how to upload a script.
Scripts Engine	<p>The scripts engine that you want to use to execute custom scripts.</p> <p>You can select one of the items from the list:</p> <ul style="list-style-type: none"> • FESI • Nashorn <p>Note: The FESI EcmaScript engine originally supported by TIBCO BusinessConnect is out of support by the vendor. It is good practice to use the Nashorn script engine as a substitute because the Nashorn script engine is roughly compatible with the FESI EcmaScript engine.</p>
Secure Transport Mode	<p>(FTPS only) The secure protocol employed in the transport layer.</p> <p>You can select one of the items from the list:</p> <ul style="list-style-type: none"> • SSL_ONLY • SSL • TLS

Field	Description
	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.
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)	<p>This field defines how often polling occurs.</p> <p>By default, the frequency is 5 minutes (300 seconds). The default value is set in the <code>bc.ftpget.pollingInterval</code> property, which you can access by selecting System Settings > Activated Protocol Plug-ins and Properties > BC > ftpget.</p> <p>Since the system-level property dictates the minimum frequency for <code>ftpget</code>, the value assigned in the Frequency field will be effective only if it is greater than the system level property. If the value assigned in the Frequency field is smaller than the system-level property, it will have no effect.</p> <p>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.</p>
Delete File	<p>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.</p> <p>Note: This option does not work for all FTP servers.</p>
Require PGP Processing	Select this checkbox 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.

Field	Description
	<p>This checkbox 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.</p> <p>If PGP unpackaging is required, the PGP keys used for the unpackaging are configured in the Inbound Document Exchange portion of the Document Security tab in a Business Agreement.</p> <p>If unselected, the message is sent to back office as pass through, even if the message is PGP packaged.</p>
PGP Policy	<p>The PGP policy only takes effect if the Require PGP Processing checkbox is selected. Four policies are available:</p> <ul style="list-style-type: none"> • 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.

8. Click **Save** three times.

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. Select this transport for the partner in a specific business agreement using the Edit Protocol Binding dialog. See [Business Agreement: Transports Tab](#) for more details.

Configuring FTP/S Outbound

1. In TIBCO Administrator, expand **BusinessConnect > Participants**.
2. Click a partner participant link.
3. Click the **Protocols** tab.
4. Click the protocol link.
5. In the Edit Enabled Protocol, click the **Transports** tab.
6. Click **Add**.
7. Enter the transport name.
8. Select **FTP/S** from the Transport **Type** list.
9. Click **OK**.

The New FTP/S Transport dialog is displayed.

This action adds the FTP/S item to the list in the Transport Defaults area, which can be selected for the business agreement in [Business Agreement: Transports Tab](#).

10. Configure the options listed in [Outbound FTP/S Settings](#).

Outbound FTP/S Settings

Field	Description
Transport Name	An identifier for these transport settings.
URL	<p>The URL for the directory on the FTP server, which is ftp://<i>host_name</i>:<i>port</i>/<i>path_name</i>/ where</p> <ul style="list-style-type: none">• <i>host_name</i> is the name of the machine where the FTP server is running• <i>port</i> is the port on the machine to which the FTP server is listening to

Field	Description
	<ul style="list-style-type: none"> <i>path_name</i> 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.
fetch from ssl server	<p>(FTPS only) Retrieve the public keys of FTPS servers using the FTPS Server Public Key Retriever. The servers are identified by the hostname and port number in the URL field of the given connection.</p> <p>After you click this link, TIBCO BusinessConnect tries to retrieve and present the currently effective FTPS public key used by the FTPS server. No keys will be added to the keystore unless you explicitly accept the presented key as trusted. The FTPS Server Public Key Retriever does not verify the origin of these keys.</p>
Data Transfer	The format for transferring files: ASCII or BINARY.
Username	The username for the trading partner's FTP server.
Password	The password for the trading partner's FTP server.
File Processing	<p>The mechanism for deciding which files to retrieve. There are two choices:</p> <ul style="list-style-type: none"> File Mask Choose to control file renaming. Enter a mask in the File Mask field. Script Choose for processing files. Specify a script in the Scripts field.
File Mask	<p>(FTPS only) The mask that controls file renaming. The value entered in the field works as a template for the actual file name.</p> <p>For more information, see Supported File Mask Options. For information on pre-defined and user-defined options for outbound file masks for EDI, see the File Masks section in <i>TIBCO BusinessConnect™ EDI Protocol powered by Instream User Guide</i> for information on pre-defined and user-defined options for outbound file masks for EDI.</p>

Field	Description
Output File Mask	<p>(FTP only) The mask that controls file renaming. The value entered in the field works as a template for the actual file name.</p> <p>For more information, see Supported File Mask Options. For information on pre-defined and user-defined options for outbound file masks for EDI, see the File Masks section in <i>TIBCO BusinessConnect™ EDI Protocol powered by Instream User Guide</i>.</p>
Scripts	Specify an FTP script. See Scripts for information on how to write scripts, and File Specification Dialog for information on how to upload a script.
Scripts Engine	<p>The scripts engine that you want to use to execute custom scripts.</p> <p>You can select one of the items from the list:</p> <ul style="list-style-type: none"> • FESI • Nashorn <p>Note: The FESI EcmaScript engine originally supported by TIBCO BusinessConnect is out of support by the vendor. It is good practice to use the Nashorn script engine as a substitute because the Nashorn script engine is roughly compatible with the FESI EcmaScript engine.</p>
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

Field	Description
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.
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.

11. Click **Save** three times.

Setting Up FTP Proxies

To use a proxy connection for FTP, you have to perform the following tasks:

Configure an Outbound Proxy for a Host

To add and select an outbound proxy for a host, see the following:

- [Adding a Proxy for a Host](#)
- [Selecting the Default Proxy for a Host](#)

Select the Default Proxy for a Trading Partner

To assign proxy settings for a trading partner, see the following:

- [Proxy Settings Tab for Partners](#)

SSHFTP Transport

This section describes how to use SSHFTP (SFTP) transport for document exchange.

SSHFTP Transport Overview

The SSHFTP (SFTP) transport, one of the public transports in TIBCO BusinessConnect, is used to establish secured SSH tunnels for the communication between TIBCO BusinessConnect 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).

Information on SSHFTP transport basics and its implementation for BusinessConnect is available in *TIBCO BusinessConnect Concepts*, "SSHFTP Implementation in TIBCO BusinessConnect."

**Note**

When an inbound or outbound message arrives but the protocol cannot be determined, the message is written to the audit log under the special protocol name `LostandFound`, which is a substitute name for an unidentified protocol.

Setting Up SSHFTP for a Trading Host

To set up SSHFTP inbound for a trading host, follow the instructions in the sections:

- [Enabling SSHFTP Inbound](#)
- [Selecting and Configuring SSHFTP Inbound](#)

Enabling SSHFTP Inbound

1. In TIBCO Administrator, expand **BusinessConnect > System Settings > Inbound Public Transport Types**.
2. Check the **SSHFTP** check box.
3. Click **Enable**.

The enabled protocol will now appear with a red checkmark in the Enabled column.

Selecting and Configuring SSHFTP Inbound

1. In TIBCO Administrator, expand **BusinessConnect > Business Agreements**.
2. Click the business agreement link.
3. Click a protocol link.
4. In the Edit Protocol Binding dialog, click the **Transports** tab.
5. Select the **SSHFTP** checkbox in the Allowed Inbound Transports area.
6. Click **Edit Settings** next to the selected transport.
7. Configure the options listed in the following table:

Inbound SSH Settings

Field	Description
URL	<p>The URL for the directory on the SSHFTP server, which is <code>sshftp://host_name:port/path_name/</code>, where</p> <ul style="list-style-type: none"> • <i>host_name</i> is the name of the machine (server) where the SSHFTP server is running • <i>port</i> is the port on the machine to which the SSHFTP server is listening to • <i>path_name</i> 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:

Field	Description
	<ul style="list-style-type: none"> • 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 Server SSH private key must be configured. • Public Key and Password BusinessConnect Server SSH private key and user account's password must be configured. <p>Note: ClientAuthenticationIdentity (for SSHFTP) under Business Agreement must have the TIBCO BusinessConnect Server SSH private key if either Public Key or Public Key and Password is selected.</p>
Username	The username for the trading partner's SSHFTP server. The username 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 Credential	<p>(Required) The SSH server's public key must be specified.</p> <p>Choose between the following:</p> <ul style="list-style-type: none"> • sshkey • None
fetch from ssh server	<p>Retrieve the public keys of SSH servers using the SSH Server Public Key Retriever. The servers are identified by the hostname and port number in the URL field of the given connection.</p> <p>Once you click this link, TIBCO BusinessConnect tries to retrieve and present the currently effective SSH public key used by the SSH server. No keys will be added to the keystore unless you explicitly accept the presented key as trusted. The SSH Server Public Key Retriever does not verify the origin of these keys.</p> <p>See SSH Server Public Key Retriever for more details.</p>

Field	Description
Preferred Cipher	<p>Choose among the following ciphers:</p> <ul style="list-style-type: none"> • AES128_CBC • AES192_CBC • AES256_CBC • AES128_CTR • AES192_CTR • AES256_CTR • ARCFOUR • ARCFOUR_128 • ARCFOUR_256 • AES_GCM_128 • AES_GCM_256 • BLOWFISH_CBC • CHACHA20_POLY1305 • TRIPLEDES_CBC • TRIPLEDES_CTR • ANY (accept the server's preference if available)
Preferred MAC	<p>Choose among these options:</p> <ul style="list-style-type: none"> • HMAC_SHA1 • HMAC_SHA1_ETM • HMAC_SHA1_96 • HMAC_MD5 • HMAC_MD5_ETM • HMAC_MD5_96

Field	Description
	<ul style="list-style-type: none"> • HMAC_SHA256 • HMAC_SHA256_ETM • HMAC_SHA256_96 • HMAC_SHA512 • HMAC_SHA512_ETM • HMAC_SHA512_96 • HMAC_RIPEMD160 • HMAC_RIPEMD160_ETM • ANY (accept the server's preference if available)
Preferred Compression	<p>Choose among these compression algorithms:</p> <ul style="list-style-type: none"> • ANY (accept the server's preference if available) • None (do not use compression even if the server offers this choice) • ZLIB • ZLIB@OPENSSH.COM
File Processing	<p>The mechanism for deciding which files to retrieve. There are two choices:</p> <ul style="list-style-type: none"> • 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	<p>Controls which files to retrieve. If you enter an asterisk (*), BusinessConnect searches for all files in the specified FTP directory.</p> <p>To prevent the retrieval of files that have already been retrieved, there are two options:</p> <ul style="list-style-type: none"> • Select the Delete File check box, which causes each file to be

