IBM WebSphere Business Integration Connect Enterprise
and
Advanced Editions

Administrator Guide

IBM WebSphere Business Integration Connect Enterprise
and
Advanced Editions

Administrator Guide

Note!
Before using this information and the product it supports, read the information in "Notices" on page 103.

29June2004

This edition applies to Version 4, Release 2, Modification 2, of IBM WebSphere Business Integration Connect Advanced Edition (5724-E75) and Enterprise Edition (5724-E87), and to all subsequent releases and modifications until otherwise indicated in new editions.

To send us your comments about IBM WebSphere Business Integration documentation, email doc-comments@us.ibm.com. We look forward to hearing from you.

When you send information to IBM, you grant IBM a nonexclusive right to use or distribute the information in any way it believes appropriate without incurring any obligation to you.

Contents

About this book

This document describes how Business Integration Connect can be maintained to suit the requirements of the business-to-business (B2B) trading community.

New in this release

This section describes changes made to this guide since its last release (4.2.1).

- This guide has been modified to contain only information that is necessary to administer and maintain the WebSphere Business Integration Connect environment. All information for configuring the environment has been moved to the new *Hub Configuration Guide*.
- Information for enhancing product performance has been added. See Appendix A, "Performance considerations," on page 75.
- Information for archiving data has been added. See Chapter 8, "Archiving," on page 61.
- The option to delete Participants is documented. See, "Deleting Participants" on page 16.
- The option to delete transports is documented. See, "Deleting transports" on page 18.
- The new accessibility features that have been added to Community Console to support screen readers are documented.

Who should read this book

Administrators maintain Business Integration Connect. This book assumes two types of administrators:

- Hub Admin
- Account Admin

The Hub Admin is the super-administrative user in the community. The Hub Admin is responsible for overall hub community configuration and management, including Participant configuration and connection activation. The Operator Admin can access nearly all of the same features as the Hub Admin, except for the Hub Admin features.

Note: Some features can also be accessed by Community Participants and Community Managers. Though shared, Community Participants and Community Managers may not always see or have access to the same controls available to Hub Admin and Operator Admin personnel.

Related documents

The complete set of documentation available with this product describes the features and components of WebSphere Business Integration Connect Enterprise and Advanced Editions.

You can download the documentation or read it directly online at the following site:

http://www.ibm.com/software/integration/wbiconnect/library/infocenter/

Note: Important information about this product may be available in Technical Support Technotes and Flashes issued after this document was published. These can be found on the WebSphere Business Integration Support Web site:

http://www.ibm.com/software/integration/websphere/support/

Select the component area of interest and browse the Technotes and Flashes section.

Conventions and terminology used in this book

This document uses the following conventions:

bold	Indicates a selection on a screen.
blue text	Blue text, which is only visible when you view the manual online, indicates a cross-reference hyperlink. Click any blue text to jump to the object of the reference.
italics	Indicates a variable.
/	In this document, forward slashes (/) are used as the convention for directory paths. For Windows installations, substitute backslashes (\) for forward slashes. All WebSphere Business Integration Connect pathnames are relative to the directory where the product is installed on your system.

Terms

The following terms are unique to this product and document processing.

Action. Also called a business action. A message with content of a business nature such as a Purchase Order Request or Request For Quote. The exchange of business actions and business signals make up the message choreography that is necessary to complete a business activity specified by a RosettaNet PIP.

Business action. See Action.

Business process. A predefined set of business transactions that represent the steps required to achieve a business objective.

Community Console. A Web-based tool used to configure Business Integration Connect and to manage the flow of business documents to and from the Community Manager and Participants.

Community Manager. The company that purchased and distributed Business Integration Connect to members in their hub community. The Community Manager has one administrative user, the Manager Admin, who is responsible for the health and maintenance of the Community Manager's portion of the community. Community Console features excluded from the Community Manager's view relate to system configuration.

Community Operator. The individual responsible for the configuration and overall health and maintenance of the system, hub-wide (Hub Admin). The Hub Admin can access all features.

Community Participant (Participant). The Participant sends business transactions to and receives business transactions from the Community Manager. Participants can access features that support their role in the community. Features excluded from the Participant's view relate to system configuration.

Document. A collection of information adhering to an organizational convention. In Business Integration Connect, multiple documents make up a process.

Document protocol. A set of rules and instructions used to format and transmit information across a computer network. Examples include RosettaNet, XML, flat file, and EDI.

Hub Community. The Business Integration Connect system, which is made up of the Community Manager, Community Operator, and Community Participants.

Package. In Business Integration Connect, a document that has been encrypted and formatted for transmission over the Internet.

Participant connection. The connection between two community member environments in which one process is executed according to the associated action.

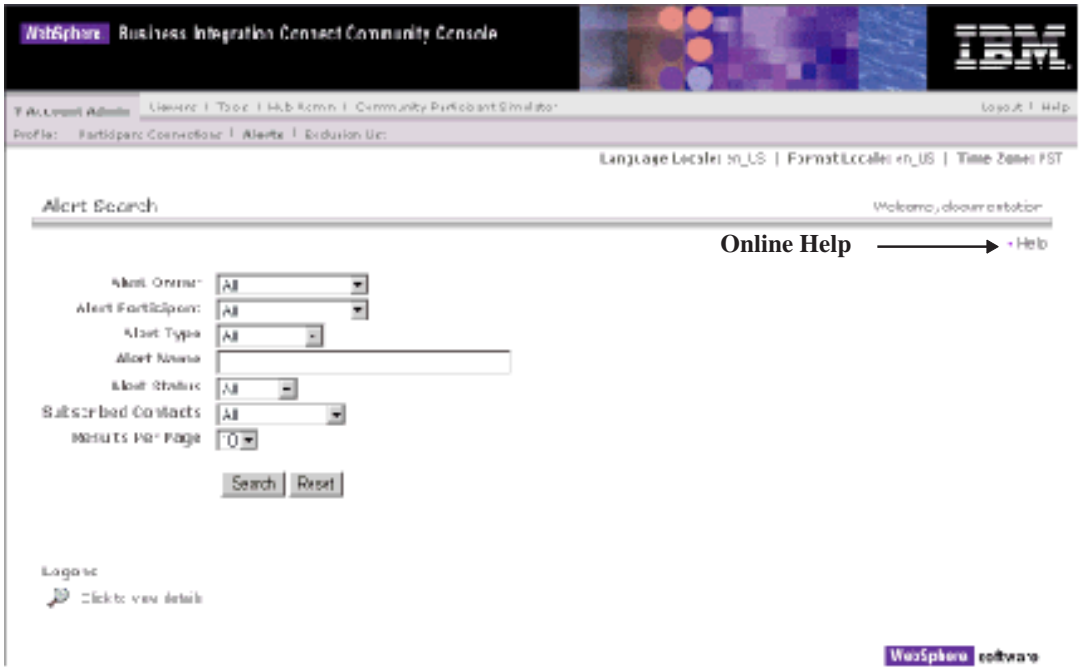
Process. In Business Integration Connect, a series of documents or messages executed between Community Managers and Participants. Taken as a whole, the documents make up a complete business process.

RosettaNet PIP (Partner Interface Process). A model that depicts the activities, decisions, and Partner Role Interactions that fulfill a business transaction between two partners in a supply chain. (In Business Integration Connect, partners are called Participants.) Each Participant in the Partner Interface Process must fulfill the obligations specified in a PIP instance. If a party fails to perform a service as specified in the PIP implementation guide, the business transaction is null and void.

Getting help

Click the **Help** link to access the online help.

Note: If you do not see a help window after clicking help, check to make sure you are not running a popup blocker.



Customer service

Software support

www.ibm.com/software/support

Passport Advantage

www.ibm.com/software/howtobuy/passportadvantage/

Product documentation

www.ibm.com/software/integration/wbiconnect/library/infocenter

Chapter 1. Logging in to Community Console

The tasks described in this guide are performed through WebSphere Business Integration Connect Community Console. Community Console is a Web-based facility that provides a secure access point.

Topics covered in this chapter include:

Starting Business Integration Connect Console

To start Business Integration Connect, run one of the following scripts:

- UNIX - INSTALLATION_DIRECTORY/console/was/bin/startServer.sh server1
- Windows - INSTALLATION_DIRECTORY/console/was/bin/startServer.bat server1

Note: When running this command, a warning message appears. You can safely ignore it.

Logging in to Community Console

Community Console requires one of the following Web browsers:

- Microsoft Internet Explorer versions 5.5 or later
- Netscape Navigator versions 6.x or later

Be sure to install the latest available Service Pack and updates for your browser.

Note: Community Console requires cookie support to be turned on to maintain session information. No personal information is stored in the cookie and it expires when the browser is closed.

For optimum viewing, use a screen resolution of 1024 x 768 DPI.

To log in to Community Console, follow these steps:

1. Type the following URL in the location field of any Web browser:
   http://*hostname.domain*:58080/console (unsecure)
   http://*hostname.domain*:58443/console (secure)
   where *hostname* and *domain* are the name and location of the computer hosting the Community Console component.

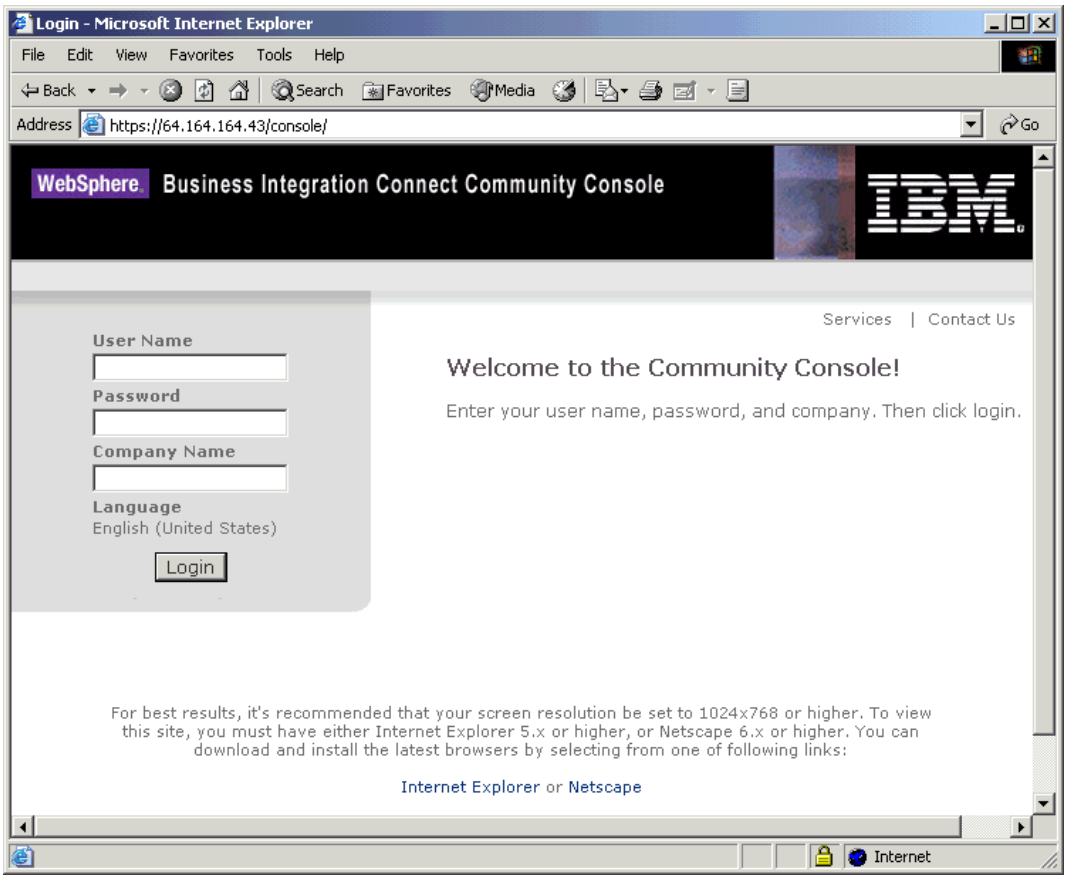


Figure 1. Community Console Login Screen

2. In the Community Console login screen, in the **User Name** field, enter the appropriate name:
   - For the Hub Admin, the default user name is **hubadmin**.
   - For the Operator Admin, the default user name is **Admin.**
3. In the **Password** field, enter the password for your site. The default password is Pa55word.
4. In the **Company Name** field, enter the Admin login name. The default login name for both the Hub Admin and Operator Admin user is **Operator**
5. Click **Login**.
6. The first time you log in, the system prompts you to create a new password. Enter a new password, then enter it again in the **verify** field.
7. Click **Save**.

