



TIBCO BusinessConnect™

Concepts

Version 7.3.0
April 2022



Contents

Figures	vi
Tables	viii
Chapter 1 Introduction	1
Product Overview	2
Deploying TIBCO BusinessConnect and Protocols	4
Chapter 2 TIBCO BusinessConnect Architecture	5
TIBCO BusinessConnect Installation	6
Interior Server and Gateway Server Architecture	8
TIBCO BusinessConnect Interior Server	8
TIBCO BusinessConnect Gateway Server	9
Interior and Gateway Server Communication	10
Private Processes	12
TIBCO Rendezvous	12
JMS Transport	15
Relationship Between Private and Public Processes	19
TIBCO BusinessConnect Participants and Business Agreements	20
Participants	20
Business Agreements	20
Operations	21
Business Protocols	21
Schemas	23
System Configuration	25
Database Connections	25
Proxy Servers	26
Visibility	27
TIBCO BusinessConnect Visibility via tibbr	27
TIBCO BusinessConnect Visibility via TIBCO BusinessEvents	28
Application Monitoring and Management via TIBCO Hawk	31
Chapter 3 Server Management Overview	33
Using TIBCO Administrator	34

Using TIBCO ActiveMatrix BusinessWorks	37
Using TIBCO Designer	39
Chapter 4 TIBCO BusinessConnect User Management	41
Overview	42
TIBCO Administrator User Management	43
TIBCO Administrator User Access Rights	43
TIBCO BusinessConnect User Management	45
Participants Access Rights	45
Business Agreements Access Rights	46
Default Access Rights	46
TIBCO BusinessConnect Users	47
TIBCO BusinessConnect Group Management	51
TIBCO Administrator Roles	51
TIBCO BusinessConnect Groups	52
Chapter 5 TIBCO BusinessConnect Transports and Protocols	55
Transports	56
Public Transports	56
TIBCO Implementation of AS Standards	58
SSHFTP Implementation in TIBCO BusinessConnect	58
Protocols	60
Chapter 6 Fault Tolerance and Load Balancing	61
Overview	62
Fault Tolerance and Load Balancing for the Interior Server	63
Fault Tolerance for the Interior Server	63
Load Balancing and Public Smart Routing for the Interior Server	64
Configuring the Interior Server	64
Chapter 7 Smart Routing	65
Overview	66
Private Process Smart Routing	67
Configuring Private Process Smart Routing	67
Public Smart Routing	69
Distributing Workload Among Engines	70
Processing of Inbound Documents	70
Routing Messages to the Designated Clusters	72
Defining Rules for Public Smart Routing	73
Server Groups and Clusters	74

Chapter 8 Security	.77
Overview	.78
Secure Data	.78
Secure Communication	.79
Public and Private Keys	.80
Digital Certificates	.81
Using Certificates with TIBCO BusinessConnect	.82
Shadow Credentials	.84
Digital Signatures	.86
Encryption	.87
Digest Algorithms	.88
Encryption Algorithms	.88
Supported SSHFTP Ciphers	.90
Cipher Suites	.92
Non-Repudiation	.95
Non-Repudiation Logging Scenarios in TIBCO BusinessConnect	.95
SSHFTP Support in TIBCO BusinessConnect	.98
Authentication Methods for SSHFTP	.98
Selecting Algorithms and Methods during Tunnel Negotiation	.99
Glossary	.101
Index	.111
TIBCO Product Documentation and Support Services	.115
How to Access TIBCO Documentation	.115
How to Contact TIBCO Support	.117
How to Join TIBCO Community	.117
Legal and Third-Party Notices	.118

Figures

Figure 1	TIBCO BusinessConnect Installed and Deployed on One Machine	4
Figure 2	Installing and Deploying a Protocol	4
Figure 3	TIBCO BusinessConnect Components	6
Figure 4	Gateway and Interior Server Communication	8
Figure 5	Secure JMS Transport Diagram.	17
Figure 6	TIBCO BusinessConnect Private and Public Processes	19
Figure 7	TIBCO Administrator, Application Management Console	34
Figure 8	TIBCO Administrator, TIBCO BusinessConnect Console	35
Figure 9	TIBCO ActiveMatrix BusinessWorks Communicating with TIBCO BusinessConnect	37
Figure 10	TIBCO Designer.	39
Figure 11	TIBCO Administrator Super User.	44
Figure 12	TIBCO BusinessConnect Super User	49
Figure 13	Physical Location of Public Transports	56
Figure 14	Inbound Public Transport Types	57
Figure 15	SSHFTP Tunnels	59
Figure 16	Interior Server: Load Balancing and Fault Tolerance.	63
Figure 17	Smart Routing	68
Figure 18	Message Queues and Clusters	72
Figure 19	Server Group Assignment	75

Tables

Table 1	The aeRvMsg Format.	14
Table 2	TIBCO BusinessConnect Message Types	29
Table 3	Access Right Mapping for BusinessConnect User Management.	46
Table 4	TIBCO Administrator User Role Assignments	47
Table 5	User Access for a User Belonging to Two Roles	51
Table 6	User with Default Access Rights	52
Table 7	Type of Credentials Used During Different Periods	85

Chapter 1 **Introduction**

This chapter provides a broad introduction to TIBCO BusinessConnect™ architecture, components, and various usage and deployment scenarios. It also explains the basic business and transport protocols used with BusinessConnect™.

Topics

- [Product Overview, page 2](#)
- [Deploying TIBCO BusinessConnect and Protocols, page 4](#)

Product Overview

TIBCO BusinessConnect is a business-to-business (B2B) gateway that your company can use to engage in electronic commerce with your partners. It enables secure transmission of documents and messages between partners using disparate internal business systems.

TIBCO BusinessConnect supports multiple protocols (also called standards) for electronic commerce, such as TIBCO BusinessConnect™ EDI Protocol powered by Instream®, TIBCO BusinessConnect™ RosettaNet Protocol, and TIBCO BusinessConnect™ SOAP Protocol.

TIBCO BusinessConnect includes the following major features:

- TIBCO BusinessConnect Server engine, which handles transport, messaging, and business message content.
- User access control, where administrative users can set the access control permissions of other users. Access controls can be used to restrict which trading partner information a user can access in the administration interface.
- Trading partner management system and certificate store.
- Non-repudiation database.
- Audit log database.
- TIBCO BusinessConnect Palette for TIBCO ActiveMatrix BusinessWorks.
- Enhanced reporting, using an export interface for repository log and audit data for use by the external reporting system.
- Integration with TIBCO JasperReports. Dashboard - a single screen that captures your transaction data into different charts. Charts such as, Transaction Count, Transaction Trends, and Transaction Details help you gain insights into your transaction data in real time. You can create custom Audit reports and Configuration Store reports independently or combine them with existing predefined reports. You can also create drill-down reports using custom report functionality by creating independent reports and by adding predefined filters to them. In addition to this, other features like deep linking functionality, import/export JasperReports configurations to *.csx file are implemented in TIBCO BusinessConnect.
- Creation of new custom Audit reports by querying the transaction data whereas Configuration Store reports by querying the configuration data. JasperPoller is used to extract the configuration data and store it as key-value pairs in new tables introduced for use by JasperReports. Also a predefined set of filters are made available in TIBCO BusinessConnect which can be selected while generating custom reports.

- Integration with TIBCO BusinessEvents, tibbr, and TIBCO Hawk. This integration allows TIBCO BusinessConnect to publish critical information about the health of its installation and the state of transactions to these other TIBCO products. Administrative users of TIBCO BusinessConnect and TIBCO BusinessEvents, tibbr, and TIBCO Hawk can gain greater, real-time insight into the TIBCO BusinessConnect implementation.
- Ability to receive emails from multiple email servers.
- SSO implementation using OAuth 2.0 for accessing TIBCO BusinessConnect client applications: TIBCO BusinessConnect™ Trading Community Management and TIBCO PartnerExpress™

TIBCO BusinessConnect uses TIBCO Administrator as its graphical user interface, making it especially familiar and easy-to-use for existing TIBCO customers.

Business agreements, an essential component of any B2B implementation, can be easily constructed with TIBCO BusinessConnect. A business agreement defines the protocol or protocols that you use to exchange documents with your partner. It defines the transport method, for example, HTTPS or email, and the operations that each partner is allowed to transact.

An operation is the sending or receiving of a business document. Each operation is associated with the type of the exchanged document, the information needed to process, receive, and send the document.

When you set up operations at the system level for use with multiple partners, TIBCO BusinessConnect gives you the flexibility to override individual aspects of an operation as needed for specific partners.

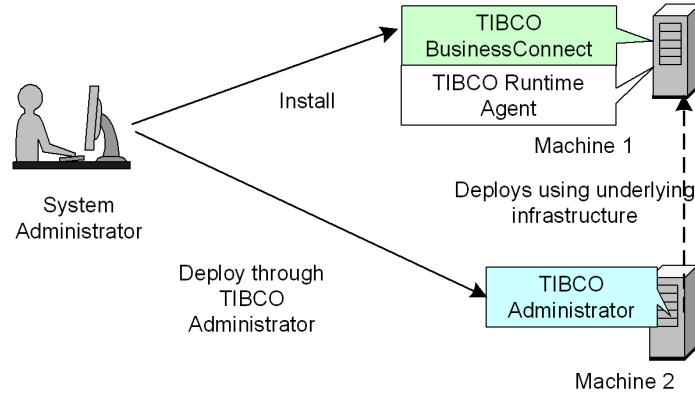
Local hosts and remote partners are both participants with very similar requirements in terms of identifying information and technical specifications. For example, in configuring both types of participants, you have to provide information about locations, contacts, available protocols, and security credentials. For ease of use, TIBCO BusinessConnect makes smart distinctions between the two in the user interface.

Deploying TIBCO BusinessConnect and Protocols

To install and deploy TIBCO BusinessConnect and protocols:

1. Install TIBCO BusinessConnect on the machine where TIBCO Runtime Agent was previously installed.

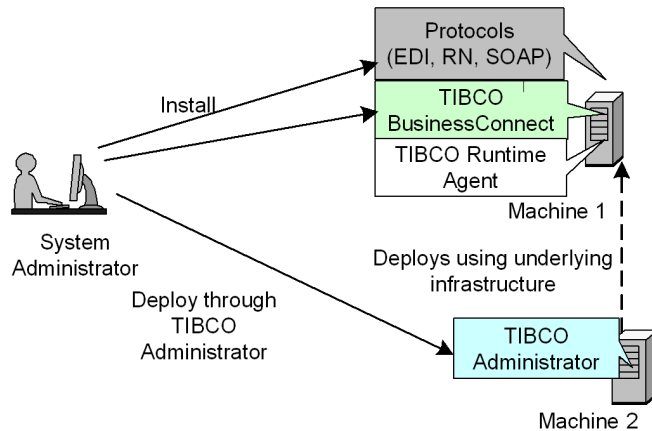
Figure 1 TIBCO BusinessConnect Installed and Deployed on One Machine



Configure TIBCO BusinessConnect and deploy it.

2. Install any of the supported protocols on the machine where TIBCO BusinessConnect was previously installed.

Figure 2 Installing and Deploying a Protocol



After the protocol is installed, it gets deployed through TIBCO Administrator. Installation of supported protocols is explained in the product documentation for each protocol.

Chapter 2

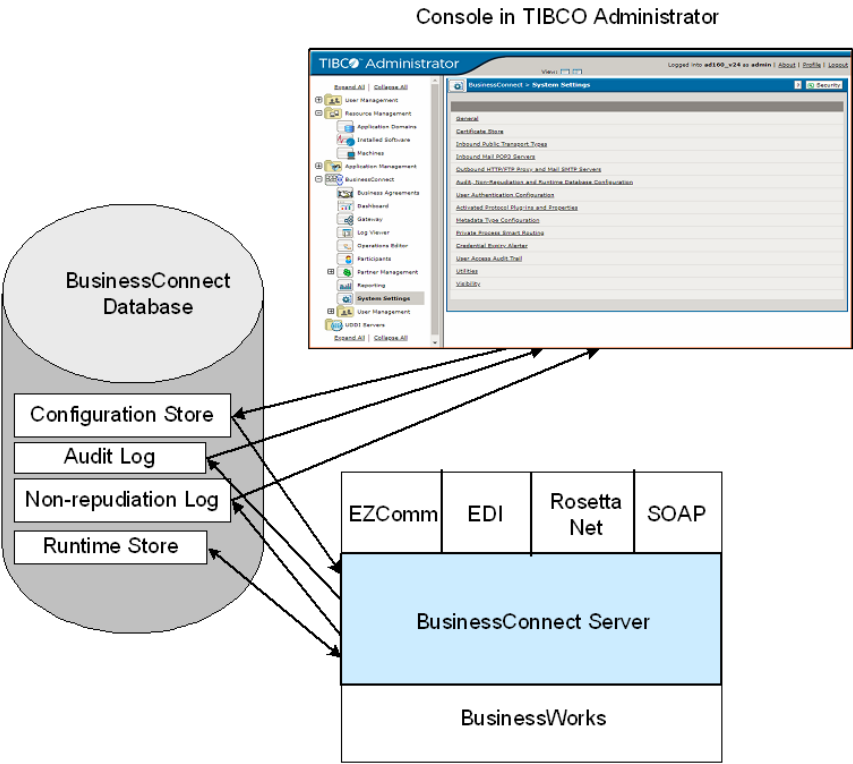
TIBCO BusinessConnect ArchitectureTopics

- [TIBCO BusinessConnect Installation, page 6](#)
- [Interior Server and Gateway Server Architecture, page 8](#)
- [Private Processes, page 12](#)
- [Relationship Between Private and Public Processes, page 19](#)
- [TIBCO BusinessConnect Participants and Business Agreements, page 20](#)
- [Operations, page 21](#)
- [System Configuration, page 25](#)
- [Visibility, page 27](#)

TIBCO BusinessConnect Installation

Before starting the TIBCO BusinessConnect installation, you have to understand the components comprising the TIBCO BusinessConnect architecture and how they interact.

Figure 3 TIBCO BusinessConnect Components



In Figure 3, you can see three components:

- **TIBCO BusinessConnect server** This is a runtime engine that provides services to the TIBCO BusinessConnect protocols. The protocols are responsible for the primary TIBCO BusinessConnect functionality, which is processing B2B transactions.

The runnable version of the TIBCO BusinessConnect server is a TIBCO ActiveMatrix BusinessWorks application, and it is created when you deploy it on the Interior Server. See *TIBCO BusinessConnect Interior Server Administration*.

- **TIBCO BusinessConnect database** This database contains the following information:
 - Configuration information used by TIBCO BusinessConnect protocols



The complete configuration information and guidelines are stored in the configuration store, TIBCO BusinessConnect database.

- Data log created by TIBCO BusinessConnect protocols
 - Runtime data used by the TIBCO BusinessConnect server and protocols

TIBCO BusinessConnect database configuration and table creation are explained in *TIBCO BusinessConnect Installation and Configuration*, "Initializing a Database."
- **TIBCO BusinessConnect console in TIBCO Administrator** This console is used by administrators to do the following operations:
 - Create the TIBCO BusinessConnect database
 - Configure participants and business agreements
 - View data logs created by TIBCO BusinessConnect protocols

Interior Server and Gateway Server Architecture

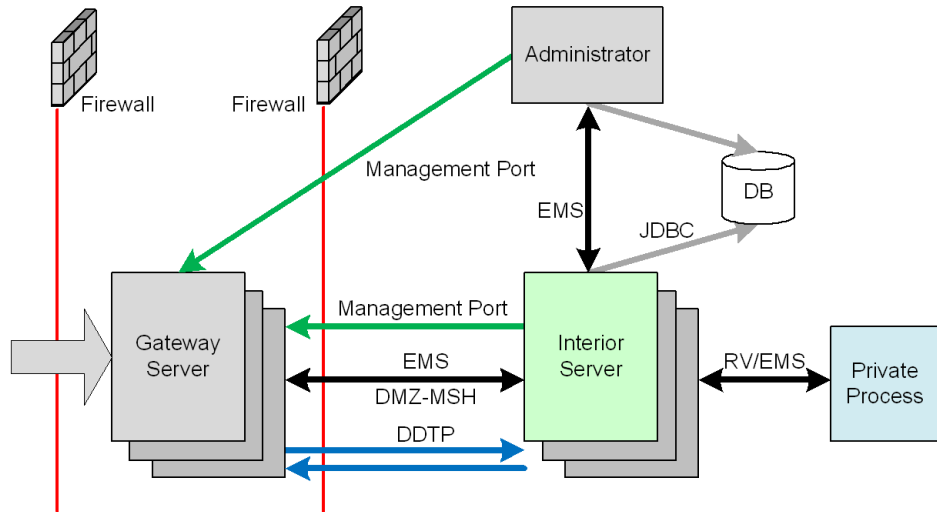
TIBCO BusinessConnect Interior Server is the server on which TIBCO BusinessConnect is installed on top of the other required TIBCO software products: TIBCO Runtime Agent, and TIBCO Administrator.

Multiple Interior Servers can work as a cluster to achieve load balancing and fault tolerance. For a list of all required TIBCO and other third party software products, see *TIBCO BusinessConnect Installation and Configuration*, Installation Requirements.

TIBCO BusinessConnect Gateway Server is located in the demilitarized zone (DMZ), and functions as the front gate by receiving the inbound transactions from trading partners. It is installed on its own, and does not rely on TIBCO Runtime Agent or TIBCO Administrator. Multiple Gateway Servers can work together for load balancing.

Figure 4 depicts a diagram of the Gateway Server and Interior Server communications.

Figure 4 Gateway and Interior Server Communication



TIBCO BusinessConnect Interior Server

This server is located inside the company's firewall and performs the following tasks:

- Handles all messaging level activities, such as message packaging and unpacking, encryption and decryption, signature and verification, and so on, according to numerous transport and vertical business standards.
- Takes care of business level logic to be executed by each individual protocol, such as document schema validation, EDI data conversion, batching, business level acknowledgment generation, and so on.

TIBCO BusinessConnect Gateway Server

TIBCO BusinessConnect Gateway Server is located in the demilitarized zone (DMZ), and can have several restrictions on the networks it can access.

It is used to host various gateway services such as HTTP/S, FTP/S, SSHFTP, and so on, to receive B2B communications directly from the Internet with security features such as SSL and SSH. The firewall between the Gateway Server and the rest of your system protects against the threat of malicious communications.

TIBCO BusinessConnect Gateway Server is a standalone Java executable that is not dependent either on TIBCO ActiveMatrix BusinessWorks or on TIBCO Runtime Agent installation; however, it still needs TIBCO Enterprise Message Service to communicate with the Interior Server. The Gateway Server can host several components:

- **File Service** This server provides a central location on your network where you can store and share files.
- **HTTP Service** This server supports HTTP, HTTPS, and HTTPSCA transports for document exchange.
- **PartnerExpress Service** This server provides a secure web-based access for trading partners, so that the external users associated with these trading partners can log in and perform simple file uploads and downloads.
- **FTP Service** With this server, the external users running an FTP Client can connect to the host site, and perform simple file uploading and downloading.
- **TCM Service** This server provides a web browser interface for trading partners to manage their exchange profiles, and assists the trading host in serving the partners in the trading community. All services are provided through a browser-based interface that allows partners to self-register, modify their profiles, and receive alerts about security and transport updates.
- **SSHFTP Service** With this server, the external users running an SSHFTP Client can connect to the host site, and perform simple file uploading and downloading.

Interior and Gateway Server Communication

Three types of communication are used between the Gateway and Interior Servers: JMX, DMZ Data Transfer Protocol (DDTP), and TIBCO Enterprise Message Service.

JMX Communication

The management of the Gateway Server is performed by using the JMX management protocol.

On the Gateway Server side, the JMX management port is opened for receiving management instructions from either TIBCO Administrator or TIBCO BusinessConnect Interior Servers. The JMX management port is configurable in TIBCO Administrator when you create the Gateway Server token; the default value is 11000.

JMX communication is used between TIBCO Administrator and the Gateway Servers. When a Gateway Server is started for the first time, an empty service container is started without any gateway services running on it; you can assign Gateway service instances to each Gateway Servers and start them, such as HTTP, FILE, SSHFTP, FTPS, FTP, TCM, and PX, from TIBCO Administrator GUI remotely. Therefore, you do not have to physically access the Gateway Server machines located in the DMZ.

JMX communication is also used between the Interior Servers and Gateway Servers. When an empty Gateway Server container is started, it first publishes a TIBCO Enterprise Message Service message with information about its JMX management port. The Interior Servers listen to the message, and then the JMX communication is established. Examples of the Gateway Server management by Interior Servers include monitoring the Gateway Servers heartbeats; automatically restarting Gateway service instances, such as SFTP, FTPS, HTTPS, and so on, when a Gateway Server is restarted.

DDTP

DDTP is designed for transferring large size messages between Gateway Servers and Interior Servers.

When the inbound message size exceeds the value of the **Data Streaming Threshold** field configurable on each gateway service's (such as HTTPS, PX, FTPS, and so on) transport configuration, the message data is transferred by using the DDTP transport rather than by using the TIBCO Enterprise Message Service transport.

