TIBCO BusinessConnect™ Container Edition

Administration

Version 1.2.0
October 2022

Contents

Introduction

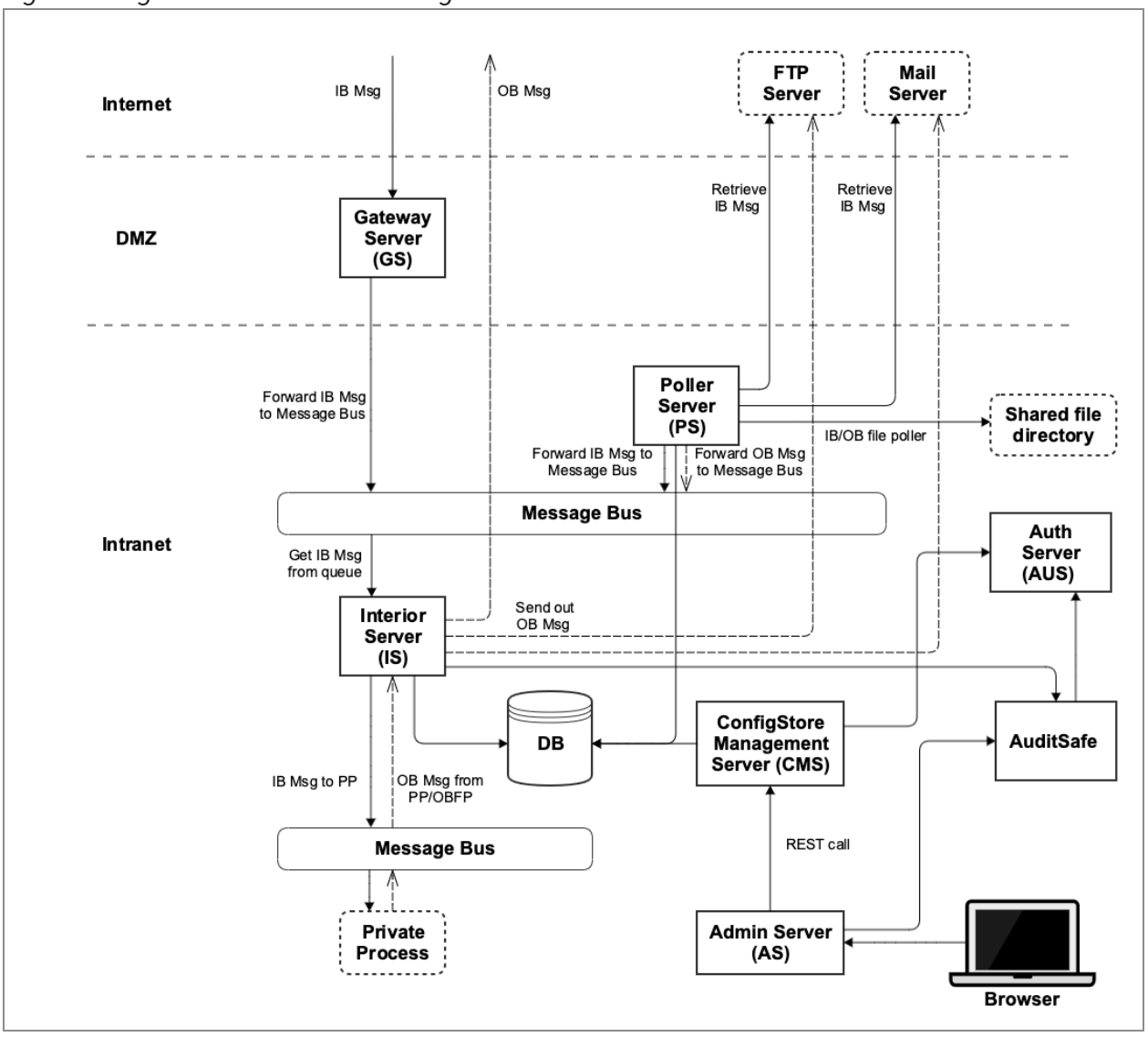
TIBCO BusinessConnect™ Container Edition contains the following major components that facilitate the secure transmission of documents and messages between partners using disparate internal business systems.

- Gateway Server
- Interior Server
- Poller Server
- ConfigStore Management Server
- Admin Server

When all these components are deployed, each server is a separate Docker container instance.

Here is a High-Level Architecture diagram of BusinessConnect™ Container Edition.