Navigating through Community Console

Community Console consists of various menus used to configure Business Integration Connect.

The following two links appear at the top-right corner of each screen:

- **Logout** allows you to log off from the current WebSphere Business Integration Connect session. The application continues to run in the background. To log in again, follow the procedure under "Logging in to Community Console" on page 1.

- **Help** allows you to access the online help for Business Integration Connect.

  Note: If you do not see a help window after clicking help, check to make sure you are not running a popup blocker.

Community Console icons

For your convenience, Community Console uses icons on various screens. Some of these icons can be clicked to perform a task, while other icons indicate information. Table 1 lists the icons used throughout Community Console screens.

Table 1. Community Console Icons

Icon	Description
Task icons	
	View detailed information.
	Modify a selected item.
	Delete one or more selected items or activate the associated inactive item.
	Display a raw document.
	View validation errors.
	Continue.
	Pause.
	Print a document or report.
	Export a report.
	Select calendar dates.
	View the groups to which a user belongs.
	View users in a group.
	Click to create a new action based on the selected action.
	Export information from the system.
	Deactivate the associated active item.
	Edit a Document Flow Definition.
	View the Document Flow Definition attribute setup.
	Upload a new map.
	Download a map.
	Edit attribute values.
	Edit RosettaNet attribute values.

Table 1. Community Console Icons (continued)

Icon	Description
	View a previously sent original document when there is a duplicate document event.
	Hide the search criteria.
	View permissions.
	Create role. Role is not active.
	View the Help system.
Information icons	
	The field requires input from the user.
	A Trade Participant Agreement (TPA) has been entered.
	A Participant or gateway is disabled.
	The document currently in progress.
	The document processing was successful.
	The document processing failed.
	Synchronous data flow. No icon is displayed for asynchronous transactions.
	Click to see where an item is used.
	Data is contained.
	No data is contained.
	A hierarchical tree is in the “collapsed” view.
	A hierarchical tree is in the “expanded” view.

Logging off from Community Console

When you finish using Community Console, click **Logout** at the top-right side of any Console screen. The system logs you out and returns you to the Console Login screen.

Stopping Community Console

To stop Community Console, run one of the following scripts:

- UNIX - INSTALLATION_DIRECTORY/console/was/bin/stopServer.sh server1
- Windows - INSTALLATION_DIRECTORY/console/was/bin/stopServer.bat server1

Note: When running this command, a warning message appears. You can ignore it.

Stopping the Document Manager and Receiver

To stop Document Manager and Receiver, run one of the following scripts:

- UNIX - INSTALLATION_DIRECTORY/router/was/bin/./shutdown_bcg.sh
- Windows - INSTALLATION_DIRECTORY/router/was/bin/shutdown_bcg.bat
- UNIX - INSTALLATION_DIRECTORY/receiver/was/bin/./shutdown_bcg.sh
- Windows - INSTALLATION_DIRECTORY/receiver/was/bin/shutdown_bcg.bat

Note: If a warning message appears, you can ignore it.

Chapter 2. Hub administration tasks

This chapter describes the tasks that only a Hub administrator can perform. These tasks are:

Managing password policy

The Password Policy screen lets you set up the password policy for the Hub community:

- You can implement a strong password policy that includes limiting a password's life span.
- You can use special characters in the password to prevent susceptibility to dictionary attack.
- You can prevent the use of passwords that resemble those previously used or passwords that are similar to a user's login or full name.

The following procedure describes how to view password policy details and set policy passwords: minimum length, expire time, uniqueness, special character, and name variation checking parameters.

1. Click **Hub Admin** > **Console Configuration** > **Password Policy**.
2. On the Password Policy screen, click the  icon to edit the contents.

3. Set the parameters described in Table 2:

Table 2. Password policy details

Parameter	Description
Minimum Length	The minimum number of characters required for the password.
Expire Time	The number of days until the password expires.
Uniqueness	Numeric history of previously used passwords. An old password cannot be reused if it exists in the history file.
Special Characters	When this box is selected, passwords must contain at least three of the following types of special characters: • Uppercase characters • Lowercase characters • Numeric characters • Special characters This setting allows for the setting of stricter security requirements when using passwords composed of English characters (ASCII). The default setting is Off. Turn off this parameter when using passwords composed of international characters. Non-English character sets might not contain the required three out of four character types. The special characters supported by the system are: #, @, $, &, +.
Name Variation Checking	When this box is selected, you cannot use passwords that comprise an easily guessed variation of the user's login name or full name.

4. Click **Save**.

Managing targets

The Target List screen is used to view and edit existing targets details, and enable, disable, or delete targets.

Viewing and editing target details

The following procedure describes how to view details for a target. As part of this procedure, you can edit the target's parameters.

1. Click **Hub Admin** > **Hub Configuration** > **Targets**.
2. On the Target List screen, click the  icon next to the target whose details you want to view. The Console displays the Target Details screen.
3. On the Target Details screen, click the  icon to edit the parameters of the target.
4. Edit the parameters as needed.
5. Click **Save**.

Enabling or disabling targets

You can enable or disable targets from the Target List screen by clicking **Enabled** or **Disabled** in the **Status** column. To do this, follow these steps:

1. Click **Hub Admin** > **Hub Configuration** > **Targets**.
2. On the Target List screen, click the  icon to edit the target.
3. Click **Enabled** or **Disabled** next to the target whose status you want to change.

Deleting targets

You can delete targets that you do not need. Note that the deletion occurs immediately. There is no warning message asking you to confirm this step.

1. Click **Hub Admin** > **Hub Configuration** > **Targets**.

   Note: The target in the following step is immediately deleted without a warning message. Be sure that you want to delete the target.

2. On the Target List screen, click the ✗ icon next to the target you want to delete.

Managing interactions

To enable, disable or edit interactions, follow these steps:

1. Click **Hub Admin** > **Hub Configuration** > **Document Flow Definition**.
2. Click **Manage Interactions**.
3. Enter search criteria that Business Integration Connect uses to find the interaction you want to enable, disable, or edit.
4. Click **Search**. The system finds all interactions that meet your search criteria.
5. To enable an interaction, click the ✗ icon next to the interaction you want to enable. When a precautionary message asks whether you are sure, click **OK**.

   Business Integration Connect replaces the ✗ icon with the ✓ icon to show that you have enabled the interaction.
6. To disable an interaction, click the ✓ icon next to the interaction you want to disable. When a precautionary message asks whether you are sure, click **OK**.

   Business Integration Connect replaces the ✓ icon with the ✗ icon to show that you have disabled the interaction.
7. To edit an interaction, click the  icon next to the interaction. In the editing window, edit the interaction, then click **Save**.

Updating alert mail addresses

Alerts are text-based e-mail messages that notify participants of the occurrence of a system event.

After installation, you may want to update the alert mail information.

1. Edit the BCG.Properties file, located in the <install_root>/wbic/config directory to change the SMTP host e-mail addresses for alert notification. The elements in BCG.Properties are:
   - bcg.alertNotifications.mailHost
   - bcg.alertNotifications.mailFrom
   - bcg.alertNotifications.mailReplyTo
   - bcg.alertNotifications.mailEnvelopeFrom
2. Restart the router for the changes to take effect.

Managing XML formats

You can edit and delete existing XML formats on the Manage XML Formats screen. For information on creating XML formats, see the *Hub Configuration Guide*.

Editing XML format values

To edit XML format values, follow these steps:

1. Click **Hub Admin** > **Hub Configuration** > **XML Formats**.
2. On the Manage XML Formats screen, click the icon next to the XML format you want to edit.
3. On the View XML Protocol screen, edit the appropriate values.
4. Click **Save**.

Deleting an XML format

If you no longer need an XML format, follow these steps to delete it:

Important: Deleting an XML format disables pre-existing connections based on that protocol. Any document exchanged using that connection fails with an Unknown Document event. However, the Document Flow Definition associated with the deleted protocol remains in the system.

1. Click **Hub Admin** > **Hub Configuration** > **XML Formats**.
2. On the Manage XML Formats screen, click the icon next to the XML format you want to delete. The XML format is deleted.

Note: No warning message is displayed prior to deleting an XML format. Therefore, be sure you do not need an XML format before you delete it.

Enabling or disabling actions

The Actions screen displays all actions available for use in a transformation map or connection. Both system-supplied actions (which are labeled Product in the Provider column) and user-created actions are listed.

Click **Hub Admin** > **Hub Configuration** > **Actions** to display the Actions screen. See Figure 2 on page 11.

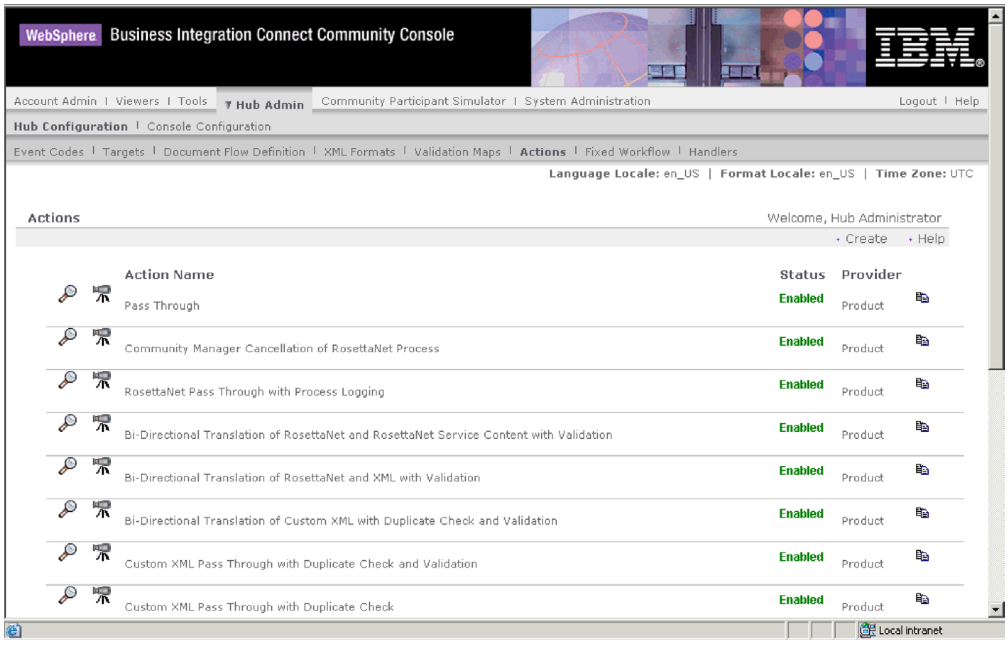


Figure 2. Actions screen

The following parameters are displayed for each action:

- The name of the action
- The status (Enabled or Disabled) of the action
- The provider of the action - either Business Integration Connect, indicated by **Product**, or a user.

You can click the icon to see details about an action. You can modify the information for user-created actions.

You can click the icon to see the transformation maps and connections currently using the action.

You can click the icon to to create a new action based on the selected action.

You can click **Create** to create a new action and make it available for use.

Managing event codes

When an event occurs within Business Integration Connect, an event code is generated. Using the Event Codes screen, you can see the generated event codes and export them to other applications.

Viewing and editing event codes

The following procedure describes how to view the details of an event code. You can edit the visibility and alertable status of the event code and view its severity.