The DDTP port is opened on the Gateway Servers side waiting for connections from Interior Servers. When a large message comes in from the trading partner side, the Gateway Server publishes TIBCO Enterprise Message Service messages to Interior Servers, with information about the message identification and the DDTP port on which the Gateway Server is waiting for connections. The Interior Server that receives the TIBCO Enterprise Message Service messages initiates a DDTP connection to the Gateway Server and brings back the large message data. By using DDTP, the data is transferred from a DMZ to the interior network in a secure way, without the need of opening a port from the interior network.

The DDTP port, also called Data Port, is also configurable in TIBCO Administrator when you create a Gateway Server token. The default value is 12000.

TIBCO Enterprise Message Service Communication

As described earlier in this section, the TIBCO Enterprise Message Service transport is used between the Gateway Server and Interior Server for many purposes, such as the initial notifications when a Gateway Server is started, and the notification when a large message arrives from trading partners.

Besides this, TIBCO Enterprise Message Service is also used for transferring configurations necessary for starting the gateway services, such as the HTTPS server keys and so on. TIBCO Enterprise Message Service is also used for transferring small size messages between the Gateway Server and Interior Server. The load balancing feature of TIBCO Enterprise Message Service is leveraged by Interior Servers, so the inbound traffic is load balanced between these servers.

Private Processes

Private processes in TIBCO BusinessConnect refer to the internal processes within your company. Private processes send data to the TIBCO BusinessConnect server or receive data from the TIBCO BusinessConnect server, and communicate using TIBCO Rendezvous (Rendezvous Certified Messaging (RVCN) or JMS.

TIBCO Rendezvous

TIBCO Rendezvous subject names, the aeRvMsg message format, and Rendezvous Certified Messaging (RVCN) are described in the following sections.

TIBCO Rendezvous Subject Names

All TIBCO Rendezvous messages have a unique subject name. This applies to interactions on both the Initiator and Responder side.

The following are the subject name formats:

- Request from Initiator's private process to the local TIBCO BusinessConnect:
Property name: `requestFromPPSubject=prefix.installation.standardID.fixed`
Example: `AX.BC.BC-ACME.EZComm.INITIATOR.REQUEST`
- Response to Initiator's private process from the local TIBCO BusinessConnect:
Property name: `responseToPPSubject=prefix.installation.standardID.fixed`
Example: `AX.BC.BC-ACME.EZComm.INITIATOR.RESPONSE`
- Request to a Responder's private process from the local TIBCO BusinessConnect:
Property name: `requestToPPSubject=prefix.installation.standardID.fixed`
Example: `AX.BC.BC-ACME.EZComm.RESPONDER.REQUEST`
- Response from Responder's private process to the local TIBCO BusinessConnect:
Property name: `responseFromPPSubject=prefix.installation.standardID.fixed`
Example: `AX.BC.BC-ACME.EZComm.RESPONDER.RESPONSE`
- Acknowledgment of receipt of asynchronous request/response message:
Property name: `ackToPPSubject=prefix.installation.standardID.fixed`
Example: `AX.BC.BC-ACME.EZComm.RESPONDER.ACK`
- Error notification:
Property name: `errorNotifySubject=prefix.installation.standardID.fixed`

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

TIBCO Rendezvous publishes this message globally, but a private process can also listen to it.



Not all of these subjects are available with all protocols.

Refer to the individual protocols guide for a detailed set of supported subjects, explanations, and structure.

The following is a key to the italicized terms above:

- *prefix*: The product or domain name. The default is AX . BC. This refers to TIBCO BusinessConnect (BC) on TIBCO ActiveExchange (AX). The installation and the prefix uniquely identify messages exchanged between an external private process and TIBCO BusinessConnect.

This is displayed in the **Installation Prefix** field under **BusinessConnect > System Settings > General**. For example, AX . BC.

- *installation*: The installation name. This is displayed in the **Installation Name** field under **BusinessConnect > System Settings > General**. For example, BC-ACME.
- *standardID*: The business protocol. For example, EZComm.
- *fixed*: TIBCO BusinessConnect determines this internally depending on the type of message. The following are the only possible values:
 - INITIATOR . REQUEST
 - RESPONDER . REQUEST
 - RESPONDER . RESPONSE
 - INITIATOR . RESPONSE
 - RESPONDER . ACK
 - ERROR

aeRvMsg Message Format

Messaging between private processes and TIBCO BusinessConnect uses the aeRvMsg format. The aeRvMsg message format is the TIBCO BusinessConnect standard message format. This section provides a brief overview of aeRvMsg. For more information on aeRvMsg, see *TIBCO Adapter SDK Concepts*.

When a private process or TIBCO BusinessConnect uses the aeRvMsg format to package data before sending the data to each other, the data is packaged in an envelope called the message control block. The ^pfmt^, ^ver^, and ^type^ message control block tags allow these components do extra validation on messages.

The aeRvMsg format is shown in [Table 1](#):

Table 1 The aeRvMsg Format

Type	Control Data Tag Name	Description	Value
TIBRVMSG_INT	^pfmt^	Package format	Constant value: 10
TIBRVMSG_INT	^ver^	Version of the TIBCO ActiveExchange message format. In this case, version 3.0 is needed (value=30).	Constant value: 30
TIBRVMSG_INT	^type^	How the payload in the ^data^ tag is packed. The value 1 is reserved for “AE wire format” with nested TIBCO Rendezvous messages. The value 10 is reserved for XML, in which the data is an XML string.	Constant value: 1
TIBRVMSG_RVMSG	^data^	Payload. The message that the private process or TIBCO BusinessConnect is packaging and sending.	

In this message format, the ^pfmt^, ^ver^, and ^type^ tags precede the message, which is carried in the ^data^ tag. In turn, within the ^data^ tag, the actual data is carried in the request or response field.

Rendezvous Certified Messaging (RVCM)

When an internal application, such as an ERP system, generates a document (request, acceptance, or notify), the private process translates the raw Rendezvous message in an appropriate format and forwards it to the TIBCO BusinessConnect server.

The TIBCO BusinessConnect server, in active state and running, waits for any RVCN message that will arrive on the subject name on which it is listening. After the message is received, the server expects it to conform to a certain structure. Therefore, it is the job of the private process to send a message in a proper format so that the server can process it; it is also the job of the private process to receive a RVCN message from the server and process it accordingly.

For more information about RVCN, please refer to the TIBCO Rendezvous documentation about Distributed Queues and Certified Messaging.

JMS Transport

JMS message format and secure JMS transport are described in the following sections.

JMS Message Format

JMS messages consist of several properties and header fields that help a processing agent, such as TIBCO BusinessConnect Palette, to dispatch the messages to the corresponding listeners. The destination of the messages is: *PREFIX.INSTALLATION.MESSAGE_TYPE_SPECIFIC_SUFFIX*. For example, *AX.BC.MYSERVER.RESPONDER.REQUEST*

Notice the following differences compared to TIBCO Rendezvous:

- **Subject names** JMS destinations are not accompanied with the business protocol name. The suffixes are identical to the corresponding TIBCO Rendezvous message suffixes. Regarding the several different types of miscellaneous messages, the documentation of the individual business protocols provides more details.
- The header and property fields are as follows:
 - **JMSType** Mandatory. The format is *<the name of the business protocol>*. It is defined as *standardID* in the AE messages encoded by TIBCO Rendezvous.
 - **JMSCorrelationID** Mandatory. It is either *global*, or the *correlationID* from the published Responder request message that was expecting a synchronous response.
 - **operationID** Mandatory. This is the operation name of the business message, such as *BC/1.0/Notify*.
 - **smartID** Optional. It only exists in messages sent from the TIBCO BusinessConnect server towards the private process. If Smart Routing is configured and the incoming message is smart routed, the *smartID* value is the Smart Routing ID that has been determined by the TIBCO

BusinessConnect server during the message processing through the Private Process Smart Routing.

- The payload (JMS message body), such as the AE message, is transferred as a serialized `java.util.HashMap` instance. This instance carries the names of the AE message fields in its key and the corresponding values in their values. The JMS-encoded message type is `javax.jms.Object Message`.

JMS Transport Types Used for Various Messages

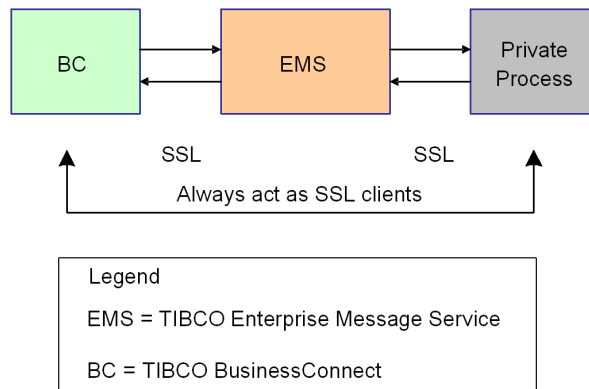
Messages use the following JMS transport types:

- Messages that carry either notifications, requests, or responses use the JMS queue transport type.
See messages sent on destinations with suffixes `INITIATOR.REQUEST`, `INITIATOR.RESPONSE`, `RESPONDER.REQUEST`, and `RESPONDER.RESPONSE`.
- Miscellaneous messages, such as error advisories with the suffix `ERROR`, use a JMS topic transport type, except for the `RESPONDER.ACK` advisory which uses a JMS queue transport type.

This behavior has the potential to be overridden by individual business protocols; if it is not specifically mentioned, the explained behavior should be assumed.

Secure JMS Transport

Figure 5 Secure JMS Transport Diagram



The secure JMS transport is closely integrated with the existing JMS transport on both the TIBCO BusinessConnect server and the private process side.

Generally, the capabilities are considered identical to those offered by TIBCO Enterprise Message Service.

The transport utilizes the SSL transport to provide security services (two-way authentication, integrity, and confidentiality) to the business layer. It is assumed that the secure transport configuration on the TIBCO Enterprise Message Service provider has been done prior to using the server and the palette where the secure JMS transport is configured.



Secure JMS transport can only be used with TIBCO Enterprise Message Service as the JMS provider.

To configure the secure JMS transport for TIBCO BusinessConnect, see *TIBCO BusinessConnect Interior Server Administration Guide*, JMS Transport.

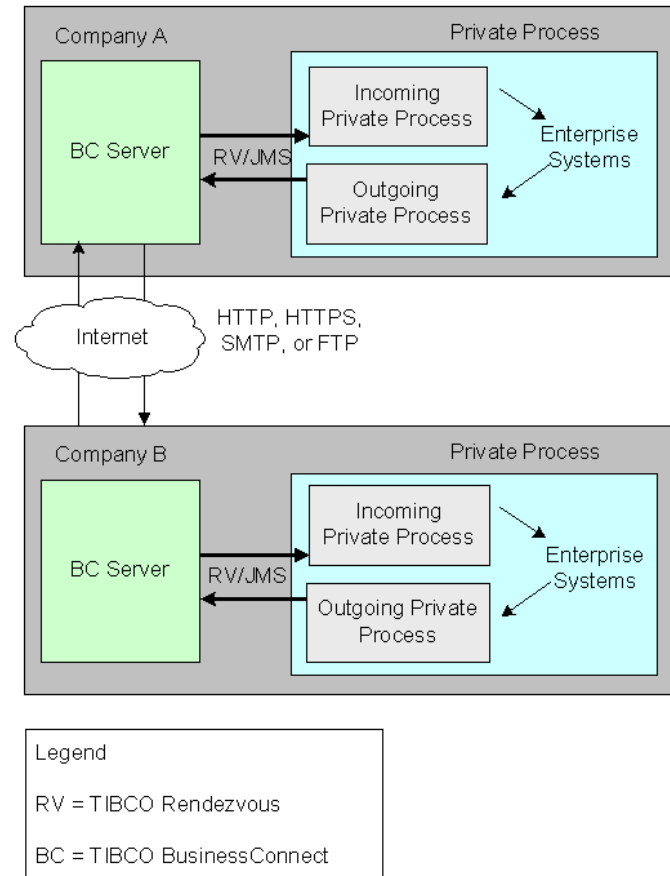
For more guidelines on configuring secure JMS on TIBCO Enterprise Message Service, refer to *TIBCO Enterprise Message Service User's Guide*, Using the SSL Protocol.

In addition to these sources, details on the client side configuration concepts are available in *TIBCO ActiveMatrix BusinessWorks Palette Reference*, JMS Palette.

Relationship Between Private and Public Processes

Figure 6 shows a diagram that explains the relationship between public and private processes in a company using a TIBCO BusinessConnect server.

Figure 6 TIBCO BusinessConnect Private and Public Processes



You can use TIBCO ActiveMatrix BusinessWorks to build these private processes, specifically using the tool TIBCO Designer, which is installed with TIBCO Runtime Agent. To learn more about working with this tool, [Using TIBCO Designer](#).

TIBCO BusinessConnect Participants and Business Agreements

TIBCO BusinessConnect participants and business agreements are described in the following parts.

Participants

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.

A participant profile details the basic identifying information for a host or partner and the required technical and security-related information.

Participant profiles include information about business agreements; participant type (host or partner); business locations including contacts; security credentials; and business protocols.

For more information on how to manage participants in TIBCO BusinessConnect, see *TIBCO BusinessConnect Trading Partner Administration, Participants*.

Business Agreements

A business agreement details all of the information on which you and your partner must agree before you can exchange business documents with each other. Agreements revolve in large part around the chosen protocols.

Each participant lists the protocols that are available for use by that participant. TIBCO BusinessConnect determines for you which protocols two participants have in common.

For each protocol enabled for document exchange between the two participants, the following protocol-specific information is required: transport method, valid operations, and security.

For more information on how to manage business agreements in TIBCO BusinessConnect, see *TIBCO BusinessConnect Trading Partner Administration, Business Agreements*.

Operations

An operation, also called transaction, transmission, message, or message type, is the submitting of an electronic document to a partner. An important part of preparing TIBCO BusinessConnect for deployment is to define all operations that are valid for this B2B gateway. For example, a typical B2B implementation allows purchase order, invoice, and receipt operations. Operations require detailed definitions.

An operation definition is comprised of the following information:

- **Name** A name for the operation.
- **Protocol** The business protocol to be used to create the schema and carry out the transaction. For more information about protocols, see [Business Protocols](#).
- **Schema** Defines what TIBCO BusinessConnect can expect and what it needs to do with the information it receives. For more information on schema validation, see [Schemas](#).

Business Protocols

Business protocols provide a set of standards for use in defining both the content of electronic business documents and the operations, or technical tasks, required to carry out the transaction. Both parties to a transaction must use the same business protocol; otherwise, the recipient of the document will not be able to process it electronically. Participants identify which business protocols are available for use by that participant.

When you create a business agreement, TIBCO BusinessConnect presents a list of business protocols that are common to both parties.

A business protocol defines a set of behaviors and rules that trading partners agree on before exchanging business documents over the Internet. Through the sharing of a common protocol beforehand, trading partners can simplify their e-commerce transactions. The following is the anatomy of a business protocol:

- **Process** Definition of a high-level business process. This is the business logic for message sequence, decisions, and roles for each trading partner in a transaction. Technical details are not addressed.
- **Vocabulary and Data Dictionary** The technical aspects of creating a business message involve using vocabulary and data dictionary standards.
 - The vocabulary describes the structure and lists the elements in a message. This enables recipients to parse and validate XML and other types of message content. A vocabulary can be defined in a .dtd or .xsd file.

- Like a vocabulary, a data dictionary defines the structure and lists the elements in a message. However, a data dictionary can also define valid values for certain elements, data formats for elements, any constraints, and validation rules. A data dictionary can be defined in an .xsd file. For example, the data dictionary below provides the structure and elements in a quote request. Elements in the data dictionary refer to fields like name:

```
<?xml version = "1.0" encoding = "UTF-8"?>
<!--Generated by XML Authority. Conforms to w3c
http://www.w3.org/2000/10/XMLSchema-->
<xsd: xmlns:xsd =
    "http://www.w3.org/2000/10/XMLSchema">
    <xsd:element name = "WidgetQuoteRequest">
        <xsd:complexType>
            <xsd:sequence>
                <xsd:element ref = "widgetName"/>
            </xsd:sequence>
        </xsd:complexType>
    </xsd:element>
    <xsd:element name = "widgetName" type = "xsd:string"/>
</xsd:>
```

In this example, the data dictionary lists the `WidgetQuoteRequest` element and defines the string data format for the type element.

- **Implementation Framework Core** The vocabulary and data dictionary standards are in turn built on packaging the message and transferring it to a trading partner using an implementation framework core. This core defines the technical details of how trading partners exchange information. For example, this core includes areas like the transport protocols that partners agree to use. This is the key to interoperability.

The following is the structure of an implementation framework core:

Partner Agreement	Conversation	Security
	Message Envelope	
	Transport Protocol	

- **Partner Agreement** This is a specific agreement between partners. It refers to the particular conversation, message structure, transport protocol, and security attributes that partners choose for their communications. Depending on the business protocol, this also includes technical details like the certificates file and the URL for HTTPS transport.
- **Conversation** This includes certain communication options. Depending on the business protocol, these include transaction types like notify and synchronous or asynchronous request-response, and options like time-outs, retries, and exception handling.

- **Message Envelope** Depending on the business protocol, this includes MIME, S/MIME, XML, or CSV. Each business protocol must provide a message envelope to carry the message body. This envelope and message are then wrapped in an envelope provided by the transport protocol.
- **Transport Protocol** Depending on the business protocol, this includes HTTP, HTTPS, FTP, or SMTP.
- **Security** Depending on the business protocol, this includes authentication, access control, non-repudiation, and encryption.

The following protocols are available for use with TIBCO BusinessConnect, but are not limited to:

- TIBCO BusinessConnect™ Services Plug-in
- TIBCO PartnerExpress™
- TIBCO BusinessConnect™ Plug-in for FTP Server
- TIBCO BusinessConnect™ Plug-in for SSH Server

Contact TIBCO sales for more information.

Schemas

An XML Schema describes the vocabulary and structures that exist within an XML instance document conforming to that schema. Schemas use their own formal grammars to express document structures and vocabulary. If a set of documents uses the same schema, the documents have markedly different contents, but can share common processing. Applications check documents against the schema, and process them only if the document passes inspection (more commonly called validation).

By providing a common formal vocabulary for describing the terms on which information will be exchanged, schemas act as an easily enforced contract between senders and receivers (and creators and consumers) of information.

For the detailed information about schemas, see documentation for the products TIBCO Designer and TIBCO ActiveMatrix BusinessWorks.

Schema Validation in TIBCO BusinessConnect

In TIBCO BusinessConnect, nested schemas of unlimited depth are supported for validation. They need to be configured as file references, including the root schema, with the exception of TIBCO BusinessConnect SOAP Protocol where interfaces that use these nested schemas have been imported using the WSDL import tool. Also, nested schema closures can be referenced with either relative or absolute paths. See File Specification Dialog in *TIBCO BusinessConnect Trading Partner Administration*.

It is recommended to use relative paths for closure references. In case a full path is preferred and the references are of type `file`, the valid URI is as follows:

- `file:/// <drive>:/dir1/dir2/<schema.xsd>`

For a mapped drive location.

- `file://<host>/dir1/dir2/<schema.xsd>`

If the file system is available on a different host. See the manual of the operating system for details on mapping or accessing remote/local file systems.

If nested schemas are configured as **File Reference**, their location should not change compared to the configured location under **BusinessConnect > Operations Editor**. This is because the content of the schema components are loaded into TIBCO BusinessConnect schema cache on demand from the specified location.

In addition, if the TIBCO BusinessConnect palette-based private process imports operations that have been configured with such referenced schemas, the original location, with the same path, must be accessible from the importing project only for the duration of the update. After the update on the palette-based project is completed, there is no further correlation between the original schema file resources and the imported schemas as long as the operations are not updated.

System Configuration

This section provides conceptual information about configurable aspects of TIBCO BusinessConnect. For procedural information, see System Settings in *TIBCO BusinessConnect Trading Partner Administration*.

Database Connections

TIBCO BusinessConnect requires a database to function: it uses databases for logging and data stores. You can configure TIBCO BusinessConnect to use different databases for different functionality if desired. The default database connection, and any additional database connections, can be configured using the manage installation feature, which is accessible under the **BusinessConnect > Manage > Configuration Repository** tab. For information about adding a database connection to TIBCO BusinessConnect, see *TIBCO BusinessConnect Installation and Configuration*, "Initializing a Database."



After changing database assignments for the audit, or non-repudiation logs, or the runtime data store, restart all TIBCO BusinessConnect engines for this application.

Logging

By default, TIBCO BusinessConnect logs audit and non-repudiation data to the default database. You can turn logging off if desired and you can assign logging to a different database. Both tasks are performed in the JDBC Configuration area accessed under **BusinessConnect > System Settings > Audit, Non-Repudiation and Runtime Database Configuration**.

- **Audit Logging** Audit logs allow you to retrace the path of a transaction. For example, TIBCO BusinessConnect can log messages from the private process and the trading partner, recording when messages were sent, received, decrypted, and saved.



Audit logs cannot be disabled.

- **Non-Repudiation Logging** Non-repudiation logs allow you to confirm the legitimacy of a transaction. Non-denial, or non-repudiation, is important because a trading partner cannot deny a valid transaction later. Details of the transactions are stored by both partners' databases, along with the relevant digital signatures and a timestamp of when the transaction took place.

Data Stores

TIBCO BusinessConnect uses two types of data stores: Runtime data store, and Configuration store.