Field	Description
	<p>deleted after it is retrieved, if this is allowed by the FTP server.</p> <ul style="list-style-type: none"> Specify a file mask that prevents the retrieval of the same files again. <p>See Supported File Mask Options for more information.</p> <p>See <i>TIBCO BusinessConnect™ EDI Protocol powered by Instream User Guide</i> for information on pre-defined and user-defined options for input file masks for EDI.</p>
Include Full File Path	<p>The complete file path is enabled to distinguish this file from other files.</p> <p>If the complete file path is required, select this checkbox to send the getting request by SSHFTP poller file full path to the original file field of the Business Connect ReceiveRequest palette.</p>
Scripts	<p>Specify an SSHFTP script. See Scripts for information on how to write scripts, and File Specification Dialog for information on how to upload a script.</p> <p>See the JavaDoc on the TIBCO BusinessConnect SSH API in <i>TIBCO BusinessConnect API Reference</i>.</p>
Scripts Engine	<p>The scripts engine that you want to use to execute custom scripts.</p> <p>You can select one of the items from the list:</p> <ul style="list-style-type: none"> FESI Nashorn <p>Note: The FESI EcmaScript engine originally supported by TIBCO BusinessConnect is out of support by the vendor. It is good practice to use the Nashorn script engine as a substitute because the Nashorn script engine is roughly compatible with the FESI EcmaScript engine.</p>
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

Field	Description
	FTP server occurs.
Frequency (seconds)	<p>This field defines how often polling occurs.</p> <p>By default, the frequency is 5 minutes (300 seconds).</p>
Delete File	<p>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.</p>
Require PGP Processing	<p>Select this checkbox 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.</p> <p>This checkbox 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.</p> <p>If PGP unpackaging is required, the PGP keys used for the unpackaging are configured in the Inbound Document Exchange portion of the Document Security tab in a Business Agreement.</p> <p>If unselected, the message is sent to back office as pass through, even if the message is PGP packaged.</p>
PGP Policy	<p>Select one item from this list.</p> <p>PGP policy only takes effect if the Require PGP Processing checkbox is selected. The following options are available in the list:</p> <ul style="list-style-type: none"> • 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;

Field	Description
	<ul style="list-style-type: none"> • 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	<p>Select this checkbox to enable the TCP No Delay feature.</p> <p>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.</p> <ul style="list-style-type: none"> • 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. <p>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.</p>

8. Click **Save** three times.

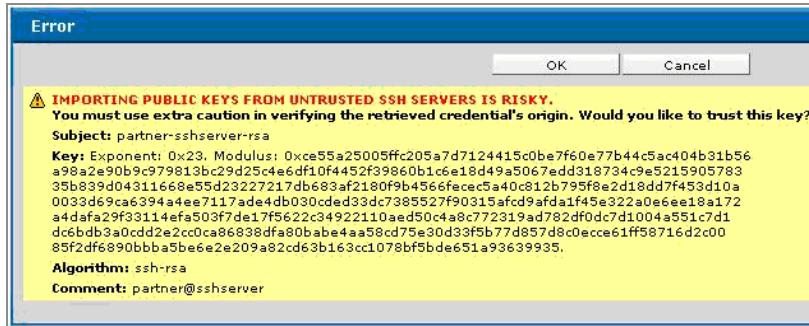
SSH Server Public Key Retriever

When presenting the SSH server's retrieved public key, TIBCO BusinessConnect always indicates one of these four basic situations:

- **No key is configured; present the currently used key on the SSH server**

TIBCO BusinessConnect currently has no public key configured on this transport instance and, along with warning of the risks of importing unverified public keys, it presents the properties of the public key (such as algorithm, exponent, modulus, and so on) for the administrator's acceptance.

Figure 44: No Key Configured

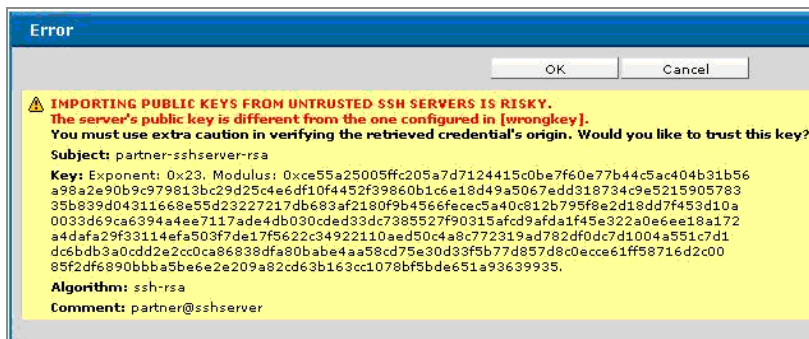


- A key is configured, but found different from the currently used key on the SSH server

TIBCO BusinessConnect currently has a public key configured on this transport instance, but that key is different from what the server uses.

Similarly to the first situation, along with warning of the risks of importing unverified public keys, it presents the properties of the public key (such as algorithm, exponent, modulus, and so on) for the administrator's acceptance.

Figure 45: Configured Key is Different

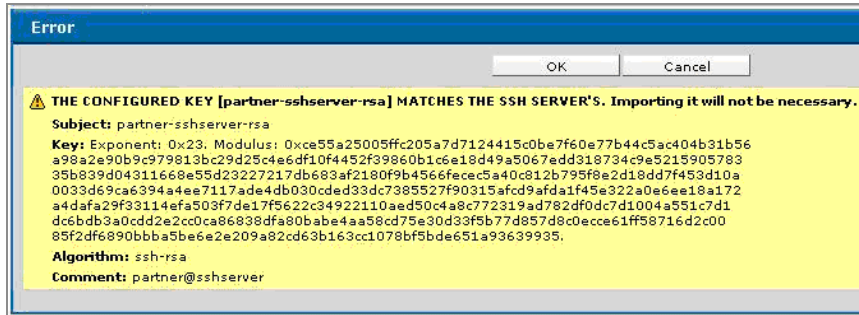


- A key is configured and it matches the one currently used by the SSH server

TIBCO BusinessConnect currently has a public key configured on this transport instance, and it has been found identical to the one used by the SSH server.

The GUI still presents the properties of the key, but the key cannot be added to the keystore (as it is unnecessary).

Figure 46: Configured and Retrieved Keys Match



- A transport error occurred during the key negotiation

These are the transport/application errors that might occur during key negotiation:

Figure 47: Server Is Not Available

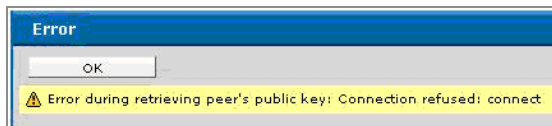


Figure 48: Server Did Not Respond to the SSH Query as Expected

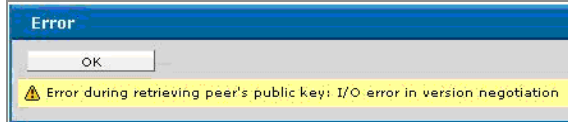
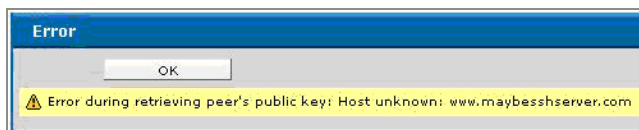


Figure 49: The Configured Server Hostname Is Not Valid



Accepting and importing the credential

After the administrator accepted the presented credential by clicking on OK, TIBCO BusinessConnect imports the key to the keystore and binds it to the participant owning the given transport instance (outbound case) or using the given business agreement (inbound case).

The credential will be normally named with a pattern <partner-name>-<hostname>-<port>-<algorithm>-<index>, such as partner-sshserver.com-10022-rsa-2 OR partner-sshserver-dsa.

(The variable <port> is used only when the server port is not the default value 22)

The indexes are only used if the generated name already exists. The credentials imported through this feature are exportable in all the supported formats.

**Note**

TIBCO BusinessConnect will attempt to retrieve the server's key with the DSA algorithm first. If the server has not been configured with, or it does not prefer using a DSA key, TIBCO BusinessConnect will attempt to retrieve an RSA key instance.

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 using the Edit Protocol Binding dialog. See [Business Agreement: Transports Tab](#) for more details.

Configuring SSHFTP Outbound

1. In TIBCO Administrator, expand **BusinessConnect > Participants**.
2. Click a partner participant link.
3. Click the **Protocols** tab and then on the protocol link.
4. In the Edit Enabled Protocol, click the **Transports** tab.
5. Click **Add**.
6. Enter the transport name.
7. Select **SSHFTP** from the **Type** list.
8. Click **OK**.

This action adds the SFTP item to the list in the Transport Defaults area, which can be selected for the business agreement in [Business Agreement: Transports Tab](#).

9. In the New SSHFTP Transport dialog, configure the options listed in the following table:

Outbound SSHFTP Settings

Field	Description
Transport Name	Specify an identifier for these transport settings.
URL	<p>Specify the URL for the directory on the FTP server, which is <code>sshftp://host_name:port/path_name/</code>, where</p> <ul style="list-style-type: none"> • <i>host_name</i> is the name of the machine (server) where the SSHFTP server is running • <i>port</i> is the port on the machine to which the SSHFTP server is listening to • <i>path_name</i> is the relative path that starts from the base directory of the SSHFTP server
Authentication Mode	<p>Select one authentication mode that you want to use from this list.</p> <ul style="list-style-type: none"> • 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 Server SSH private key must be configured • Public Key and Password BusinessConnect Server SSH private key and user account's password must be configured <p>Note: ClientAuthenticationIdentity (for SSHFTP) under Business Agreement must have the TIBCO BusinessConnect Server SSH private key if either Public Key or Public Key and Password is selected.</p>
Username	Specify the username for the trading partner's SSHFTP server. The username must always be configured
Password	Specify the password for the user account with the name

Field	Description
	specified in the Username field on the trading partner's SSH server.
Server Credential fetch from ssh server Preferred Cipher Preferred MAC Preferred Compression File Processing File Mask Scripts Scripts Engine	See explanation for these fields in Inbound SSH 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 Security** 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.
Compression Algorithm	Select the compression algorithm: ZIP or ZLIB .
ASCII Armor	Specify whether the files have to be sent in the ASCII armor format.

Field	Description
TCPNoDelay	<p>Select this checkbox to enable the TCP No Delay feature.</p> <p>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.</p> <ul style="list-style-type: none">• 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. <p>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.</p>

10. Click **Save** three times.

HTTP, HTTPS, and HTTPSCA Transports

This section describes how to use HTTP, HTTPS, and HTTPS (Client Authentication) transports for document exchange.

Overview

TIBCO BusinessConnect supported the following HTTP transports:

- **HTTP** HTTP is a request/response protocol between clients and servers.
TIBCO BusinessConnect 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 [Server Identities and Certificates Tab](#).
TIBCO BusinessConnect supports the HTTPS transport for the trading hosts and trading partners.
- **HTTPSCA** 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 [New Certificate](#).