1. Click **Hub Admin** > **Hub Configuration** > **Event Codes**.
2. On the Event Codes screen, click the icon next to the event code whose details you want to view.
3. On the Event Code Details screen, set the parameters described in Table 3 on page 12:

Table 3. Event code details

Parameter	Description
Event Code	A read-only field that shows the unique number for this event code.
Event Name	A read-only field that shows the name used to identify the event in relation to the action that triggered the event.
Internal Description	A read-only field that describes the circumstances that triggered it.
Visibility	Select the users who can view the event code: Community Operator, Manager, Participant, or any combination of the three.
Severity	A read-only field that shows the seriousness associated with this event code, from Debug (least serious) to Critical (most serious): • Debug – for low-level system operations and support. Visibility and use of the debug information are subject to the permission level of the user. • Info – for successful system operations. These events also provide the status of documents being processed. Informational events require no user action. • Warning – for non-critical anomalies in document processing or system functions that allow the operation to continue. • Error – for anomalies in document processing that cause the process to end. • Critical – for services that end due to system failure. Critical events require intervention by support personnel.
Alertable	Select to display the Event Name in the list on the Define tab of the Alert screen. This allows an alert to be set for this event.

Saving event code names

You can choose to save only the event name in the event list (**Export Names**), or to save the internal descriptions (**Export List**) in the event list in text format. Follow these steps:

1. Click **Hub Admin** > **Hub Configuration** > **Event Codes**.
2. On the Event Codes screen, click **Export Names** to save the list of events with the event names only. Or, click **Export List** to save the list of events with their internal descriptions only.

Viewing system activity

Business Integration Connect periodically summarizes data about system activity. This summary-service data is the information you see when you use the Document Analysis or Document Volume Report functions.

The Summary Service Properties screen allows you to view the summary data and edit how often the data is generated. This screen also displays the date and time that the summary data was last updated.

To change the time interval, follow these steps:

1. Click **System Administration** > **Event Processing** > **Summary Service**.
2. On the Summary Service Properties screen, click the  icon next to **Processing Interval (in Minutes)**.

3. Enter a value (from 1 through 60), indicating the number of seconds before data is summarized again. The default value is 30.
4. Click Save.

Managing event delivery

With Business Integration Connect, you can choose to publish system-generated events to an application (for example, a monitoring application). You publish these events to a JMS queue. From the Event Publishing Properties page, you can view the status of event publishing and the associated JMS configuration (if one exists), or you can change the status.

To activate event publishing, follow these steps:

1. Click **System Administration** > **Event Processing** > **Event Delivery Information**.
2. On the Event Publishing Properties screen, click the  icon next to **Enable Event Publication**. Then enter or change the values for the JMS properties.
3. Click Save.

Managing Handlers

The HandlersList screen displays all the handlers that are available for use with an action, target, gateway, or fixed workflow. Both system-supplied handlers (which are labeled Product in the Provider column) and any user-defined handlers that have been uploaded are listed.

You can use the HandlersList screen to view information about the available handlers, including the type of handler, its class name, and whether it is supplied by WebSphere Business Integration Connect or by a user. You can also import or delete a handler.

Importing a handler

To import a new handler into your environment, follow these steps:

1. Click **Hub Admin** > **Hub Configuration** > **Handlers**.
2. On the HandlersList screen, click **Import**.
3. For **File**, type the name of an XML file that represents the handler you want to import, or use the **Browse** button to navigate to the file.
4. Optionally indicate whether you want the handler committed to the database. If you click **Yes**, the handler will be available for use. If you click **No**, the handler will not be available for use. The default is **Yes**.
5. Optionally indicate whether you want the file to overwrite a file with the same name. If you click Yes, and the file you are uploading matches the name of an existing handler file, the existing file will be replaced by the uploaded file. You would use this feature if changes had been made to a user-supplied handler and you wanted to replace the existing handler with an updated version. The default is **No**.
6. Click **Upload**.

After a handler file is uploaded, it appears in the list of available handlers.

Deleting a handler

To delete a handler, follow these steps:

1. Click **Hub Admin** > **Hub Configuration** > **Handlers**.
2. On the HandlersList screen, click the  icon next to the handler you want to delete.

Managing API calls

Participants can make application program interface (API) calls (instead of using Community Console) to perform certain tasks.

To change the setting of the administration API, follow these steps:

1. Click **System Administration** > **Feature Administration** > **Administration API**.
2. On the Administration API Properties screen, click the  icon next to **Enable the Administration API**.
3. Select the check box to enable the use of the API, or clear the check box to disable the use of the API.
4. Click Save.

Changing the database, database user, and password

After installation, you can change the database that the Business Integration Connect components use. You can also change the name of the database user and the database user's password.

- On a Windows platform, change to the *server_root*\bin directory and type:

  ```
  wsadmin.bat -f bcgdbup.jacl -conntype NONE db_type dbNAME dbUserID
  dbPassword nodeName serverName
  ```

- For all other platforms, type:

  ```
  /wsdadmin.sh -f bcgdbup.jacl -conntype NONE dbType dbName dbUserID
  dbPassword nodeName serverName
  ```

The following is an example of the use of this command:

```
./wsdadmin.sh -f bcgdbup.jacl -conntype NONE DB2 hub_db  george
ABCD123 DefaultNode server1
```

Chapter 3. Account administration tasks

This chapter describes the following Business Integration Connect Account Admin tasks:

The tasks can be performed by the Hub Admin, Manager Admin, or Participant Admin, with the following limitations:

- **Managing Participants**: Manager Admin and Participant Admin users cannot edit Participant Type, Parent, and Action parameters.
- **Managing Gateway**: Manager Admin and Participant Admin users can edit only a subset of parameters.

Managing Participant profiles

The Account Admin Participants feature allows Hub Admin users to create, view, edit, and delete Participant profiles. A Participant profile identifies companies (participants) to the system. See the *Hub Configuration Guide* for information on creating Participant profiles.

Note: Participant Admin and Manager Admin users can edit only their own participant profile.

Viewing and editing participant profiles

Follow these steps to view and edit Participant profiles:

1. Click **Account Admin** > **Profiles > Community Participant**.
2. Click **Search**.
3. Click the  icon next to the Participant whose details you want to view.
4. On the Participant Details screen, click the  icon to edit the profile details.
5. Modify the Participant profile as necessary.

   Note: If you click **Reset User Passwords**, Community Console displays the message in Figure 3 on page 16. Click **OK** to proceed or click **Cancel** to retain the passwords.

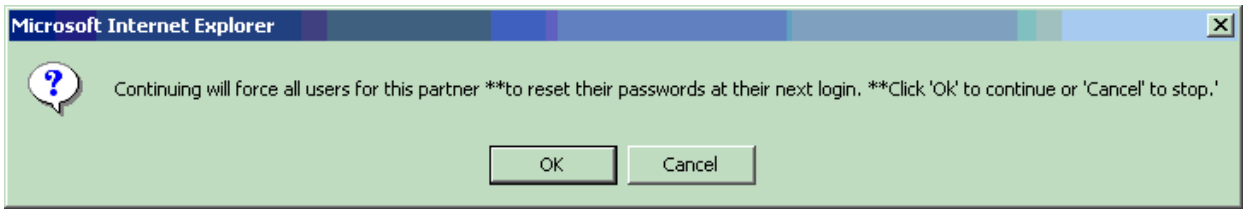


Figure 3. Reset user password message

6. Click **Save**.

Searching for Participants

The Participants screen allows the system to find Participants that meet your search criteria. Follow these steps to find a participant:

1. Click **Account Admin** > **Profiles** > **Community Participant**.
2. Type the Participant name or business ID in the appropriate field.
3. Click **Search**. The system finds the participants that match your criteria.
4. To change the Participant status, click **Enabled** or **Disabled** in the **Status** column.
5. To view the details for a Participant, click the icon next to the Participant.
6. To edit the Participant profile, click the icon.
7. Click **Save**.

Deleting Participants

To delete a participant, follow these steps:

1. Click **Account Admin** > **Profiles** > **Community Participant**.
2. Type the Participant name or business ID in the appropriate field.
3. Click **Search**. The system finds the participants that match your criteria.
4. Click the icon to delete a participant.
5. Confirm the deletion and save your changes.

Managing gateway configurations

Gateways manage the transport information used in routing documents to their proper destination in the hub community. The outbound Transport protocol determines which information is used during gateway configuration. For information on creating gateways, see the *Hub Configuration Guide*.

Viewing and editing gateways

To view and edit gateways, follow these steps:

1. Click **Account Admin** > **Profiles** > **Gateways**.
2. Click **Online** or **Offline** in the **Access** column to change the access of a gateway.
3. Click **Enabled** or **Disabled** in the **Status** column to change the status of a gateway.
4. Click the icon to view gateway details.

5. Click the  icon.
6. On the Gateway Detail screen, edit the gateway details that are described in Table 4 on page 17.
7. Click **Save**.

   You can also delete the gateway by clicking **Delete**.

Table 4. Gateway detail screen

Parameter	Description
Gateway Name	Name used to identify the gateway. Note: Gateway Name is a user-defined free format field. While uniqueness is not required, users should use different names for individual gateways to avoid potential confusion.
Status	Indicates whether the gateway is enabled or disabled. If disabled, documents passing through the gateway fail processing.
Online / Offline	Indicate whether the gateway is online or offline. If offline, documents are queued until the gateway is placed online.
Description	Optional description of the gateway.
Gateway Configuration	
Transport	Protocol for routing documents (see “Information required for gateway configuration” on page 19).
Target URI	Uniform Resource Identifier (URI) of the Participant.
User Name	User name for secure access through the Participant firewall.
Password	Password for secure access through the Participant firewall.
Retry Count	Maximum number of times the system tries to send a document before failing it. Default value is 3.
Retry Interval	Number of seconds the system pauses before trying to resend a document that was not sent successfully. Default value is 300 (5 minutes).
Number of Threads	Number of threads allocated for routing a document. Default value is 3. This parameter is available to Hub Admin users only.
Validate Client IP	Validates the IP address of the sending partner before processing the document.
Validate Client SSL Cert	Validates the sending Participant’s digital certificate against the DUNS number associated with the document before processing the document.
Auto Queue	If enabled, documents are placed in a temporary repository if the gateway is placed offline. If disabled and the gateway is placed offline, the document fails to route and an error occurs.
Authentication Required	If enabled, user name and password are supplied with JMS or SMTP messages.
JMS Factory Name	Name of the Java class the JMS provider will use to generate connection to the JMS queue.
JMS Message Class	Class of message.
JMS Message Type	Type of JMS message.
Provider URL Package	Name of classes or JAR file that Java uses to understand JMS Context URL.
JMS Queue Name	Queue name where JMS messages are stored.
JMS JNDI Factory Name	Factory name used to connect to the name service.
Connection Timeout	Number of seconds a socket will remain open with no traffic. Default value is 120 (2 minutes).

Viewing and editing default gateways

Follow these steps to view default gateways configured for the system and edit them:

1. Click **Account Admin** > **Profiles** > **Gateways**.
2. Click **View Default Gateways** in the upper right corner of the screen. The Console displays a list of all gateway types with their associated gateway.
3. To view information associated with a default gateway, click the  icon next to the gateway .
4. Edit the information as desired, then click **Save**.

Deleting gateway configurations

If you no longer need a gateway configuration, use the following procedure to delete it. A precautionary message does not appear before you delete a gateway configuration. Therefore, be sure you do not need the gateway configuration before you delete it.

1. Click **Account Admin** > **Profiles** > **Gateways**.
2. Click the  icon next to the gateway you want to delete.
3. Click the  icon.
4. Click **Delete**.

Deleting transports

If you no longer need a transport, use the following procedure to delete it.

1. Click **Account Admin** > **Profiles** > **Gateways**.
2. Select **Delete Transport Type**.
3. Select the Transport Type from the **Transport** drop-down list and click the **Delete** button.

Transport and gateway retries

When delivery of a document to a Participant gateway fails, Business Integration Connect will attempt to deliver the document again. Each repeated attempt is termed a `retry`. Retry functionality exists at two different levels within Business Integration Connect: transport and gateway.