By default, the data stores use the default database connection. You can assign a different database to the data stores under **BusinessConnect > System Settings > Audit, Non-Repudiation and Runtime Database Configuration**.

Runtime Data Store

The runtime data store tracks the information flowing through the engine, recording the same information that can be recorded in audit and non-repudiation logs plus information about hibernation, database locking, resend, and alert messages.

This information, however, is for use by the TIBCO BusinessConnect engine itself, serving as a memory of what tasks it has already performed. TIBCO BusinessConnect cannot function without a valid runtime database.

Configuration Store

The configuration store records all the information that you provide to TIBCO BusinessConnect. For example, it stores information about business partners, configuration parameters, and transport settings.

Proxy Servers

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

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

- **HTTP Proxy and SOCKS4/ SOCKS5** For outbound HTTP transport protocols
- **SMTP Server** For outbound EMAIL transport protocols
- **FTP Proxy and SOCK4 / SOCKS5 Proxy Servers** For outbound FTP transport protocols.

You can configure TIBCO BusinessConnect to use a proxy server by identifying its location and the connection information. You can also assign proxy servers at partner participant level.

For information about how to assign proxy servers, see *TIBCO BusinessConnect Trading Partner Administration*, Outbound HTTP/FTP Proxy and Mail SMTP Servers.

Visibility

This section provides conceptual information about aspects of TIBCO BusinessConnect that provide real-time visibility of the overall TIBCO BusinessConnect implementation. TIBCO BusinessConnect achieves such visibility by sending information to several other TIBCO applications that are designed to monitor, organize, and assess information. TIBCO BusinessConnect can send error messages to tibbr, status messages about individual transactions to TIBCO BusinessEvents, and server and process health information to TIBCO Hawk. For procedural information about these aspects, see System Settings in *TIBCO BusinessConnect Trading Partner Administration*.

TIBCO BusinessConnect Visibility via tibbr

tibbr is a workplace communication tool with which you can follow subjects that relate to your work and interests in addition to following people, as in typical social networking applications. This gives you much more flexibility in obtaining the right information at the right time in the right context; in fact, the information will find you.

TIBCO BusinessConnect can post error messages and alerts generated by the Interior Server to specified tibbr subjects. Posting such messages to tibbr allows a wide range of users, including business analysts and IT personnel, to monitor TIBCO BusinessConnect errors as they occur instead of having to rely on audit logs that may be hours, or even days, older than the errors themselves. All the real-time error-related information posted to tibbr is also available to users on all mobile devices supported by tibbr.

You can enable error message posting and define the subjects to which the errors are posted. You can also specify which protocols are enabled to post error messages to tibbr. All of this can be done at both the global and trading partner level. Posting error messages globally and for trading partners are independent of each other. For example, you can enable global error posting for the X12 protocol with the subject prefix **bc.X12**. Any error messages generated by an X12 transaction for any trading partner are posted to the specified tibbr instance with that subject prefix. If you have a trading partner with another protocol for whom you want to post error messages, you can enable error messages generated by EZComm transactions for that trading partner to be posted to tibbr with the subject prefix **bc.tradingpartner1.ezcomm**.

To enable global error posting to tibbr in TIBCO Administrator GUI, go to **BusinessConnect > System Settings > Visibility > tibbr**. For more information about how to configure the tibbr host, see System Settings in *TIBCO BusinessConnect Trading Partner Administration*.

To enable error posting for a specific partner in TIBCO Administrator, go to **BusinessConnect > Participants** and select a participant. In the Edit Partner dialog, select the **Visibility** tab. You can enable partner-related error posting and define the subject prefix and protocols that are used specifically for this partner. For more information about configuring these settings, see System Settings in *TIBCO BusinessConnect Trading Partner Administration*.

For more procedural information about TIBCO BusinessConnect's integration with tibbr, see System Settings in *TIBCO BusinessConnect Trading Partner Administration*. For more information about tibbr, see the related product documentation.

TIBCO BusinessConnect Visibility via TIBCO BusinessEvents

TIBCO BusinessEvents helps companies identify and quantify the impact of meaningful events by sending notifications to the right people and systems. This allows processes to be adapted on-the-fly and people to take action. TIBCO BusinessEvents uses a unique model-driven approach to collect, filter, and correlate events and deliver real-time operational insight.

TIBCO BusinessConnect can send messages processed by the Interior Server to TIBCO BusinessEvents as events via JMS (as a queue or topic) or TIBCO Rendezvous (as a subject). TIBCO BusinessConnect does not send the message payload to TIBCO BusinessEvents. Rather, TIBCO BusinessConnect publishes the message state as an event to TIBCO BusinessEvents, which processes the information. You can configure the TIBCO BusinessEvents rule engine to take any proactive action required by their business needs on any message before the message even reaches a private process. For example, you configure an alert to notify certain users if TIBCO BusinessConnect receives a new message, which is sent to TIBCO BusinessEvents as an Inbound Message event. See [TIBCO Rendezvous Subject Names on page 12](#) for more information about message types.

TIBCO BusinessConnect can send six types of messages to TIBCO BusinessEvents as events: Initiator Request, Initiator Response, Responder Request, Responder Response, Inbound Message, Error Advisory. The message type indicates the message status. You must enable and define a destination name and JMS channel type for each message type. See [Table 2, TIBCO BusinessConnect Message Types](#)

for a description of each message type and an example of the output you see in the TIBCO BusinessEvents console for each message type. See [TIBCO Rendezvous Subject Names](#) on page 12 for more information about message types.

Table 2 TIBCO BusinessConnect Message Types

Message Type	Description	Example BE Console Output
Initiator Request	Request from Initiator's private process to local TIBCO BusinessConnect	InitiatorRequestJMSMsg:standardID=EZComm InitiatorRequestJMSMsg:operationID=BC/1.0/Notify InitiatorRequestJMSMsg:transactionID=yys1ZRb05MmrBEkUN9D1jnJ-G_2U InitiatorRequestJMSMsg:host=null InitiatorRequestJMSMsg:tpName=Partner
Initiator Response	Response to Initiator's private process from local TIBCO BusinessConnect	InitiatorResponseJMSMsg:standardID=EZComm InitiatorResponseJMSMsg:operationID=BC/1.0/Notify InitiatorResponseJMSMsg:transactionID=h-Iqrjxd6q-V-jzvZD1jGhkG_2U InitiatorResponseJMSMsg:host=Host InitiatorResponseJMSMsg:tpName=Partner InitiatorResponseJMSMsg:statusCode=200 InitiatorResponseJMSMsg:statusMsg=OK
Responder Request	Request to a Responder's private process from local TIBCO BusinessConnect	ResponderRequestJMSMsg:standardID=EZComm ResponderRequestJMSMsg:operationID=BC/1.0/Notify ResponderRequestJMSMsg:transactionID=5FKE58-UA6BR6-0003AN-0NAFLZ-01J8 ResponderRequestJMSMsg:host=Host ResponderRequestJMSMsg:tpName=Partner ResponderRequestJMSMsg:duplicate=false
Responder Response	Response from Responder's private process to local TIBCO BusinessConnect	ResponderResponseJMSMsg:standardID=EZComm ResponderResponseJMSMsg:operationID=ManageWidgets/1.0/getWidgetQuote ResponderResponseJMSMsg:transactionID=null ResponderResponseJMSMsg:statusCode=200 ResponderResponseJMSMsg:statusMsg=OK

Table 2 TIBCO BusinessConnect Message Types (Cont'd)

Message Type	Description	Example BE Console Output
Inbound Message	New message received by local TIBCO BusinessConnect from partner (that is, not a response or receipt)	InboundMessageJMSMsg:standardID=EZComm InboundMessageJMSMsg:operationID=BC/1.0/Notify InboundMessageJMSMsg:transportType=HTTP
Error Advisory	Error notification	ErrorAdvisoryJMSMsg:standardID=EZComm ErrorAdvisoryJMSMsg:operationID=Manage Widgets/1.0/buyWidget ErrorAdvisoryJMSMsg:transactionID=02JJ7X-3LN7SE-000PF-NW2P3E-04NJ ErrorAdvisoryJMSMsg:host=Seller ErrorAdvisoryJMSMsg:tpName=Buyer ErrorAdvisoryJMSMsg:statusCode=634 ErrorAdvisoryJMSMsg:statusMsg=ERROR_SMIME_VERIFY ErrorAdvisoryJMSMsg:details=Failed to verify signed S/MIME message. Please check Document Security-Verification Certificate setting in the Business Agreement. DN of the partner certificate does not match.

To enable integration with TIBCO BusinessEvents globally in TIBCO Administrator, go to **BusinessConnect > System Settings > Visibility > BusinessEvents**. In the BE Settings dialog, select the **Enable BE Integration** check box. At the global level, you can specify which message types are published to TIBCO BusinessEvents, change the destination name, and define the type of JMS channel (topic or queue) used to publish messages.

Each trading partner must have integration with TIBCO BusinessEvents enabled for message events to be published to TIBCO BusinessEvents. To enable publishing to TIBCO BusinessEvents for trading partners in TIBCO Administrator, go to **BusinessConnect > Participants** and select a participant. In the Edit Partner dialog, click the **Visibility** tab. In the **BE** area, select the **Enable Publishing to Business Events for this Partner** check box. To publish to TIBCO BusinessEvents, the functionality must be enabled both globally and for each partner. If the integration is not enabled in both locations, no messages will be published to TIBCO BusinessEvents. Enabling the integration at the trading partner level gives TIBCO BusinessConnect users finer-grained control of what is published to TIBCO BusinessEvents.

For more procedural information about TIBCO BusinessConnect integration with TIBCO BusinessEvents, see System Settings in *TIBCO BusinessConnect Trading Partner Administration*. For more information about TIBCO BusinessEvents, see the related product documentation.

Application Monitoring and Management via TIBCO Hawk

TIBCO Hawk is a tool for monitoring and managing distributed applications and operating systems. TIBCO Hawk is an event-based system built around the concept of a distributed, autonomous smart agent that operates on each managed machine in the network. TIBCO Hawk software uses TIBCO Messaging software for communication and inherits benefits such as a flexible architecture and enterprise-wide scalability.

The health and statistical information of TIBCO BusinessConnect Interior Server Instances and Gateway Instances can be exposed to TIBCO Hawk.

You can monitor this information by using TIBCO Hawk and manage this information through TIBCO Hawk Display. Rulebases can be used to take actions when a certain situation occurs. For example, you can use rulebases to send an alert or a notification when the health information changes. Rulebases can also be used to manage the pollers based on the status they report. For example, you can establish a rule to restart any poller with a status of Hung.

TIBCO Hawk is integrated with TIBCO Administrator, so you can monitor and manage TIBCO applications such as TIBCO BusinessConnect Interior and Gateway Servers in TIBCO Administrator. To enable application monitoring and management for TIBCO BusinessConnect in TIBCO Administrator, go to **BusinessConnect > System Settings > Visibility > Application Monitoring & Management**. In the Application Monitoring & Management dialog, select an Administrator user. The TIBCO Hawk Agent uses the selected Administrator user for authentication to connect to TIBCO BusinessConnect and to monitor and manage the server processes described above. On the TIBCO Hawk Agent side, it uses TIBCO Hawk® JMX Plug-in to connect to BusinessConnect servers, so the user name and password must be specified in the configuration `JMXPluginConfig.xml` file in the `TIBCO_HOME\hawk\version\plugin` directory.

Here, `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`.

For details about how to specify these values in the `JMXPluginConfig.xml` file, see *TIBCO BusinessConnect Trading Partner Administration*, "System Settings."

You must enable application monitoring and management for each TIBCO BusinessConnect Interior Server Instance you want to monitor. To enable this function in TIBCO Administrator, go to **Application Management > BusinessConnect > Configuration** and select a service instance. In the Edit Service Instance dialog, click the **Process Configuration** tab. In the **Application Monitoring & Management** area, select the **Enable** check box and enter the port number the monitoring service listens on.

For TIBCO BusinessConnect Interior Server, you can use TIBCO Hawk to monitor the information about Heartbeat, inboundReceived, outboundSent,

For TIBCO BusinessConnect Gateway Server, you can use TIBCO Hawk to monitor the information about lastHeartbeatInfo, inboundReceived for FILE, and inboundReceived for HTTP.

TIBCO BusinessConnect Interior Server Instances play the bridge role between the Gateway Instances and TIBCO Hawk Agent, so no special network settings exist regarding the DMZ to monitor the states of Gateway Servers.

For more information about application monitoring and management for TIBCO BusinessConnect, see "System Settings" in *TIBCO BusinessConnect Trading Partner Administration*. For more information about TIBCO Hawk, see the related TIBCO Hawk documentation.

Chapter 3 **Server Management Overview**

Topics

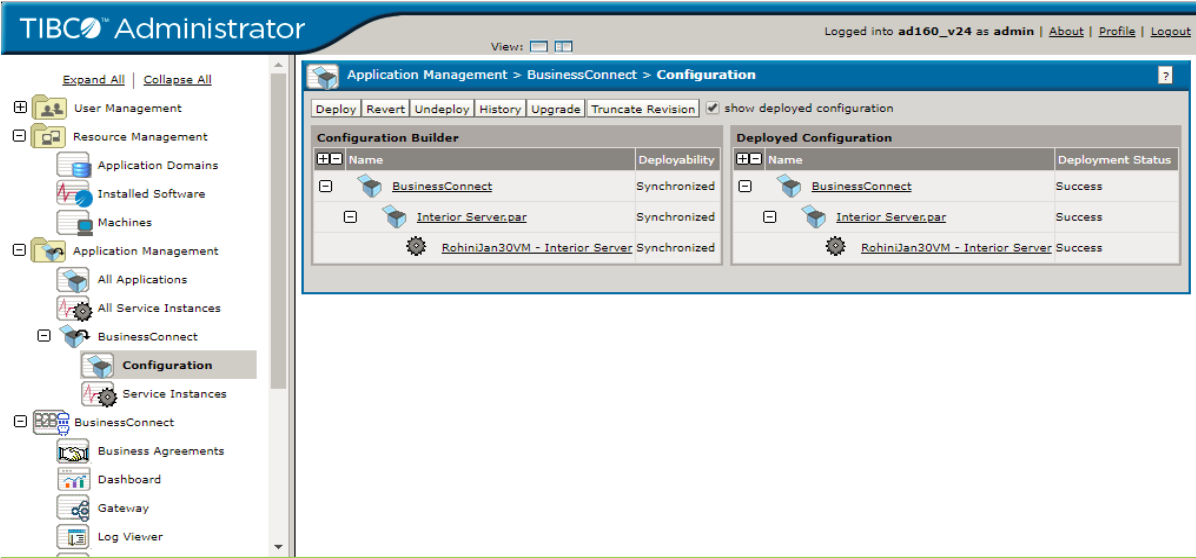
- [Using TIBCO Administrator, page 34](#)
- [Using TIBCO ActiveMatrix BusinessWorks, page 37](#)
- [Using TIBCO Designer, page 39](#)

Using TIBCO Administrator

TIBCO Administrator is used to deploy and undeploy TIBCO BusinessConnect applications, configure process transports and TIBCO BusinessConnect components, and start and stop the TIBCO BusinessConnect server.

You can access the necessary links and buttons through the application management node in the left panel. You can also access through the management screens, for example, User, Resource, Application, and TIBCO BusinessConnect management in the right panel.

Figure 7 TIBCO Administrator, Application Management Console



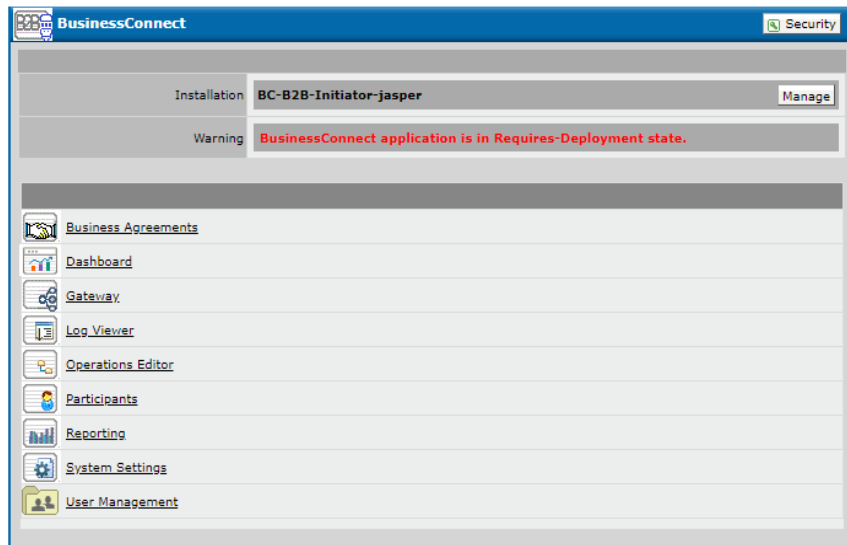
Application Management

The application management panel, Figure 7, provides access to all of the top-level screens associated with the TIBCO BusinessConnect application and TIBCO BusinessConnect server configuration.

TIBCO BusinessConnect

The TIBCO BusinessConnect console, Figure 8, is one of the management consoles that opens in the right panel.

Figure 8 TIBCO Administrator, TIBCO BusinessConnect Console



This console is used to manage all aspects of the TIBCO BusinessConnect application, such as:

- **Business Agreements** This link is used for adding and deleting business agreements. To manage business agreements, see Business Agreements in *TIBCO BusinessConnect Trading Partner Administration*.



A warning is shown only when TIBCO BusinessConnect is in a deployable state.

- **Dashboard** This link is used for viewing your transaction data using different charts on a single screen. To view this data, see Dashboard in *TIBCO BusinessConnect Trading Partner Administration*.
- **Gateway** This link is used for configuring and managing the Gateway server, as described in detail in *TIBCO BusinessConnect Gateway Server Administration*.
- **Log Viewer** This link is used for managing audit, non-repudiation, and resend logs. To manage logs, see Log Viewer in *TIBCO BusinessConnect Trading Partner Administration*.
- **Operations Editor** This link is used for importing, exporting, adding new, and deleting operations. To manage operations, see Operations Editor in *TIBCO BusinessConnect Trading Partner Administration*.
- **Participants** This link is used for importing, exporting, adding, copying, and deleting participants. To manage participants, see Participants in *TIBCO BusinessConnect Trading Partner Administration*.

- **Reporting** This link is used for generating reports for inbound and outbound transactions per protocol. To generate reports, see Log Viewer in *TIBCO BusinessConnect Trading Partner Administration*.
- **System Settings** This console lets you manage the following functions of your TIBCO BusinessConnect server.
 - General
 - Certificate Store
 - Inbound Public Transport Types
 - Inbound Mail POP3 Servers
 - Outbound HTTP/FTP Proxy and Mail SMTP Servers
 - Audit, Non-Repudiation and Runtime Database Configuration
 - User Authentication Configuration
 - Activated Protocol Plug-ins and Properties
 - Metadata Type Configuration
 - Private Process Smart Routing
 - Credential Expiry Alerter
 - User Access Audit Trail
 - Utilities
 - Visibility



All these listed functions you can access using the System Settings console are explained in *TIBCO BusinessConnect Trading Partner Administration, System Settings*.

- **User Management** This console lets you manage users and groups using [TIBCO BusinessConnect User Management, page 45](#) and [TIBCO BusinessConnect Group Management, page 51](#).

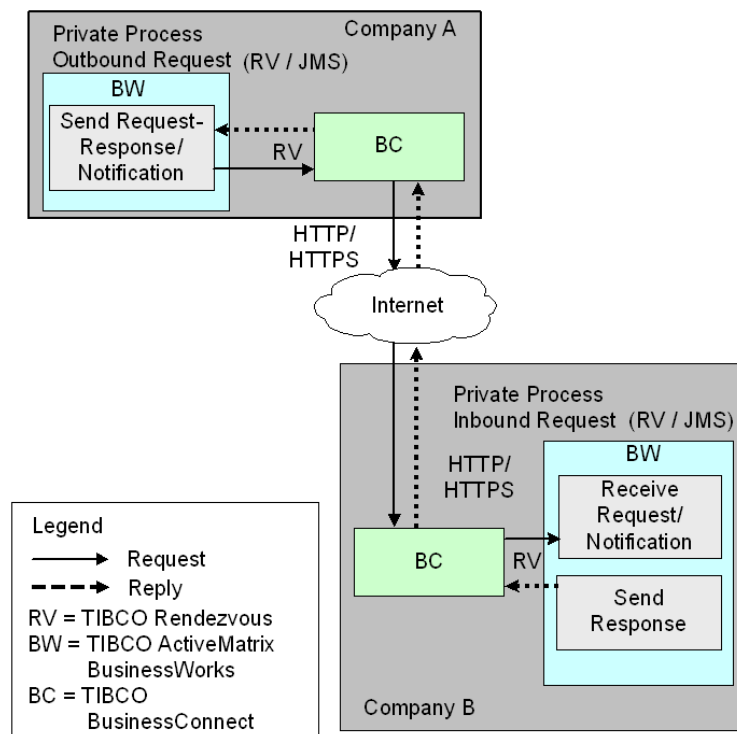
Using TIBCO ActiveMatrix BusinessWorks

With the TIBCO BusinessConnect Palette and TIBCO ActiveMatrix BusinessWorks, you can create process definitions that serve as private processes for a TIBCO BusinessConnect installation.