For inbound HTTP and HTTPS transports, HTTP basic authentication is supported. The user and password available in the incoming HTTP message are authenticated against the External User information configured in TIBCO BusinessConnect. The user information can also be set in LDAP servers. The password is passed in plain text across the network. It is good practice to use HTTPS with this feature. See RFC 2617, HTTP Authentication for more information.

**Note**

When an inbound or outbound message arrives but the protocol cannot be determined, the message is written to the audit log under the special protocol name `LostandFound`, which is a substitute name for an unidentified protocol.

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 a specific business agreement.

See [Business Agreement: Transports Tab](#) for more details.

Configuring HTTP/S for a Trading Partner

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

1. Select the transport for the trading partner on the business agreement level:
In TIBCO Administrator, expand **BusinessConnect** > **Business Agreements** > **Business Agreement Name** > **Protocol** > **Transports Tab**.
For more details, see [Business Agreement: Transports Tab](#)
2. Configure transport for the trading partner on the partner level:
Expand **BusinessConnect** > **Participants** and then click the partner's name.
In the window Edit Participant, select the **Protocols** tab.
Click the protocol link.
The Edit Enabled Protocol dialog is displayed.
3. In the **General** tab, enter information as mentioned in the following table:

Configuring HTTP/S for a Trading Partner: General Tab

Field	Select/Enter
AS2 Identifier	Add a new AS2 Identifier or select from the list

Field	Select/Enter
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	<p>This option only applies to the HTTP and HTTPS transports for the TIBCO BusinessConnect Services Plug-in. This option does not apply to the AS2 and AS1 Email transports.</p> <p>For more information, see <i>TIBCO BusinessConnect™ Services Plug-in User Guide</i>, "Partner Settings: General Tab."</p>

Add New HTTP/S Transport

- In the **Transports** tab, you can add the transport for this participant.
- Click **Add**.
The New Transport dialog is displayed.
- Name the transport.
- Select the transport type from the list: HTTP or HTTPS.
- Click **OK**.
- Configure the options listed in the following table:

Configuring HTTP/S for a Trading Partner: Transports Tab

Field	Description
Transport Name	An identifier for these transport settings.
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.

Field	Description
Server Certificate	<p>(HTTPS only) The participant's certificate used to encrypt communication.</p> <p>Note: You must configure the credentials in advance, before creating this transport. For more details about server certificates, see New Certificate .</p>
fetch from ssl server	<p>(HTTPS only) Retrieve the public keys of HTTPS servers using the HTTPS Server Public Key Retriever. The servers are identified by the hostname and port number in the URL field of the given connection.</p> <p>Once you click this link, TIBCO BusinessConnect tries to retrieve and present the currently effective HTTPS public key used by the HTTPS server. No keys will be added to the keystore unless you explicitly accept the presented key as trusted. The HTTPS Server Public Key Retriever does not verify the origin of these keys.</p>
Use HTTP Basic Authentication	<p>Enable basic authentication at the trading partner. The username 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 username and password. Note that the password is passed in plain text across the network.</p>
Username	<p>Specify a username for authenticating the host on the partner HTTP/S service.</p>
Password	<p>Specify a password for authenticating the host on the partner HTTP/S service.</p>
Retry Count	<p>The maximum number of times BusinessConnect will try to re-connect to the remote HTTP server, in case of failures.</p>
Retry Interval	<p>The interval TIBCO BusinessConnect will wait before another re-connect is attempted.</p>
Socket Timeout (seconds)	<p>The amount of time a socket will block on a read operation.</p> <p>Note: If you want to receive the timeout error when no response</p>

Field	Description
	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)	<p>Select the cipher grade (strength) from the list.</p> <p>The options are:</p> <ul style="list-style-type: none"> • All • Only Stronger Than Export • Only 128-Bit and Stronger • Only Stronger Than 128-Bit • Only 256-Bit and Stronger <p>All ciphers are listed in <i>TIBCO BusinessConnect Concepts</i>, "Cipher Suites."</p>
Can Use TLS (HTTPS only)	<p>TLS protocol is supported.</p> <p>If you select this checkbox, TLS protocol is used to establish connection to the trading partner server.</p>
TLS Version (HTTPS only)	<p>Select the version of TLS protocol.</p> <p>TLS protocol versions 1.0, 1.1, 1.2, and 1.3 are supported.</p>
Can Use SSLv3 (HTTPS only)	<p>SSL protocol version 3.0 is supported.</p> <p>If you select this checkbox, SSL protocol version 3.0 is used to establish connection to the trading partner server.</p>

4. Click **Save**.

Setting Up HTTP Proxies

To use a proxy connection for HTTP, you have to perform the following tasks:

Configure an Outbound Proxy for a Host

To add and select an outbound proxy for a host, see the following:

- [Adding a Proxy for a Host](#)
- [Selecting the Default Proxy for a Host](#)

Select the Default Proxy for a Trading Partner

To assign a default proxy server for a trading partner, see the following:

- [Proxy Settings Tab for Partners](#)

FIPS Mode Support

The Federal Information Processing Standard (FIPS 140-2) is a standard that specifies enhanced security requirements for complying applications.

To support the FIPS mode, you can configure TIBCO BusinessConnect as follows:

TIBCO Administrator

- For the inbound HTTPS transports, set the `bc.security.restrictVersion` property to TLSv1 in **System Settings > Activated Protocol Plug-ins and Properties > BC**.



Note

The SSLv3 is not supported in the FIPS mode.

- For the outbound HTTPS transports configured on partners, clear the **Can Use SSLv3** check box. Also, you are required to upload the certificate with the proper Subject Common Name or Subject Alternative Name, as the host name gets verified in the FIPS mode.
- For the intercomponent and secured private process JMS transports, the **Verify JMS Server** flag must be set. In addition, the following configuration is required in the EMS server `factories.conf` file for the SSL connection factories. The following displays the configuration for the EMS sample certificates in which use the appropriate values for `ssl_trusted` and `ssl_expected_hostname`.

```
[SSLQueueConnectionFactory]
  type = queue
  url = ssl://7243
  ssl_verify_host = enabled
  ssl_trusted = ../samples/certs/server_root.cert.pem
  ssl_expected_hostname = server
[SSLTopicConnectionFactory]
  type = topic
  url = ssl://7243
  ssl_verify_host = enabled
  ssl_trusted = ../samples/certs/server_root.cert.pem
  ssl_expected_hostname = server
```

Interior Server

You are required to set the following properties in one or more deployed engines' tra files:

```
java.property.TIBCO_SECURITY_VENDOR=bcfips
```

```
java.property.org.bouncycastle.rsa.allow_multi_use=true
```

Gateway Server

You can set the desired FIPS compliant ciphers as comma separated list in the gsengine. tra files as follows:

```
java.property.https.cipherSuites=<comma separated list>
```

For more details about the algorithms supported in FIPS, see <https://csrc.nist.gov/csrc/media/publications/fips/140/2/final/documents/fips1402annexa.pdf>

The actual cipher names should be as per Java specifications. For more information about the ciphers supported by Java 8, see Cipher Suites section in

<https://docs.oracle.com/javase/8/docs/technotes/guides/security/SunProviders.html>

Configuring Internal Key and Certificates for FIPS

The large file transfer (DDTP) and monitoring (JMX) channels use a secure SSL connection and the key/certificates are created during installation without any user intervention.

However, due to the mandatory host name verification done for FIPS, in order to match the

generated certificate subject name with all the deployed Gateway engine host names perform the following steps:

1. Add the BusinessConnect system settings property `bc.gs.cert.fqdn` and revoke the token from the **Manage Installation** page.
2. Create and export the Gateway token and place the token in `\bc\home\gs\token` folder.
3. Restart the Interior engine and the Gateway engine.

The property value for `bc.gs.cert.fqdn` property can be a comma separated list of IP addresses, host names, wildcard domain names, or the combination of all three.

For example,

```
bc.gs.cert.fqdn=10.0.2.15,10.0.2.16  
bc.gs.cert.fqdn=host.abc.com  
bc.gs.cert.fqdn=*.abc.com,10.0.2.16
```

The values should match the canonical host name of one or more Gateway Server machines. This can be seen in the Gateway Server instances page after the Gateway Server runs in the normal mode.

Typically, it is fully qualified hostname, which should suffice the wildcard domain name. In development environments, where the virtual machines that do not have a fully qualified host names are used, the explicit IP address or hostname is required.

**Note**

Currently, the FIPS mode is not supported for Microsoft SQL database.

AS2 Transport

This section 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).

**Note**

When an inbound or outbound message arrives but the protocol cannot be determined, the message is written to the audit log under the special protocol name `LostandFound`, which is a substitute name for an unidentified protocol.

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 Services Plug-in (EZComm protocol). See *TIBCO BusinessConnect™ Services Plug-in User Guide* for more information.

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 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 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 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 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 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 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 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 to enforce the renegotiation of the peer's credentials, the **Disable Session Cache** checkbox can be selected for any individual outgoing transport. When selected, each time when TIBCO BusinessConnect has business data to be delivered to the corresponding trading partner, the peer's credentials are requested and reverified.

For more information and the right location for disabling and enabling session cache see [bc.ssl.disableSessionCache](#).

AS2 Identifiers

TIBCO BusinessConnect 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 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 **BusinessConnect > Participants > Participant_Name > Protocols > Protocol_Name > 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, 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. In TIBCO Administrator, expand **BusinessConnect > Participants**.
2. Click a participant link.
3. Click the **Protocols** tab and then the protocol link.
4. Click the **Add New** link next to the AS2 Identifier field.
5. Click **Add New**.

6. Select an AS2 domain from the **AS2 Domain** list and enter the AS2 domain's identity in the **AS2 Identity** field (required).
7. Click **Save**.

**Note**

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>.

8. Click **OK**.

Setting Up AS2-HTTP/S for a Trading Host

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

1. "Step 3: Configuring Smart Routing", *TIBCO BusinessConnect Interior Server Administration*
2. [Setting the Host's AS2 Identifier for a Protocol](#)
3. Click **Save**.
4. Redeploy BusinessConnect.

Setting the Host's AS2 Identifier for a Protocol

1. In TIBCO Administrator, expand **BusinessConnect > Participants**.
2. Click a host participant link.
3. Click the **Protocols** tab.
4. Click a protocol link.
5. Select the host's AS2 Identifier from the **AS2 Identifier** list.
See [Disabling Session Cache for HTTPS](#).
6. Click **Save** twice.

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 a specific business agreement using the Edit Protocol Binding dialog.

See [Business Agreement: Transports Tab](#) for more details.

Configuring AS2-HTTP/S for a Trading Partner

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

1. In TIBCO Administrator, expand **BusinessConnect > Participants**.
2. Click the participant's name.
3. Select the **Protocols** tab.
4. Click a protocol link.

The Edit Enabled Protocol dialog is displayed. The General tab is selected by default.

5. Select or enter data as described in [AS1_Email Transport Settings](#).
6. Select the **Transports** tab to add the transport for this participant.
7. Click **Add**.