1. Transport Retries

   Transport retries are built-in, low-level retries that are always applied regardless of the gateway specification. The motivation for low-level retries is that transient failures are inherent in the networks over which delivery is attempted, particularly the Internet. Thus, the delivery system is designed to retry automatically without requiring the user to define the retry parameters explicitly. The number of transport retries (`bcg.delivery.gwTransportMaxRetries`) and the time interval between retries (`bcg.delivery.gwTransportRetryInterval`) are defined in the document manager `BCG.Properties` file and apply to all gateways. The default values are three retries at three second intervals.

2. Gateway Retries (also known as document retries)

   Gateway retry parameters (number of retries allowed and interval between retries) are configured by the user in the gateway properties. Usually the retry interval is much longer than the built-in transport retries described above. The intent is to allow sufficient time for the user to correct the problem that is

preventing delivery. For example, the destination Web server might be down, or the destination URL might be incorrect. Setting the parameter values requires some judgment from the user on what is reasonable for each particular gateway.

For each gateway retry (user defined), Business Integration Connect will automatically perform the transport retries. For example, if three gateway retries are specified, the system retry pattern is:

First attempt fails
- Transport retry 0 fails
- Transport retry 1 fails
- Transport retry 2 fails

Gateway retry 1 fails
- Transport retry 0 fails
- Transport retry 1 fails
- Transport retry 2 fails

Gateway retry 2 fails
- Transport retry 0 fails
- Transport retry 1 fails
- Transport retry 2 fails

Gateway retry 3 fails

Document fails delivery

Every failed delivery attempt will generate a warning event that is visible in Community Console.

Information required for gateway configuration

The transport type selected determines the information needed for gateway setup. The boxes marked with an X require configuration information, boxes marked with the letter O are optional.

Note: The ability to edit certain gateway configuration values varies with the permission level of the user.

Transport	HTTP	HTTPS	FTP	FTPS	JMS	File Directory	SMTP
Target URI	X	X	X	X		X	X
User Name	O	O	O	O	O	O	O
Password	O	O	O	O	O	O	O
Retry Count	X	X	X	X	X	X	X
Retry Interval	X	X	X	X	X	X	X
Number of Threads	X	X	X	X	X	X	X
Validate Client IP	O	O	O	O			
Validate Client SSL Cert		O					
Auto Queue	O	O	O	O	O		O
Authentication Required					O		O
JMS Factory Name					X		
JMS Message Class					X		
JMS Message Type					O		
Provider URL Package					O		

Transport	HTTP	HTTPS	FTP	FTPS	JMS	File Directory	SMTP
JMS Queue Name					X		
JMS JNDI Factory Name					X		
Connection Timeout	X	X	X				

Notes:

1. When a gateway's Authentication Required option is on, and the User Name and Password are provided, the gateway will pass the User Name and Password to the non-WebSphere Business Integration Connect external system that it connects to for document delivery. The gateway does not enforce authentication, it simply passes these authentication credentials to the system that it is trying to connect to. For a JMS gateway, the User Name and Password are used as the credentials for JNDI look up of the JMS Queue Connection Factory. Note that JMS over Websphere MQ does not enforce JNDI authentication when file-based JNDI is used to connect to a JMS queue.
2. Username and password are required for FTPS authentication unless the FTPS server you are negotiating with is mapping the user, based on a presented client certificate. Check with the FTPS server administrator for implementation details.

Managing certificates

A digital certificate is an online identification credential, similar to a driver's license or passport. It verifies an individual with a guarantee of identity. Part of a digital certificate is digital signatures. Digital signatures are calculations based on an electronic document using public-key cryptography. Through this process, the digital signature is tied to the document being signed, as well as to the signer, and cannot be reproduced. With the passage of the federal digital signature bill, digitally signed electronic transactions have the same legal weight as transactions signed in ink.

Business Integration Connect uses digital certificates to verify the authenticity of business document transactions between the Community Manager and Participants. They are also used for encryption and decryption. Digital certificates were uploaded and identified during the configuration process.

Note: Before you can use the procedures in this section, the certificates must be loaded into the system. For more information on loading the certificates, refer to the *Hub Configuration Guide*.

Certificates not loaded

If no certificates are loaded into the system, the following event codes will be generated every minute:

- `240018 Digital Signature Key Not Loaded for Operator`
- `240019 Encryption Key Not Loaded for Operator`

When certificates are not required by Business Integration Connect, these events may be suppressed by adding the following property to the `bcg.properties` file for the Document Manager:

```
bcg.event_log_exclude=240018,240019
```

Viewing and editing digital certificates

Use the following procedure to view a list of the digital certificates that have been defined for the system and to edit them.

1. Click **Account Admin** > **Profiles** > **Certificates**. The Console displays the Digital Certificate List.

   Note: Red digital certificate dates indicate that the certificate has expired or is not yet valid.

2. Click the  icon next to a certificate to view the details. The Console displays the Viewing Certificate Details screen.

3. Click the  icon to edit the digital certificate.
4. Update the following parameters in the screen, then click **Save**. Alternatively, you can delete the certificate by clicking **Delete**.

Table 5. Digital Certificate Parameters

Parameter	Description
Certificate Type	Type of digital certificate: • Digital Signature Validation – authenticates the digital signature on documents coming from a Participant. • Encryption — contains the public key for encrypting outgoing documents to a Participant. • SSL Client — authenticates a Participant's certificate used for initiating an SSL connection. • Root Certificate — certificate issued from certifying authority for establishing certificate chain.
Description	Text that describes the certificate.
Status	Enables or disables the certificate.
Gateway Type	Select the type of gateway associated with the certificate.

Disabling a digital certificate

If you do not want to use a digital certificate, use the following procedure to disable it.

1. Click **Account Admin** > **Profiles** > **Certificates**. The Console displays the Digital Certificate List.
2. Click the  icon next to the certificate you want to disable.

3. Click the  icon to edit certificate details.
4. For **Status** select **Disabled**.
5. Click **Save**.

Changing B2B attribute values

To change the attribute values in a Document Flow Definition, use the following procedure.

Note: Changes to the attribute values for a higher-level Document Flow Definition will be inherited by the lower-level definitions within the same node.

1. Click **Account Admin** > **Profiles** > **B2B Capabilities**. The Console displays the B2B capabilities screen.

2. Click to individually expand a node to the appropriate Document Flow Definition level or select a number from 0-4 or All to expand all displayed Document Flow Definition nodes to the selected level.

3. Click the  icon to modify the appropriate attribute values in the **Update** column.

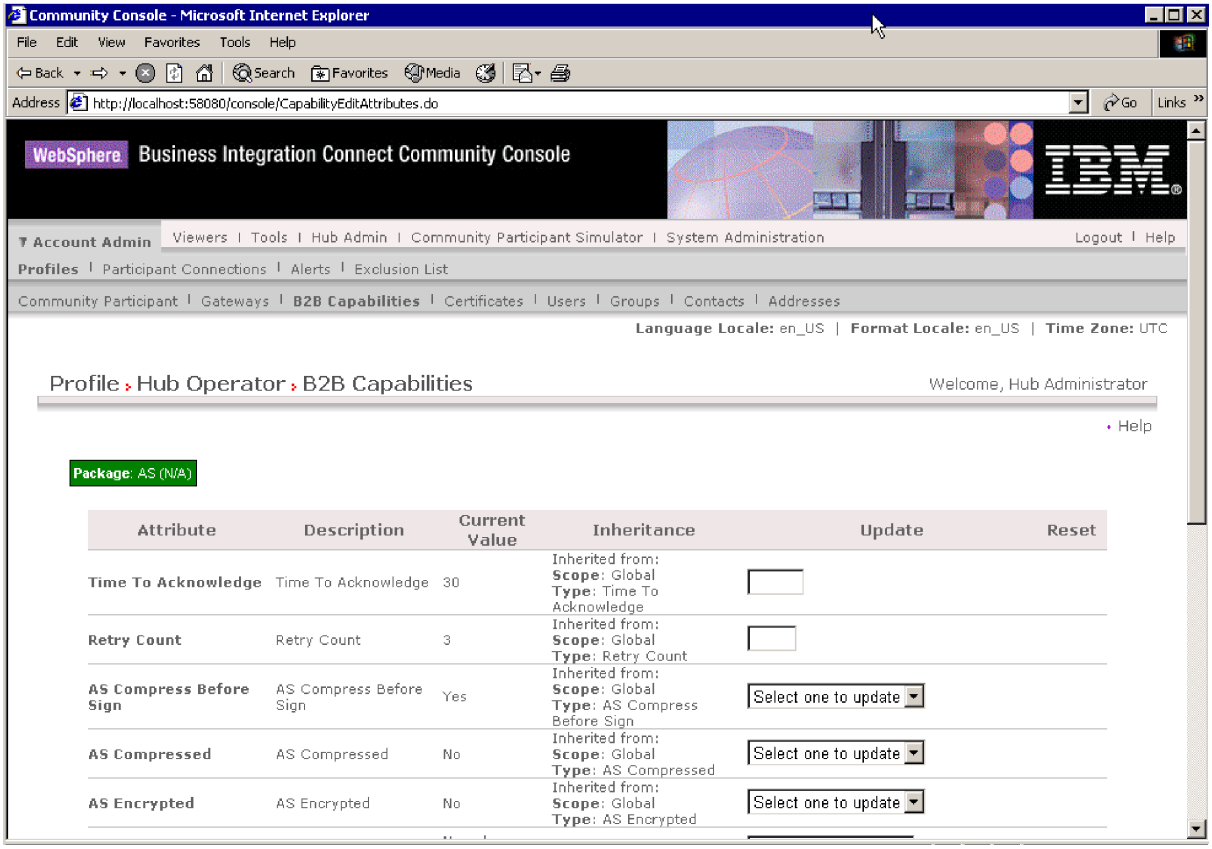


Figure 4. Screen for Changing B2B Attribute Values

4. Click **Save**.

Managing Participant connections

Participant connections are the mechanism that enables the system to process and route documents between the Community Manager and its various Participants. Connections contain the information necessary for the proper exchange of each document flow including RosettaNet TPA attributes, transport protocol, document processing action, gateway type, and Participant gateway. A document cannot be routed unless a connection exists between the Community Manager and one of its Participants.

The system automatically creates connections between the Community Manager and Participants based on their B2B capabilities. The data typed in the B2B Capabilities module of Community Console determines the functionality of each available connection. The configuration of each connection can be modified to fit the needs of the hub community.

Connection components

Individual connections are composed of four components:

- Attributes
- Action
- Gateway
- Gateway type

Once the system creates a connection, all four components can be modified to tailor its routing and processing functionality. Table 6 describes each component.

Table 6. Manage Participant Components

Component	Description
Attributes	Attributes are the information the connection uses for various document processing and routing functions such as validation, checking for encryption, and retry count. To increase the efficiency when creating connections, the attributes for a new connection are inherited from the B2B capabilities of the Manager and Participant automatically.
Action	Action is the sequence of steps the system uses to process a particular document. Each connection typically consists of one or more steps, including transformation, duplicate check, validation, or pass-through routing. You can select the appropriate action for each connection.
Gateway	Each connection contains a source and target gateway. The source gateway contains the URI and transport information of the Participant initiating a document flow. Business signals such as receipt acknowledgments and general exceptions are sent to the initiating Participant through the source gateway. The gateway options Validate Client IP and Validate Client SSL Cert apply to the source gateway. The target gateway contains the URI and transport information of the Participant receiving a document flow.
Gateway Type	Gateway type identifies the nature of a document being exchanged. A connection can contain multiple types of gateways to accommodate the routing and processing of the same document to more then one system. This improves connection efficiency by multiplying the use of a single connection for production, test, or routing to multiple systems within one organization.