Figure 1: High-Level Architecture Diagram



Legend

--- Inbound Request

— Outbound Message

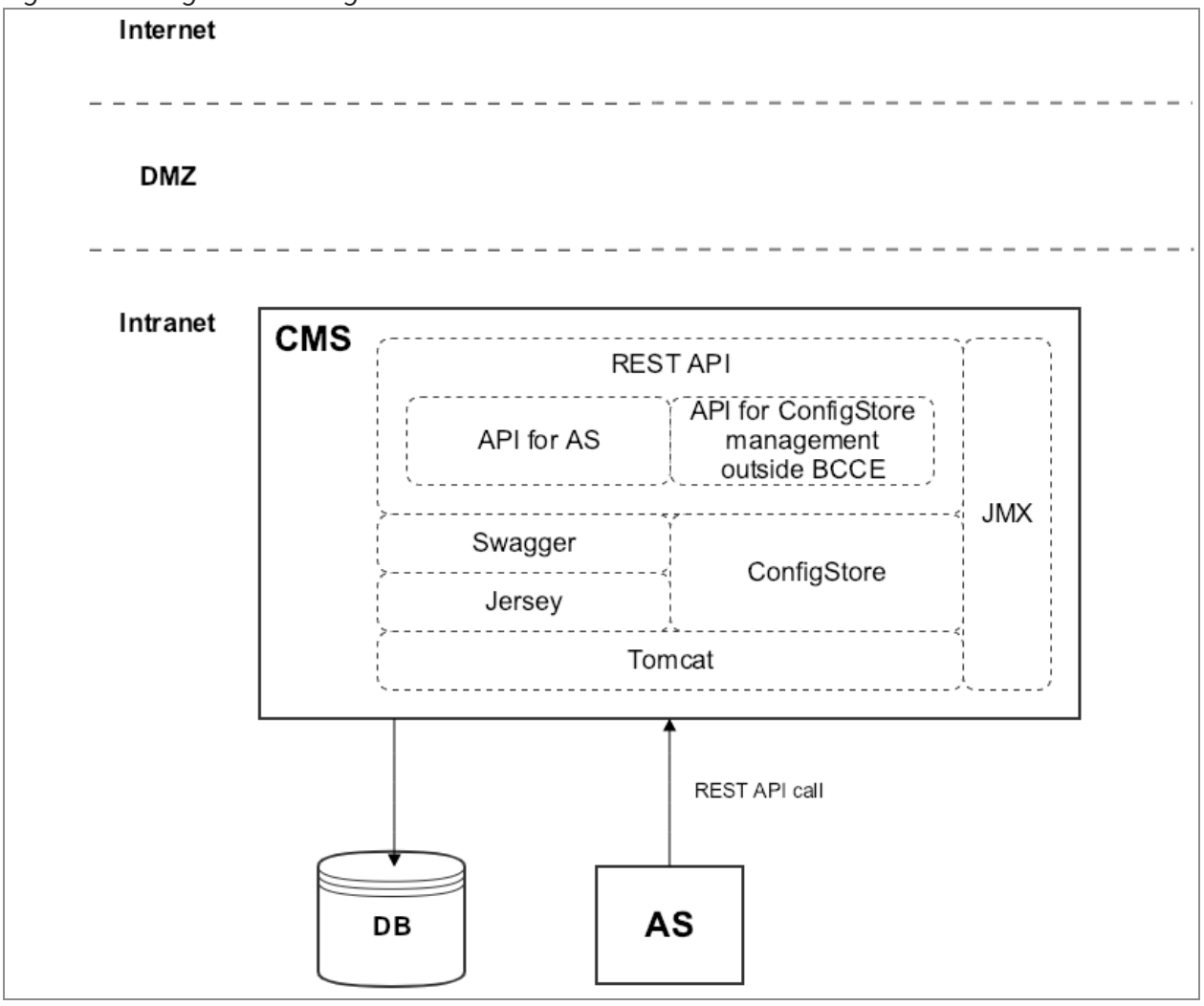
Basic Admin Tasks

The Admin task is to configure the trading partner, protocols, and operations of the transactions. Admin also can monitor the transactions between trading partners.

ConfigStore Management Server

ConfigStore Management Server (CMS) receives REST call requests from Admin Server, performs CRUD operations on ConfigStore, and sends the information to Auth Server. This server also communicates with the database when required.