TIBCO ActiveMatrix BusinessWorks can either send requests to a TIBCO BusinessConnect server or receive replies from a TIBCO BusinessConnect server.

Figure 9 illustrates TIBCO ActiveMatrix BusinessWorks operating in conjunction with TIBCO BusinessConnect.

Figure 9 TIBCO ActiveMatrix BusinessWorks Communicating with TIBCO BusinessConnect



In Figure 9, Company A implements a private process in TIBCO ActiveMatrix BusinessWorks and uses the Send Request/Notification activity to invoke a pre-configured B2B operation on a TIBCO BusinessConnect server.

TIBCO BusinessConnect in Company A sends the request to TIBCO BusinessConnect server at Company B, which has a process definition with the Receive Request/ Notification process starter.

This process definition receives the incoming request, processes it, and sends a response back to the TIBCO BusinessConnect server using the Send Response activity. TIBCO BusinessConnect then routes the reply back to the original requestor.

It is not necessary for TIBCO ActiveMatrix BusinessWorks to be used to implement the private process at both Company A and Company B. A different application can be used to send the request or receive the request. However, it is necessary for TIBCO BusinessConnect to be used at any site where TIBCO ActiveMatrix BusinessWorks is used to send or receive TIBCO BusinessConnect messages.

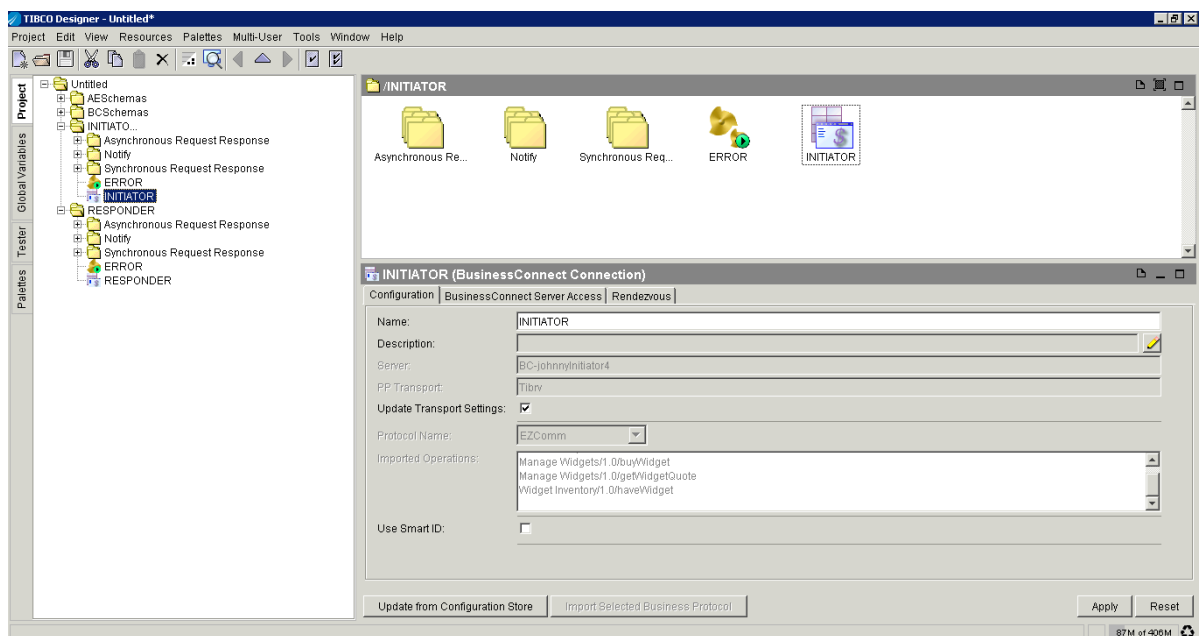
Using TIBCO Designer

TIBCO Designer is an easy-to-use GUI for configuring, designing, and testing TIBCO ActiveMatrix BusinessWorks projects. TIBCO Designer provides an integrated development environment including these components:

- Project directory
- Project resources
- Process design
- Activity configuration

As shown in [Figure 10](#), you can use TIBCO Designer as a modeling tool to design business processes as a part of your business-to-business integration.

Figure 10 TIBCO Designer



TIBCO Designer is used in the design time environment for designing and testing business processes and to prepare documents for secure transmission over the Internet. It contains a number of native palettes, including the TIBCO BusinessConnect palette.

To learn more about these palettes and how to work with the application, please refer to *TIBCO Designer User's Guide*.

Chapter 4

TIBCO BusinessConnect User Management

This chapter explains how to manage user and groups in TIBCO Administrator and in TIBCO BusinessConnect.

Topics

- [Overview, page 42](#)
- [TIBCO Administrator User Management, page 43](#)
- [TIBCO BusinessConnect User Management, page 45](#)
- [TIBCO BusinessConnect Group Management, page 51](#)

Overview

The User Management feature of TIBCO BusinessConnect expands upon the user management capabilities provided with TIBCO Administrator. TIBCO BusinessConnect User Management provides the ability to manage access restrictions on users of the TIBCO BusinessConnect administration console.

For example, previously when TIBCO Administrator User Management was used to give a user read and write access to TIBCO BusinessConnect trading partner configurations, the user had read and write access to all TIBCO BusinessConnect trading partner configurations. Now, with TIBCO BusinessConnect User Management, a user can be further restricted to only have read and write access to particular trading partner configurations.

With TIBCO BusinessConnect User Management, access restrictions can be narrowed for:

- Trading Partner Configurations
- Business Agreement Configurations
- Logs and Reports
- Dashboard

The TIBCO BusinessConnect User Management feature has been designed with backward compatibility in mind. If you do not use the TIBCO BusinessConnect User Management feature, user access will remain the same as for previous versions of TIBCO BusinessConnect where user access rights to TIBCO BusinessConnect were configured using only TIBCO Administrator User Management.

TIBCO BusinessConnect User Management provides the ability to view an audit trail of a user's activities while using TIBCO BusinessConnect. To learn how to audit all the activities that users perform on trading partners, see User Access Management in *TIBCO BusinessConnect Trading Partner Administration*.

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.

TIBCO Administrator User Access Rights

To understand how TIBCO BusinessConnect User Management access rights work in conjunction with TIBCO Administrator, it is important to understand how TIBCO Administrator user access rights work.

The following is a summary of the access rights which can be assigned to resources managed through TIBCO Administrator.

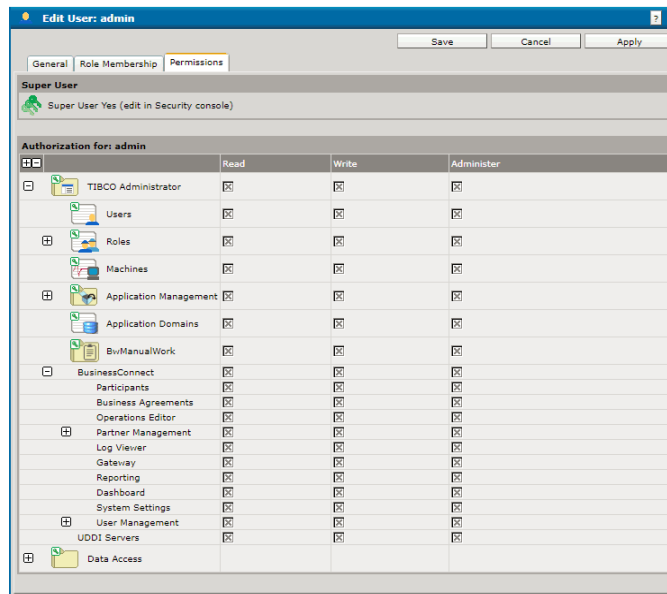
- **Read Access** A user with read access to a resource can view that resource.
- **Write Access** A user with write access to a resource can modify that resource. Write access to a resource implies read access.
- **Administer Access** A user with administrator access to a resource can assign permission to other users and roles to access that resource. This access gives automatically the Read access, while the Write access can be added if desired.
- **Super User Access** A Super User has Read, Write and Administer permissions to all resources in the administration domain without explicitly having been granted those permissions.

See [Figure 11](#) to review the permissions granted to the TIBCO Administrator Super User.

The domain administrator automatically has Super User Access privileges. A Super User has the following rights:

- Managing all parts of a domain
- Adding a machine to a domain
- Resetting password of another user
- Adding other users to the list of super users

Figure 11 TIBCO Administrator Super User



For more details about TIBCO Administrator user management, see *TIBCO Administrator User's Guide*, Managing Users and Roles.

TIBCO BusinessConnect Component User Access

Using TIBCO Administrator User Management, users can be given Read, Write or Administer access to the following components of TIBCO BusinessConnect:

- BusinessConnect
- Business Agreements
- Dashboard
- Gateway
- Log Viewer
- Operations Editor
- Participants
- Reporting
- System Settings
- User Management

To set the TIBCO BusinessConnect access rights for a user under TIBCO Administrator User Management, see *TIBCO BusinessConnect Trading Partner Administration*, Using TIBCO Administrator User Management.

TIBCO BusinessConnect User Management

The user management capabilities of TIBCO BusinessConnect are integrated with the user management capabilities of TIBCO Administrator. After a user is created and given access rights to one or more components of TIBCO BusinessConnect using TIBCO Administrator User Management, that user can be added to TIBCO BusinessConnect User Management and can have its access rights fine tuned with respect to trading partner, business agreement, log viewer, reports, and dashboard access.

With TIBCO BusinessConnect User Management, the access rights of a user can be reduced but never increased. For example, if TIBCO Administrator User Management is used to give a user read but not write access to the **BusinessConnect > Participants** component, you cannot use TIBCO BusinessConnect User Management to grant the user Update Access for a participant.

Participants Access Rights

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. The following is a summary of the access rights users can be assigned to allow access to participant configurations under **BusinessConnect > Participants**:

- **Read Access** A user with read access to a participant can view that participant's configuration information.
- **Create Access** (implies Read Access) A user with create access can create new participants. The create access privilege can only be enabled for all participants.
- **Update Access** (implies Read Access) A user with update access to a participant can modify the configuration settings of an existing participant.
- **Delete Access** (implies Read Access) A user with delete access to a participant has the ability to delete the participant's configuration from TIBCO BusinessConnect.
- **Logs and Reports** This setting is used to further restrict the user access rights for Log Viewer or Reporting, granted using TIBCO Administrator User Management, to apply to particular participants. By default these access rights apply to all participants. This setting does not control the read and write access rights to the Log Viewer or Reporting. Read and write access rights to

the Log Viewer and Reporting are controlled using TIBCO Administrator User Management.

- **Dashboard** This setting is used to further restrict the user access rights for Dashboard, granted using TIBCO Administrator User Management. This setting does not control the read and write access rights to the Dashboard.

Business Agreements Access Rights

For Business Agreements, users can be assigned access rights to all Business Agreements or to particular Business Agreements. The following is a summary of the access rights users can be assigned to allow access to Business Agreement configurations under **BusinessConnect > Business Agreements** tab:

- **Read Access** A user with read access to a business agreement can view that business agreement's configuration.
- **Create Access** (implies Read Access) A user with create access can create new business agreements. The create access privilege can only be enabled for all business agreements.
- **Update Access** (implies Read Access) A user with update access to a business agreement can modify the configuration settings of an existing business agreement.
- **Delete Access** (implies Read Access) A user with delete access to a business agreement has the ability to delete the business agreement's configuration from TIBCO BusinessConnect.

Default Access Rights

When TIBCO Administrator User Management is used to give a user access rights to TIBCO BusinessConnect Participants, Business Agreements, Log Viewer, Reporting, or Dashboard, the following describes the default mapping of those access rights under BusinessConnect User Management:

Table 3 Access Right Mapping for BusinessConnect User Management

Administrator Access Right	TIBCO BusinessConnect Access Right
Participants Read Access	All Participants Read Access
Participants Write Access	All Participants Read, Create, Update, Delete Access
Business Agreements Read Access	All Business Agreements Read Access

Table 3 Access Right Mapping for BusinessConnect User Management (Cont'd)

Administrator Access Right	TIBCO BusinessConnect Access Right
Business Agreements Write Access	All Business Agreements Read, Create, Update and Delete Access
Log Viewer Read Access	All Participants Logs and Reports Access (user has Log Viewer read access for all participants)
Log Viewer Write Access	All Participants Logs and Reports Access (user has Log Viewer read and write access for all participants)
Reporting Read Access	All Participants Logs and Reports Access (user has Reporting read access for all participants)
Reporting Write Access	All Participants Logs and Reports Access (user has Reporting read and write access for all participants)
Dashboard Read Access	All Participants Dashboard Access (user has Dashboard read access for all participants)

TIBCO BusinessConnect Users

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 BusinessConnect Super User access rights are depicted in [Table 4](#).

Table 4 TIBCO Administrator User Role Assignments

TIBCO Administrator User	Could be assigned to a TIBCO BusinessConnect Super User role	Has automatic TIBCO BusinessConnect user management access
Super User who created the TIBCO BusinessConnect installation	Gains automatic access	Gains automatic access
Super User who did not create the TIBCO BusinessConnect installation	Yes	Yes

Table 4 TIBCO Administrator User Role Assignments

TIBCO Administrator User	Could be assigned to a TIBCO BusinessConnect Super User role	Has automatic TIBCO BusinessConnect user management access
Regular user with Read/Write access to all TIBCO BusinessConnect links	Yes	No
Regular user with Read/Write access to only a few TIBCO BusinessConnect links	No	No
Regular user with Read access to all TIBCO BusinessConnect links	No	No

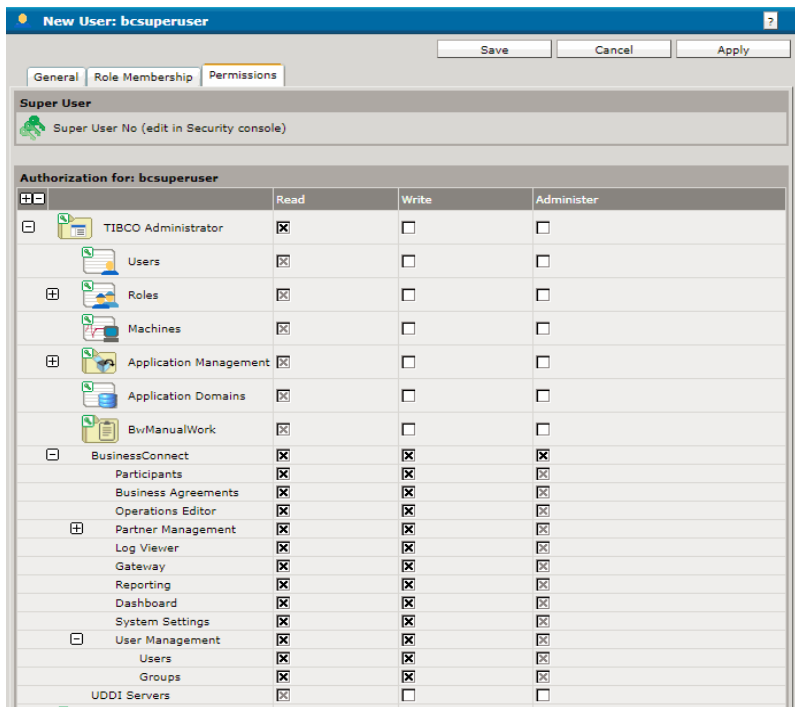
The TIBCO Administrator user who creates the TIBCO BusinessConnect installation is automatically the TIBCO BusinessConnect Super User.

To create a TIBCO BusinessConnect installation, a user must be one of the following:

- A TIBCO BusinessConnect Super User
- A TIBCO Administrator Super User
- A TIBCO Administrator user who has been granted read and write access privileges to all of the TIBCO BusinessConnect components under TIBCO Administrator User Management.

A TIBCO BusinessConnect Super User can assign super user privileges to other TIBCO Administrator users who are TIBCO Administrator Super Users or TIBCO Administrator users with read and write access privileges to all of the TIBCO BusinessConnect components.

Figure 12 TIBCO BusinessConnect Super User



Authorization for: bcsuperuser			
	Read	Write	Administer
TIBCO Administrator	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Users	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Roles	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Machines	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Application Management	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Application Domains	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
BwManualWork	<input checked="" 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"/>
Users	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Groups	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
UDDI Servers	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

A TIBCO Administrator Super User will always be allowed full access to the configuration information of TIBCO BusinessConnect. However, the TIBCO Administrator Super User will not be automatically assigned to be a TIBCO BusinessConnect Super User unless it is the user who created the TIBCO BusinessConnect installation, or unless it has been explicitly assigned to be a TIBCO BusinessConnect Super User.

To delete a TIBCO BusinessConnect Super User from TIBCO BusinessConnect User Management, you must first remove the TIBCO BusinessConnect super user access right for this user.



If the users are removed from the TIBCO Administrator User Management by the TIBCO Administrator Super User, TIBCO BusinessConnect Users will be automatically removed from the TIBCO BusinessConnect User Access Control as part of the synchronization. A trace is added about the removal of the user from the TIBCO BusinessConnect User Management.



If the user permissions set in TIBCO Administrator for **BusinessConnect > (Participants, Business Agreements, Log Viewer, and Reporting)** are either Read or no permissions, but the permissions set at **BusinessConnect > User Management** are higher (such as Create, Read, Update or Delete) for Participants, Business Agreements, Log Viewer, Dashboard, and Reporting, a warning is shown about the inconsistent permissions. Users are still allowed to save after this warning.

TIBCO BusinessConnect Internal User

The internal users are assumed to be communicating with TIBCO BusinessConnect inside the company firewall.

TIBCO Administrator with access rights to TIBCO BusinessConnect and its components can manually add Internal users to TIBCO BusinessConnect, or these users will be automatically added once they log in.

The new TIBCO BusinessConnect Internal user will have its corresponding access rights for TIBCO BusinessConnect User Management automatically set as described in the section [Default Access Rights on page 46](#).

TIBCO BusinessConnect External User

After the TIBCO BusinessConnect Administrator sets up a trading partner, he can associate one or more external users with that trading partner.

These external users can log in using a web browser and start performing basic upload or download transactions with the Host, which their trading partner has an agreement with.

The external users can connect with PartnerExpress Service, Trading Community Management Service, SSH Service, and FTP Service that are hosted by the Gateway Server in the DMZ zone.

The external users can also be used for HTTP Basic Authentication and WSS Username Token Authentication for inbound transactions from trading partners.

TIBCO BusinessConnect Group Management

Both TIBCO Administrator User Management and TIBCO BusinessConnect User Management have support for group access rights.

TIBCO Administrator User Management uses the term Role instead of group. User access rights can be easier to manage when roles or groups are used. The following sections describe using TIBCO Administrator roles and TIBCO BusinessConnect groups to assign access rights to a user.

TIBCO Administrator Roles

In TIBCO Administrator User Management, you can define roles that have particular access rights, and users can be assigned to one or more roles. The access rights of a user belonging to a role include the access rights specifically assigned to the user, plus the access rights of the role. There is no concept of being able to use a role to take away a user's access rights, so the complete set of access rights for the user consists of those access rights assigned to the individual user plus those access rights allowed for each of the roles a user belongs to.

For example, imagine you have a user named 'user' who has specific access rights for TIBCO BusinessConnect, and has membership in roleA and roleB, as shown in Table 5.

Table 5 User Access for a User Belonging to Two Roles

	User	roleA	roleB	Total Access Rights
Business Connect	Read			Read
Participants		Read	Read, Write	Read, Write
Business Agreements		Read	Read, Write	Read, Write
Log Viewer	Read	Read, Write		Read, Write
Reporting	Read	Read, Write		Read, Write
Dashboard	Read	Read, Write		Read, Write

TIBCO BusinessConnect Groups

In TIBCO BusinessConnect User Management, you can define groups that have particular access rights and 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.

The access rights of a user belonging to a group include the access rights specifically assigned to the user plus the access rights of the group. There is no concept of being able to use a group to take away a user's access rights, so the complete set of access rights for the user consists of those access rights assigned to the individual user plus those access rights allowed for each of the groups a user belongs to.

Group Access Right Examples

For example, suppose that userA is defined in TIBCO Administrator User Management to have the total set of access rights as follows:

- BusinessConnect - Read
- Log Viewer - Read, Write
- Reporting - Read, Write
- Business Agreements - Read, Write
- Dashboard - Read, Write
- Participants - Read, Write

These permissions map to the following default access rights for userA in TIBCO BusinessConnect User Management which allow userA to have full access to all participants and all business agreements.

Table 6 User with Default Access Rights

Default Access Rights of userA	
All Participants	Read, Create, Update, Delete, Logs&Reports
All Business Agreements	Read, Create, Update, Delete

Suppose there is also a group defined in TIBCO BusinessConnect User Management to provide read and write access to a particular trading partner, tpA, and its associated Business Agreement as follows:

- **Group Name:** tpA

- **Participant Permission:** All participants access rights cleared; tpA access rights set to Read, Update, Delete, Logs and Reports
- **Business Agreement Permission:** All agreements access rights cleared; Business Agreement for tpA access rights set to Read, Update, Delete

If you wanted to restrict the access rights of userA so that userA would only have access rights for tpA instead of for all participants, you could try to assign userA to group 'tpA'. However that would not solve the problem as userA would still have access rights to all participants and business agreements because of the logical ORing of userA's default access rights and the access rights of group 'tpA'.