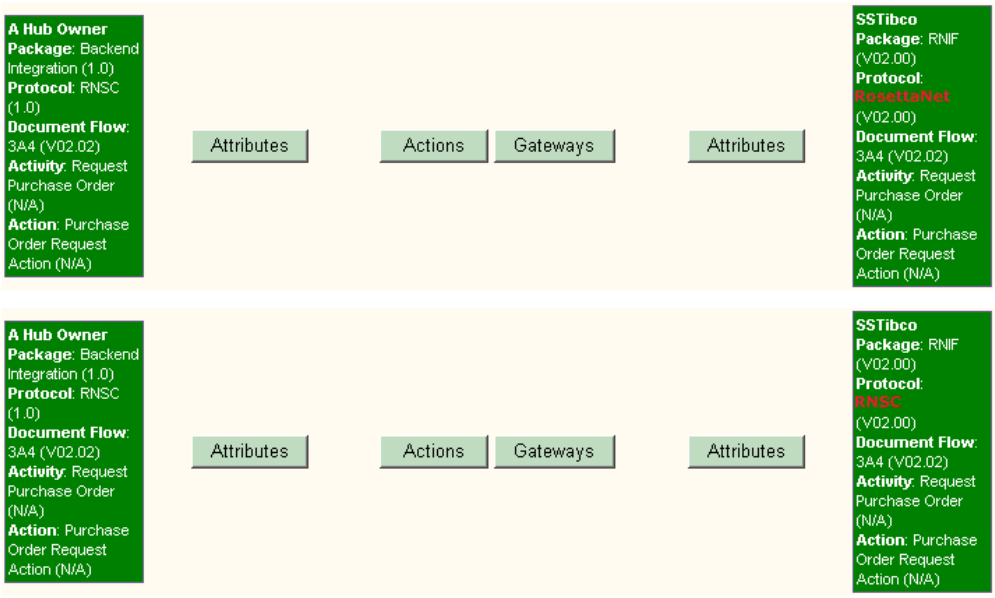
Connection duplication

The system avoids the inadvertent duplication of connections by uniquely identifying each connection based on the following parameters:

- Target
- Source
  - Source package & version
  - Source protocol & version
  - Source process & version

In the following example, for instance, the system will not activate two connections using the same source participant and attributes with the same target participant — even though the target participant is using the RosettaNet protocol in one connection and the RNSC protocol in the other. In this case, the connection containing the target RosettaNet protocol must be deactivated before the system

allows the other connection containing the target RNSC protocol to be used.



Searching for connections

To access connections, you search for them. There are two ways to search for connections:

- Using the Managing Connections screen to search for connections by selecting the source and target. See "Performing a basic search for connections," below.
- Using the system's Advanced Search facility to specify additional search criteria including Business ID, initiating and receiving packages and protocols, and initiating and receiving document flows. See "Performing an advanced search for connections" on page 25.

Performing a basic search for connections

Use the following procedure to perform a basic search for connections. When selecting a Source and a Target, observe the following guidelines:

- The Source and Target must be unique.
- Do not mix a production gateway with a test gateway when selecting Source and Target; otherwise, an error occurs. Both the Source and the Target must be production or test gateways.

1. Click **Account Admin** > **Participant Connections**. The Console displays the Manage Connections screen.
2. Under **Source**, select a Source.
3. Under **Target**, select a Target.

   Note: To create a new connection, the Source and Target must be unique.
4. Click **Search** to find the connections that match your criteria.
5. To activate a connection, click **Activate**. The Console displays the Manage Connections screen. This screen shows the package, protocol, and document flow for the source and target. It also provides buttons you can click to view and change partner-connection status and parameters.
6. Click the appropriate item as necessary:

- Clicking the  disables a connection.
- Clicking the  enables a connection.
- Clicking **Attributes** displays the Connection Attributes screen, where you can view and change connection attributes. For more information, see "Changing Participant attribute values" on page 26.
- Clicking **Actions** displays the Connection Details screen, where you can view and change the Action. For more information, see "Selecting a new action" on page 26.
- Clicking **Gateways** displays the Connection Management Gateway screen, where you can view and change the source or target gateway. For more information, see "Changing the source or target gateway" on page 26.

Performing an advanced search for connections

Use the following procedure to conduct an advanced search for connections. When selecting a Source and a Target, observe the following guidelines:

- The Source and Target must be unique.
- Do not mix a production gateway with a test gateway when selecting Source and Target; otherwise, an error occurs. Both the Source and the Target must be production or test gateways.

1. Click **Account Admin** > **Participant Connections**. The Console displays the Manage Connections screen.
2. Click **Advanced Search** in the upper right corner of the screen.
3. Complete the following parameters as shown in Table 7:

Table 7. Advanced Search Screen

Parameter	Description
Search By Participant Name	Names of the Source and Target.
Search By Business ID	Business IDs of the Source and Target. Includes DUNS, DUNS+4, and Freeform.
Source Package	Package used by the Source.
Target Package	Package used by the Target.
Source Protocol	Protocol used by the Source.
Target Protocol	Protocol used by the Target.
Source Document Flow	Document Flow used by the Source.
Target Document Flow	Document Flow used by the Target.
Connection Status	Allows you to search for enabled and disabled connections.

4. Click **Search**. The system finds the connections that match your criteria.

Changing connection configurations

To change the configuration of a connection, use the following procedure.

1. Click **Account Admin** > **Participant Connections**. The Console displays the Manage Connections screen.
2. Perform a basic search for connections (see "Performing a basic search for connections" on page 24) or advanced search for connections ("Performing an advanced search for connections" on page 25).
3. See the appropriate section:
   - To change Participant attribute values, see "Changing Participant attribute values" on page 26, below.
   - To select a new action, see "Selecting a new action" on page 26, below.

- To change the source or target gateway, see “Changing the source or target gateway.”
- To disable or activate a configuration, see “Disabling or deactivating a connection.”

Changing Participant attribute values

To change Participant attribute values, use the following procedure.

1. Click **Attributes** for either the Source or Target Participant.
2. In the **Scope** drop-down list, select **Connection** if the attribute changes will apply to all the gateway types associated with the connection, or select a gateway type to which the changes will apply.
3. Click the  icon and expand the node to the Document Flow Definition whose attribute values will be changed.
4. Update the attribute value as needed.
5. Click **Save**.

Selecting a new action

To select a new action, use the following procedure.

1. Click **Actions**.
2. Select the new action from the drop-down list.
3. Click **Save**.

Changing the source or target gateway

To change the source or gateway target, use the following procedure.

1. Click **Gateways**.
2. Select the source or target gateway from the drop-down list.
3. Click **Save**.

Disabling or deactivating a connection

To disable a connection, click the  in the **Enabled** column. The connection display color changes to red, indicating that the connection has been disabled. To re-enable the connection, click the  icon.

To deactivate a connection, click the  icon. The connection display color changes to gray and the icon disappears. To re-enable the connection, click **Activate**.

Managing Exclusion Lists

An Exclusion List lets the Community Operator configure the Document Manager to restrict notifications sent to the Manager from its trading partners. Trading partners are identified by name and business ID.

The following notifications can be selected for routing restriction:

- 0A1 - Notification of Failure — sent to the Manager by a Participant that cannot complete a particular document flow.
- Backend Event — a system-generated XML file sent to the Manager to notifying him or her that their Participant has received a business document successfully.

Adding Participants to the Exclusion List

Use the following procedure to add a Participant to the Exclusion List.

1. Click **Account Admin** > **Exclusion List**. The Console displays the Exclusion List screen.
2. Select a Participant from the **Participant Name** drop-down list. The Console displays a list of Participants and their business ID and exclusion status. **Send All Notifications** is selected by default.

Editing the Exclusion List

There might be times when you need to edit the Exclusion List. For example, you might want to restrict a notification from being routed to the Community Manager.

1. Click **Account Admin** > **Exclusion List**. The Console displays the Exclusion List screen.
2. Select a Participant from the **Participant Name** drop-down list. The Console displays a list of Participants, their business ID and exclusion status.
3. Click the  icon next to the notification you want to edit.
4. Check the check box below the notification to restrict the notification from being routed to the Community Manager. Select **Send All Notifications** to remove all routing restrictions.

Chapter 4. Managing gateways

The Gateway Queue lets you view documents queued for delivery from any gateway in the system. It also allows you to view all gateways that have documents queued for delivery, display and remove documents in a queue, and enable or disable gateways.

The Gateway Queue can be used to ensure that time-sensitive documents are not left standing in the queue. It can also be used to ensure that the maximum number of documents to be queued is not exceeded. Using the Gateway Queue, you can:

- See a list of all gateways containing documents queued for delivery
- View a document that has been in a gateway queue for an extended amount of time (30 seconds or more). This may indicate a problem with the document itself. You can also view document details to troubleshoot or delete documents from the queue.
- View gateway details to ensure proper operation. Documents backing up in a gateway queue can indicate a fault in the delivery manager or gateway.
- Confirm gateway status. An offline gateway causes documents to collect in the queue until the gateway is placed online. Gateway status does not affect connection functionality. Documents continue to be processed and placed in the queue for delivery.

Viewing the gateway list

To view a list of documents residing in the gateway, use the following procedure.

1. Click **Viewers** > **Gateway Queue**. The Console displays the Gateway Queue screen.
2. Input the parameters shown in Table 8.

Table 8. Gateway Queue Screen

Criteria	Description
Queued at least	Minimum number of minutes a document has been waiting in gateway queue. For example, if six minutes is selected, all gateways containing documents that have been waiting for delivery six minutes or more will be displayed. Default is 0.
Minimum Queued	Minimum number of documents in a gateway queue. Default is 1.
Sort By	Sort search results by Participant (default), Gateway Name, or Last Sent Timestamp.
Direction	Click **Ascend** to display documents starting with the oldest time stamp or end of the alphabet, or **Descend** to display documents starting with the most recent time stamp or beginning of the alphabet.
Refresh	Turn refresh on or off (default).
Refresh Rate	Number of seconds the Console waits before updating displayed data.

3. Click **Search**. The system finds all documents in the gateway that match your search criteria. **Table 9** shows the information returned form the search.

Table 9. Results After Gateway Queue Search

Criteria	Description
Participant	Trading partner associated with gateway.
Gateway	Name of the gateway.
Queued	Number of documents in the gateway queue waiting for delivery. Link to gateway details.
State	Shows whether the gateway is online or offline.
Last Sent	Last date and time when a document was sent to the gateway successfully.

Note: For the Console to display a gateway, the gateway must meet all the requirements of the search criteria in an "and" fashion.

Viewing queued documents

To have the system search for queued documents that meet your search criteria, use the following procedure.

1. Click **Viewers** > **Gateway Queue**. The Console displays the Gateway Queue screen.
2. Click **Search**.
3. Complete the following parameters in the screen:

Table 10. Search Criteria for the Gateway Queue

Parameter	Description
Participant	Name of the partner receiving the document.
Gateway	Name of the gateway.
Reference ID	Unique identification number assigned to document by system.
Document ID	Unique identification number assigned to document by source participant.
Sort By	Sorts search results by Participant (default), Reference ID, Document ID, or time document entered gateway queue.
Direction	Click **Ascend** to display documents starting with the oldest time stamp or end of the alphabet, or **Descend** to display documents starting with the most recent time stamp or beginning of the alphabet.

4. To view in-depth document details, click **Reference ID**. For information about the in-depth information displayed when viewing document details, see the topic "About document viewer" in the online help.

Removing documents from the queue

The following procedure describes how to remove documents from the delivery queue. You must be logged in as Hub Admin to delete documents from the queue.

1. Click **Viewers** > **Gateway Queue**. The Console displays the Gateway Queue screen.
2. Click **Search**.
3. Complete the parameters in the screen (see Table 10 on page 30).
4. Click the  icon to delete document.

Viewing gateway details

To view information about a particular gateway, including a list of documents in the queue, use the following procedure.

1. Click **Viewers** > **Gateway Queue**. The Console displays the Gateway Queue screen.
2. Type the search criteria (see Table 8 on page 29).
3. Click **Search**. A list of gateways appears.
4. Click the document count link in the **Queued** column. Gateway details and a list of queued documents appear.