Figure 2: ConfigStore Management Server Architecture



Legend

AS	Admin Server
DB	Database
DMZ	Demilitarized Zone

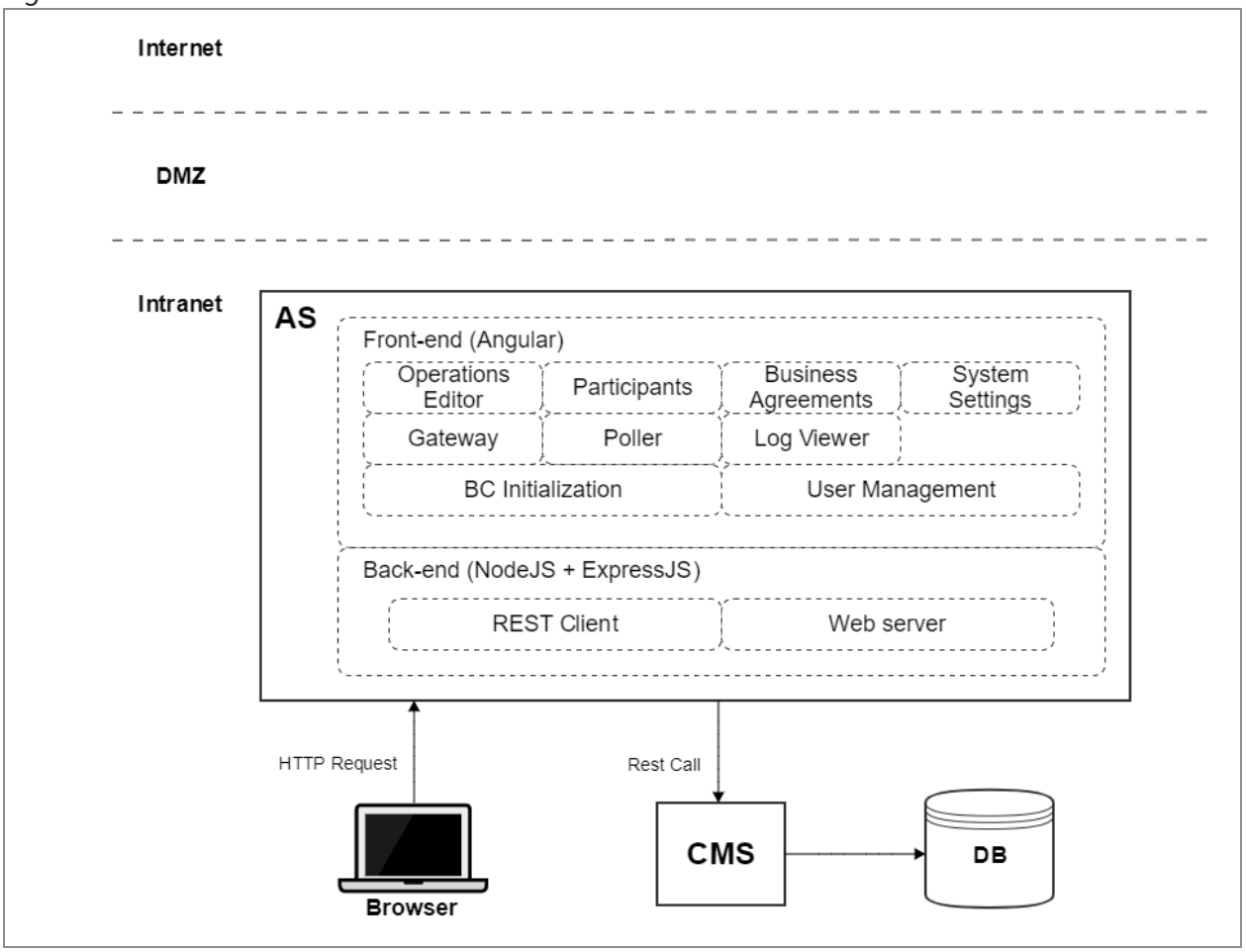
Legend

JMX Java Management Extensions

Admin Server

With Admin Server (AS), you can configure and manage the BusinessConnect Container Edition features such as configuration of participants, operation editor, business agreement, and creating and managing participants. It exchanges data with ConfigStore Management Server using REST calls.

Figure 3: Admin Server Architecture



Legend

CMS	ConfigStore Management Server
DB	Database
DMZ	Demilitarized Zone

Interior Server

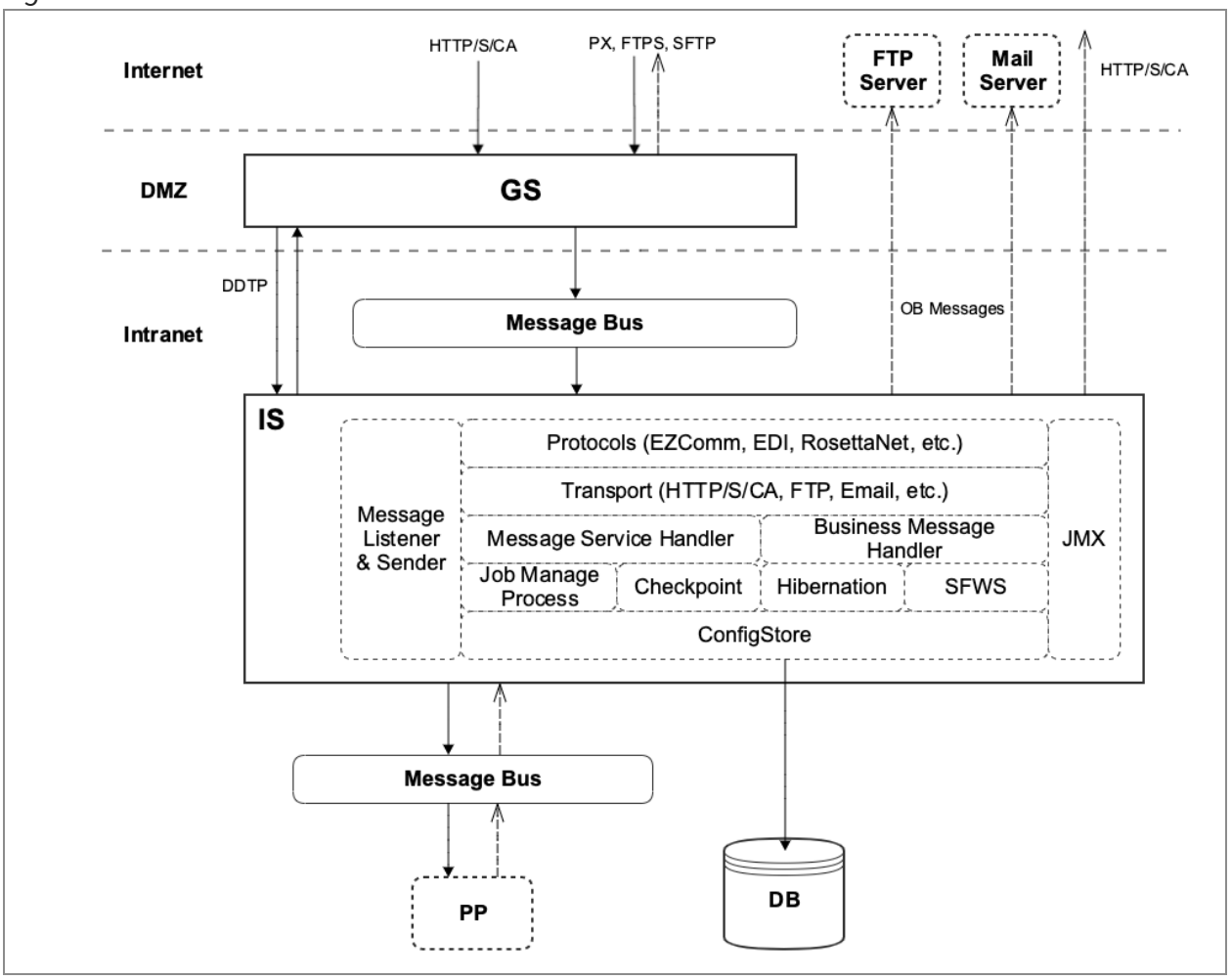
BusinessConnect Container Edition is installed on Interior Server (IS). You can deploy multiple Interior Servers as a cluster for load balancing and fault tolerance. This server is located inside the company's firewall and performs the following tasks:

- 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, business level acknowledgment generation, and so on.
- Communicates with Gateway Server and Poller Server using TIBCO Enterprise Message Service™ message bus for inbound messages.
- Communicates with AuditSafe Server using REST APIs to post audit logs.

Interior Server must be deployed and started before Gateway Server.