To configure userA so that it only had access rights to tpA, you would need to clear the access rights for userA under **Participant Permission > ALL** and under **Business Agreements Permission > ALL** and then add Group Membership to group 'tpA' for userA. This will result in userA only having access rights to tpA as defined by group 'tpA'.

As one last example of how TIBCO Administrator access rights work with TIBCO BusinessConnect access rights, suppose we have userA with TIBCO Administrator access rights for TIBCO BusinessConnect as follows:

- BusinessConnect - Read
- Log Viewer - Read, Write
- Reporting - Read, Write
- Business Agreements - Read
- Dashboard - Read, Write
- Participants - Read

If userA is configured with TIBCO BusinessConnect User Management so that the default access rights for Participants and Business Agreements are cleared and userA is configured to belong to group 'tpA', this would result in userA having Read permissions for participant tpA and the business agreement associated with tpA. The userA would not get Update or Delete permissions because userA was only granted Read access for Participants and Business Agreements in its TIBCO Administrator User Management settings.

In other words, the access rights given to a user using TIBCO BusinessConnect User Management are logically ORed with the access rights for any groups the user is assigned to. The total TIBCO BusinessConnect access rights for the user are then logically ANDed with the total Administrator access rights for the user to determine the overall access rights for the user.

Chapter 5

TIBCO BusinessConnect Transports and Protocols

Topics

- [Transports, page 56](#)
- [Protocols, page 60](#)

Transports

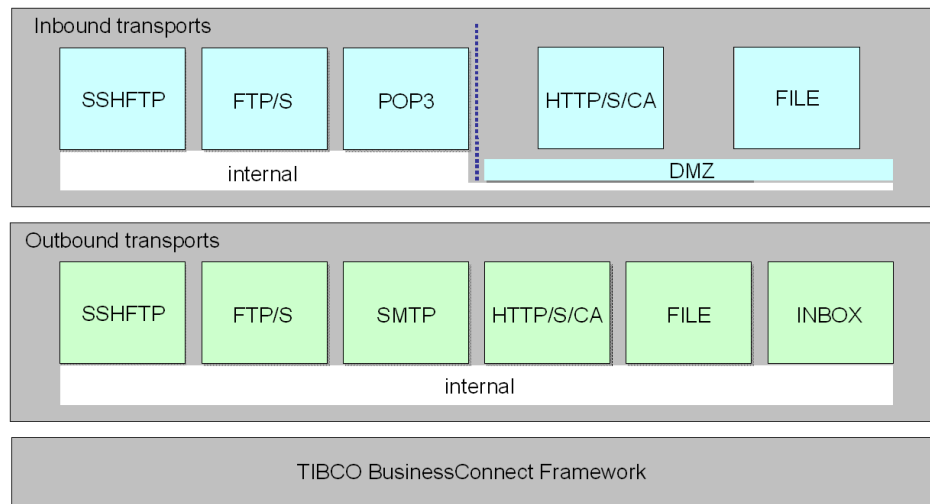
Transports provide a set of standards for use in moving information across the Internet. Different transports are used in the different parts of the process, such as:

- Within server components: TIBCO Enterprise Message Service
- Between TIBCO BusinessConnect and private processes: TIBCO Rendezvous or JMS
- Between TIBCO BusinessConnect and the Internet: public or private transports

Public Transports

Public transports can be used in TIBCO BusinessConnect as inbound or outbound. For the physical transport location, see [Figure 13](#).

Figure 13 Physical Location of Public Transports



The following public transports are supported in TIBCO BusinessConnect:

- Inbound public transports are configured for the host during the deployment process. You can reach them by expanding **BusinessConnect > System Settings > Inbound Public Transport Types**.

Figure 14 Inbound Public Transport Types

Inbound Public Transport Types			
<div> <div>Enable</div> <div>Disable</div> </div> <div>Done</div>			
<input type="checkbox"/>	Transport Type	Description	Enabled
<input type="checkbox"/>	Email	Mail POP3 Server Polling Service - Mailbox #1	X
<input type="checkbox"/>	Email	Mail POP3 Server Polling Service - Mailbox #2	X
<input type="checkbox"/>	Email	Mail POP3 Server Polling Service - Mailbox #3	X
<input type="checkbox"/>	FTP	Plain FTP Get Client	✓
<input type="checkbox"/>	FTPS	Secure FTP Get SSL Client	✓
<input type="checkbox"/>	SSHFTP	Secure FTP Get SSH Client	X
<input type="checkbox"/>	HTTP	Gateway Plain HTTP Service	✓
<input type="checkbox"/>	HTTPS	Gateway Secure HTTP SSL Service	✓
<input type="checkbox"/>	HTTPSCA	Gateway Secure HTTP SSL Service with Client Authentication	X
<input type="checkbox"/>	FILE	Gateway File Polling Service	✓
<input type="checkbox"/>	FTPD	Gateway FTP Service	X
<input type="checkbox"/>	FTPSD	Gateway FTP Secure Service	X

To learn how to add an inbound public transport for a host, see *TIBCO BusinessConnect Interior Server Administration*, Configuring Smart Routing.

- Outbound public transports are configured for the partner in a business agreement.

All outbound transports and their configuration are explained in detail in the following chapters in *TIBCO BusinessConnect Trading Partner Administration*:

- Chapter 8, Email Transport
- Chapter 9, FTP and FTPS Transports
- Chapter 10, SSHFTP Transport
- Chapter 11, HTTP, HTTPS, and HTTPSCA Transports
- Chapter 12, AS2 Transport
- Chapter 13, AS1 Transport
- Chapter 14, File Transport.



The File transport cannot transport documents across the Internet; it can only save a file locally. However, you can use scripts in conjunction with the File transport to transport documents from the local server to a remote server using any transport protocol available to you.

TIBCO Implementation of AS Standards

TIBCO BusinessConnect uses the following implementations of the AS1 and AS2 standards for exchanging documents over the Internet:

TIBCO BusinessConnect AS1 Transport

Vendor applications can use this TIBCO implementation of the AS1 standard to exchange EDI documents over the Internet using S/MIME and SMTP.

For more information, see *TIBCO BusinessConnect Trading Partner Administration*, "AS1 Transport Overview."

TIBCO BusinessConnect AS2 Transport

Vendor applications can use this TIBCO implementation of the AS2 standard to exchange EDI documents over the Internet using S/MIME and HTTP/S.

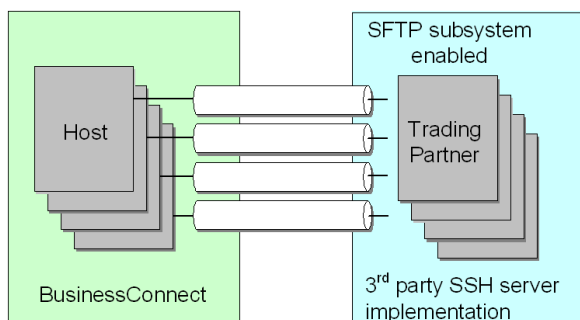
For more information, see *TIBCO BusinessConnect Trading Partner Administration*, "AS2 Transport Overview."

SSHFTP Implementation in TIBCO BusinessConnect

The SSHFTP (SFTP) transport is one of the public transports used for TIBCO BusinessConnect and is introduced in version 5.2.0. It is used to establish multiple tunnels for secure communication between two participants.

The established secure tunnels, if inactive, will be removed by TIBCO BusinessConnect.

Figure 15 SSHFTP Tunnels



1 tunnel / TP / transport (direction)

1 or 2 tunnels between any host and trading partner
(1 tunnel if the inbound and outbound transport
configuration is identical, 2 tunnels otherwise)

Implementation of the SSHFTP transport is based on the following:

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



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

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

Cache Timeout

The cache timeout is time after which a tunnel will be removed if it is not in use (default is 2 hours).

Properties for configuring the cache timeout are available on the server side. When changing the cache timeout configuration, keep in mind that any new or pending transactions will use the tunnel that has been open *after* the configuration was changed.

All configuration steps for setting up trading partners for SSHFTP, and configuring of the cache timeout, are explained in *TIBCO BusinessConnect Trading Partner Administration*, SSHFTP Transport.

Protocols

The TIBCO BusinessConnect supports the following protocols:

- TIBCO BusinessConnect Services Plug-in
For details, see *TIBCO BusinessConnect Services Plug-in User's Guide*.
- TIBCO PartnerExpress
For details, see *TIBCO PartnerExpress User's Guide* for details.
- TIBCO BusinessConnect Plug-in for FTP Server
For details, see *TIBCO BusinessConnect Plug-in for FTP Server User's Guide*.
- TIBCO BusinessConnect Plug-in for SSH Server
For details, see *TIBCO BusinessConnect Plug-in for SSH Server User's Guide* for details.
- TIBCO BusinessConnect™ EDI Protocol powered by Instream®
For details, see *TIBCO BusinessConnect EDI Protocol powered by Instream User's Guide*.
- TIBCO BusinessConnect™ ebXML Protocol
For details, see *TIBCO BusinessConnect ebXML Protocol User's Guide*.
- TIBCO BusinessConnect™ SOAP Protocol
For details, see *TIBCO BusinessConnect SOAP Protocol User's Guide*.
- TIBCO BusinessConnect™ Trading Community Management
For details, see *TIBCO BusinessConnect Trading Community Management User's Guide*.
- TIBCO BusinessConnect™ ConfigStore Management Interface Protocol
For details, see *TIBCO BusinessConnect ConfigStore Management Interface Protocol User's Guide*.
- TIBCO BusinessConnect RosettaNet Protocol™
For details, see *TIBCO BusinessConnect RosettaNet Protocol User's Guide*.
- TIBCO BusinessConnect™ cXML Protocol
For details, see *TIBCO BusinessConnect cXML Protocol User's Guide*.

Chapter 6

Fault Tolerance and Load Balancing

This chapter explains support for fault tolerance and load balancing in TIBCO BusinessConnect.

Topics

- [Overview, page 62](#)
- [Fault Tolerance and Load Balancing for the Interior Server, page 63](#)

Overview

Load balancing among servers running TIBCO BusinessConnect components is achieved when more than one component shares reception of incoming messages. TIBCO BusinessConnect allows you to add multiple engines to share load.

Fault tolerance for a server running TIBCO BusinessConnect is achieved when one engine acts as active or passive backup to another engine. If the first engine stops for any reason, the backup engine starts and takes over the jobs that the first engine was processing.

Fault Tolerance and Load Balancing for the Interior Server

The Interior Server can be deployed to provide both for fault tolerance and load balancing. Machines that belong to one group provide for fault tolerance within that group, while machines in different groups provide for load balancing among these groups.

Figure 16 Interior Server: Load Balancing and Fault Tolerance

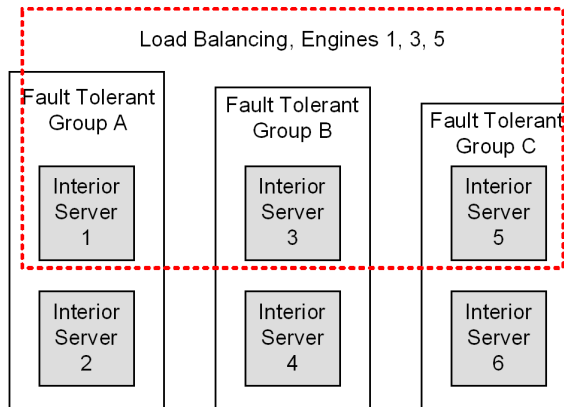


Figure 16 shows a configuration with three fault tolerant groups, where servers are grouped as follows:

- Servers 1 and 2 are in the fault tolerant group A.
- Servers 3 and 4 are in the fault tolerant group B.
- Servers 5 and 6 are in the fault tolerant group C.

Fault Tolerance for the Interior Server

Fault tolerance is achieved since each server in a group acts as a backup for the other server in the same group. Multiple groups can coexist, each containing two or more servers. In each of these groups, servers are started in a sequence so that the server that starts first works until it fails.

Upon the first server's failure, the second server installed in the same group takes its role, and so on. Servers have no primary or secondary functions, and the order in which they provide fault tolerance is based on the order in which they were started.

Load Balancing and Public Smart Routing for the Interior Server

Load balancing for the Interior component is achieved by adding multiple Interior engines or multiple fault tolerant groups.

Using the Public Smart Routing feature, you can distribute the workloads and alleviate the likelihood of bottlenecks by using multiple server cluster based on preset rules (predefined set of criteria). A rule-based routing mechanism makes decisions, based on a combination of configurable conditions and dispatches workloads to the best fitting cluster for processing.

To learn more, see [Public Smart Routing](#), page 69.

Configuring the Interior Server

The Interior Server must be configured with the following information:

- **Checkpoint Database** This database contains all checkpoints (transaction execution records) from an Interior component. This way, in the case of the machine's failure, these saved transaction records are transferred from the disabled machine to the one that takes over its function.

When you initially set up TIBCO BusinessConnect, the connection for the Checkpoint Database is set and is named *bc-check-point-db* by default.

You can modify the configuration of the Checkpoint database and any other databases by clicking the connection alias.

- **All required parameters** The Interior component parameters, such as Service, Network, Daemon Host, Daemon Port, Heartbeat Interval, Activation Interval, and Activation Delay, must be set to support fault tolerance.

These parameters are set during deployment.

For more details, see *TIBCO BusinessConnect Interior Server Administration*, "Configuring Interior Server.par."

Chapter 7 **Smart Routing**

This chapter explains the concept of Private Process Smart Routing and Public Smart Routing in TIBCO BusinessConnect.

Topics

- [Overview, page 66](#)
- [Private Process Smart Routing, page 67](#)
- [Public Smart Routing, page 69](#)

Overview

Messages that are routed in TIBCO BusinessConnect fall into these categories:

- **Messages received from trading partners** These messages are commonly referred as inbound messages from trading partners.

These messages are processed using Public Smart Routing.

- **Messages routed to the private processes** These messages are processed using Private Process Smart Routing.

Private Process Smart Routing makes it possible for users to route preferred messages to selected private process instances while other messages can be received and processed by the rest of the instances in the same or in the different TIBCO ActiveMatrix BusinessWorks projects.

Public Smart Routing uses a combination of configurable conditions and predefined set of criteria to dispatch the workloads to the best fitting cluster for processing of messages received from trading partners. The Public Smart Routing component in TIBCO BusinessConnect does *not* support Smart Routing for messages received from the private processes (outbound messages).

Private Process Smart Routing

TIBCO BusinessConnect allows you to define simple business rules to route messages to specific private processes.

You can configure which messages should be routed to which private process instance using the TIBCO BusinessConnect server through the TIBCO Administrator GUI. You can specify a set of business rules, such as to route all messages from the trading partner A to the host B towards the private process C.

Configuring Private Process Smart Routing

Smart routing requires the following:

- Configuring the TIBCO BusinessConnect server through TIBCO Administrator
- Configuring of the private processes through the TIBCO BusinessConnect Palette in TIBCO Designer

Using TIBCO Administrator, you can set up the business rules and specify the smart ID to be assigned to messages that meet the conditions of the rule.

Business Rules for Private Process Smart Routing

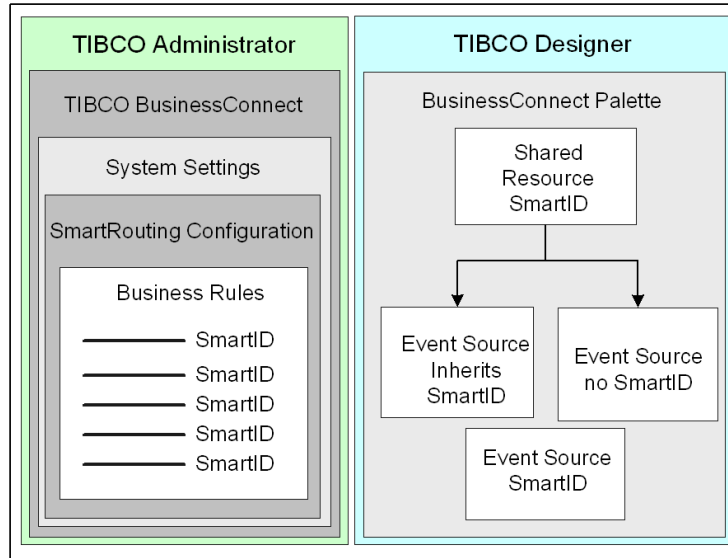
Business rules identify a set of messages based on one or more of these variables:

- Business protocol
- Sending partner
- Receiving partner
- Message direction (inbound or outbound)
- Operation ID

Using the TIBCO BusinessConnect Palette, you can configure which private processes will receive messages that include specific smart IDs.

As shown in [Figure 17](#), private processes can inherit a smart ID from a shared resource but do not have to. You can specify no Smart Routing for a private process within a shared resource, and you can also specify a smart ID for a private process outside of a shared resource.

Figure 17 Smart Routing



To see a step-by-step explanation on configuring Smart Routing for private processes, see *TIBCO BusinessConnect Trading Partner Administration, Private Process Smart Routing*.

To see how to configure rules for Smart Routing for private processes, see *TIBCO BusinessConnect Trading Partner Administration, Creating Business Rules for Private Process Smart Routing*.

Configuring Private Process Smart Routing for the TIBCO BusinessConnect Palette

When you select the check box **Use Smart Routing**, a text field named **Smart Routing ID** becomes visible and editable. By enabling this option on the shared resource, you can allow for the referencing event sources to use the specified smart ID value and inherit changes in the ID's value made on the given shared resource.

If you want the specific event source to define its own Smart Routing ID, the check box **Shared Smart ID** must be cleared and an individual smart ID can be specified to take precedence over the ID (if any) on the referenced shared resource.

Public Smart Routing

TIBCO BusinessConnect allows you to define simple business rules to route inbound public messages coming from your trading partners to be processed by multiple clusters of load balanced engines.

By defining the proper rules, you can strategically configure multiple clusters to prioritize and distribute workloads among a group of runtime engines so that you can optimize your hardware resources and maximize throughput. Here are a few examples:

- You can delegate one cluster to process EDI documents and another cluster for process RosettaNet documents by defining rules based on the various transport types.
- You can delegate a cluster for handling large messages by defining a rule based on the message size.
- You can delegate a cluster for handling Email messages sent from a specific trading partner by defining a rule based on the sender address.

Public Smart Routing utilizes a rule based engine that evaluates based on a set of fixed and known attributes that are available for each transport type. These attributes are checked against an inbound public message and the cluster that fits the best is designated for processing.

Inbound public transports that are supported for Public Smart Routing are as follows:

- HTTP/S
- Inbound File poller
- Inbound FTP-Get poller
- Inbound Email poller

The following sections discuss the concepts in details and describe the components that facilitate the functionality of Public Smart Routing:

- [Distributing Workload Among Engines](#)
- [Processing of Inbound Documents](#)
- [Routing Messages to the Designated Clusters](#)
- [Defining Rules for Public Smart Routing](#)
- [Server Groups and Clusters](#)

Distributing Workload Among Engines

In a single cluster deployment, a machine called Scheduler is selected and is responsible for dispatching each incoming document to a Worker engine for processing. Each Worker engine is configured identically to process documents in the same way, which results into a variety of documents being assigned to the Worker engine in a single queue. Under high load scenarios, workloads could become a backlog and processing of documents pending in the queue can be delayed.

A rule-based mechanism alleviates the likelihood of bottlenecks in cases such as:

- Large EDI documents may take hours to process while a small RosettaNet document requiring a synchronous response within minutes could time out.
- Documents received from specific trading partners that require faster response time may be delayed.
- A Worker engine that is heavily loaded with inbound documents may slow down the processing of outbound requests to the trading partners.
- Better hardware with high processing power may not be utilized efficiently within the cluster.

Processing of Inbound Documents

In TIBCO BusinessConnect, the inbound documents from trading partners are received through inbound public transports that reside either in the Gateway engines, or on one of the interior runtime engines in the cluster behind the firewall.

Gateway Engines

Gateway engines host many services, which are also called public transports:

- **HTTP/S** HTTP/S is supported for almost all protocols. Many message packaging and delivery standards such as AS2, S/MIME, and SOAP are also based on HTTP/S and are supported.
- **Inbound File Poller** This transport is only supported for limited protocols, such as EZComm and EDI.



For the HTTP/S and Inbound File Pollers transports, the Public Smart Routing component intercepts each incoming message and implements rule based logic in routing them to the internal clusters.

- **FTP Server** This transport is protocol specific and does not support inbound document smart routing.

- **PartnerExpress** This transport is protocol specific and does not support inbound document smart routing.
- **TCM Server** This transport is protocol specific and does not support inbound document smart routing.
- **SSH Server** This transport is protocol specific and does not support inbound document smart routing.

Interior Runtime Engines

The Interior runtime engines host the following:

- Inbound Email
- FTP-Get Pollers

The inbound Email and FTP-Get pollers transports are running behind the firewall and are responsible for receiving public messages on the POP and FTP servers. For these transports, the Public Smart Routing component intercepts each incoming Email and File message implements rule based logic in routing them to the internal clusters.

Rule Based Message Processing

Each transport type contains a set of fixed and known attributes available through the MIME headers, such as content type, content size, subject, URI, and so on. These attributes serve as the criteria to define rules and determine a designated unit for processing.