Changing gateway status

To place a gateway online or offline, use the following procedure.

1. Click **Viewers** > **Gateway Queue**. The Console displays the Gateway Queue screen.
2. Type the search criteria (see Table 8 on page 29).
3. Click **Search**. A list of gateways appears.
4. Click the document count link in the **Queued** column. Gateway details and a list of queued documents appear.
5. Click **Online** in **Gateway Info** to place a gateway offline or click **Offline** to place gateway online. (You must be logged in as Hub Admin to change gateway status.)

Chapter 5. Analyzing document flows

Use the Document Analysis tool to get a detailed overview of the number of documents in the system, by state (Received, In Progress, Failed, and Successful). Search criteria includes date, time, type of process (To or From), gateway type, protocol, document flow, and process version. Use the search results to locate and view the documents that failed, to investigate the reason for the failures.

The Document Volume Report is a valuable tool used to manage, track, and troubleshoot the flow of your business documents. The report displays the volume of documents processed by the system within a specific time period. This report can be viewed, printed, and saved (exported) to send to other staff members. You can customize this report to view information based on specific search criteria.

The Test Participant Connection tool is used to test the gateway or Web server.

Table 11. Tools

What feature do you want to use?	See
Document Analysis	page 33
Document Volume Report	page 35
Test Participant Connection	page 36

Document Analysis

Use the Document Analysis tool to get a detailed overview of the number of documents in the system, by state, within a specific time period.

Use the search criteria to locate failed documents and investigate the reason for the failures.

The Document Analysis screen includes an alarm. If a process has failed, the row containing the failed process flashes red.

Document States

The following table describes the different document states.

Table 12. Document States

State	Description
Received	The document has been received by the system and is waiting for processing.
In Progress	The document is currently in one of the following processing steps: • **Incomplete**. For example, the system is waiting for other documents. • **Data Validation**. For example, the system is checking document content. • **Translation**. For example, the system is converting the document to another protocol. • **Queue**. For example, the document is waiting to be routed to the participant or Community Manager.
Failed	Document processing was interrupted due to errors in the system, data validation, or duplicates.
Successful	The final message that completes document processing has been transmitted from the system to the target participant.

Viewing documents in the system

1. Click **Tools** > **Document Analysis**. The system displays the Document Analysis Search screen.
2. Select the search criteria from the drop-down lists.

Table 13. Document Search Criteria

Value	Description
Start Date & Time	The date and time the process was initiated.
End Date & Time	The date and time the process was completed.
Source Participant	The participant that initiated the business process (Community Manager only).
Target Participant	The participant that received the business process (Community Manager only).
Search On	Search on From document flow or To document flow.
Gateway Type	For example, Production or test. Test is only available on systems that support the test gateway type.
Package	Describes document format, packaging, encryption, and content-type identification.
Protocol	Document protocol available to the participants.
Document Flow	Specific business process.
Sort By	Sort results by From Participant Name or To Participant Name.
Refresh	Controls if the search results are refreshed periodically (Community Manager only).
Refresh Rate	Controls how often search results are refreshed (Community Manager only).

3. Click **Search**. The system displays the Document Analysis Summary.

Viewing process and event details

1. Click **Tools** > **Document Analysis**. The system displays the Document Analysis Search screen.

2. Select the search criteria from the drop-down lists.
3. Click **Search**. The system displays the Document Analysis Summary.
4. Click  next to the Source and Target participants that you want to view. The system displays a list of all documents for the selected participants. Document quantity is arranged in columns by document processing state.
5. Select the quantity link in the Received, In Progress, Failed, or Successful columns. The system presents document processing details in the Document Analysis Report. If you selected Failed, the report also includes a Document Event Summary.

Document Volume Report

The Document Volume Report is a valuable tool used to manage, track, and troubleshoot the flow of your business documents. The report displays the volume of documents processed by the system within a specific time period. This report can be viewed, printed, and saved (exported) to send to other staff members.

You can customize this report to view information based on specific search criteria.

The Document Volume Report shows the number of documents currently in process by their state:

Table 14. Document States

Value	Description
Total Received	The total number of documents received by system.
In Progress	Documents that are In Progress are being tested and validated. No error has been detected, but the process is not yet complete.
Failed	Document processing was interrupted due to error.
Successful	The final message that completes document processing has been transmitted from the system to the target participant.

Use this report to perform the following tasks:

- Determine if key business processes have completed.
- Track trends in process volume for cost control.
- Manage process quality - success and failure.
- If you are the Community Manager, help participants track process efficiency.

Create a Document Volume Report

1. Click **Tools** > **Document Volume Report**. The system displays the Document Volume Report Search screen.

2. Select the search criteria from the drop-down lists.

Table 15. Document Volume Report Search Criteria

Value	Description
Start date & time	The date and time the process was initiated.
End date & time	The date and time the process was completed.
Source Participant	The participant that initiated the business process (Community Manager only).
Target Participant	The participant that received the business process (Community Manager only).
Search on	Search on From document flow or To document flow.
Gateway Type	Production or test. Test only available on systems that support the test gateway type.
Package	Describes document format, packaging, encryption, and content-type identification.
Protocol	Type of process protocol, for example, XML, EDI, flat file.
Document Flow	Specific business process.
Sort By	Sort results by this criteria (Document Flow or Target Document flow).
Results Per Page	Number of records displayed per page.

3. Click **Search**. The system displays the report.

Exporting the Document Volume Report

1. Click **Tools** > **Document Volume Report**. The system displays the Document Volume Report Search screen.
2. Select the search criteria from the drop-down lists.
3. Click **Search**. The system displays the report.
4. Click  to export the report**.** Navigate to the desired location to save the file.

Note: Reports are saved as comma-separated value (.CSV) files. The file name has an ".csv" suffix.

Printing reports

1. Click **Tools** > **Document Volume Report**. The system displays the Document Volume Report Search screen.
2. Select the search criteria from the drop-down lists.
3. Click **Search**. The system displays the report.
4. Click  to print the report**.**

Test Participant Connection

The Test Participant Connection feature allows you to test the gateway or Web server. If you are the Community Manager, you can also select a specific participant. The test consists of sending a blank POST request to a gateway or URL. The request is similar to entering the Yahoo's URL (www.yahoo.com) into your browser address field. Nothing is sent; it is an empty request. The response received from the gateway or Web server will indicate its status:

- If a response is returned, the server is up.
- If nothing is returned, the server is down.

Important: The Test Participant Connection feature works with HTTP that does not require any connection parameters.

To test a participant connection:

1. Click **Tools > Test Participant Connection**. The system displays the Test Participant Connection screen.
2. Select the test criteria from the drop-down lists.

Table 16. Test Participant Connection Values

Value	Description
Participant	Participant to be tested (Community Manager only).
Gateway	Displays available gateways based on the participant selected above.
URL	Dynamically populated based on the Gateway selected above.
Command	Post or Get.

3. Click **Test URL**. The system displays the test results. For information on the status code returned, see the following sections.

Web Server result codes

200 Series:

- 200 - OK - Successful transmission. This is not an error. Here is the file that you requested.
- 201 - Created - The request has been fulfilled and resulted in the creation of a new resource. The newly created resource can be referenced by the URLs returned in the URL-header field of the response, with the most specific URL for the resource given by a Location header field.
- 202 - Accepted - The request has been accepted for processing, but the processing has not yet completed.
- 203 - Non-Authoritative Information - The returned META information in the Entity-Header is not the definitive set as available from the origin server, but is gathered from a local or third-party copy.
- 204 - No Content - The server has fulfilled the request, but there is no new information to send back.
- 206 - Partial Content - You requested a range of bytes in the file, and here they are. This is new in HTTP 1.1

300 Series:

- 301 - Moved Permanently - The requested resource has been assigned a new permanent URL and any future references to this resource should be done using one of the returned URLs.
- 302 - Moved Temporarily - The requested resource resides temporarily under a new URL. Redirection to a new URL. The original page has moved. This is not an error; most browsers invisibly fetch the new page when they see this result.

400 Series:

- 400 - Bad Request - The request could not be understood by the server because it has a malformed syntax. Bad request was made by the client.
- 401 - Unauthorized - The request requires user authentication. The response must include a WWW-Authenticate header field containing a challenge applicable to the requested source. The user asked for a document but did not provide a valid username or password.

- 402 - Payment Required - This code is not currently supported, but is reserved for future use.
- 403 - Forbidden - The server understood the request but is refusing to perform the request because of an unspecified reason. Access is explicitly denied to this document. (This might happen because the web server doesn't have read permission for the file you're requesting.) The server refuses to send you this file. Maybe permission has been explicitly turned off.
- 404 - Not Found - The server has not found anything matching the requested URL. This file doesn't exist. What you get if you give a bad URL to your browser. This can also be sent if the server has been told to protect the document by telling unauthorized people that it doesn't exist. 404 errors are the result of requests for pages which do not exist, and can come from a URL typed incorrectly, a bookmark which points to a file no longer there, search engines looking for a robots.txt (which is used to mark pages you don't want indexed by search engines), people guessing filenames, bad links from your site or other sites, etc.
- 405 - Method Not Allowed - The method specified in the request line is not allowed for the resource identified by the request URL.
- 406 - None Acceptable - The server has found a resource matching the request URL, but not one that satisfies the conditions identified by the Accept and Accept-Encoding request headers.
- 407 - Proxy Authentication Required - This code is reserved for future use. It is similar to 401 (Unauthorized) but indicates that the client must first authenticate itself with a proxy. HTTP 1.0 does not provide a means for proxy authentication.
- 408 - Request Time out - The client did not produce a request within the time the server was prepared to wait.
- 409 - Conflict - The request could not be completed due to a conflict with the current state of the resource.
- 410 - Gone - The requested resource is no longer available at the server and no forwarding address is known.
- 411 - Authorization Refused - The request credentials provided by the client were rejected by the server or insufficient to grant authorization to access the resource.
- 412 - Precondition Failed
- 413 - Request Entity Too Large
- 414 - Request URI Too Large
- 415 - Unsupported Media Type

500 Series:

- 500 - Internal Server Error - The server encountered an unexpected condition that prevented it from filling the request. Something went wrong with the web server and it couldn't give you a meaningful response. There is usually nothing that can be done from the browser end to fix this error; the server administrator will probably need to check the server's error log to see what happened. This is often the error message for a CGI script which has not been properly coded.
- 501 - Method Not Implemented - The server does not support the functionality required to fulfill the request. Application method (either GET or POST) is not implemented.
- 502 - Bad Gateway - The server received an invalid response from the gateway or upstream server it accessed in attempting to fulfill the request.

- 503 - Service Temporarily Unavailable - The server is currently unable to handle the request due to a temporary overloading or maintenance of the server. Server is out of resources.
- 504 - Gateway Time out - The server did not receive a timely response from the gateway or upstream server it accessed in attempting to complete the request.
- 505 - HTTP Version Not Supported

Chapter 6. Viewing events and documents

The Viewers module includes the following features:

- Event Viewer
- RosettaNet Viewer
- AS1/AS2 Viewer
- Document Viewer

These features give you a view into overall system health. They are also troubleshooting tools for event resolution.

You can locate a specific event and then research why it occurred. The Event Viewer allows you to search for events by time, date, event type, event code, and event location. The Hub Admin can also search by Participant, Source IP, and Event IP.

The data that the Event Viewer generates identifies, among other things, the Event Code, TimeStamp, and Source IP, and allows you to view the event and document details to diagnose the problem. You can also view the raw document, which identifies the field, value, and reason for the error.

Use the RosettaNet Viewer to locate a specific process that generated an event. When you identify the target process, you can view process details and the raw document.

Use the AS1/AS2 Viewer to search for and view transport information for documents using the AS1 or AS2 communication protocol. You can view message IDs, Message Disposition Notification (MDN) destination URI and status, and document details (the document and wrapper).