The following diagram shows Gateway Server and Interior Server communications:

Figure 4: Interior Server Architecture



Legend

DB	Database
DMZ	Demilitarized Zone
GS	Gateway Server
PP	Private Process
SFWS	Store and Forward Service

Gateway Server

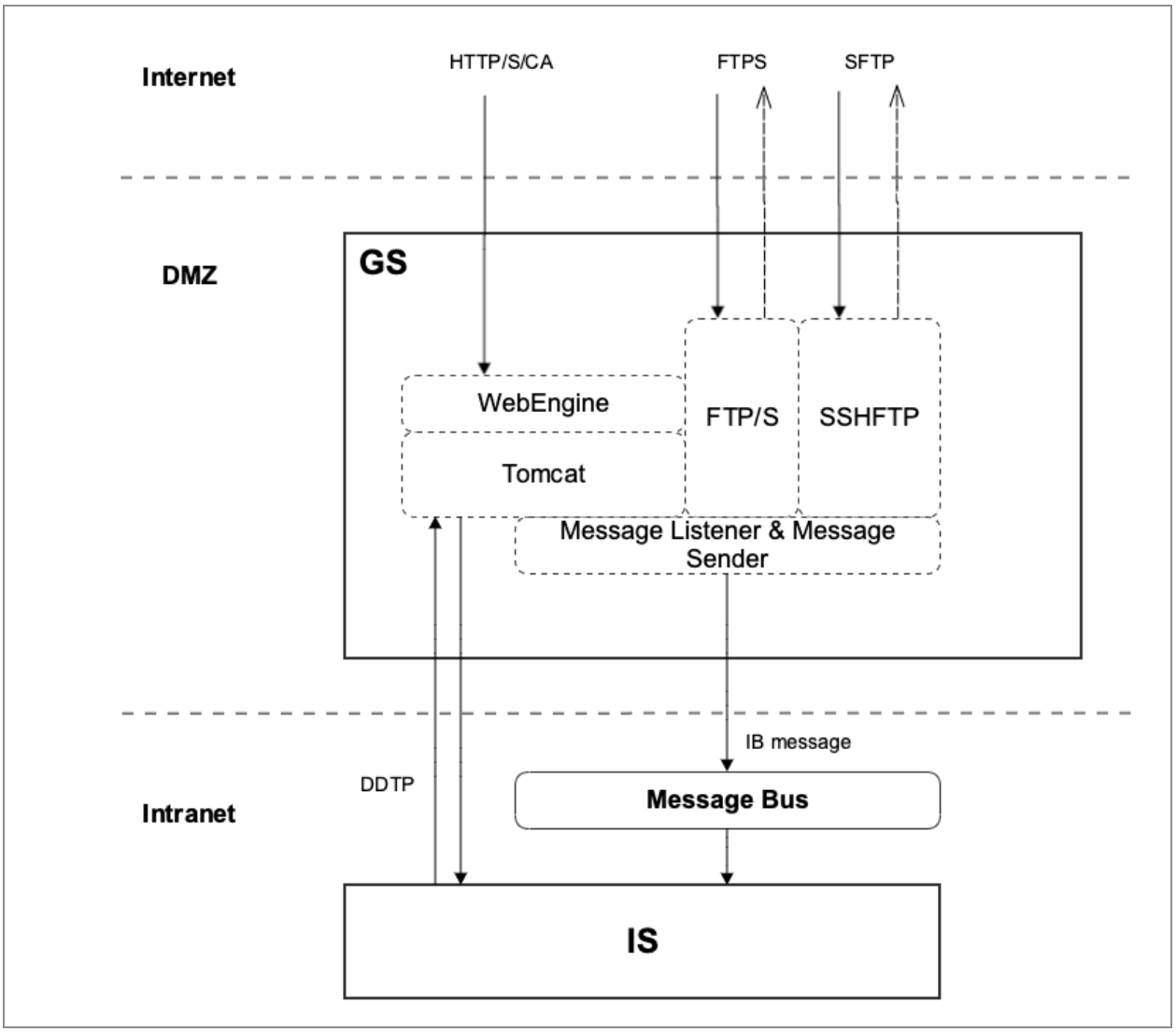
Gateway Server (GS) is located in the demilitarized zone and functions as the front gate by receiving the inbound transactions from trading partners. Multiple Gateway Servers can work together for load balancing.

This server has several restrictions on the networks it can access. It is used to host various gateway services such as HTTP/S, to receive B2B communications directly from the internet with security features such as SSL and SSH. The firewall between the Gateway Server and rest of your system protects against the threat of malicious communications. BusinessConnect Container Edition's Gateway Server is a standalone Java executable that is not dependent on TIBCO ActiveMatrix BusinessWorks™. However, it still needs Enterprise Message Service™ to communicate with the Interior Server.

This server performs the following tasks:

- Receives inbound request through HTTP/S/CA transports protocols.
- Communicates with the Interior Server using Enterprise Message Service message bus for inbound messages that are received.
- Allows trading partners to exchange messages using business protocols.
- Hosts HTTP Service which supports HTTP, HTTPS, and HTTPSCA transports for document exchange.

Figure 5: Gateway Server Architecture



Legend

IS	Interior Server
DMZ	Demilitarized Zone

Configuring Gateway Services (HTTP)

If a Gateway Service has been started successfully and registered with Interior Server at least once and using at least one Gateway Service; then Gateway Server will remember that information and will automatically restarts next time with the same groups.

After a restart, users do not have to return to the GUI and reassign these groups to that same Gateway Server container, provided no changes to the groups are needed. Gateway Server itself returns to the GUI and captures the latest information associated with a specific container.

In order to make changes to the Gateway Services, make any desired changes to the groups using the GUI; then restart the edited Gateway Service so that the new setting is captured.

To configure a Gateway Service, configure the required ports, encryption, and credentials as described in the following steps:

Procedure

1. On the Admin UI, go to System Settings > Transport Protocols > **Inbound Protocols** tab.
2. Select the **HTTP** check box and click **Save**.
3. Click **Configure Service** of **HTTP** and click **Add**  .
4. Enter **Gateway Service Name**, select **HTTP** from **Gateway Service Type** list and click **Proceed**.