Here is how the messages are processed:

1. The Smart Routing component intercepts each inbound message and evaluates the corresponding list of attributes based on the transport type.
2. Based on the set of rules configured for each available cluster, the Smart Routing component derives a destination cluster and publishes an inter-component message that notifies the selected cluster.

If no rules are defined, the Smart Routing component is disabled by default and the one and only one cluster always receives notification for each public inbound message.

The inter-component message essentially triggers the processing of the inbound message by the corresponding selected cluster.

Routing Messages to the Designated Clusters

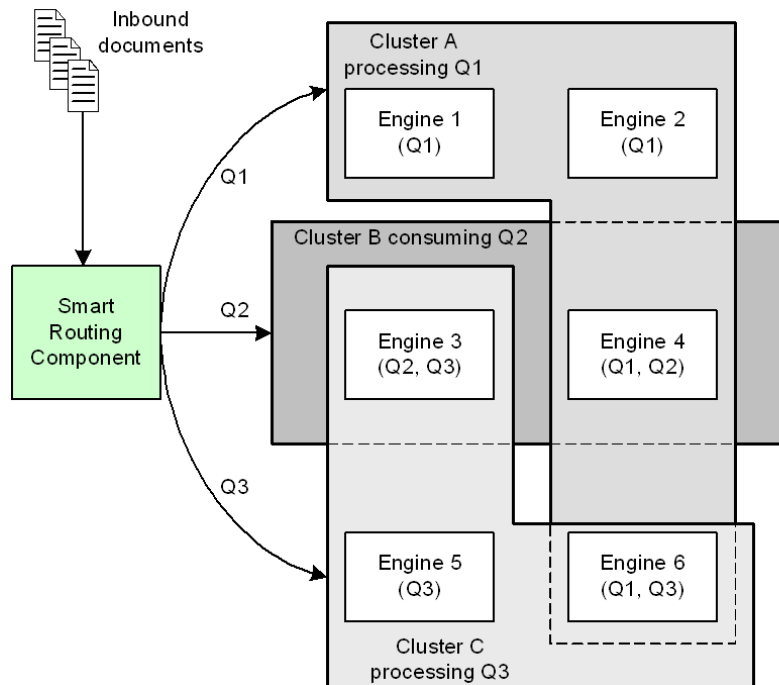
The public event sources are responsible for routing the messages to the designated cluster using a message queue.

A Scheduler machine within the cluster of runtime engines that participate in the message queue dispatches the message to a Worker engine for processing. The consumer of the message queue receives a notification messages from the public transport receivers and starts processing the messages from the queue.

Each runtime engine can be configured to process messages from more than one message queue, and can be load-balanced with more than one group of runtime engines.

Figure 18 shows three message queues processed by three clusters that consist of six runtime engines, where three of these engines are simultaneously participating in two clusters.

Figure 18 Message Queues and Clusters



Defining Rules for Public Smart Routing

The Smart Routing component is responsible for placing the inbound public messages to the appropriate queue for processing. It evaluates an incoming message against a set of rules in a predefined order of precedence. Each rule is bound to a single cluster and a cluster can be bound to multiple rules.

A destination cluster is selected when the first rule satisfies the conditions set forth in each rule. The Smart Routing rule is defined as a set of available email criteria based on the transport type, such as the following:

- Email size is less than 1MB (`Content_Size less than 1.000.0 bytes`)
- The sender address is `john@acme.com` (`Sender = john@acme.com`)

Depending on the configurations, a rule is satisfied when all or any of the criteria are met.

For the multiple clusters of runtime engines, the following definitions apply:

- Each public event source (Email, FTP-Get) dispatches to only one cluster of runtime engines.
- Each cluster contains one or more runtime engines.
- Each runtime engine participates in one or more message queues; each cluster has a separate message queue.
- Each message queue is identified by one or multiple rules.
- Each rule consists of one or more conditions
- Each condition consists of an attribute, an operator, and an operand
- Each attribute is defined based on the public inbound transport type.

Attributes, Operators, and Operands

The rules for defining clusters consist of the following elements:

- **Attributes** These are objects of a given type that extends the operand implementation by adding a name, default value, and transport property.
- **Operators** These objects determine the relationship between two (or more) operands.

Operators follow this rule:

- numeric operands support the following operators: `=`, `greater_than (>)`, `less_than (<)`, and `range`
- string operands support operators `matches`, and `=`
- Boolean operands support the operator `is`

- **Operands** These are objects that are a string, numeric, or Boolean.

For TIBCO BusinessConnect Public Smart Routing, a condition can have one attribute, operator, and one or more operands (in that order).

After you have defined all conditions, a rule for the routing mechanism is put together and displayed.

The routing mechanism based on the rules you have defined using the configurable conditions is now displayed in the field Rule Expressions, such as the following:

```
((Content_Size greater than 1000.0) and (Secure_SSL is false))
```

In this case, Smart Routing will occur when the file size is larger than 1KB *and* client authentication is not required.

Creating Smart Routing Rules

In many cases, you can create rules for different variations of the same protocol by using generic routing attributes. To rout messages received using a certain protocol, you can create the following rules:

- HTTPS or HTTPS_CA: create a rule for HTTP and use the expression `Secure_SSL = true`
- FTPS: create a rule for FTP and use the expression `Secure_SSL = true`
- Any HTTP transport (HTTP/S/CA) and messages which are larger than 2MB: create a rule for the transport HTTP and use the expression `Content_Size greater_than 2,097,152 bytes`

You can also use predefined (preconfigured) properties in expressions.

- File transport and messages which are larger than the currently specified threshold size: create a rule for the transport File and use the expression `Large_File = true`

Server Groups and Clusters

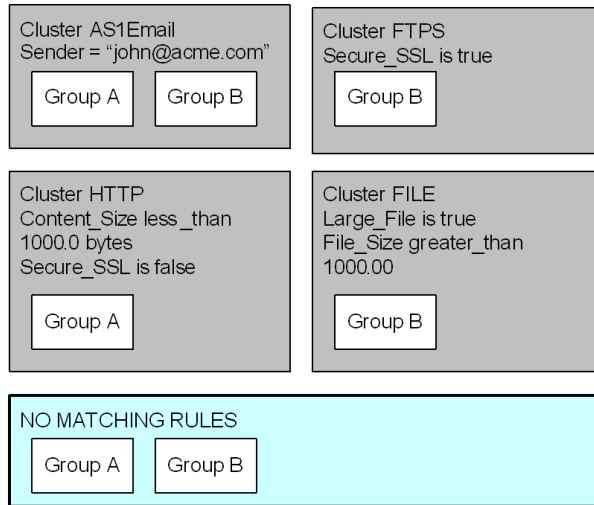
You will assign servers to fault tolerant groups using the procedure described in *TIBCO BusinessConnect Interior Server Administration*, Enable Service.

These fault tolerant groups of servers are later assigned to a cluster, or have rules configured which define the way they will be used in the system. Assigning (or adding) a group to a cluster does not mean that you are actually moving a group from one cluster to another: clusters can overlap and groups can share loads.

Assigning Groups to Clusters

An example of server groups assignments to multiple clusters is shown in Figure 19.

Figure 19 Server Group Assignment



In this example, the server groups Group A and Group B are assigned as follows:

- Group A is assigned to two clusters: Cluster AS1Email (processing email from the sender john@acme.com) and Cluster HTTP (Content_Size less_than 1000.0 bytes, and Secure_SSL is false)
- Group B is assigned to Cluster FILE (Large_File is true and File_Size greater_than 1000.00 bytes), Cluster FTPS (Secure_SSL is true), and Cluster AS1 Email (Sender = "john@acme.com").
- Both groups, and any not assigned groups, will be also assigned to the cluster called NO MATCHING RULES

When the described cluster rules are implemented, email messages will be routed as follows:

- Emails from the sender john@acme.com are routed to Group A or Group B for processing, where Group A and Group B will work in load balanced mode.
- Emails with file sizes less than 1000.00 bytes will be routed to Group A.
- Emails with file sizes greater than 1000.00 bytes will be routed to Group B.
- Emails that require a secure SSL connection will be routed to Group B, while the ones that do not require a secure SSL connection will be routed to Group A.
- Messages that don't match any rule will be discarded if no group was assigned to the default cluster (NO MATCHING RULES).

Assignment Order

Inbound messages will be delivered to the cluster that is defined by the *first* matching rule. In the example in [Figure 19](#), there are the following defined rules for the existing clusters:

```
Cluster AS1 Email: Sender = "john@acme.com"
Cluster HTTP: Content_Size less_than 1000.0 bytes; Secure_SSL is
false
```

If an inbound message comes in that corresponds to the rules

```
Sender = "john@acme.com"
```

and

```
Content_Size less_than 1000.0 bytes,
```

the following will happen:

- If the rule `Sender = "john@acme.com"` comes first and is true, the message will be assigned to the cluster AS1 Email.
- If the rule `Content_Size less_than 1000.0 bytes` comes first and is true, then the cluster HTTP will be used.

Any message may be evaluated as `true` for more than one rule and, therefore, the first matching rule will decide the group assignment.

NO MATCHING RULES

One group can belong to multiple clusters, including the cluster called NO MATCHING RULES (the cluster with no rules defined). When an inbound document is received that does not match any of the defined rules, it is sent to this cluster. By default, all service instances are added to this cluster and later can be assigned to another cluster. After you assign a fault tolerant group to a specific cluster, it is still listed under the cluster NO MATCHING RULES, where it can be added or removed at any time.

If there are no groups assigned to this cluster, all non-corresponding messages will be discarded.

Chapter 8 **Security**

This chapter gives an overview of the security mechanisms supported by TIBCO BusinessConnect.

Topics

- [Overview, page 78](#)
- [Public and Private Keys, page 80](#)
- [Digital Certificates, page 81](#)
- [Shadow Credentials, page 84](#)
- [Digital Signatures, page 86](#)
- [Encryption, page 87](#)
- [Digest Algorithms, page 88](#)
- [Supported SSHFTP Ciphers, page 90](#)
- [Cipher Suites, page 92](#)
- [Non-Repudiation, page 95](#)
- [SSHFTP Support in TIBCO BusinessConnect, page 98](#)

Overview

This chapter gives you a brief overview of the security methods used in TIBCO BusinessConnect. Use it only as an introduction and make sure that you understand how to protect your business data and communications by consulting other resources.

Secure Data

Confidentiality of the business data is protected using **encryption**, while the data **integrity** is protected by digest algorithms. These algorithms are utilized by digital signature algorithms to provide authentication services.

Encryption

Encryption means that plain text is converted into ciphertext to prevent any but the intended recipient from reading the data.

Encryption also achieves **privacy**, or concealing of information from unauthorized parties. It is based on the use of **private** and **public keys**, combined with secret key algorithms).



TIBCO BusinessConnect uses either PKI (Public Key Infrastructure) or OpenPGP for public and private keys.

Public key encryption is based on the premise that anyone is permitted to encrypt a message intended for a recipient, while only the recipient can decrypt such message. The person who created the ciphertext message cannot decrypt their own message since they do not have the private key it was encrypted for: only the holder of the matching private key can decrypt the message encrypted with a specific public key.

For more details, see [Encryption, page 87](#).

See also [Digest Algorithms, page 88](#) and [Cipher Suites, page 92](#).

Secure Communication

Secure communication is achieved using HTTPS over SSL or SSH, where the whole communication pipe is encrypted.

Authentication

Authentication is used to assure the identity of the partner with whom you are communicating. In a communication system, authentication verifies that messages do originate from their stated source, like the signature on a paper document. Authentication is based on **X.509 certificates** (for more information, see [Digital Certificates, page 81](#)).

Authorization

Authorization is secured through trading partner management, where permissions are set through binding to operations.

After the sender of a message has been authenticated, TIBCO BusinessConnect determines which operations the sender is currently allowed (authorized) to perform by checking trading partner information in the repository.

TIBCO BusinessConnect uses repository information to determine how it responds to a message from the partner. In some cases, the partner may not be authorized to perform certain interactions.

To conceal information from unauthorized parties and to assure privacy of business data, TIBCO BusinessConnect uses data encryption.

Non-repudiation

This is a property achieved through cryptographic methods that prevents an individual or entity from denying having performed a particular action related to data (such as mechanisms for non-rejection or authority, that is, origin; for proof of obligation, intent, or commitment; or for proof of ownership).

For more information, see [Non-Repudiation, page 95](#).

Non-repudiation depends on the use of **digital signatures** (for more information, see [Digital Signatures, page 86](#)).

Public and Private Keys

TIBCO BusinessConnect uses both PKI and PGP encryption methods to validate private and public keys. Both in PKI and in PGP method, each key pair has a public and a private part and messages are encrypted with the public part of the key and can only be decrypted with the associated private part of the key. This is done to ensure that only the intended recipient of the message can actually read it.

For creating and verifying signatures on messages, the holder of the private part of the key pair uses the private key to sign the message. Entities which have the public part of the key pair are then able to verify that the signature on the message was created by the holder of the private part of the key pair and therefore be assured that the message was sent by the holder of the private part of the key pair.

The following keys are supported in TIBCO BusinessConnect:

- **Public Keys** They are given to trading partners so that they can encrypt data and verify signatures.
 - **For PKI:** PKCS#7 public key identity format, which comes in the following file formats: .p7b and .p7c. Storing of individual X509 certificates in PEM (base64) and DER (ASN.1 Distinguished Encoding) formats is also supported.
 - **For PGP:** Key types supported are DSA/ElGamal and RSA public key.
- **Private Keys** They are used to decrypt data and to sign messages. The extension of the private key file name is most commonly referenced as .p12, but it may be anything else as long as the data in the file is compliant with the PKCS#12 specification.

Supported types for PGP are DSA/ElGamal and RSA private keys.

- **SSH Private and Public Keys** They are used to support the SSHFTP transport in TIBCO BusinessConnect.

To learn more about this topic, see [SSHFTP Implementation in TIBCO BusinessConnect, page 58](#). Follow the instructions given for the private or public keys (certificates) and make sure to upload an SSH key. Sample SSH keys are provided in the following location: `BC_HOME/samples/keys/ssh`. The disclaimer for use and information about these keys are available in the file `BC_HOME/samples/keys/ssh/Readme.txt`.

Digital Certificates



This section applies when using the PKI validation method since PGP keys do not use certificates for validation.

Digital certificates are data strings that a Certificate Authority (CA) creates after the CA verifies the identity of an entity that has submitted a CSR (Certificate Signing Request). When the CA signs and issues a certificate to a user, the CA's signature on the certificate verifies the authenticity of the link between the user's public key and the user's actual identity. A user can then use its certificate, as contained in its certificates file, to identify itself during e-commerce. The three basic items in a certificate are the CA's signature, the user's identity, and the user's public key.

A certificate is like a driver's license in that both are issued by a recognized authority (a CA or a governmental agency, respectively) and both identify the holder. Certificates are specified by the X.509 standard, such as X.509v3.

Digital certificates perform these functions:

- Certify the identity of the holder of the certificate
- Allow for non-repudiation of transactions
- Encrypt email messages
- Sign mobile code that can be downloaded by a web server

These certificates contain both a private key for the certificate holder and a public key for distribution to partners. They expire on a predetermined date. Digital certificates are based on the trust that both trading partners hold in the certificate authority. Some CAs are themselves authenticated using a certificate by a higher-level CA, which may in turn be authenticated by a certificate from an even higher-level CA. This results in a certificate chain.

Parties to a transaction exchange digital certificates. Then one party to a transaction — Party A — uses the other's public key to encrypt the transaction data. Then the other party — Party B — uses their own private key to decrypt the data.

Using Certificates with TIBCO BusinessConnect

There are three kinds of certificates you will use while working with TIBCO BusinessConnect and the PKI validation method:

Obtaining a Certificate

A large number of certificate authorities (CAs) are in the business of providing digital certificates (also called SSL certificates) to authenticate the identity of the certificate holder. You can obtain an SSL certificate from the web site of any authorized certificate authority (CA), such as:

- VeriSign: <http://www.verisign.com/>
- GeoTrust: <http://www.geotrust.com/>.



TIBCO BusinessConnect supports X509 certificates versions 1, 2, and 3.

All digital certificates used in TIBCO BusinessConnect must be compliant with the PKIX standard RFC #3280, which described on the following website:

<http://www.ietf.org>

Certificates Authority (CA)

This is a trusted third party that validates identities and issues X.509 certificates by signing the certificate with its signature. Any client or server software that supports certificates has a collection of trusted CA certificates, which determine the certificate issuers that the software can trust.

The root CA's certificate is unique in that it is a self-signed certificate. It is signed by the root CA itself. The CAs that are directly subordinate to the root CA in the CA hierarchy have CA certificates that were verified and signed by the root CA.

Certificate Chain

A certificate chain is a list of certificates, beginning with a Root certificate and ending with the user's X.509 certificate. Each certificate in the chain verifies the authenticity of the certificate that follows. Certification is achieved by the presence of a **digital signature** belonging to the authority issuing the certificate and authenticated by the preceding certificate in the chain.

The root certificate authenticates its own signature, which means that it is self-signed. Root certificates from well-known certifying authorities, such as VeriSign, or Thawte, are distributed with applications and kept in an application's trusted certificate store.

- **Root certificates** The certificate issued by the highest level certificate authority (CA) is called the root certificate.



You can add CA certificates directly to the certificate store outside of the partner configuration process. For information, see *TIBCO BusinessConnect Trading Partner Administration*, Adding Certificate Authority.

- **Leaf certificates** These certificates are issued to you directly from a CA. They are also called identity certificates.

You will acquire a leaf certificate from a CA by sending a Certificate Signing Request (CSR), which is associated with the private key of your server. To learn how to obtain a leaf certificate using CSR, see *TIBCO BusinessConnect Trading Partner Administration*, Creating New Identity.

- **Intermediate certificates** The certificates in the chain that lead up to the highest-level CA are called subordinate or intermediate certificates.



TIBCO BusinessConnect supports X509 certificates versions 1, 2, and 3. All digital certificates used in TIBCO BusinessConnect must be compliant with the PKIX standard RFC #3280, which is described on: <http://www.ietf.org>

Certificates File

A file that contains the private key's certificate chain. Unlike a key identity, it contains no private key and is not protected with a password. Trading partners exchange certificates files during the setup phase of their relationship. Each trading partner then installs the other partner's certificates file. For a host to verify the validity of a trading partner's certificate, the host must trust each CA's certificate in the certificate chain within the trading partner's certificates file. The certificates file defines how each trading partner should expect the other to identify itself in e-commerce transactions.

The supported format is PKCS#7 certificates only, which can have file extensions like .p7b and .p7c. When setting up an installation for e-commerce, the key identity file relates to the trading host and certificates file(s) relate to any trading partner(s) that the host has.

Storing Certificates

A certificate exists in a system file. To exchange business documents with a trading partner you must store the certificates as part of that participant. Hosts require a private key in addition to a public key certificate; partners only include public key certificates.

TIBCO BusinessConnect stores all certificates, including root, leaf, and intermediate certificates, in a central location: the credential store.

Shadow Credentials

Shadow credentials stand ready to take over for credentials that will expire. You define when the shadow credential takes effect. You can assign a shadow credential to any private key or certificate if all of these criteria are met:

- The valid time period for the shadow and base credentials overlap
- Shadow and base credentials are both valid at the time you assign the shadow
- Both credentials are still valid at the time when the shadow credential is to take effect



You cannot assign a shadow credential to another shadow credential. After the shadow credential takes effect, it is still a shadow credential. You have to remove or update the original credential and remove or promote the shadow credential.



HTTPS/HTTPSCA Only a shadow credential is used during overlay and shadow credential period for HTTPS and HTTPSCA transport level handshake of SSL/TLS and for client authentication.

TIBCO BusinessConnect supports shadow credentials to be on standby whenever the primary configured credential is about to expire. The activation of shadow credential can be set at the participant level, and it takes effect on the date that is specified.

The following terms and definitions are used to describe when shadow credential gets picked for different usages:

- **Original credential period** This is defined as the period between the date when the original credential was uploaded to the date before the activation date was set for the shadow credential.
- **Overlay period** This definition is applicable only when the shadow credential is associated with the original credential. It is defined as the period between the activation date of the shadow credential and the end of the original credential's expiration time.
- **Shadow credential period** This period starts when the original certificate expires and lasts until the shadow credential expires.

[Table 7](#) explains which credentials get picked for different operations. This behavior is valid for protocols that support plain Email/AS1/AS2 SMIME messaging.

Check the appropriate protocol documentation for behavior of SMIME message processing other than plain Email/ AS1/ AS2.

Table 7 *Type of Credentials Used During Different Periods*

Usage Description	Message Flow Direction	Type of Credential Used During Different Periods		
		Original Cred. Period	Overlay Period	Shadow Cred. Period
Message signing, encryption	Outbound to Partner	Original credential used	Shadow credential only	Shadow credential only
Message authentication and decryption	Inbound message from partner	Original credential used	Shadow credential used first, if it fails the original credential is tried	Shadow credential only

Digital Signatures

Authentication using digital signatures is done using S/MIME authentication. It involves adding a digital signature to the outgoing message.

Digital signatures are verifiable transformation made on a piece of data by the private key, which can be verified by using the corresponding public key. They bind a document to the possessor of a particular key.

Digital signatures are used to bind information to the identity of its originator. They can be used to provide data origin authentication, data integrity, and non-repudiation.