The New Transport dialog is displayed. Select or enter data as described in the following table:

New Transport Dialog for AS2-HTTP/S

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 Editing Protocol Bindings: Transports Tab . Click OK .

8. In the New AS2-HTTP/S Transport dialog, configure the options according to the following table:

AS2-HTTP/S Transport

Field	Description
Transport Name	An identifier for these transport settings.
URL	<p>Required.</p> <p>The URL for the trading partner. Syntax: <code>https://host:port/dmz/protocol</code>. Example: <code>https://host_machine8:6705/dmz/EZComm</code>.</p>
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	
MIME Subject	<p>A short string identifying the topic of the AS2 message; for example, "Purchase Order from ABC Company".</p> <p>For more information on the Subject Header field for MIME messages, refer to RFC C2822, Internet Message Format.</p>
Non Repudiation of Receipt	<p>Enable logging of receipts in the non-repudiation table.</p> <p>If you check this option, you must also check the Sign checkbox 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.</p> <p>For more information, see <i>TIBCO BusinessConnect™ Concepts</i>, "Non-Repudiation."</p>
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.

Field	Description
	<p>TIBCO BusinessConnect can <i>process</i> messages which contain message digests computed using the SHA1 hash algorithm. By default, TIBCO BusinessConnect will use the SHA1 hash algorithm when signing outbound messages for the AS1 and AS2 transports. To override this behavior, set the TIBCO BusinessConnect property <code>bc.ediint.digestAlgorithmEnabled</code> to <code>true</code> under System Settings. This will cause TIBCO BusinessConnect to compute the message digests for AS1 and AS2 using the digest algorithm setting specified for the business agreement in the Document Security screen.</p> <p>Whether an outbound receipt is signed or not is controlled by the setup in the requesting partner's Request Receipt list.</p>
Signature Scheme	<p>Select the desired signature algorithm from the list of options: RSA, RSA-PSS.</p> <p>The default option is RSA.</p> <p>Note: Ensure to enable the Sign checkbox to apply the signature scheme.</p>
Encrypt	<p>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 will be used to encrypt the email messages.</p>
Encryption Scheme	<p>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</p> <p>The default option is RSA-PKCS1-v1_5.</p> <p>Note: Ensure to enable the Encrypt checkbox to apply the encryption scheme.</p>
Compress	<p>If selected, each outgoing message is compressed in ZLIB format.</p>
Compression Order	<p>File compression is performed in the following orders:</p> <ul style="list-style-type: none"> • Before Signing File compression is performed before signing.

Field	Description
	<ul style="list-style-type: none"> • After Signing File compression is performed after signing.
Request Receipt	<p>The type of receipt returned from the trading partner. The following options are available:</p> <ul style="list-style-type: none"> • 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. <p>If you choose to request a receipt of any kind, you must have a valid email address set for the trading host.</p> <p>If you checked Non Repudiation of Receipt, you should select Signed. For computing the message digest, BusinessConnect uses the digest algorithm that was configured for the business agreement in the Document Security screen.</p> <p>For more information on receipts, see Message Disposition Notification Receipts.</p>
Return Receipt URL	The URL to which receipts are sent if you selected asynchronous receipts in the Request Receipt list.
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 will try to re-connect to the remote HTTP server, in case of failures.
Retry Interval	The interval TIBCO BusinessConnect will wait before another re-connect is attempted.
Socket Timeout	Socket timeout is the maximum amount of time (in seconds) to wait for

Field	Description
(seconds)	<p>a response before disconnecting the socket.</p> <p>Note: If you want to receive the timeout error when no response 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.</p>
Use HTTP Basic Authentication	HTTP basic authentication uses a username and password.
Username	Specify a username for authenticating the host on the partner HTTP/S service.
Password	Specify a password for authenticating the host on the partner HTTP/S service.
Cipher Suite Grade	<p>(HTTPS only) Select the cipher grade (strength) from the list.</p> <p>The options are:</p> <ul style="list-style-type: none"> • All • Only Stronger Than Export • Only 128-Bit and Stronger • Only Stronger Than 128-Bit • Only 256-Bit and Stronger <p>All ciphers are listed in <i>TIBCO BusinessConnect Concepts</i>, "Cipher Suites."</p>
Can Use TLS	<p>(HTTPS only) Whether TLS protocol is supported.</p> <p>If you select this checkbox, TLS protocol is used to establish connection to the trading partner server.</p>
TLS Version	<p>(HTTPS only) Select the version of TLS protocol.</p> <p>TLS protocol versions 1.0, 1.1, 1.2, or 1.3 are supported.</p>

Field	Description
	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 checkbox, SSL protocol version 3.0 is used to establish connection to the trading partner server.

9. Click **Save** three times.

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 section 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

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.

**Note**

When an inbound or outbound message arrives but the protocol cannot be determined, the message is written to the audit log under the special protocol name `LostandFound`, which is a substitute name for an unidentified protocol.

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-edint-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 will contain the main document, while the subsequent body parts will 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 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 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 was 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 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 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 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 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 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 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 will ignore 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 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 **BusinessConnect > Participants > Participant_Name > Protocols > Protocol_Name > 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. In TIBCO Administrator, expand **BusinessConnect > System Settings > Inbound Mail POP3 Servers**.
2. Configure the POP3 Server as explained in [Inbound Mail POP3 Servers](#).
3. Redeploy BusinessConnect.

Configuring an SMTP Server for a Host

To enable communication for a host through an SMTP server, see

- [Adding a Proxy for a Host](#)
- [Selecting the Default Proxy for a Host](#)

Configuring an SMTP Server for a Partner

To enable use of an SMTP server for a partner, see

- [Proxy Settings Tab for Partners](#).

Setting Up AS1 Email for a Trading Host

Selecting AS1 Email for the Trading Host

1. In TIBCO Administrator, expand **BusinessConnect > Business Agreements**.
2. Click a business agreement link.
3. Click the protocol link.
4. In the Edit Protocol Binding dialog, click the **Transports** tab.
5. Check the **Email** checkbox in the Allowed Inbound Transports area.
6. Click **Save** twice.

Setting the Host's Email Address for a Protocol

1. In TIBCO Administrator, expand **BusinessConnect > Participants**.
2. Click the host link and then the **Protocols** tab.
3. Click the protocol link.
4. Add the host's email address to the Valid Email Address List field.

**Note**

Email addresses entered in the Valid Email Address List box must be separated either by a semicolon or by a comma.

5. Click **Save** twice.

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 a specific business agreement using the Edit Protocol Binding dialog

See [Business Agreement: Transports Tab](#) for more details.

Configuring AS1 Email for a Trading Partner

i Note: For email transport to work as expected, remove TLSv1 from the java security `jdk.tls.disabledAlgorithms` as follows:

```
jdk.tls.disabledAlgorithms=SSLv3, TLSv1.1, RC4, DES, MD5withRSA, \DH
keySize < 1024, EC keySize < 224, 3DES_EDE_CBC, anon, NULL, \
include jdk.disabled.namedCurves
```

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

1. In TIBCO Administrator, expand **BusinessConnect > Participants**.
2. Click a partner participant link.
3. Click the **Protocols** tab.
4. Click the protocol link.
The General tab is selected by default.
5. Click the **Transports** tab.
6. Click **Add**.
7. Enter the transport name.
8. Select **AS1_Email** from the list.
9. Select or enter data as described in the following table:

AS1_Email Transport Settings

Field	Description
Transport Name	An identifier for these transport settings.
URL	(Required) The URL for the trading partner. <code>mailto: e-mailID@domain.com.</code>

Field	Description
Subject	<p>A short string identifying the topic of the email message; for example, "Purchase Order from ABC Company".</p> <p>For more information on the Subject Header field for MIME messages, refer to RFC C2822, Internet Message Format.</p>
Base64 Encode Clear Text Messages	<p>Base64 encode plain outbound email messages. Plain messages are those messages which are not signed, not encrypted, and not compressed.</p>
Non Repudiation of Receipt	<p>Enable logging of receipts in the non-repudiation table.</p> <p>If you check this option, you must also check the Sign checkbox 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.</p> <p>For more information, see <i>TIBCO BusinessConnect™ Concepts</i>, "Non-Repudiation."</p>
Sign	<p>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.</p> <p>TIBCO BusinessConnect can <i>process</i> messages which contain message digests computed using the SHA1 hash algorithms. By default, TIBCO BusinessConnect will use the SHA1 hash algorithm when signing outbound messages for the AS1 and AS2 transports. To override this behavior, set the TIBCO BusinessConnect property <code>bc.ediint.digestAlgorithmEnabled</code> to <code>true</code> under System Settings. This will cause TIBCO BusinessConnect to compute the message digests for AS1 and AS2 using the digest algorithm setting specified for the business agreement in the Document Security screen.</p> <p>Whether an outbound receipt is signed or not is controlled by the setup in the requesting partner's Request Receipt list.</p>

Field	Description
Signature Scheme	<p>Select the desired signature algorithm from the list of options: RSA, RSA-PSS.</p> <p>The default option is RSA.</p> <p>Note: Ensure to enable the Sign checkbox to apply the signature scheme.</p>
Encrypt	<p>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 will be used to encrypt the email messages.</p>
Encryption Scheme	<p>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</p> <p>The default option is RSA-PKCS1-v1_5.</p> <p>Note: Ensure to enable the Encrypt checkbox to apply the encryption scheme.</p>
Compress	<p>If selected, each outgoing message is compressed in ZLIB format.</p>
Compression Order	<p>File compression is performed in the following orders:</p> <ul style="list-style-type: none"> • Before Signing File compression is performed before signing. • After Signing File compression is performed after signing.
Request Receipt	<p>The type of receipt returned from the trading partner. The following options are available:</p> <ul style="list-style-type: none"> • 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.

Field	Description
	<ul style="list-style-type: none"> • Unsigned An unsigned receipt is requested from the trading partner for each message. <p>If you choose to request a receipt of any kind, you must have a valid email address set for the trading host.</p> <p>If you checked Non Repudiation of Receipt, you should select Signed. For computing the message digest, BusinessConnect uses the digest algorithm that was configured for the business agreement in the Document Security screen.</p> <p>For more information on receipts, see Message Disposition Notification Receipts.</p>
Receipt Timeout (minutes)	<p>The amount of time within which a receipt should be returned by the trading partner.</p> <p>Example: 5</p>

10. Click **Save** two times.

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. In TIBCO Administrator, expand **BusinessConnect > Participants**.
2. Click the partner participant's link.
3. Click the **Protocols** tab.
4. Click the specific protocol link.
5. Add the partner's email address in the field Valid Email Addresses.
Make sure that addresses are separated by a semicolon (;) or by a comma (,).
6. Click **Save** three times.

Configuring AS1 Email for a Business Agreement

To configure the AS1 Email transport for a business agreement, see [Business Agreement: Transports Tab](#).

File Transport

This section describes how to use File transport for document exchange.