   > **Note:** Default **Gateway Service Name** is set to `http` in the `deployment.properties` file. To use another **Gateway Service Name**, set **`<service name>`** for `gs_services=HTTP:<service name>` in the `deployment.properties` file.

5. Select the **Enable** check box to enable the Gateway Service and configure the following tabs; then click **Save**.

   Ports Tab

Field	Description
Plain Port	The default value is set to *30003*. • **Plain Port** is the **`gs_port`** that you have set in the `deployment.properties` file.
Secure Port	The default value is set to *30004*.

Field	Description
	• **Secure Port** is the **`gs_secure_port`** that you have set in the `deployment.properties` file. • To disable secure communications on HTTP, enter `0` or leave the **Secure Port** or **Secure CA Port** fields empty.
Secure CA Port	The default value is set to *30005*. • **Secure CA Port** is the **`gs_secure_ca_port`** that you have set in the `deployment.properties` file. • To disable secure communications on HTTP, enter `0` or leave the **Secure Port** or **Secure CA Port** field empty.
Private Key Credential for Secure Ports	Select a private key that was previously configured for the Gateway Service for HTTP (on the **Credentials** Tab).

Note: The default values for **Plain Port**, **Secure Port**, and **Secure CA Port** on the GUI are *6700*, *6705*, and *6707* respectively but when assigned to a container, external accessible ports are *30003*, *30004*, and *30005* respectively as configured in the `deployment.properties` file.

Advanced Tab

Field	Description
Security:	Select the required security options.
Minimum Encryption Strength	Select the encryption strength from available options.
Gateway to Interior	Select the required gateway to interior settings.

Field	Description
Settings	
Data Streaming Threshold (KB)	This threshold value controls when data streaming is used to transfer the payload data between Gateway Server and Interior Server. The default value is set to *10000*.
Request Timeout (secs)	This timeout value controls how long Gateway Server has to wait for the request to be replied by Interior Server. This timeout must be shorter than the HTTP timeout value set by the trading partner waiting for the reply from the BusinessConnect Container Edition server. The default value is set to *3600*.

6. On the **Credentials Tab**, click **New Credential** and enter the following details.

Field	Description
Alias	Enter the name for the new private key.
Upload file	Upload the new private key from your machine.
Password	Required. Add the password to protect the key.

Exporting Gateway Server Configuration

Gateway Server does not have direct access to the database as it exists between two firewalls in the demilitarized zone for security reasons. Hence, a separate exporting of the Gateway Server configuration is required.

To export Gateway Server configuration, performing the following steps:

Procedure

1. Log in to the BusinessConnect Container Edition application using the URL:

`http://<host_ip>:<as_port>`.

> **Note:** Use the **<host_ip>** and **<as_port>** that you have set in the `deployment.properties` file.

2. Go to System Settings > General, click **Installation Properties**.
3. Click **Export GS configuration** to download the `GSToken.zip` file, which contains the `intercomProps`, `hostKey`, and `peerCert` files that are required to deploy Gateway Server.
4. Extract the contents of the `GSToken.zip` file to the **<gstoken_unzip>** directory.

> **Note:** Use the **<gstoken_unzip>** that you have set in `deployment.properties`.