The Document Viewer is used to locate and view a specific document that you want to research. You can search for documents based on date, time, type of process, (From Process or To Process), Participant connection, gateway type, document status, protocol, document flow, and process version. The search results display all documents that meet your search criteria, and identify time stamps, process, participant connection, and gateway types. Locate the target document and use the viewer's features to view the raw document.

Note: The term Participants is used on the Viewer screens to identify a hub community member, including the Community Manager.

The RosettaNet and AS1/AS2 Viewers include additional search criteria for the Hub Admin. For more information, see the *Hub Configuration Guide*.

Table 17. Viewers

What feature do you want to use?	See
Event Viewer	page 42
RosettaNet Viewer	page 46
AS1/AS2 Viewer	page 48
Document Viewer	page 48

Event Viewer

Use the Event Viewer to view and research events.

An event tells you know that something unusual has happened in the system. An event can let you know that a system operation or function was successful (for example, a Participant was successfully added to the system, or a Participant connection was successfully created between Community Manager and Participant). An event can also identify a problem (for example, the system could not process a document or the system detected a non-critical error in a document). Most types of documents are resent multiple times, so when a document fails and generates an alert, it is something that you should investigate and correct to prevent similar failures in the future.

WebSphere Business Integration Connect includes predefined events. Use the product's Alerts feature, Account Admin module, to create event-based alerts. This process identifies the events that are of concern to you. Then use the Contacts feature, also in the Account Admin module, to identify the staff members that the system will notify if those events occur.

The Event Viewer displays events based on specific search criteria. You can locate a specific event and then research why it occurred. The Event Viewer allows you to search for events by time, date, event type (debug, information, warning, error, and critical), event code (for example, 210031), and event location.

Data available through the Event Viewer includes event name, time stamp, user, and Participant information. This data helps you identify the document or process that created the event. If the event is related to a document, you can also view the raw document, which identifies the field, value, and reason for the error.

Event types

WebSphere Business Integration Connect includes the following event types.

Table 18. Event types

Event type	Description
Debug	Debug events are used for low-level system operations and support. Their visibility and use is subject to the permission level of the user. Not all users have access to Debug events.
Information	Informational events are generated at the successful completion of a system operation. These events are also used to provide the status of documents currently being processed. Informational events require no user action.
Warning	Warning events occur due to non-critical anomalies in document processing or system functions that allow the operation to continue.
Error	Error events occur due to anomalies in document processing that cause the process to terminate.
Critical	Critical events are generated when services are terminated due to system failure. Critical events require intervention by support personnel.

Performing Event Viewer tasks

Table 19. Event Viewer tasks

What do you want to do?	See
Search for events.	page 43
View event details.	page 43

Searching for events

1. Click **Viewers** > **Event Viewer**.

   Events are organized by severity from left to right in the Event Viewer Search screen. Information on the left is the least severe event type; Critical on the right is the most severe. (Debug events cannot be viewed by all users.) For any selected event, that event and all events with greater severity are displayed in the Event Viewer. For example, if the Warning event type is selected in the search criteria, Warning, Error, and Critical events are displayed. If Informational events are selected, all event types are displayed
2. Select the search criteria from the drop-down lists.

Table 20. Event Search criteria

Value	Description
Start date and time	Date and time the first event occurred. Default is ten minutes prior.
End date and time	Date and time the last event occurred.
Participants	Select all Participants or a specific Participant (Community Manager only).
Event type	Type of event: Debug, Info, Warning, Error, or Critical.
Event code	Search on available event codes based on selected event type.
Event location	Location where event was generated: all, unknown, source (from), target (to).
Sort by	Value used to sort results.
Descend	Sort in descending or ascending order.
Results per page	Number of records displayed per page.
Refresh	Default setting is Off. When Refresh is On, the Event Viewer will first perform a new query, then remain in refresh mode.
Refresh Rate	Controls how often search results are refreshed (Community Manager only).

3. Click **Search**. The system displays a list of events.

Tip: The event list can be re-filtered based on the event type selected at the top of the Event Viewer screen. The next screen refresh reflects the new selected event type.

Viewing event details

1. Click **Viewers** > **Event Viewer**.
2. Select the search criteria from the drop-down lists.
3. Click **Search**. The system displays a list of events.
4. Click the  icon next to the event you want to view. The system displays event details and associated documents.
5. Click the  icon next to the document that you want to view, if one exists.

6. Click to view the raw document, if one exists.
7. Click to view validation errors.

Tip: If a duplicate document event is displayed in the Event Viewer Detail, view the previously sent original document by selecting in Document Details.

AS1/AS2 Viewer

Use the AS1/AS2 Viewer to view packaged B2B transactions and B2B process details that use the AS1 or AS2 (Applicability Statement 1 or 2) communication protocol. You can view the choreography of the B2B process and associated business documents, acknowledgment signals, process state, HTTP headers, and contents of the transmitted documents.

Like its predecessor AS1, which defines a standard for data transmissions using SMTP, AS2 defines a standard for data transmissions using HTTP.

AS2 identifies how to connect, deliver, validate, and reply to data; it does not concern itself with the content of the document, only the transport. AS2 creates a wrapper around a document so that it can be transported over the Internet using HTTP or HTTPS. The document and wrapper together is called a message. AS2 provides security and encryption around the HTTP packets. Another bonus with AS2 is that it provides a measure of security not found in FTP. AS2 provides an encryption base with guaranteed delivery.

An important component of AS2 is the receipt mechanism, which is referred to as an MDN (Message Disposition Notification). This ensures the sender of the document that the recipient has successfully received the document. The sender specifies how the MDN is to be sent back (synchronously or asynchronously; signed or unsigned).

Note: When decryption fails for an incoming encrypted AS2 document, a failure MDN is not sent back. To correct this issue, a participant connection must be activated, whether used or not, between the two participants' AS Binary capability. If the AS Binary capability is not enabled, then it must enabled for both the participants and then a participant connection must be activated between them.

You can use the AS1/AS2 Viewer to view the message ID, Time Stamps, Document Flow, Gateway Type, Synchronous status, as well as document details. Additional document processing information is displayed when viewing document details.

Performing AS1/AS2 Viewer tasks

Table 21. AS1/AS2 Viewer tasks

What do you want to do?	See
Search for messages	page 46
Viewing RosettaNet process details	page 47
Viewing raw documents	page 48

Searching for messages

1. Click **Viewers** > **AS1/AS2 Viewer**. The system displays the AS1/AS2 Viewer screen.

2. Select the search criteria from the drop-down lists.

Table 22. AS1/AS2 Viewer search criteria

Value	Description
Start Date and Time	Date and time the process was initiated.
End Date and Time	Date and time the process was completed.
Source and Target Participant	Identifies the source (initiating) and the target (receiving) Participants (Community Manager only).
Participant	Identifies if the search applies to all Participants or the Community Manager (Participant only).
My role is the	Identifies if the search looks for documents in which the Participant is the Target or Source (Participant only).
Initiating Business ID	Business identification number of the source Participant, for example, Duns.
Gateway Type	Production or test. Test is only available on systems that support the test gateway type.
Package	Describes the document format, packaging, encryption, and content-type identification.
Protocol	Document format available to the Participants, for example, RosettaNet of XML.
Document Flow	The specific business process.
Message ID	ID number assigned to the AS1 or AS2 packaged document. Search criteria can include the asterisk (*) wildcard. Maximum length, 255 characters.
Synchronous Filter	Search for documents received in synchronous mode. This means that the connection between the initiator and the Document Manager stays open until the transaction is complete, including request and Message Disposition Notification (MDN).
Sort by	Sort results by this value.
Descend or Ascend	Ascend. Displays the oldest time stamp first or the end of the alphabet. Descend. Displays the most recent time stamp or the beginning of the alphabet.
Results per page	Use to select the number of records displayed per page.

3. Click **Search**. The system displays a list of messages.

Viewing message details

1. Click **Viewers** > **AS1/AS2 Viewer**. The system displays the AS1/AS2 Viewer screen.
2. Select the search criteria from the drop-down lists.
3. Click **Search**. The system displays a list of messages.
4. Click the  icon next to the message that you want to view. The system displays the message and the associated document details.

Table 23. AS1/AS2 Viewer: Package Details

Value	Description
Message ID	ID number assigned to the AS1 or AS2 packaged document. This number identifies the package only. The document itself has a separate Document ID number that is displayed when viewing the document details. Maximum length, 255 characters.
Source Participant	Participant initiating a business process.
Target Participant	Participant receiving the business process.
Initiating Time Stamp	Date and time the document begins processing.
Gateway Type	Test or production. Test is only available on systems that support the test gateway type.
MDN URI	The destination address for the MDN. The address can be specified as a HTTP URI, or an e-mail address.
MDN Disposition Text	This text provides the status of the originating message that was received (either successful or failed). Examples include the following: • Automatic-=action/MDN-sent-automatically; processed. • Automatic-action/MDN-sent-automatically;processed/Warning;duplicate-document. • Automatic-action/MDN-sent-automatically;processed/Error;description-failed. • Automatic-action/MDN-sent-automatically;failed:unsupported MIC-algorithms.

5. (Optional) Click  to view the raw document.

RosettaNet Viewer

RosettaNet is a group of companies that created an industry standard for e-business transactions. Participant Interface Processes (PIPs) define business processes between members of the hub community. Each PIP identifies a specific business document and how it is processed between the Community Manager and Participants.

The RosettaNet Viewer displays the choreography of documents that make up a business process. Values that are viewable using the RosettaNet Viewer include process state, details, raw documents, and associated process events.

The RosettaNet Viewer displays processes based on specific search criteria.

Performing RosettaNet Viewer tasks

Table 24. RosettaNet Viewer tasks

What do you want to do?	See
Search for RosettaNet processes.	page 46
View RosettaNet process details.	page 47
View raw documents.	page 48

Searching for RosettaNet processes

1. Click **Viewers** > **RosettaNet Viewer**. The system displays the RosettaNet Viewer Search screen.

2. Select the search criteria from the drop-down lists.

Table 25. RosettaNet search criteria

Value	Description
Start Date and Time	The date and time that the process was initiated.
End Date and Time	The date and time that the process was completed.
Source and Target Participant	Identifies the source (initiating) and the target (receiving) Participants (Community Manager only).
Participant	Identifies if the search applies to all Participants or the Community Manager (Participant only).
My role is the	Identifies if the search looks for documents in which the Participant is the Target or Source (Participant only).
Initiating Business ID	Business identification number of initiating Participant, for example, DUNS.
Gateway Type	Production or test. Test is only available on systems that support the test gateway type.
Protocol	Protocols available to the Participants.
Document Flow	The specific business process.
Process Instance ID	Unique identification number assigned to the process. Criteria can include asterisk (*) wildcard.
Sort By	Sort results, for example, by Received Time Stamp.
Descend or Ascend	Ascend - Displays oldest time stamp first or end of the alphabet. Descend - Displays most recent time stamp or beginning of the alphabet.
Results Per Page	Display n number of results per page.

3. Click **Search**. The system displays RosettaNet processes that match your search criteria.

Viewing RosettaNet process details

1. Click **Viewers** > **RosettaNet Viewer**. The system displays the RosettaNet Viewer Search screen.
2. Select the search criteria from the drop-down lists.
3. Click **Search**. The system displays the results of your search.

Table 26. Document processing details

Value	Description
Participants	Participants involved in the business process.
Time Stamps	Date and time the first document begins processing.
Document Flow	The specific business process, for example RosettaNet (1.1): 3A7.
Gateway Type	For example, Production.
Process Instance ID	Unique number assigned to the process by the initiating community member.
Document ID	Proprietary document identifier assigned by the sending Participant. The field is not in a fixed location and varies by document type.
Source Participant	Initiating Participant.
Target Participant	Receiving Participant.

4. Click the  icon next to the RosettaNet process you want to view. The system displays details and associated documents for the selected process.