File Transport Overview

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. This is different from other transports that are used for communication between trading partners.

**Note**

When an inbound or outbound message arrives but the protocol cannot be determined, the message is written to the audit log under the special protocol name `LostandFound`, which is a substitute name for an unidentified protocol.

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 a specific business agreement using the Edit Protocol Binding dialog.

See [Business Agreement: Transports Tab](#) for more details.

Configuring Outbound File Transport for a Partner

1. Using TIBCO Administrator, expand **BusinessConnect > Participants**.
2. Click a partner participant link.
3. Click the **Protocols** tab.
4. Click a protocol link.
5. In the Edit Enabled Protocol dialog, click the **Transports** tab.
6. Click **Add**.
7. Enter the transport name.
8. Select **File** from the Transport **Type** list.
9. Click **OK**.

This action adds the File item to the list in the Transport Defaults area, which can be selected for the business agreement in and to the areas described in [Business Agreement: Transports Tab](#).

10. In the dialog New File transport, configure the options listed in [Outbound File Transport](#).

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.

Field	Description
File Processing	<p>The mechanism for deciding how files are sent to the trading partner. There are two choices:</p> <ul style="list-style-type: none"> • 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	<p>The mask to control file naming. The value entered in the field is used as the name of the file.</p> <p>See Supported File Mask Options for more information.</p> <p>See the File Masks section in <i>TIBCO BusinessConnect™ EDI Protocol powered by Instream® User Guide</i> for information on pre-defined and user-defined options for outbound file masks for EDI.</p> <p>If no value is entered, Business Connect will generate the outbound request in a pre-defined format.</p>
Scripts	<p>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.</p>
Scripts Engine	<p>The scripts engine that you want to use to run custom scripts.</p> <p>You can select one of the items from the list:</p> <ul style="list-style-type: none"> • FESI • Nashorn <p>Note: The FESI EcmaScript engine originally supported by TIBCO BusinessConnect is out of support by the vendor. It is good practice to use the Nashorn script engine as a substitute because the Nashorn script engine is roughly compatible with the FESI EcmaScript engine.</p>

11. Click **Save** three times.

Outbound File Pollers

Configuration for Outbound File Pollers is explained in *BusinessConnect Interior Server Administration*, "Outbound File Pollers."

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 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 existing files when the engine starts up.

Enabling and Configuring Inbound File Poller

To enable and configure an inbound File poller on the BusinessConnect server, perform these steps:

1. Using TIBCO Administrator, expand **BusinessConnect > System Settings > Inbound Public Transport Types**.
2. Check the checkbox next to the **File** transport.
3. Click **Enable**.

The enabled protocol will now appear with a red checkmark in the Enabled column.

The File Poller is configured on the Gateway Server, as explained in *TIBCO BusinessConnect Gateway Server Administration*, Poller Tab.

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. In TIBCO Administrator, expand **BusinessConnect > Business Agreements**.
2. Click the business agreement link.
3. Click a protocol link.
4. In the Edit Protocol Binding dialog, click the **Transports** tab.
5. Make sure that the **File** checkbox in the Allowed Inbound Transports area is selected.

Inbox Transport

This section describes how to use Inbox transport for document exchange.

Inbox Transport Overview

BusinessConnect now allows documents to be securely stored internally in the database to make it available for trading partners to download them from one of the supported TIBCO BusinessConnect Plug-ins such as FTP Server, or PartnerExpress (a Web Portal) via the Gateway Services. To make this possible, the Inbox transport is available for business protocols such as TIBCO BusinessConnect Services Plug-in.

To use the Inbox transport, the trading partners must have user access available and enabled, so that they can download their payloads from the supported TIBCO BusinessConnect Plug-ins.

Outbound Inbox Transport

The Inbox transport can be configured for a business protocol if that protocol supports this transport, such as TIBCO BusinessConnect Services Plug-in.

Configuring Outbound Inbox Transport for a Partner

To configure the outbound Inbox transport for a partner:

1. Using TIBCO Administrator, expand **BusinessConnect > Participants**.
2. Click the partner participant link.
3. Click the **Protocols** tab.
4. Click the protocol link.
5. In the Edit Enabled Protocol dialog, click the **Transports** tab.

6. Click **Add**.
7. Enter the transport name.
8. Select **Inbox** from the Transport **Type** list.
9. Click **OK**.

This action adds the File item to the list in the Transport Defaults area, which can be selected for the business agreement in and to the areas described in [Business Agreement: Transports Tab](#).

10. In the dialog New Inbox transport, configure the options listed in [New Inbox Transport](#).

New Inbox Transport

Field	Description
mailto	mail URL of the Partner to receive email message when a Business Protocol message is stored internally. Users must configure the SMTP Proxy Server to enable the mail to be sent to Partner.
Subject	Email Subject name to be used for the Partner.



Note

When using Inbox transport to send messages to a trading partner, at least one valid email address must be specified in the **Valid Email Address List** field under **BusinessConnect > Participants > host > Protocols > Protocol_Name > General** tab.



Note

You can customize the Email template to override the sender's email address and subject line and add text at the start of the Email body. To customize these, you must add the following properties listed in [Customize Email Properties](#) in the BusinessConnect-Interior_Server.tra file.

Customize Email Properties

Field	Description
bc.email.body.append	Add text at the start of the Email body.
bc.email.subject.override	Overwrite the Email subject.
bc.email.name.override	Overwrite the sender's Email id. Note: You must ensure it is a valid Email address. If the value for the property is not specified, it will pick the value specified in the Administrator.

Message Disposition Notification Receipts

This section describes receipts in Email, AS1 Email, AS2-HTTP, and AS2-HTTPS transports.

Overview

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 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 non-repudiation scheme.

For Email, TIBCO BusinessConnect follows the AS1 specification for MDN receipts. For AS2-HTTP/S, TIBCO BusinessConnect 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

For more information on how to configure MDN receipts, see [Business Agreement: Transports Tab](#).

Enabling Receipts

You can enable MDN receipts in the Request Receipt list when configuring a transport for the trading partner, as explained in [Request Receipt](#). 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 BC/Receipt entry.

Setting Up Receipt Timeouts

When TIBCO BusinessConnect 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 [AS2 Async MDN Remote Server Certificate](#).

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 [AS2 Async MDN Reply Transport](#).

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. For example when a document is validated by the EDI engine it would send back a business acknowledgment back to the trading partner.

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 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.

Some of the protocols, such as TIBCO BusinessConnect Services Plug-in, do not suppress these messages, and some of them do (SOAP). Consult documentation for a specific business protocol for more information.

If AS2 is used with EDI protocol and receipts are used, then the MDN messages will occur. 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™ Palette Reference*, Receive Misc. Msg.

If you are not using the TIBCO BusinessConnect palette to implement your private process, you can listen for these miscellaneous messages on the following TIBCO Rendezvous subject names:

- `prefix.installation.standardID.INFO.RECEIPT.RECEIVED` This is sent when MDN receipt is received from a trading partner
- `prefix.installation.standardID.INFO.RECEIPT.SENT` This is sent when MDN receipt is sent to a trading partner
- `prefix.installation.standardID.ERROR.RECEIPT.RECEIVED` This is sent when an Error MDN receipt is received from a trading partner
- `prefix.installation.standardID.ERROR.RECEIPT.SENT` This is sent when an Error MDN receipt is sent to a trading partner
- `prefix.installation.standardID.ERROR.TIMEOUT.RECEIPT` This is sent when an MDN receipt is not received from a trading partner within the configured timeout period

Troubleshooting

This section offers advice on resolving transport and database problems.

Troubleshooting Transport Problems

All Transports

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 Security Tab](#).

Issues with messages not shown in audit logs

When an inbound or outbound message arrives but the protocol cannot be determined, the message is written to the audit log under the special protocol name LostandFound, which is a substitute name for an unidentified protocol.

FTP Transport

Error message when FESI jars are missing

If you see such an error when using custom scripts:

```
com.tibco.plugin.gateway.InvokeOperationActivity$OperationThread
java.lang.NoClassDefFoundError: FESI/Data/ESValue
  at java.lang.Class.forName0(Native Method)
  at java.lang.Class.forName(Class.java:141)
  at com.tibco.ax.fw.runtime.outbound.transport.ftp.FtpPutTransport.send
(FtpPutTransport.java:126)
```

This error indicates that you are missing the FESI jars.

To use scripts, you must install the FESI EcmaScript Interpreter as described in *TIBCO BusinessConnect Installation and Configuration*, Installing FESI EcmaScript Interpreter to Support Custom Scripts.

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 returns the following error message:

```
Error retrieving Host or Trading Partner. Check email configuration.
```

BusinessConnect logs the message to the protocol log.

Read [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 returns the following error message:

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

BusinessConnect logs the message to LostandFound.

Read [Identifying the Sender and Receiver](#) for information about providing the email address for the host.

Troubleshooting Database Problems

Changes to database assignments for logs or stores did not take effect

After changing the database assignments for logs or stores using **BusinessConnect > System Settings > Audit, Non-Repudiation and Runtime Database Configuration**, restart the BusinessConnect engines.

See [User Authentication Configuration](#) for more information.

Changes to database configuration did not take effect

After modifying the configuration using **BusinessConnect > Manage** Installation, redeploy the BusinessConnect application.

See [User Authentication Configuration](#) for more information.

Database creation error

If you do not have the correct database permissions, when TIBCO BusinessConnect attempts to create the required tables, it will return an invocation target exception. To correct, set up the correct database permissions.

Database connection to the Configuration store is lost

If database connection to the Configuration store is lost when you log in after re-connection, you must go to the Manage Installation dialog and perform the following steps:

1. Choose the database for the correct configuration store installation.
2. Select **Test the Connection**.
3. Click **Save**.



Note

It is important to click **Save** before you log in or log out whenever you are switching to a different configuration store.

4. Log out and then again log in. You will now get back the previous configuration.

Scripts

This section describes scripts that BusinessConnect uses to manage the FTP inbound, FTP outbound, and File outbound transports.

Overview

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

**Note**

To use scripts you must install the FESI EcmaScript Interpreter as described in *TIBCO BusinessConnect Installation and Configuration*, Installing FESI EcmaScript Interpreter to Support Custom Scripts.

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 considers the scripts as having completed successfully.

TIBCO BusinessConnect provides a Java API for use within scripts. For information on this API, see the *TIBCO BusinessConnect™ API Reference*.

This section 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 in *TIBCO BusinessConnect™ API Reference*.

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 in *TIBCO BusinessConnect™ API Reference*.

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's Document Exchange. For more details, see [Business Agreement: Document Security Tab](#).

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 in TIBCO Administrator:

1. Expand **Application Management > BusinessConnect > Configuration**.
2. Click **BusinessConnect**.
3. Select the **Component Settings** tab.
4. Click the **Intercomponent Advanced** link.
5. Enter the value for the Local Temporary Directory.

If the value is `C:\temp\local`, the files are temporarily stored in `C:\temp\local\protocol\tpName`.