A digital signature includes the following parts:

- A certificate authority's distinguished name of the signer
- A sender's public key (optional)
- The serial number of the signer's certificate

To enable non-repudiation, TIBCO BusinessConnect uses S/MIME to add a digital signature to each outbound public message, checks inbound public messages for a digital signature, and stores incoming messages in the non-repudiation database. Non-repudiation depends on authentication using digital signatures.

To learn more about non-repudiation in TIBCO BusinessConnect, see [Non-Repudiation, page 95](#).

Encryption

Encryption is available through the following security mechanisms:

- **SSL** This protocol uses public and private keys to enable encryption of the transport protocol on which an encrypted or unencrypted message travels.
- **S/MIME** This message packaging and signing protocol uses public and private keys to enable encryption and decryption of a message.
- **SSH** SSH keys are used to support the SSHFTP transport in TIBCO BusinessConnect. This protocol provides transport layer security with both server and client authentication by establishing a secured channel through key negotiation and strong encryption algorithms.

For more information about SSH, see [SSHFTP Support in TIBCO BusinessConnect](#), page 98.

Digest Algorithms

Digest algorithms utilized in digital signatures provide help in detecting changes in the signed payload since the signature has been generated on the content. The procedure of verifying that no unauthorized changes were made on the signed content is called the “verification of the digital signature”. If verification is successful, parties can be certain that the document has been created by the signing party and that it was unaltered since its signing.

TIBCO BusinessConnect offers these digest algorithms to verify digital signatures:

- SHA1
- SHA-256
- SHA-384
- SHA-512

Encryption Algorithms

Encryption algorithms are used in two different contexts:

- Transport layer
- Business layer

In the transport layer, the encryption takes place on the transport connection, which considers the data moved through it opaque. The negotiation of the symmetric keys takes place by an asymmetric algorithm utilized and defined in SSL/TLS or SSH.

In the business layer, business documents' payloads are encrypted as per the specification of the given business protocol.

These options can be used independently from each other.

There are multiple encryption algorithms available for use. You and your business partner must use the same encryption algorithm; otherwise, decryption is not possible.

The number included in the name of the algorithm is the number of bits. This is independent of the bit size of the certificate. The larger the algorithm bit size, the more secure the encryption.

TIBCO BusinessConnect supports following encryption algorithms for the encryption of transport layer and business layer:

- DES3

- AES-128
- AES-192
- AES-256

Supported SSHFTP Ciphers

The following ciphers are supported for SSHFTP protocol:

Key Exchange Algorithms

ECDH-SHA2-NISTP256
 ECDH-SHA2-NISTP384
 ECDH-SHA2-NISTP521
 DIFFIE-HELLMAN-GROUP14-SHA256
 DIFFIE-HELLMAN-GROUP14-SHA1
 DIFFIE-HELLMAN-GROUP-EXCHANGE-SHA256
 DIFFIE-HELLMAN-GROUP-EXCHANGE-SHA1
 DIFFIE-HELLMAN-GROUP1-SHA1

Encryption

AES128-CTR
 AES128-CBC
 AES192-CTR
 AES192-CBC
 AES256-CTR
 AES256-CBC
 BLOWFISH-CTR
 BLOWFISH-CBC
 3DES-CTR
 3DES-CBC
 ARCFOUR128
 ARCFOUR256
 ARCFOUR
 RIJNDAEL-CBC@LYSATOR.LIU.SE

Server host keys

ECDSA-SHA2-NISTP256
 ECDSA-SHA2-NISTP384
 ECDSA-SHA2-NISTP521
 RSA-SHA2-512
 RSA-SHA2-256
 SSH-RSA
 SSH-DSA

Macs

HMAC-SHA2-256*
 HMAC-SHA2-512*
 HMAC-SHA256@SSH.COM*
 HMAC-SHA512@SSH.COM*
 HMAC-SHA1
 HMAC-SHA1-96*
 HMAC-MD5-96

* Macs that can not be selected from the TIBCO BusinessConnect GUI.

Compression
NONE
ZLIB
ZLIB@OPENSSH.COM

Cipher Suites

The following cipher suites are supported for TIBCO BusinessConnect:



The ciphers for all SSL/TLS based secure protocols are implemented by the underlying Java platform. For more information about supported ciphers, see the official Java documentation.

Displayed in the Gateway Server Logs

```
TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384
TLS_RSA_WITH_AES_256_CBC_SHA256
TLS_ECDH_ECDSA_WITH_AES_256_CBC_SHA384
TLS_ECDH_RSA_WITH_AES_256_CBC_SHA384
TLS_DHE_RSA_WITH_AES_256_CBC_SHA256
TLS_DHE_DSS_WITH_AES_256_CBC_SHA256
TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA
TLS_RSA_WITH_AES_256_CBC_SHA
TLS_ECDH_ECDSA_WITH_AES_256_CBC_SHA
TLS_ECDH_RSA_WITH_AES_256_CBC_SHA
TLS_DHE_RSA_WITH_AES_256_CBC_SHA
TLS_DHE_DSS_WITH_AES_256_CBC_SHA
TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256
TLS_RSA_WITH_AES_128_CBC_SHA256
TLS_ECDH_ECDSA_WITH_AES_128_CBC_SHA256
TLS_ECDH_RSA_WITH_AES_128_CBC_SHA256
TLS_DHE_RSA_WITH_AES_128_CBC_SHA256
TLS_DHE_DSS_WITH_AES_128_CBC_SHA256
TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA
TLS_RSA_WITH_AES_128_CBC_SHA
TLS_ECDH_ECDSA_WITH_AES_128_CBC_SHA
TLS_ECDH_RSA_WITH_AES_128_CBC_SHA
TLS_DHE_RSA_WITH_AES_128_CBC_SHA
TLS_DHE_DSS_WITH_AES_128_CBC_SHA
TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384
TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256
TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
TLS_RSA_WITH_AES_256_GCM_SHA384
TLS_ECDH_ECDSA_WITH_AES_256_GCM_SHA384
TLS_ECDH_RSA_WITH_AES_256_GCM_SHA384
TLS_DHE_RSA_WITH_AES_256_GCM_SHA384
TLS_DHE_DSS_WITH_AES_256_GCM_SHA384
TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
TLS_RSA_WITH_AES_128_GCM_SHA256
TLS_ECDH_ECDSA_WITH_AES_128_GCM_SHA256
```

```

TLS_ECDH_RSA_WITH_AES_128_GCM_SHA256
TLS_DHE_RSA_WITH_AES_128_GCM_SHA256
TLS_DHE_DSS_WITH_AES_128_GCM_SHA256
TLS_ECDHE_ECDSA_WITH_3DES_EDE_CBC_SHA
TLS_ECDHE_RSA_WITH_3DES_EDE_CBC_SHA
SSL_RSA_WITH_3DES_EDE_CBC_SHA
TLS_ECDH_ECDSA_WITH_3DES_EDE_CBC_SHA
TLS_ECDH_RSA_WITH_3DES_EDE_CBC_SHA
SSL_DHE_RSA_WITH_3DES_EDE_CBC_SHA
SSL_DHE_DSS_WITH_3DES_EDE_CBC_SHA

```

Export and Stronger

```

TLS_RSA_WITH_AES_128_CBC_SHA (0x002f)
TLS_RSA_WITH_RC4_128_SHA (0x0005)
TLS_RSA_WITH_RC4_128_MD5 (0x0004)
TLS_RSA_WITH_3DES_EDE_CBC_SHA (0x00a)
TLS_RSA_WITH_DES_CBC_SHA (0x0009)
TLS_RSA_EXPORT_WITH_RC4_40_MD5 (0x0003)
TLS_RSA_EXPORT_WITH_RC2_CBC_40_MD5 (0x0006)
TLS_RSA_EXPORT_WITH_DES40_CBC_SHA (0x0008)
TLS_DHE_DSS_WITH_AES_128_CBC_SHA (0x0032)
TLS_DHE_DSS_WITH_3DES_EDE_CBC_SHA (0x0013)
TLS_DHE_DSS_WITH_DES_CBC_SHA (0x0012)
TLS_DHE_DSS_EXPORT_WITH_DES40_CBC_SHA (0x0011)
TLS_DHE_RSA_WITH_AES_128_CBC_SHA (0x0033)
TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA (0x0016)
TLS_DHE_RSA_WITH_DES_CBC_SHA (0x0015)
TLS_DHE_RSA_EXPORT_WITH_DES40_CBC_SHA (0x0014)
TLS_RSA_WITH_AES_256_CBC_SHA (0x0035)
TLS_DHE_DSS_WITH_AES_256_CBC_SHA (0x0038)
TLS_DHE_RSA_WITH_AES_256_CBC_SHA (0x0039)

```

Stronger than Export

```

TLS_RSA_WITH_AES_256_CBC_SHA (0x0035)
TLS_DHE_DSS_WITH_AES_256_CBC_SHA (0x0038)
TLS_DHE_RSA_WITH_AES_256_CBC_SHA (0x0039)
TLS_RSA_WITH_3DES_EDE_CBC_SHA (0x00a)
TLS_DHE_DSS_WITH_3DES_EDE_CBC_SHA (0x0013)
TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA (0x0016)
TLS_RSA_WITH_AES_128_CBC_SHA (0x002f)
TLS_RSA_WITH_RC4_128_SHA (0x0005)
TLS_DHE_DSS_WITH_AES_128_CBC_SHA (0x0032)
TLS_DHE_RSA_WITH_AES_128_CBC_SHA (0x0033)
TLS_RSA_WITH_RC4_128_MD5 (0x0004)
TLS_RSA_WITH_DES_CBC_SHA (0x0009)
TLS_DHE_DSS_WITH_DES_CBC_SHA (0x0012)
TLS_DHE_RSA_WITH_DES_CBC_SHA (0x0015)

```

128-Bit and Stronger

```

TLS_RSA_WITH_AES_256_CBC_SHA (0x0035)
TLS_DHE_DSS_WITH_AES_256_CBC_SHA (0x0038)

```

```
TLS_DHE_RSA_WITH_AES_256_CBC_SHA (0x0039)
TLS_RSA_WITH_3DES_EDE_CBC_SHA (0x00a)
TLS_DHE_DSS_WITH_3DES_EDE_CBC_SHA (0x0013)
TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA (0x0016)
TLS_RSA_WITH_AES_128_CBC_SHA (0x002f)
TLS_RSA_WITH_RC4_128_SHA (0x005)
TLS_DHE_DSS_WITH_AES_128_CBC_SHA (0x0032)
TLS_DHE_RSA_WITH_AES_128_CBC_SHA (0x0033)
TLS_RSA_WITH_RC4_128_MD5 (0x0004)
```

Stronger than 128-Bit

```
TLS_RSA_WITH_AES_256_CBC_SHA (0x0035)
TLS_DHE_DSS_WITH_AES_256_CBC_SHA (0x0038)
TLS_DHE_RSA_WITH_AES_256_CBC_SHA (0x0039)
TLS_RSA_WITH_3DES_EDE_CBC_SHA (0x00a)
TLS_DHE_DSS_WITH_3DES_EDE_CBC_SHA (0x0013)
TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA (0x0016)
```

256-Bit and Stronger

```
TLS_RSA_WITH_AES_256_CBC_SHA (0x0035)
TLS_DHE_DSS_WITH_AES_256_CBC_SHA (0x0038)
TLS_DHE_RSA_WITH_AES_256_CBC_SHA (0x0039)
```

Non-Repudiation

Non-repudiation is a technical solution to a legal issue: it prevents trading partners from falsely denying having participated in a communication or denying the validity of the communication or its parts.

For example, a non-repudiation protocol for a digital, certified document should ensure that the sender cannot deny sending the message and the receiver cannot deny receiving it. A public key digital signature can provide non-repudiation of electronic transactions if it can be guaranteed that the digital signature was created when the public key credentials were valid.

TIBCO BusinessConnect implements Public Key Infrastructure (PKI) to support non-repudiation for document exchange. This approach to non-repudiation uses public key signatures to provide authentication.

TIBCO BusinessConnect uses digital signatures, authentication, and logging to support the following non-repudiation scenarios:

- NRO (Non-Repudiation of Origin)
- NRR (Non-Repudiation of Receipt for AS1/AS2 Transport)



Only signed MDN receipts can be logged in the TIBCO BusinessConnect non-repudiation scheme. See Message Disposition Notification Receipts in *TIBCO BusinessConnect Trading Partner Administration* for more information.

Non-Repudiation Logging Scenarios in TIBCO BusinessConnect

After the inbound message is validated, the Responder logs the signed original request in its non-repudiation database because non-repudiation of request is selected in the Responder's trading partner setup for that Initiator. Non-repudiation for inbound transactions can be enabled in the trading partner setup.

Non-Repudiation of Origin

For more information, see the chapter on Acknowledgments in *TIBCO BusinessConnect EDI Protocol powered by Instream User's Guide*.

Non-Repudiation Logging of Acknowledgments on Responder

1. The Responder creates an acknowledgment because the Initiator's setup for the trading partner was configured to ask for an acknowledgment. The Responder signs the acknowledgment with its private key because, in the

trading partner transport setup for the Initiator, non-repudiation is selected, the Sign check box is selected, and a signed receipt for the acknowledgment is selected.

2. The Responder sends the signed acknowledgment to the Initiator.
3. The Responder logs the signed acknowledgment in its non-repudiation database after the message is successfully posted to the Initiator. This occurs because non-repudiation was selected in the Initiator's outbound transport setup for the trading partner.
4. The Initiator receives the signed acknowledgment and sends a receipt to the Responder because a receipt was requested in the transport setup for the Responder trading partner.
5. The Responder logs the receipt from the Initiator in its non-repudiation database because non-repudiation was selected in the transport setup for the Initiator trading partner.

Non-Repudiation Logging of Acknowledgments on Initiator

1. The Initiator authenticates acknowledgments for content integrity.
2. The Initiator reconciles acknowledgments and logs the original, signed acknowledgment from the Responder in the non-repudiation database.
3. The Initiator calculates the message digest for the acknowledgment.
4. The Initiator sends a signed receipt to the Responder.

Non-Repudiation of Receipt for AS1/AS2 Transport

Non-Repudiation Logging on Initiator

1. The Initiator creates a request document and uses its private key to sign it because non-repudiation is selected in the outbound host to partner transport setup for the trading partner. The outbound document includes a request for a synchronous or asynchronous signed receipt from the Responder because a signed receipt is requested in the outbound transport setup for the trading partner.
2. The Initiator sends the request.
3. The Initiator logs the request after a successful HTTPS post of the message to the trading partner or VAN. This also true for an email sent successfully through SMTP to the trading partner or VAN.
4. The Responder receives the request from the Initiator.

5. The Responder sends a receipt to the Initiator because the inbound document contains a request for a receipt.
6. The Initiator logs the receipt from the Responder because non-repudiation was selected in the Initiator's outbound host to partner transport setup for the trading partner.

Non-Repudiation Logging on Responder

1. When a Responder receives a signed document that includes a request for a synchronous or asynchronous signed receipt, the Responder uses the Initiator's public certificate to verify the content integrity.
2. The Responder calculates the message digest for the document.
3. The Responder creates the receipt, uses its private key to sign it, and sends it back to the Initiator.
4. The Responder logs the signed original request in its non-repudiation database because non-repudiation of request is selected in the Responder's trading partner setup for that Initiator.

SSHFTP Support in TIBCO BusinessConnect

To support the SSHFTP transport in TIBCO BusinessConnect, the following types of keys, certificates, and algorithms are available:

- Key types: RSA, DSA
- Public key formats: OpenSSH PEM and Ssh.Com* (with import and export)
- Private key formats: OpenSSH PEM and Ssh.Com** (with import); OpenSSH PEM (with export)
- Host signature algorithms: SSH-RSA and SSH-DSS
- Server public key algorithms: DSA and RSA.

Authentication Methods for SSHFTP

The supported authentication methods are password, public key, and a combination of password and public key. The client is always identified by a user name, whether the authentication takes place over password, public key or both. The SSH server drives the authentication (requests the preferred authentication methods) and the SSH client obeys by submitting the credentials, which are specific to the requested/agreed-upon method or methods.

- **Password** The configured password is used to complete the user authentication phase with the SSH server.
- **Public key** The configured public key (retrieved from the user's SSH private key) is used to complete the user authentication phase with the SSH server.
- **Public key and Password** TIBCO BusinessConnect is allowed authenticate using password, public key, or both password and public key. If the SSH server indicates both options, TIBCO BusinessConnect starts using the 'public key' method. If it is successful and the server requires no further authentication steps to be executed, the negotiation is successful and the tunnel is established.

If the server rejects the authentication attempt, TIBCO BusinessConnect will move to password mode, in which case the outcome depends on the success of this attempt. If the password fails, the transport creation fails and the framework sends the corresponding error message to the business protocol.

When either 'Public Key' or 'Public Key and Password' is selected, the sending participant must be configured with an SSH private key since the transport assumes that this credential is made available to (and may be requested by) the SSH server. The client's private key for any inbound or outbound SSHFTP transport is configured through the field 'Client Authentication Identity for SSHFTP' on the corresponding business agreement of the sending and receiving participants.

SSH Server Public Key Retriever

As an administrator, you may face problems finding, installing and configuring the public keys of SSH servers of the trading partners while setting up and configuring inbound and outbound SSH transports in TIBCO BusinessConnect. Sometimes, it is a priority to be able set up a working connection quickly, instead of taking enough time to ensure that the identities of the peer trading partners' SSH servers be trusted by retrieving the servers' credentials only from verified/trusted sources.

The SSH Server Public Key Retriever was added to facilitate speedy setup of a working connection, and to help establish a trusted connection. To use the SSH Server Public Key Retriever, see the **fetch from ssh server** field in *TIBCO BusinessConnect Trading Partner Administration*, "SSHFTP Transport."

Selecting Algorithms and Methods during Tunnel Negotiation

Tunnel negotiation is driven by the SSH server and controlled by the SSH client. This means that the ciphers, MAC, compression algorithms and authentication methods are specified by a list that is offered by the server and chosen by the client. If the option ANY is set for either cipher, MAC, or compression, the server's first choice of preference will be used, which is also supported by the client. TIBCO BusinessConnect always acts as the SSH client, regardless of the direction of the transport (such as inbound or outbound).

Supported Ciphers for SSHFTP

For the list of supported ciphers, see [Non-Repudiation](#). If configured to ANY, then any of the supported ciphers can be selected by the server.

Supported MACs for SSHFTP

HMAC-SHA2-256*
 HMAC-SHA2-512*
 HMAC-SHA256@SSH.COM*
 HMAC-SHA512@SSH.COM*
 HMAC-SHA1
 HMAC-SHA1-96*
 HMAC-MD5-96

* Macs that can not be selected from the TIBCO BusinessConnect GUI.

If configured to ANY, then any of the supported MACs can be selected by the server.

Supported Compression Algorithms for SSHFTP

Zlib
 Zlib@openssh.com

If `NONE` is selected, no compression is enforced by the client. This assumes that the SSH server also considers '`NONE`' to be a valid option.

Glossary

A

ack

A return message in a B2B request/response transaction indicating that data has been received correctly. Typically, if the sender of the original data does not receive an ack message before a predetermined time, or receives a nack, the sender re-sends the original data. See also *nack*.

asynchronous transaction type

A request/response transaction type in which the Responder sends a response on a channel other than the sending channel. See also *synchronous transaction type*.

B

B2B

Business to Business. Electronic, integrated communication between businesses, usually over the Internet or over a VPN. See also *VPN*.

BLOB Data

Binary Large Object is a large collection of binary data which is stored in the database system.

C

CA

Certificate Authority. See also *Certificate Authority*.

CDATA

Character data. CDATA has two very different meanings in XML. The first meaning is used within document type declarations, where CDATA is used within attribute declarations to indicate that an attribute should contain character content, and that no enumerated set of values is provided to constrain that content.

The second meaning applies only within documents, where CDATA marked sections (beginning with `<![CDATA[` and ending with `]]>`) label text within documents that is purely character data, containing no elements or entities that need to be processed. CDATA sections provide an escape mechanism supporting documents containing characters (typically `<`, `>`, and `&`) that would interfere with normal processing.

certificate

A data string that a Certificate Authority (CA) creates after the CA verifies the identity of an entity that has submitted a CSR (Certificate Signing Request).

A certificate is in a certificate chain. See also *certificate chain*.

Certificate Authority (CA)

A trusted third party that validates identities and issues X.509 certificates by signing the certificate with its signature.

certificate chain

A list of certificates made up of a user's X.509 digital certificate and the certificate chain of its CA's certificates.

A certificate chain can be in a certificates file. See also *certificates file*.

A certificate chain can also be in a key identity file. See also *key identity file*.

certificates file

A file that contains a private key's certificate chain.

ChemXML™

An XML-based data exchange standard for buying, selling, and delivering chemicals. CIDX™ (Chemical Industry Data eXchange) developed ChemXML on a non-profit basis for use in the chemical industry to conduct electronic business transactions and exchange data in company-to-company, company-to-marketplace, and marketplace-to-marketplace transactions.

CIDX™

See *ChemXML*.

ciphertext

Data that has been encrypted.

cleartext

Data that has not been encrypted.

CMS

Cryptographic Message Syntax. The internal format of an S/MIME message. See also *S/MIME*.