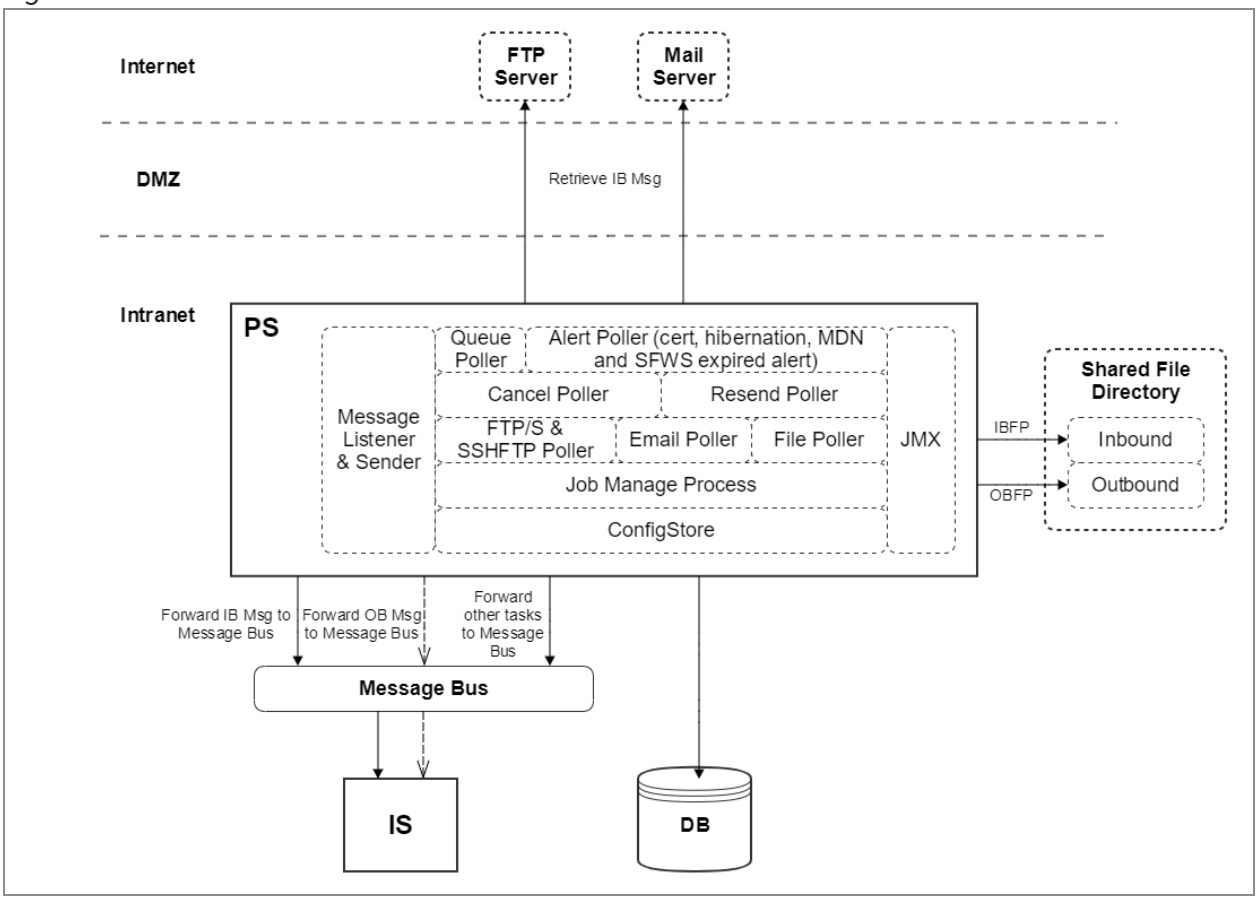
Poller Server

Poller Server (PS) retrieves inbound requests from FTP and SFTP servers, Mail server, and shared file directory. It includes both inbound and outbound file pollers.

Poller Server communicates with Interior Server using the Enterprise Message Service message bus to receive inbound messages.

A diagram of Poller Server and Interior Server communications is depicted in the following figure.

Figure 6: Poller and Interior Server Architecture



Legend

DB	Database
DMZ	Demilitarized Zone
IS	Interior Server
JMX	Java Management Extensions

Poller Server Properties

BusinessConnect Container Edition, the Poller Server framework provides various configuration properties that allows each Poller Server engine in your deployment to execute poller tasks of one or more specific types. The supported poller types are Inbound Email, Inbound FILE, Inbound FTP, and Outbound FILE. You can specify the number of

Poller Server engines to execute a specific poller type, the rate at which the trading partner configurations are to be reloaded, and the associated priority for a specific poller type.

Using the Poller Server dispatch mechanism, each Poller Server engine reads the configuration during startup and executes the pollers using Round-robin algorithm. BusinessConnect Container Edition supports the following configuration properties:

bcce_poller_engines=integer

The number of Poller Servers in your deployment. The default value is set to *1*.

bcce_poller_{ib_email|ib_file|ob_file|ib_ftp}_instances=integer

The number of engines executing a specific poller type. The default value is set to *1*. This value should be in the range of 1..<bcce.poller.engines>. A zero value implies that the poller tasks of this type are never run.

bcce_poller_{ib_email|ib_file|ob_file|ib_ftp}_refresh_rate=integer

The refresh rate (in seconds). The default value is set to *300*. The trading partner configurations are reloaded periodically after the specified interval. Any running poller tasks are terminated before reloading the trading partner configurations and then restarted.

bcce_poller_{ib_email|ib_file|ob_file|ib_ftp}_weight=integer

The priority of the poller (1 being low - 10 being high). The default value is set to *10*. Poller tasks of specified type are started by the Poller Server engine in decreasing order of the assigned priority. The combination of priority and instance of configuration parameters enables a Poller Server engine to run poller tasks of different types, reduce the overall load on that engine, and improve its performance.

Based on the number of Poller Server engines and configuration of individual poller types you can address the requirements such as running poller tasks of a specific type in separate Poller Server engines or running poller tasks of specific type in multiple poller server engines. Ensure that the poller tasks are executed in the subsequent refresh cycles, irrespective of the number of jobs involved.

Hawk Microagents for Interior Server

The BusinessConnect engine implements a set of microagents to monitor and manage the various polling operations that happen inside the BusinessConnect engine.

Below are the microagent names and functions:

Server Name	Description
SCHDTASKPOLLER	Poller to look for scheduled tasks that need to be fired.
RESENDPOLLER	Poller to look for transactions that need to be resent.
QUEUEACTIONPOLLER	Poller to look for messages to send off the message queue (primarily batch transactions).
MDNPOLLER	Poller to look for overdue MDNs with AS2.
InteriorController	The main BC engine
HIBERPOLLER	Poller to look up transactions that have hibernated too long.
FTPPOLLER	Poller that triggers inbound FTP inbound sessions on a periodic basis. This poller is vulnerable to hanging, so it would be good to monitor it.
CREDPOLLER	Expired credential poller. Checks certificate store for expired certificates on a regular basis.
CANCELPOLLER	Poller that looks at the audit log for transactions that have been marked for cancellation. Primarily for RosettaNet and ebXML.

The most common reason for monitoring BusinessConnect Container Edition is for the FTP pollers. In an environment where there may not be reliable data connections to trading partners, there is a tendency for this poller to "hang" because of a bad connection to a SFTP trading partner. Using microagents, you can eliminate this issue with a Hawk rule and rulebase.

Private Process Configuration

JMS Messages are used for communicating between private processes and the BusinessConnect Container Edition servers. Private process messages are JMS messages that are exchanged between a private process and the BusinessConnect instance.

The private process creates a private process message when it receives a message from an internal application such as SAP. Typically, the following series of events occurs:

1. The private process message is sent from the private process to the BusinessConnect Container Edition server, which converts the private message into a public message and sends it over the internet to a trading partner.
2. The trading partner's BusinessConnect Container Edition server re-converts the public message into a private message and sends it to the appropriate private process, which forwards it to its internal application.

Configuring JMS Settings

To learn more about the JMS transport, see "Using the SSL Protocol" topic in the *TIBCO Enterprise Message Service™ User's Guide*.