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 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.unpackMessage(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 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 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™ Interior Server 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
- RNT0 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 *TIBCO BusinessConnect™ API Reference*, 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`.

Managing Errors

Retrying Document Posting

You can configure TIBCO BusinessConnect to retry posting of documents if it could not post them during the execution of the scripts. To do this, set the following in a script:

```
job.put("retryScripts", "true");
```

TIBCO BusinessConnect detects this value, and then does a retry. If you do not want retry to occur, you can set the value to be false:

```
job.put("retryScripts", "false");
```

For example, the sample script `putediexample.txt` has the `retryScripts` variable set if there are connection problems with the FTP server.

See *TIBCO BusinessConnect™ Services Plug-in User Guide*, First Tutorial Example for information on `putediexample.txt`.

For the error codes that TIBCO BusinessConnect might receive or might generate, see also `com/tibco/ax/fw/runtime/transport/ftp/FTPReply` and `com/tibco/ax/fw/runtime/transport/sshftp/SSHFTPReply` public interfaces in *TIBCO BusinessConnect API Reference*.

Returning Errors from Scripts

You can control the values returned in the `statusCode` and `statusMsg` fields following script execution. TIBCO BusinessConnect then uses these values for logging.

- `userStatusCode` Integer type
- `userStatusMsg` String message

By default, if `job.get("userStatusCode")` is not set in the script, it is assumed that the script was executed successfully. Hence, it is not necessary to specify status code 200 in the script for successful execution.

If you have to specify an error, you specify a `statusCode` other than 200, and an error will be logged and an advisory message on the Error subject will be sent. To do this, set the variable inside the scripts via the job slot variable.

Example:

```
job.put("userStatusCode", 553);
job.put("userStatusMsg", "Permission denied when storing the file on the FTP
Server");
```

Audit Logging in Scripts

You can create an audit log within the context of a script. An audit log object is available as a job slot variable and this object can be used to log, for example, FTP login issues or in a case of inability to delete files due to inadequate file permissions.

The following line of code returns a `UserLogAccess` object:

```
var logClient = job.get("logObj");
```

You invoke this object using the `log()` method:

```
logClient.log(java.lang.String state,int status,java.lang.String desc)
```

This audit log object can be used to log the following status:

- **PENDING** Use if you want to do intermediate logging.
- **COMPLETED** Use if there are no errors are encountered and you want to end your audit trail for this execution of the script.
- **ERROR** Use if you encounter an error during the execution. Marking the status as **ERROR** would also internally trigger a TIBCO Rendezvous signal to be sent out in the following subject:

```
AX.BC.BC-INSTANCENAME.PROTOCOL.ERROR.TRANSPORT.SCRIPT
```

The status values are maintained in the Java interface `UserLogAccess`. The script examples discussed in *TIBCO BusinessConnect™ Services Plug-in User Guide*, FTP Script Examples

include the `UserLogAccess` object which uses the constants to set the status of the audit log entry.

For every execution of the script, a new audit log summary row is created with the first call to the `log()` method triggering the creation of the row. This method allows the user to define the state, status, and description for the log entry. Please refer the JavaDoc API under `UserLogAccess` interface.

If logging is defined inside an FTP inbound script, the summary row would be logged with operation ID `FTPGetScript` and with a new document ID. Care should be taken when logging FTP inbound scripts.

The sample script `mgetexample.txt` (see *TIBCO BusinessConnect™ Services Plug-in User Guide*, First Tutorial Example) shows FTP Inbound scripts logging only if there is any error in the execution of the FTP scripts and thereby avoiding filling up the database with this audit trail.

If logging is defined inside an FTP outbound script, a summary row would be logged with operation ID `FTPPutScript` and a new document ID. If logging is defined inside a File script, whenever an outbound request is generated through scripts, a summary row would be logged with operation ID `FILEScript` and a new document ID.

Remote Client Service Audit Log

This section illustrates the audit log entries for a sample TIBCO BusinessConnect Remote Client startup under the TIBCO BusinessConnect Remote Client Service protocol.

Overview

TIBCO BusinessConnect Remote client service protocol enables the TIBCO BusinessConnect Remote client to download the configuration data from the TIBCO BusinessConnect server in preparation for a secure document exchange upon startup.

The configuration data includes exchange of certificate credentials for encryption and digital authentication between the TIBCO BusinessConnect Remote client service and the Business Connect server as well as the AS2 transport parameters.

Upon successful startup with the configurations provided by the TIBCO BusinessConnect Remote client service, the TIBCO BusinessConnect remote client can start exchanging documents for various business protocols, such as TIBCO BusinessConnect EDI Protocol powered by Instream and TIBCO BusinessConnect Services Plug-in, with the TIBCO BusinessConnect server.

TIBCO BusinessConnect Remote Audit Log Viewer

The activities of request from the TIBCO BusinessConnect Remote client are logged in the TIBCO BusinessConnect Remote audit log viewer, which consists of two operations:

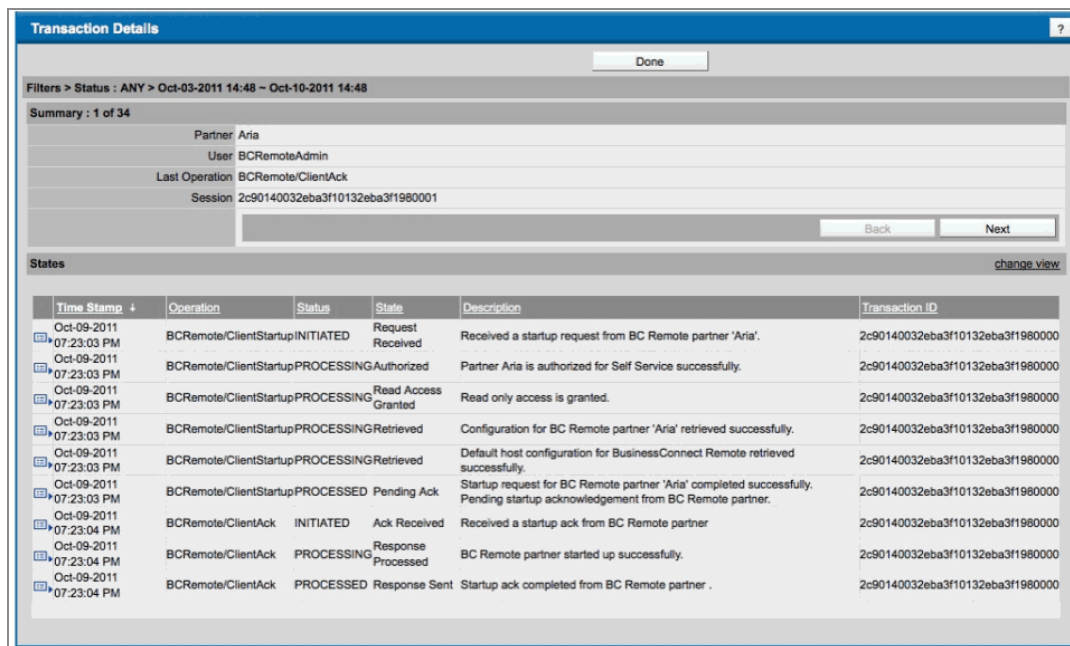
- **BusinessConnect Remote/ClientStartup** This operation captures the activities where the TIBCO BusinessConnect server constructs the response for the startup request from the TIBCO BusinessConnect Remote client.
- **BusinessConnect Remote/ClientAck** This operation captures the activities returning from the TIBCO BusinessConnect Remote client that acknowledge the successful completion of the startup.

An error acknowledgment could be returned when the TIBCO BusinessConnect Remote client fails to start up based on the response sent by TIBCO BusinessConnect server.

[TIBCO BusinessConnect Remote Audit Log Entries](#) shows audit log entries for the TIBCO BusinessConnect Remote client.

Audit log reports cannot be generated for the protocol TIBCO BusinessConnect Remote.

Figure 50: TIBCO BusinessConnect Remote Audit Log Entries



The screenshot displays the 'Transaction Details' window for the TIBCO BusinessConnect Remote client. It includes a summary section with filters and a table of audit log entries.

Filters: Status: ANY > Oct-03-2011 14:48 ~ Oct-10-2011 14:48

Summary: 1 of 34

Partner: Aria
 User: BCRemoteAdmin
 Last Operation: BCRemote/ClientAck
 Session: 2c90140032eba3f10132eba3f1980001

States [change view](#)

Time Stamp	Operation	Status	State	Description	Transaction ID
Oct-09-2011 07:23:03 PM	BCRemote/ClientStartupINITIATED	Request Received		Received a startup request from BC Remote partner 'Aria'.	2c90140032eba3f10132eba3f1980000
Oct-09-2011 07:23:03 PM	BCRemote/ClientStartupPROCESSING	Authorized		Partner Aria is authorized for Self Service successfully.	2c90140032eba3f10132eba3f1980000
Oct-09-2011 07:23:03 PM	BCRemote/ClientStartupPROCESSING	Read Access Granted		Read only access is granted.	2c90140032eba3f10132eba3f1980000
Oct-09-2011 07:23:03 PM	BCRemote/ClientStartupPROCESSING	Retrieved		Configuration for BC Remote partner 'Aria' retrieved successfully.	2c90140032eba3f10132eba3f1980000
Oct-09-2011 07:23:03 PM	BCRemote/ClientStartupPROCESSING	Retrieved		Default host configuration for BusinessConnect Remote retrieved successfully.	2c90140032eba3f10132eba3f1980000
Oct-09-2011 07:23:03 PM	BCRemote/ClientStartupPROCESSED	Pending Ack		Startup request for BC Remote partner 'Aria' completed successfully. Pending startup acknowledgement from BC Remote partner.	2c90140032eba3f10132eba3f1980000
Oct-09-2011 07:23:04 PM	BCRemote/ClientAck	INITIATED	Ack Received	Received a startup ack from BC Remote partner	2c90140032eba3f10132eba3f1980000
Oct-09-2011 07:23:04 PM	BCRemote/ClientAck	PROCESSING	Response Processed	BC Remote partner started up successfully.	2c90140032eba3f10132eba3f1980000
Oct-09-2011 07:23:04 PM	BCRemote/ClientAck	PROCESSED	Response Sent	Startup ack completed from BC Remote partner .	2c90140032eba3f10132eba3f1980000

Audit log reports cannot be generated for the protocol TIBCO BusinessConnect Remote.

Application Monitoring and Management by Processing Rulebases

This section introduces the concept of a rulebase, a configuration object that allows the TIBCO Hawk agent to monitor and manage applications on the network. This section contains simple examples that demonstrate the steps for creating rulebases and the rules that contain monitoring logic.

Overview

A TIBCO Hawk agent monitors and manages applications by processing rulebases, which are named collections of rules that contain management logic. Using TIBCO Hawk Display, you can create additional rulebases with specialized rules.