CRM

Customer Relationship Management. A type of software that automates a company's sales force, marketing efforts, and customer service needs.

CSR

Certificate Signing Request. The file that you send to a CA such as Verisign when you request a certificate. The CSR contains your email address and certain identifying information.

CSV

Common Separated Values. A message structure format.

custom reports

The reports which are created based on the combination of different user-defined specifications and requirements.

cXML

Commerce XML. An XML format developed for documents used in e-procurement. See www.cxml.org for more information. See also *XML*.

D

DBMS

Data Base Management System. A complex set of programs that controls the organization, storage, and retrieval of data for many users. Data is organized in fields, records, and files. A database management system also controls the security of the database.

deep linking

The ability to send the users directly to a specific point in the application other than an external homepage or website. In this document, deep linking refers to the functionality in which the link to the custom reports can be shared with other users directly.

digital certificate

See *certificate*.

digital signature

See *signature*.

document type declaration

A declaration that provides a document type definition (DTD) for an XML document. The document type declaration may refer to an external file (the external subset), include additional declarations (the internal subset), or combine both. The document type declaration also gives the root element for the document.

DTD

Document Type Definition. A non-XML schema file that contains a formal description of the vocabulary and structure of the elements in an associated XML file. DTDs serve the same function as XML schema documents. A DTD may also provide some content information. The DTD for an XML document is the combination of the internal and external subsets described by

the document type declaration. See also *XML*. Also see www.extensibility.com for information on TIBCO's XML Authority, the premier solution for the creation, conversion, and management of DTDs and XML schemas.

DUNS Number

A number in the Data Universal Numbering System from Dun & Bradstreet. BusinessConnect uses DUNS numbers for RosettaNet.

E

ebXML

electronic business XML. An XML e-commerce standard defined by the ebXML consortium. See www.ebxml.org.

EDI

Electronic Data Interchange. A native SAP message format. EDI is most often used by trading partners in the exchange of standardized documents. EDI uses some variation of the ANSI X12 standard (USA) or EDIFACT (UN-sponsored global standard).

element

The unit forming the basic structure of XML documents. Elements may contain attributes in their start tags, other elements, and textual content. See also *XML*.

ERP

Enterprise Resource Planning. An integrated information system that serves all departments within an enterprise. An ERP system can include software for manufacturing, order entry, accounts receivable and payable, general ledger, purchasing, warehousing, transportation and human resources.

exception

At the software level, anything that has gone wrong, typically within a lower level code module. At the business process level, an exception is anything that requires special processing to account or adjust for, such as correcting an invalid order.

F**FTP**

File Transfer Protocol. A client-server protocol which allows a user on one computer to transfer files to and from another computer over a TCP/IP network. Also used to refer to the client program the user executes to transfer files. See also *TCP/IP*.

H**HTTP**

Hypertext Transfer Protocol. A client-server TCP/IP transport protocol used on the web for exchanging documents. By default, HTTP uses port 80. See also *TCP/IP*.

HTTPS

Hypertext Transfer Protocol, Secure. A variant of HTTP used for creating secure transactions. HTTPS uses SSL to encrypt the HTTP transport. Messages sent over the secure transport are not themselves encrypted. By default, HTTPS uses port 443. See also *SSL*.

I**IMAP, IMAP4**

Internet Message Access Protocol. A transport protocol for email clients to retrieve email from a message store on a host server. IMAP is newer and has more features than the more popular POP access protocol. See also *POP*.

J**JSSE**

Java™ Secure Socket Extension. A Java standard that enables SSL. As SSL is not part of Java, different vendors offer different JSSE implementations. See also *SSL*.

K**key identity file**

A file that contains a private key and its certificate chain. It is encrypted with a password because it contains a private key. Trading partners create a key identity for their own installations. When setting up an installation for e-commerce, the key identity file relates to the trading host and certificates file(s) relate to any trading partner(s) that the host has. TIBCO ActiveExchange products support PKCS#12 (.p12 or .pfx) (as implemented by Netscape and Microsoft and others).

key pair

A private/public key pair.

M

MAPI

Messaging Applications Programming Interface. A proprietary interface to client email servers.

MIME

Multipurpose Internet Mail Extensions. A standard structured messaging format which allows a single message to contain many parts, such as plain text, web hypertext documents, graphics, audio, and fax. MIME specifies how messages must be formatted so that they can be exchanged between different email systems. MIME is a very flexible format, which can include virtually any type of file or document in an email message. MIME uses base64 and other encodings to encode non-text information as text to make sure that email messages with images or other non-text information are delivered with maximum protection against corruption. For example, a MIME message may have a header, body, and digital signature. See also *S/MIME*.

N

nack

A return message indicating that data has not been received correctly. See also *ack*.

non-repudiation

Non-repudiation of service allows the sender of a message to provide the recipient of a message proof of the origin of the message. This protects against any attempt by the sender to subsequently revoke the message or its content. This is based on a sender's unique digital signature.

P

parsed

For XML, data that has been converted to the TIBCO IntegrationManager internal representation (AttributeNode) and which can be accessed at the field level by other components. See also *unparsed*.

PGP

PGP does not use Certification Authorities and leaves it to the user to verify the fingerprint of public keys with the owner of the matching private key. Once this is done, the user can then sign the public key to validate it.

PIP

Partner Interface Process. Part of the RosettaNet business protocol.

PKI

Public Key Infrastructure. The infrastructure necessary to successfully use public key cryptography, including certificates and certificate authorities.

PKI uses a Certification Authority to issue digital certificates that certify the ownership of a public key by the named subject of the certificate.

POP, POP3

Post Office Protocol. A client-to-host transport protocol for email clients to retrieve email from a message store. POP is more widely used than the IMAP protocol, which has more features. See also *IMAP*.

private key

The part of a key pair that is kept strictly confidential. It is encrypted with a password. It is used for message decryption and for signing. A private key is kept in a key identity file.

public key

The part of a key pair that can be shared with anybody. It is used for message encryption and for verifying a signature.

public key cryptography

A system that offers encryption and digital signatures. Each user has a public key and a private key. The public key is made public while the private key remains private. A sender encrypts a document using the recipient's public key. The recipient decrypts the document using their private key. The sender also signs a document using their private key. The recipient authenticates the sender using the sender's public key. See also *symmetric key cryptography*.

R**request/response**

A type of message that requires a response from the receiver. This can be synchronous or asynchronous.

RNIF

RosettaNet Implementation Framework.

RosettaNet

An industry consortium dedicated to the development and deployment of RosettaNet, a standardized electronic business interface. See www.rosettnet.org for more information.

RV

Rendezvous protocol. A distributed TIBCO messaging protocol middleware product.

S**schema**

See *XML schema*.

SGML

Standard Generalized Markup Language. A generic language for representing hypertext documents.

signature

A verifiable transformation made on a piece of data by the private key, which can be verified by using the public key. A digital signature binds a document to the possessor of a particular key. A signature usually also contains the possibly incomplete certificate chain of the signer. See also *certificate*.

S/MIME

(Secure Multipurpose Internet Mail Extensions) presents a way of adding security to objects that are packaged with MIME. It is a messaging format for exchanging digitally signed and/or encrypted messages.

S/MIME defines a data encapsulation format for the provision of a number of security services that include data integrity, confidentiality, and authentication. S/MIME is designed for messaging clients delivering security services to distributed messaging applications. S/MIME (RFC 2311) is based on the MIME standard (RFC 1521).

SMTP

Simple Mail Transport Protocol. A host-to-host mail transport protocol for email. As it is a server-to-server protocol, other protocols such as IMAP, POP, and POP3 are used to retrieve the email from the host's mail server. SMTP is the standard for servers that move email over the Internet.

SOAP

Simple Object Access Protocol. A network protocol developed by Microsoft, among others, that provides a lightweight method for exchanging structured data. SOAP messages are XML documents contained in a mandatory SOAP envelope and sent using HTTP or HTTPS.

SQL

Structured Query Language. A language for accessing data in a database.

SSL

Secure Sockets Layer. A protocol designed by Netscape Communications Corporation to encrypt data and authenticate senders. SSL is the industry standard for sharing secured data over the web. SSL provides encryption, client and server authentication, and message integrity. SSL is part of all major browsers and web servers. Installing a digital certificate makes a browser or server's SSL capabilities available. SSL is layered beneath protocols such as HTTP, SMTP, Telnet, FTP, Gopher, and NNTP. SSL is layered above the TCP/IP connection protocol. SSL can use digital certificates to authenticate an encrypted socket. A client signs random data with a private key during the setup phase of an SSL connection to authenticate itself. Encrypted data sent after the setup phase is not signed. SSL is available at the 40-bit, 56-bit, and 128-bit levels. This refers to the length of the session key that every encrypted conversation generates. The longer the session key is, the more difficult it is to break the encryption code.

BusinessConnect supports different levels of SSL, including the highest level, which uses server and client authentication. SSL is used by HTTPS. See also *HTTPS*.

symmetric key cryptography

A system that offers encryption. The same key is used to encrypt and unencrypt data. A sender encrypts a document using the symmetric key, and the recipient decrypts the document using the same symmetric key. See also *public key cryptography*.

synchronous transaction type

A request/response transaction type in which the Responder sends a response on the sending channel. See also *asynchronous transaction type*.

T

TCP/IP

Transmission Control Protocol on top of the Internet Protocol. Protocols to enable communication between different types of computers and computer networks. TCP is a connection-oriented protocol that provides reliable communication and multiplexing. IP is a connectionless protocol that provides packet routing.

type-aware

A document that uses a schema of some sort. The in-memory representation of 'type-aware' data uses strings, numbers, and arrays, among others. See also *untyped*.

U

unparsed

For XML, an XML document in the form of a giant string or byte array. TIBCO IntegrationManager components, unless they have special support for parsing XML, can utilize XML only as a string byte array. See also *parsed*.

untyped

A document that does not use a schema. The in-memory representation of untyped data is an array of name->value pairs. For XML, it is an array of name->(string or element) pairs, and character data is represented by some 'special' name, such as `_CDATA`. See also *type-aware*.

URI

Uniform Resource Identifier. A resource identifier that describes a location (URL) or name (URN) for identifying an abstract or physical resource.

URL

Uniform Resource Locator. A resource identifier that describes its target by giving a pathway for retrieving it. A URL may include a protocol, a host computer, and how to find the target resource on that computer.

URN

Uniform Resource Number. A resource identifier that uses a naming scheme to identify resources.

V

VAN

Value-added network. A communications network in an EDI setting that provides services beyond normal transmission, such as automatic error detection and correction, protocol conversion, and message storing and forwarding.

VPN

Virtual Private Network. A network that is configured within a public network. For years, common carriers have built VPNs that appear as private national or international networks to the customer, but physically share backbone trunks with other customers. VPNs enjoy the security of a private network via access control and encryption, while taking advantage of the economies of scale and built-in management facilities of large public networks.

X

XML

eXtensible Markup Language. A standardized document formatting language that provides a set of standards for document syntax while allowing developers, organizations, and communities to define their own vocabularies. XML is a standard for passing data between Internet applications. XML lets users label information using custom tags that describe the structure and meaning of a file's content. XML documents contain data in the form of tag/value pairs. XML gives much more control than HTML over collecting, searching, combining, formatting, and delivering content to different audiences for different purposes. XML is a standard for passing data between Internet applications. XML documents contain data in the form of tag/value pairs. See also www.extensibility.com for information on TIBCO Extensibility products.

XML schema

The definition of the content in an XML document. Some features include: Data typing enables defining data by type (character, integer, etc.); Schema reuse, or schema inheritance, lets tags referenced in one schema be used in other schemas; Namespaces enables multiple schemas to be combined into one; Global attributes assign properties to all elements; Associating Java classes adds processing to the data; Authoring information adds improved documentation for schema designers.

An XML schema is an XML element information item which, along with its descendants, satisfies all the constraints on schemas in a specification. An XML schema establishes a set of rules for constraining the structure and articulating the information set of XML document instances. See

www.extensibility.com for information on XML Authority, the premier solution for the creation, conversion, and management of DTDs and XML schemas.

Unlike a DTD, an XML schema is written in XML. Although XML schemas are more verbose than DTDs, they can be created with any XML tool.

XSD

XML Schema Definition. .xsd is the suffix of an XSD schema document. An XSD file defines the structure and elements in a related XML file.

XSDL

XML Schema Definition Language. An XML schema dialect. Expressed in XML document syntax, XSDL supports an extensible data typing system, inheritance, and namespaces. See www.extensibility.com for information on TIBCO's XML Authority®, the premier solution for the creation, conversion, and management of documents in XML schema dialects, including XSDL.

XSL

Extensible Style Language. A stylesheet language for XML. XSL uses template rules that are written using XML to transform documents into formatting objects, which are then presented on screen, in print, or in other media.

XSLT

Extensible Stylesheet Language Transformations. A language for transforming XML documents into other XML documents. XSLT is designed for use as part of XSL. In addition to XSLT, XSL includes an XML vocabulary for specifying formatting. XSL specifies the styling of an XML document by using XSLT to describe how the document is transformed into another XML document that uses the formatting vocabulary.

Index

A

about system configuration [25](#)
 ack [101](#)
 activities
 see also operations
 aeRvMsg message format [13](#)
 attribute [73](#)
 attributes, operators, and operands [73](#)
 audit logging [25](#)

B

BLOB Data [101](#)
 business protocols [21](#)
 BusinessConnect
 architecture [5](#)
 installation [6](#)
 server components [12](#)
 usage scenarios [4](#)
 BusinessEvents, integration with BusinessConnect [28](#)

C

cache timeout [59](#)
 CAs [82](#)
 CDATA [101](#)
 certificate authorities [82](#)
 certificate chain [82](#)
 Certificates Authority (CA) [82](#)
 certificates file [83](#)

cipher suites [92](#)
 128-Bit and Stronger [93](#)
 256-Bit and Stronger [94](#)
 Export and Stronger [93](#)
 Stronger than 128-Bit [94](#)
 Stronger than Export [93](#)
 ciphertext [102](#)
 cleartext [102](#)
 CMS [102](#)
 configuration store [26](#)
 CRM [102](#)
 CSR [102](#)
 CSV [102](#)
 custom reports [102](#)
 cXML [102](#)

D

data stores [26](#)
 database connections [25](#)
 DBMS [103](#)
 deep linking [103](#)
 digest algorithms [88](#)
 digital certificates [81](#)
 digital signatures [86](#), [103](#)
 distributing workloads among engines [70](#)
 document type declaration [103](#)
 DTD [103](#)
 DUNS Number [103](#)

E

ebXML [103](#)
 element [103](#)
 encryption [87](#)

encryption algorithms 88
ERP 103

F

fault tolerance for the Interior Component (DMZ Mode) 63

H

Hawk, integration with BusinessConnect 31

I

inbound inter-component event source 72
Interior component 63

J

JMS message format 15
JMS queue transport type 17
JMS topic transport type 17
JMS transport types used for various messages 17
JSSE 104

K

key identity file 104
key pair 104

L

load balancing and Public Smart Routing for the Inte-

rior component (DMZ Mode) 64

M

MAPI 105
Monitoring
of BusinessConnect application 31

N

nack 105
NO MATCHING RULES 76
non-repudiation 95
 logging of acknowledgments on initiator 96
 logging of acknowledgments on responder 95
 logging scenarios 95
 of origin 95
 of receipt 96
 on Initiator 96
 on Responder 97
non-repudiation logging 25

O

obtaining certificates 82
operand 74
operations
 overview 21
operator 73

P

parsed 105
participant profiles 20
PIP 105
private keys 80

- Private Process Smart Routing [67](#)
 - business rules [67](#)
 - configuration [67](#)
- processing of inbound documents [70](#)
- product overview [2](#)
- proxy servers [26](#)
- public event sources [69](#)
- public key cryptography [106](#)
- public keys [80](#)
- public processes in BusinessConnect [19](#)
- Public Smart Routing [69](#)
 - creating rules [74](#)
 - defining rules [73](#)
 - rules [72](#)
- public transports [56](#)

R

- relationship between private and public processes [19](#)
- Rendezvous Certified Messaging (RVCM) [14](#)
- RosettaNet [106](#)
- runtime data store [26](#)
- RV [106](#)

S

- S/MIME [87, 106](#)
- schema [106](#)
- secure JMS transport [17](#)
- security overview [78](#)
- selecting algorithms and methods during tunnel negotiation [99](#)
- server groups and clusters [74](#)
- SGML [106](#)
- shadow credentials [84](#)
- SMTP [107](#)
- SOAP [107](#)
- SQL [107](#)
- SSH [87](#)

- SSHFTP
 - authentication methods [98](#)
 - selecting algorithms and methods [98](#)
 - supported ciphers [99](#)
 - supported compression algorithms [99](#)
 - supported MACs [99](#)
- SSHFTP implementation in BusinessConnect [58](#)
- SSHFTP tunnels [58](#)
- SSL [87, 107](#)
- storing certificates [83](#)
- symmetric key cryptography [107](#)

T

- TCP/IP [107](#)
- tibbr, integration with BusinessConnect [27](#)
- TIBCO Rendezvous subject names [12](#)
- tibXML [107](#)
- transactions
 - see also operations
- type-aware [107](#)

U

- unparsed [108](#)
- untyped [108](#)
- URI [108](#)
- URL [108](#)
- URN [108](#)
- using certificates with BusinessConnect [82](#)
- using TIBCO Administrator [34](#)
- using TIBCO BusinessWorks [37](#)
- using TIBCO Designer [39](#)

V

- VAN [108](#)
- Visibility [27](#)
 - in BusinessConnect

[27](#)
via BusinessEvents [28](#)
via tibbr [27](#)
VPN [108](#)

X

XML [109](#)
XML schema [109](#)
XSD [109](#)
XSDL [109](#)
XSL [109](#)
XSLT [109](#)

TIBCO Product Documentation and Support Services

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

How to Access TIBCO Documentation

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

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

Product-Specific Documentation

The following documentation for this product is available on the [TIBCO BusinessConnect](#) page.

- *TIBCO BusinessConnect Release Notes*
- *TIBCO BusinessConnect Installation and Configuration*
- *TIBCO BusinessConnect Concepts*
- *TIBCO BusinessConnect Scripting Deployment User's Guide*
- *TIBCO BusinessConnect Interior Server Administration*
- *TIBCO BusinessConnect Trading Partner Administration*

Other TIBCO Product Documentation

When working with TIBCO BusinessConnect, you may find it useful to read the documentation of the following TIBCO products:

- **TIBCO Administrator™:** This software allows you to manage users, machines and applications defined in a TIBCO Administration Domain. The TIBCO Administrator graphical user interface enables users to deploy, monitor, and start and stop TIBCO applications.
- **TIBCO ActiveMatrix BusinessWorks™:** This software is a scalable, extensible, and easy to use integration platform that allows you to develop integration projects. TIBCO ActiveMatrix BusinessWorks includes a graphical user interface (GUI) for defining business processes and an engine that executes the process.
- **TIBCO Designer™:** This graphical user interface is used for designing and creating integration project configurations and building an Enterprise Archive

(EAR) for the project. The EAR can then be used by TIBCO Administrator for deploying and running the application.

- **TIBCO Runtime Agent™:** This software suite is a prerequisite for other TIBCO software products. In addition to TIBCO Runtime Agent components, the software suite includes the third-party libraries used by other TIBCO products such as TIBCO Designer, Java Runtime Environment (JRE), TIBCO Hawk®, and TIBCO Rendezvous®.
- **TIBCO Rendezvous®:** This software enables programs running on many different kinds of computers on a network to communicate seamlessly. It includes two main components: the Rendezvous programming language interface (API) in several languages, and the Rendezvous daemon.
- **TIBCO Enterprise Message Service™:** This software provides a message service that enables integration of applications within an enterprise based on the Java Message Service (JMS) specification. This software is a prerequisite for other TIBCO software products.
- **TIBCO BusinessEvents®:** This software helps companies identify and quantify the impact of events; it notifies people and systems about meaningful events so processes can be adapted on-the-fly. TIBCO BusinessEvents uses a unique model-driven approach to collect, filter, and correlate events and deliver real-time operational insight.
- **TIBCO Hawk®:** This software is a tool for monitoring and managing distributed applications and operating systems. The software is designed specifically for monitoring distributed systems, so there is no centralized console or frequent polling across the network.
- **tibbr®, tibbr Service, tibbr Community, and tibbr Community Service:** This software is the first workplace communication tool with which you can follow subjects that relate to your work and interests besides following people as you do in typical social networking applications. That way, you have much more flexibility in obtaining the right information at the right time in the right context. In fact, the information will find you.
- **TIBCO BusinessConnect™ Palette:** This software is about the resources available in the TIBCO BusinessConnect Palette for TIBCO ActiveMatrix BusinessWorks.

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, visit [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 TIBCO Software Inc.

TIBCO, the TIBCO logo, the TIBCO O logo, and TIBCO ActiveMatrix BusinessWorks, TIBCO Administrator, TIBCO Designer, Hawk, Rendezvous, and TIBCO Runtime Agent are either registered trademarks or trademarks of TIBCO Software 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.

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. TIBCO SOFTWARE 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 TIBCO Software Inc. may be covered by registered patents. Please refer to TIBCO's Virtual Patent Marking document (<https://www.tibco.com/patents>) for details.

Copyright © 2001-2022. TIBCO Software Inc. All Rights Reserved.