Select the JMS option to enable the runtime communication with the private process over a secured or unsecured JMS connection. JMS can only be selected (and saved successfully) if the specified connection factory uses the Enterprise Message Service factory string: `com.tibco.tibjms.naming.TibjmsInitialContextFactory`. Otherwise, the transport can only be saved if this option is not selected.

When selecting a server name under Internal Messaging (JMS), the **Details** pane and the **Credentials** pane appears.

Note: BusinessConnect Container Edition sends some messages on JMS Topics, such as ERROR advisories. You can configure JMS Durable topics to avoid message loss.

You can use the JMS option to configure JMS and Intercomponent JMS.

Procedure

1. On the Admin UI, go to System Settings > General, click **Internal Messaging (JMS)**.
2. To configure Private Process JMS, click **Private Process JMS**. To configure Intercomponent JMS, click **Intercomponent JMS**.
3. Enter the information specified in the following table and click **Save**.

JMS Settings

Field	Enter
JMS Settings Details	
JMS User Name	User name to use when logging into the JMS server. If the JMS provider does not require access control, this field can be empty. Not all JMS servers require user names and passwords. Refer to your JMS provider documentation and consult your system administrator to determine if your JMS server requires a user name and password.
JMS Password	Password to use when logging into the JMS server. If the JMS provider does not require access control, this field can be empty.
JNDI Context Factory	The initial context factory class for accessing JNDI (javax.naming.Context.INITIAL_CONTEXT_FACTORY). **Note:** BusinessConnect Container Edition attempts to find the class. However, you may need to add the Java file supplied by your JNDI service provider to the **CLASSPATH** environment variable to use JNDI.
JNDI Context URL	This is the URL to the JNDI service provider (javax.naming.Context.PROVIDER_URL). See your JNDI provider documentation for the syntax of the URL. The following is a sample EMS `URL: tibjmsnaming://<EMS_URL>:7222`

Field	Enter
JNDI User Name	User name to use when logging into the JNDI server (javax.naming.Context.SECURITY_PRINCIPAL). If the JNDI provider does not require access control, this field can be empty.
JNDI Password	Password to use when logging into the JNDI server (javax.naming.Context.SECURITY_CREDENTIALS). If the JNDI provider does not require access control, this field can be empty.
Topic Connection Factory	The TopicConnectionFactory object stored in JNDI. This object is used to create a topic connection with a JMS application. See your JNDI provider documentation for more information about creating and storing TopicConnectionFactory objects.
Queue Connection Factory	The QueueConnectionFactory object stored in JNDI. This object is used to create a queue connection with a JMS application. See your JNDI provider documentation for more information about creating and storing QueueConnectionFactory objects.
Reconnect Max. Duration (mins)	This is the time during which the BusinessConnect Container Edition server will try to reconnect. After this time, there will be no attempt to reconnect. This duration time does not represent the reconnection frequency. Default is *10* minutes.
Secured	If selected, the transaction will be secured.
Verify JMS Server	If selected, the JMS server's identity (that is, its X509 certificate as well as the specified value in the “Expected JMS Server Host Name” field) will be verified against the data received during the SSL handshake.

Field	Enter
	If either the trusted CA certificates or the expected hostname doesn't match, the transport creation fails. If this verification is not required, BusinessConnect Container Edition can establish a JMS connection with an Enterprise Message Service, whose credentials are different from the configured properties.
JMS Server Certificate	The certificate credential of the JMS server. To create this certificate, follow the steps described in *TIBCO BusinessConnect™ Container Edition Trading Partner Administration* guide, Adding LDAP/JMS/Email Server Certificates. The credential is stored in the BusinessConnect Container Edition keystore and is expected to be configured on an Enterprise Message Service server according to the corresponding guidelines.
Expected JMS Server Host Name	The value of the common name component of an Enterprise Message Service server's leaf certificate. This is usually the hostname of the resource, running an Enterprise Message Service server. If it is a test system, the common name (CN) value may be any arbitrary string, which must match the value of this field if the **Verify JMS Server** check box is selected.
Strong Ciphers Only	If the box is selected, only strong encryption algorithms will be used between the server (or the palette) and the JMS provider. The below cipher suites are offered by the connecting client (either BusinessConnect Container Edition or the palette) in this mode: TLS_RSA_WITH_AES_256_CBC_SHA TLS_RSA_WITH_AES_128_CBC_SHA TLS_DHE_RSA_WITH_AES_256_CBC_SHA TLS_DHE_RSA_WITH_AES_128_CBC_SHA SSL_RSA_WITH_RC4_128_SHA SSL_RSA_WITH_3DES_EDE_CBC_SHA

Field	Enter
	SSL_DHE_RSA_WITH_3DES_EDE_CBC_SHA SSL_DHE_DSS_WITH_3DES_EDE_CBC_SHA TLS_DHE_DSS_WITH_AES_128_CBC_SHA TLS_DHE_DSS_WITH_AES_256_CBC_SHA **Note:** The unlimited strength JCE jurisdiction policy files are pre-installed on the JRE bundled with TIBCO products.
Use Trace	See comments in TIBCO ActiveMatrix BusinessWorks Palette Reference, JMS Palette section Advanced. When this option is used, the SSL-specific debug tracing for the secure JMS transport will be sent to the engine standard output only.
JMS Credentials	
New Certificate	The EMS Route certificate needs to be uploaded for authentication here when the SSL JMS server is being used and when the user selects **Verify JMS server** option. The EMS Route certificate is found in the EMS folder.

Tip: Intercomponent DMZ-JSM (Optional): You can optionally configure an EMS server in the DMZ for the communication between the Gateway and Interior servers. The component settings for Intercomponent DMZ-JMS settings are exactly the same as that of Intercomponent JMS Settings.

JMS Auto Reconnect for the BusinessConnect Container Edition Server

If the JMS server is down or the network connection is down when the BusinessConnect Container Edition engine starts, the engine tries to reconnect to the JMS server for a specified period of time (as set in the field Reconnect Max Duration). If the connection is not established within this time, the engine stops.