See Monitoring with Rulebases in *TIBCO Hawk Administrator's Guide* for more details.

Creating a Rulebase

You create rulebases using TIBCO Hawk Display. After creating the rulebase you can save it to a file or distribute it to agents on the network.

See Creating a Rulebase in *TIBCO Hawk Administrator's Guide* for more details.

Building a Rule

Most monitoring tasks consist of periodic checking for some problematic conditions. When a problem is detected, an alarm is sent or corrective actions are taken. If the application goes down, for example, capture some diagnostics and execute a startup script. If too much disk space is consumed, delete some temporary files. If duplicate processes are running, terminate the most recent one. When you create a rule, you specify this monitoring logic and package it for a TIBCO Hawk agent. The agent can apply the rule

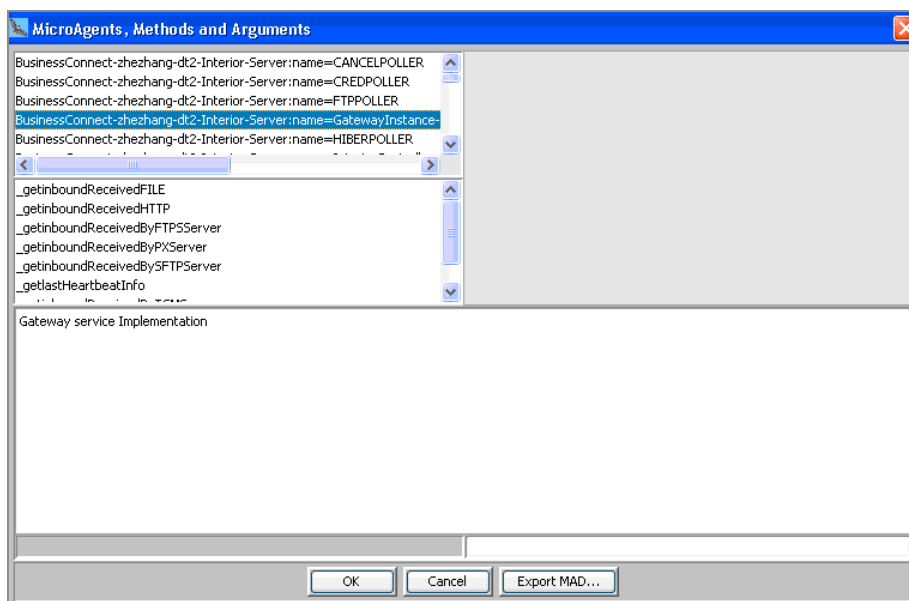
again and again without intervention. If a problem occurs, the agent can solve it by taking corrective action, or notify you that the problem requires attention, or both, depending on rule design.

For example, a notification is sent if the heartbeat of Interior Server Instance or the last heartbeat of a Gateway Instance is detected. An alarm is sent if the Poller is potentially hung, so you can execute the method to destroy the hanging thread when the Poller is hung. The inbound or outbound information can also be sent to TIBCO Administrator GUI.

Rules consist of data sources, tests, and actions. Data sources are microagent methods that periodically collect or asynchronously return information to an agent. One or more tests are applied to the resulting data set. When a particular test evaluates to true, one or more actions can be triggered.

To create a new rule on an agent, click **Edit** next to the **Data Source** field.

Figure 51: Creating a New Rule



This window contains a list of microagents you are allowed to use as a data source for the rule. TIBCO BusinessConnect microagents are listed, for example, the Gateway Instance, Interior Server Instance, and Pollers.



Note

Export MAD allows you to save the microagent descriptor in its XML representation. For more information on exporting and importing microagent descriptors using their XML representation, refer to *TIBCO Hawk Configuration Object API Reference*.

See Building a Rule in *TIBCO Hawk Administrator's Guide* for more details.

Specifying a Data Source

The data source for a rule is its source of input data, and is always a method of a microagent. When a rule is active, the TIBCO Hawk agent subscribes to the specified method and passes method results to the test. The following example uses the **BusinessConnect-zhezhang-dt-Interior-Server_name=CANCELPOLLER** microagent as a representative data source.

To define the data source of a rule, perform the following steps:

1. Click the **BusinessConnect-zhezhang-dt-Interior-Server_name=CANCELPOLLER** microagent.
2. Click the **_getisHung** method.

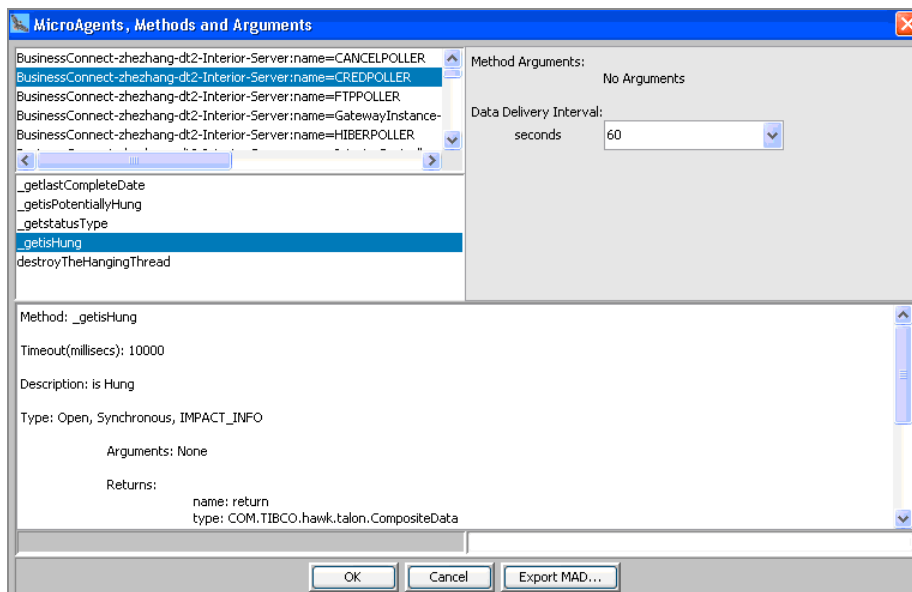
Fields for method arguments and a data delivery interval are displayed on the right side of the window. A detailed text description of the method, including arguments and return values, is displayed in the lower panel.

3. No arguments for this example method.

When invoked, the **_getisHung()** method returns information about the status of the CANCELPOLLER thread.

This is a synchronous method. When the rule is active, the agent subscribes to this method and receives data every 60 seconds, by default. For asynchronous methods, such as **onMBeanNotification()** in the **BusinessConnect-zhezhang-dt-Interior-Server:type=mgmt,name=InteriorController-Heartbeat** microagent, no collection interval is required.

Figure 52: Specifying a Data Source



4. Click **OK**.

The rule is now configured to use the **`_getisHung()`** method of the **`BusinessConnect-zhezhang-dt-Interior-Server_name=CANCELPOLLER`** microagent as a data source. In the Rule Editor window, **`_getisHung():60`** is displayed in the **Data Source** field.

Defining Tests

The data source of a rule provides information about some conditions on a managed node. After information is received, one or more tests are applied to evaluate it. Each sample of data from the data source is distributed to all tests in the rule. Each test uses the data to compute a true or false value which is used in determining when to trigger actions.



Note

A test is true only when the entire test evaluates to true, not just the test expression.

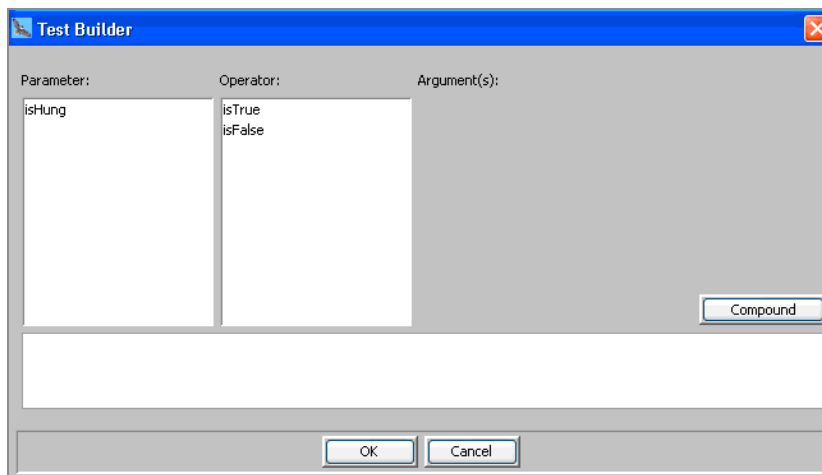
See Defining Tests in *TIBCO Hawk Administrator's Guide* for more details.

Creating a New Test

To create a new test in the current rule, perform the following steps:

1. In the Rule Editor window, click **Create** on the toolbar.
2. In the Test Editor window, the **If** field is for the test expression, which you create in the Test Builder window. You access this window by clicking **Edit**. The **Then** field is for one or more actions to perform if the test evaluates to true, which you specify in the Action Editor window. You access this window using toolbar buttons in the Test Editor window.
3. Click **Edit** next to the **If** field.

Figure 53: Creating a New Test



A test consists of a test expression and other parameters that determine how and when the test is applied. Tests created in the Test Builder window have the following form:

If <expression is true> then <perform actions>

The first set of angle brackets contains the test expression. It consists of a parameter, a return value of the microagent method used as a data source, and a test operator, such as **isTrue**. Test operators you can use in an expression depend on the type of value returned by the microagent method. Numeric, string and Boolean values can all be used as input in a test expression.

Building a Test Expression

The following procedure shows how to build a test expression by specifying a test parameter and test operator in the Test Builder window. This example uses the **BusinessConnect-zhezhang-dt-Interior-Server:name=GatewayInstance-192.168.69.105-11000** microagent **_getinboundReceivedHTTP()** method result field and a numeric operator.

1. Click **inboundReceivedHTTP** to use as the test parameter.

inboundReceivedHTTP is returned by the **_getinboundReceivedHTTP()** method, the data source for this rule. The text area in the Microagents, Methods and Arguments window displays a short description of each parameter. In the description for this method, you can see that **inboundReceivedHTTP** is a double value.

2. Click **>** in the **Operator** field. Only operators that apply to the current parameter are included in the list. **inboundReceivedHTTP** is a double value, so numeric operators are listed.
3. Type **1000** in the **Greater than** field.
4. Click **OK** to save the test expression.

This test checks the HTTP inbound value of the Gateway Instance. If the value is less than 1000, no problem occurs and the test is false. Since the **_getinboundReceivedHTTP()** is a synchronous method, the agent evaluates the test every 60 seconds by default.

See Building a Test Expression in *TIBCO Hawk Administrator's Guide* for more details.

Building Compound Tests

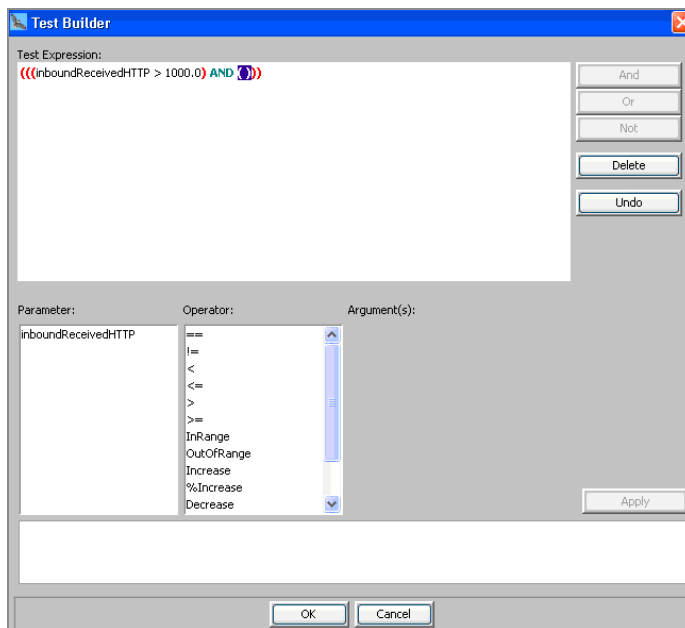
A compound test uses the same operators as a simple test, but allows you to combine multiple expressions using the logical operators AND, NOT, and OR. You can group expressions and insert operators in the compound test editor.

The following procedure shows how to build a compound test expression by modifying a simple expression. This example adds a second condition, using the **BusinessConnect-zhezhang-dt-Interior-Server:name=GatewayInstance-192.168.69.105-11000** microagent **_getinboundReceivedHTTP()** method result field and a text string operator, to the sample test expression on [Building a Test Expression](#). Both conditions in the new test expression must be satisfied for the test to evaluate to true.

To build a compound test, perform the following steps:

1. In the Test Editor window, click **Compound**. The current text expression is highlighted in the **Test Expression** field, for example:
(inboundReceivedHTTP > 1000.0)
This test checks for the **inboundReceivedHTTP** value is greater than a specific number.
2. Click **And** to group the highlighted expression and add the **AND** operator. The compound test editor automatically adds the correct number of parentheses to the expression:

Figure 54: Building a Compound Test



3. In the lower half of the window, click **inboundReceivedHTTP** in the **Parameter** field and the **<** in the **Operator** field.
4. In the **Less than** field, type 2000.
5. Click **Apply** to insert the expression into the highlighted set of parentheses. The compound test now looks like the following:

((inboundReceivedHTTP > 1000.0) AND (inboundReceivedHTTP < 2000))

This test evaluates to true when the specified value in the **inboundReceivedHTTP** process is greater than 1000, and less than 2000. If the threshold is exceeded, the test triggers an action for restarting the process and notifying the system administrator. For more information, see [Defining Actions](#).

6. Click **OK** to save the test, or **Undo** to cancel the last change.

Using Advanced Test Features

A test includes the test expression, such as **inboundReceivedHTTP > 10** and any extra conditions, for example, counters, timers and additional tests. These advanced options add extra requirements for a test to be evaluated as true or false.

**Note**

These instructions begin in the Test Editor window. For instructions on accessing this window, see [Defining Tests](#).

To access advanced test options, see Using Advanced Test Features in *TIBCO Hawk Administrator's Guide* for more details.

Defining Actions

Each test has one or more related actions. An action is the consequence of a rule, such as an alert message or a custom script. Whenever the rule receives information from its data source, tests are evaluated. If a test evaluates to true, the related actions are triggered. Once triggered, actions are performed unless advanced options delay or prevent the action.

Creating an Alert Message with Variable Substitution

The following example shows how to create an alert message with variable substitution as a representative action.

**Note**

These instructions begin in the Test Editor window. For instructions on accessing this window, see [Defining Tests](#).

To define an action, perform the following steps:

1. Click **Create** on the toolbar.
2. Select a type from the **Action Type** area: **Alert**, **Execute**, **Notification**, **Method**, **Email**, and **Post Condition**.

These types correspond to the TIBCO Hawk action types, see *Creating an Alert Message with Variable Substitution* in *TIBCO Hawk Administrator's Guide* for more details.

3. In the **Message** field, type the following:

Gateway Service: http, inbound received:

4. You can insert an internal variable, an external variable, or a data source.



Note

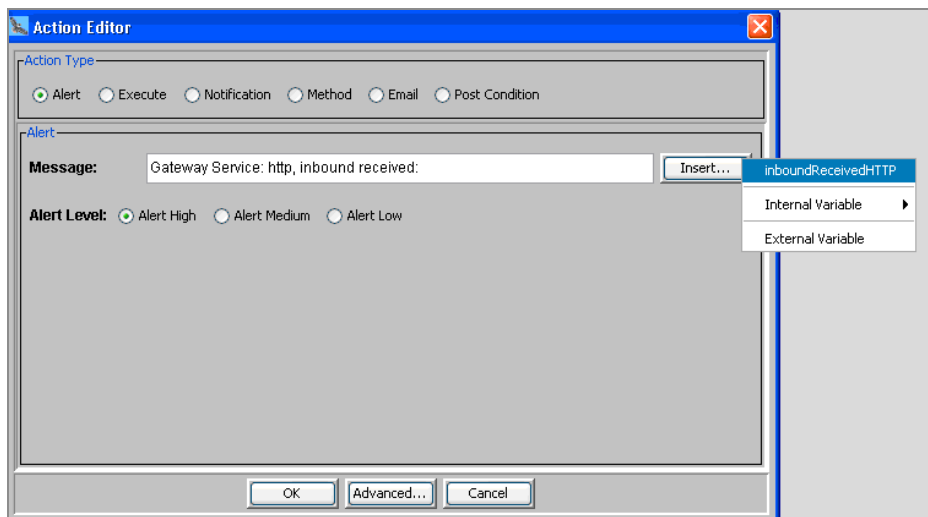
Substituting variables in string fields is supported for all action types except Post Condition.

- To insert an internal variable, right-click **Insert** and select **Internal Variable**.
Internal variables available in the Agent Menu are:

• Agent Name	• Current RuleBase	• Current Rule
• Current Test	• Current Action	• Condition True Time

- To insert an *external variable*, right-click **Insert** and select **External Variable**.
`${External.<var name>}` is inserted in the active string field. Replace `<var name>` in the syntax string with the name of the external variable defined in the properties file.
External variables are obtained from the variable file specified in the `-variable` option for the rulebase engine (suboption of `-M RuleBaseEngine`) when the agent is started.
- To insert a *data source variable* in a string argument, select a variable name from the menu.

Figure 55: Creating an Alert Message



Variable syntax is added to the string field at the cursor location. The syntax does not require modification. You can also manually type the syntax `${<return-field-name>}` in the string field for an action, where *return-field-name* is the label for a value returned by the method. The microagent method that returns this field must be the data source for the current rule.

**Note**

You can get more information for specific method return fields by viewing descriptive help text for the method in the Microagents, Methods and Arguments dialog. For instructions on accessing this window, see [Specifying a Data Source](#).

5. Click **OK**.

Using Advanced Action Features

Advanced action options add flexibility in timing when an action is performed. For example, using advanced options you can automate problem escalation procedures.

See "Using Advanced Action Features" in *TIBCO Hawk Administrator's Guide* for more details.

Saving a Rulebase

Once the creation of the rulebase is complete, there are several options for you to consider. The option you choose depends on the agent configuration mode.

See "Saving a Rulebase" in *TIBCO Hawk Administrator's Guide* for more details.

Working with Rulebase Files

When a TIBCO Hawk agent uses a rulebase in memory, the rulebase object consists of a hierarchy of linked objects describing rules and their data sources, tests and actions.

Rulebase information can also be stored in a disk file with a .hrb extension. When you save a rulebase file, this information is encoded into text.

See "Working with Rulebase Files" in *TIBCO Hawk Administrator's Guide* for more details.

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

Documentation for TIBCO BusinessConnect™ is available on the [TIBCO BusinessConnect™ Product Documentation](#) page.

To directly access documentation for this product, double-click the following file:

`TIBCO_HOME/release_notes/TIB_bc_7.4.0_docinfo.html` where `TIBCO_HOME` is the top-level directory in which TIBCO products are installed. On Windows, the default `TIBCO_HOME` is `C:\tibco`. On UNIX systems, the default `TIBCO_HOME` is `/opt/tibco`.

The following documents for this product can be found in the TIBCO Documentation site:

- *TIBCO BusinessConnect™ Installation and Configuration*
- *TIBCO BusinessConnect™ Concepts*
- *TIBCO BusinessConnect™ Interior Server Administration*
- *TIBCO BusinessConnect™ Gateway Server Administration*
- *TIBCO BusinessConnect™ Training Partner Administration Guide*
- *TIBCO BusinessConnect™ Scripting Deployment User Guide*
- *TIBCO BusinessConnect™ Release Notes*

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

SOME TIBCO SOFTWARE EMBEDS OR BUNDLES OTHER TIBCO SOFTWARE. USE OF SUCH EMBEDDED OR BUNDLED TIBCO SOFTWARE IS SOLELY TO ENABLE THE FUNCTIONALITY (OR PROVIDE LIMITED ADD-ON FUNCTIONALITY) OF THE LICENSED TIBCO SOFTWARE. THE EMBEDDED OR BUNDLED SOFTWARE IS NOT LICENSED TO BE USED OR ACCESSED BY ANY OTHER TIBCO SOFTWARE OR FOR ANY OTHER PURPOSE.

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

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

TIBCO, the TIBCO logo, the TIBCO O logo, ActiveMatrix BusinessWorks, TIBCO Administrator, TIBCO Designer, Hawk, Rendezvous, and TIBCO Runtime Agent are either registered trademarks or trademarks of Cloud Software Group, Inc. in the United States and/or other countries.

Java and all Java based trademarks and logos are trademarks or registered trademarks of Oracle and/or its affiliates.

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

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

All other product and company names and marks mentioned in this document are the property of their respective owners and are mentioned for identification purposes only.

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

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

THIS DOCUMENT COULD INCLUDE TECHNICAL INACCURACIES OR TYPOGRAPHICAL ERRORS. CHANGES ARE PERIODICALLY ADDED TO THE INFORMATION HEREIN; THESE CHANGES WILL BE INCORPORATED IN NEW EDITIONS OF THIS DOCUMENT. CLOUD SOFTWARE GROUP, INC. MAY MAKE IMPROVEMENTS AND/OR CHANGES IN THE PRODUCT(S) AND/OR THE PROGRAM(S) DESCRIBED IN THIS DOCUMENT AT ANY TIME.

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

This and other products of Cloud Software Group, Inc. may be covered by registered patents. Please refer to TIBCO's Virtual Patent Marking document (<https://www.tibco.com/patents>) for details.

Copyright © 2001-2023. Cloud Software Group, Inc. All Rights Reserved.