However, if the connection between the engine and the JMS server is established within the specified period (as set in the field Reconnect Max Duration), the engine will continue to run.

- If the connection between BusinessConnect Container Edition and the JMS server is terminated during runtime, the engine will try to establish a connection. During this time, messages from the private process to BusinessConnect Container Edition are not received.
- If the protocols are trying to send a message to a private process, the engine will hold the message for a specified period of time (as set in the field **Reconnect Max Duration**), configured in the JMS transport, to check whether the connection is established.
- If the connection is established, then the message is sent to a private process.
- If the connection is not established within this period of time, an error occurs.

Deploying Servers

Before you begin

Before you deploy any server, perform the following steps:

1. Set all the mandatory properties in the `configuration.properties` and `deployment.properties` files.

   > **Note:** You can find the property files in config folders of Installation and Deployment packages.

2. Build and push the Docker images to the Docker repository. For more information, see the “Building BusinessConnect Container Edition Component’s Docker Images” topic in *TIBCO BusinessConnect™ Container Edition Installation and Deployment* guide.
3. If you are using MySQL 5.7.*x* or above versions; then in the `my.ini` file under [**mysqld**] section, you must add **`skip_ssl`** and set **`max_allowed_packet`** to *500M*.
4. Deploy AuditSafe Services. For more information, see “Deploying AuditSafe Services” topic in *TIBCO® AuditSafe Installation* guide.

You can deploy servers onto the Kubernetes cluster by using the deployment script in the following sequence:

1. ConfigStore Management and Admin Servers
2. Poller and Interior Servers
3. Gateway Server

However, based on requirement you can skip the deployment of server/s by entering `n` in the console when you run the deployment script.

Deploying Admin and ConfigStore Management Servers

Procedure

1. To deploy Admin and ConfigStore Management Servers, run one of the following commands depending on the platform:
    - **Kubernetes**: Navigate to the `<folder>/bcce-<version>/deployment/scripts` directory and run the following command:

      ```
      ./deploy-bcce.sh
      ```

    - **Docker**: Navigate to the `<folder>/bcce-<version>/deployment/samples/docker-scripts` directory and run the following command:

      ```
      ./docker-run-bcce-all.sh
      ```

2. Enter `y` to deploy Admin and ConfigStore Management Servers.

Deploying Poller and Interior Servers

Before you begin

Before you deploy Poller and Interior Servers ensure the following:

1. Admin and ConfigStore Management Servers must be deployed and running.
2. Set the JMS Server settings:
    a. Log in to the BusinessConnect Container Edition application using the URL: `http://<host_ip>:<as_port>`.

    > **Note:** Use the **`<host_ip>`** and **`<as_port>`** that you have set in the `deployment.properties` file.

b. Go to System Settings > General, click **Internal Messaging (JMS)**.

c. Click **Private Process JMS**, enter all the mandatory fields and click **Save**.

d. Click **Intercomponent JMS**, enter all the mandatory fields and click **Save**.

e. Optional: To use different JMS between Gateway Server and Interior Server, click **Intercomponent DMZ-JMS (Optional)**, enter all the mandatory fields and click **Save**.

To configure the JMS Server settings, see Configuring JMS Settings.

Procedure

1. To deploy Poller and Interior Servers, run one of the following commands depending on the platform:
   - **Kubernetes**: Navigate to the `<folder>/bcce-<version>/deployment/scripts` directory and run the following command:

     ```
     ./deploy-bcce.sh
     ```

   - **Docker**: Navigate to the `<folder>/bcce-<version>/deployment/samples/docker-scripts` directory and run the following command:

     ```
     ./docker-run-bcce-all.sh
     ```

2. Skip the deployment of Admin and ConfigStore Management Servers by entering `n`.
3. Enter `y` to deploy Poller and Interior Servers.

Deploying Gateway Server

Before you begin

Before you deploy Gateway Server ensure the following:

1. Admin, ConfigStore Management, Poller, and Interior Servers must be deployed and running.
2. Create a Gateway Token. See Exporting Gateway Server Configuration.

3. Enable and configure the HTTP Gateway Service. See Configuring Gateway Services (HTTP).

Procedure

1. To deploy Gateway Server, run one of the following commands depending on the platform:
   - **Kubernetes**: Navigate to the `<folder>/bcce-<version>/deployment/scripts` directory and run the following command:

     ```
     ./deploy-bcce.sh
     ```

   - **Docker**: Navigate to the `<folder>/bcce-<version>/deployment/samples/docker-scripts` directory and run the following command:

     ```
     ./docker-run-bcce-all.sh
     ```

2. Skip the deployment of all other servers by entering `n`.
3. Enter `y` to deploy Gateway Server.

TIBCO Documentation and Support Services

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

How to Access TIBCO Documentation

Documentation for TIBCO products is available on the TIBCO Product Documentation website, mainly in HTML and PDF formats.

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

Product-Specific Documentation

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

- *TIBCO BusinessConnect™ Container Edition Release Notes*
- *TIBCO BusinessConnect™ Container Edition Installation and Deployment*
- *TIBCO BusinessConnect™ Container Edition Concepts*
- *TIBCO BusinessConnect™ Container Edition Trading Partner Management*
- *TIBCO BusinessConnect™ Container Edition Administration*
- *TIBCO BusinessConnect™ Container Edition Security Guidelines*

How to Contact TIBCO Support

Get an overview of TIBCO Support. You can contact TIBCO Support in the following ways:

- For accessing the Support Knowledge Base and getting personalized content about products you are interested in, visit the TIBCO Support website.
- For creating a Support case, you must have a valid maintenance or support contract with TIBCO. You also need a user name and password to log in to TIBCO Support website. If you do not have a user name, you can request one by clicking **Register** on

the website.

How to Join TIBCO Community

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

Legal and Third-Party Notices

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.