5. Click the  icon next to the document you want to view. The system displays the document and associated event details.

Viewing raw documents

1. Click **Viewers** > **RosettaNet Viewer**. The system displays the RosettaNet Viewer Search screen.
2. Select the search criteria from the drop-down lists.
3. Click **Search**. The system displays a list of processes.
4. Click the  icon next to the process that you want to view. The system displays process details and associated documents for the selected process.
5. Click  adjacent to the Document Flow to display the raw document.

Restrictions: Raw documents greater than 100K are truncated. For example, when the signature is located at the bottom of the raw document (`.rno` file), and the size of the raw document exceeds 100K, or the signature is present after the first 100K of the `.rno` file, the signature will not be shown in Document Viewer.

Tip:

- To troubleshoot documents that have failed processing, see "Viewing data validation errors" on page 50.
- The raw document viewer displays the HTTP header with the raw document.

Document Viewer

Use the Document Viewer to view individual documents that make up a process. You can use search criteria to display raw documents and associated document processing details and events.

When viewing cXML document details, all documents related to the selected request or response are displayed under the Associated Documents header. The magnifying glass icon will be missing from the first document. It represents the document that is currently being viewed in the details above.

Table 27. Document Viewer tasks

What do you want to do?	See
Searching for documents	page 43
Viewing document details, events, and raw document	page 49
Viewing data validation errors	page 50
Using the Stop Process feature	page 52

Searching for documents

1. Click **Viewers** > **Document Viewer**. The system displays the Document Viewer Search screen.

2. Select the search criteria from the drop-down lists.

Table 28. Document Viewer search criteria

Value	Description
Start date and time	Date and time the process was initiated.
End date and time	Date and time the process was completed.
Source and Target Participant	Identifies the source (initiating) and the target (receiving) Participants (Community Manager only).
Participant	Identifies if the search applies to all Participants or the Community Manager (Participant only).
My role is the	Identifies if the search looks for documents in which the Participant is the Target or Source (Participant only).
Search on	Search on From or To document flow.
Gateway Type	Production or test. Test is only available on systems that support the test gateway type.
Document status	Current document status in system: failed, successful, in-progress, or all.
Package	Describes the document format, packaging, encryption, and content-type identification
Protocol	Type of process protocol available to the Participants.
Document Flow	The specific business process.
Document ID	Created by the source Participant. Criteria can include asterisk (*) wildcard.
Synchronous Filter	Search for documents received in synchronous mode. This means that the connection between the initiator and the Document Manager stays open until the transaction is complete, including request and acknowledgement or request and response.
Sort By	Value used to sort results.
Results per page	Number of records displayed per page.
Descend	Sort results in descending or ascending order.

Note: Warning events are displayed by default. To see all events, select Debug.

3. Click **Search**. The system displays a list of documents that meet your search criteria.

Table 29. Document information available using the Document Viewer

Value	Description
Participants	Source (From) and target (To) Participants involved in the business process.
Time Stamps	Date and time the document begins and ends processing.
Document Flow	Business process that is being transacted.
Gateway Type	Test or production. Test is only available on systems that support the test gateway type.
Synchronous	Identifies that the document was received in synchronous mode. This means that the connection between the initiator and the Document Manager stays open until the transaction is complete, including request and acknowledgement or request and response.

Viewing document details, events, and raw document

1. Click **Viewers** > **Document Viewer**. The system displays the Document Viewer Search screen.
2. Select the search criteria from the drop-down lists.

3. Click **Search**. The system displays a list of documents.

   - To view a document's details and events, click the  icon next to the document. The system displays process details and events for the selected document. Click the blue arrow icon to view event details.
   - To view the raw document with HTTP header, click  next to the document. The system displays the raw document's content.

The following document processing information is displayed when you view document details:

Table 30. Document processing values available using the Document Viewer

Value	Description
Reference ID	Unique identification number assigned to the document by the system.
Document ID	Unique identification number assigned to the document by the source Participant.
Doc Time Stamp	Date and time document was created by Participant.
Gateway	Gateway the document passed through.
Connection Document Flow	Actions performed on a document by the system to ensure its compatibility with business requirements between Participants.
Source and Target	Source and target Participants involved in business process.
In Time Stamp	Date and time the document was received by the system from the Participant.
End State Time Stamp	Date and time the document was successfully routed by the system to the target Participant.
Source and Target Business ID	Business identification number of Source and Target Participants, for example, DUNS.
Source and Target Document Flow	The specific business process transacted between source and target Participants.

Restrictions: Raw documents greater than 100K are truncated. For example, when the signature is located at the bottom of the raw document (`.rno` file), and the size of the raw document exceeds 100K, or the signature is present after the first 100K of the `.rno` file, the signature will not be shown in Document Viewer.

Tip: If the system displays a Duplicate Document event, view the previously sent original document by selecting the blue arrow icon next to the Duplicate Document event, then selecting  .

Tip: To troubleshoot documents that have failed processing, see "Viewing data validation errors" on page 50.

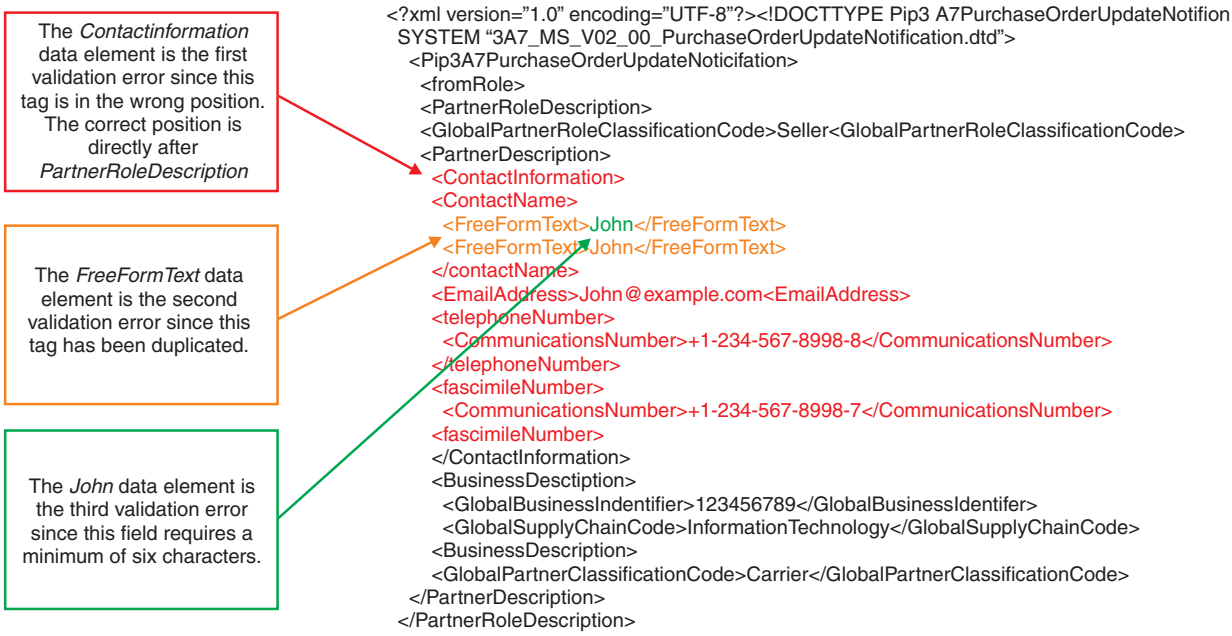
Viewing data validation errors

You can quickly search for documents that have failed processing using the color-coded text in the XML fields that contain validation errors. Fields that contain validation errors are displayed in **red**. If up to three separate validation errors occur within nested XML fields, the following colors are used to distinguish between the error fields:

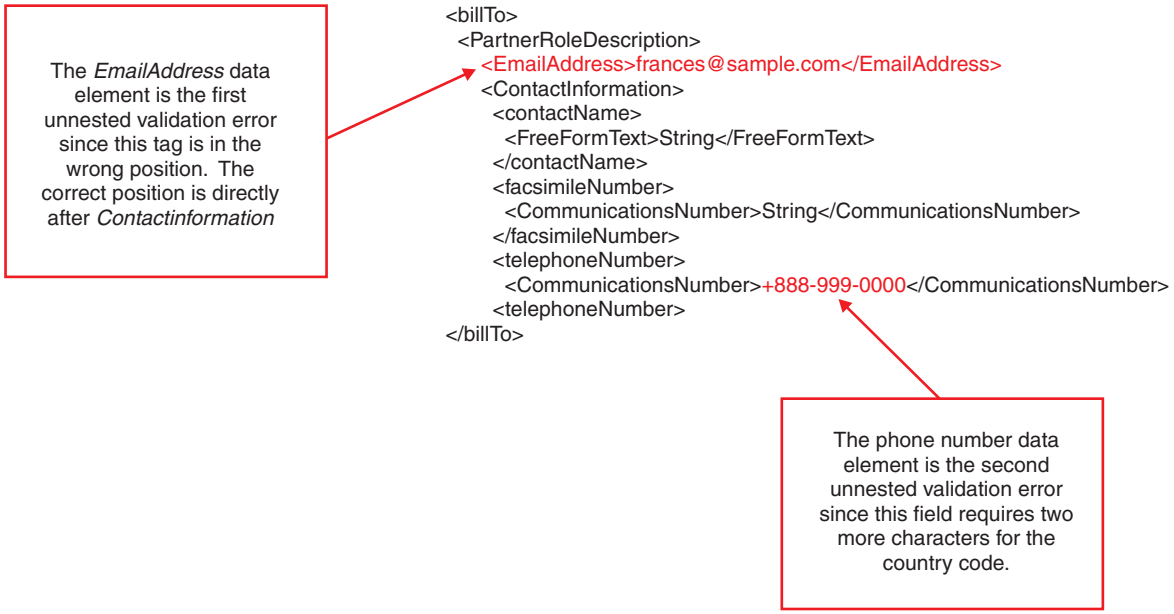
Table 31. Color-coded document validation errors

Value	Description
Red	First validation error
Orange	Second validation error
Green	Third validation error

The following is an example of nested XML validation errors:



Example of non-nested XML validation errors:



To view validation errors in a raw document, see "Viewing raw documents" on page 48.

Restrictions: The console only displays the first 100KB of a raw document. Validation errors beyond 100KB are not viewable.

Using the Stop Process feature

Click **Stop Process** to fail a document currently in progress. This feature is only available to hub admin users.

Note: It may take up to one hour for the system to fail the document. During this time, the Document Viewer will continue to display the document status as in progress.

Chapter 7. Simulating production traffic

The Community Participant Simulator (CPS) can be used before and after the Hub Community goes live to simulate production traffic (requests, responses, and acknowledgements) between the Community Manager and a Participant.

The purpose of the CPS is:

- To give you a way to simulate a community participant sending an RN request to the community manager via the hub.
- To give you a way to simulate the community manager enterprise system sending RosettaNet Service Content (RNSC) via the hub to a community participant.

The Community Manager's administrative user, the Manager Admin, uses the cps to verify that documents are formatted correctly and contain valid business content.

The CPS gives the Community Manager the ability to test their back-end systems (routers and receivers) without initiating the test from their own back-end applications, and without requiring a Participant to transmit data. As a result, they can test without engaging test systems or technical support personnel.

To initiate the test, the Manager Admin uploads a test document. This feature only accepts RNIF v2.0; it is not compatible with RNIF 1.1. The test document must be a RosettaNet Service Content file; you cannot upload a RNO (RosettaNet Object). Service Content is the primary component of the payload of a RosettaNet Business Message. It is an XML document that represents the business content specified by a particular PIP. The payload also includes any file attachments.WebSphere Business Integration Connect uses the test document to identify routing and processing information.

The CPS does not generate receipt acknowledgements. If a 3A4 confirmation is sent to CPS, the Document Manager closes the exchange with an 0A1.

Note that the installation process creates a sink gateway (that is, a bit bucket), to receive acknowledgements during the testing process:

http://<*hostname*>:<*port#*>/console/sink

or

https://<*hostname*>:<*port#*>/console/sink

Preparing for the test process

Before you start the test process, you must perform the following tasks, which are dependent on the role that you are simulating, a request or response from the Community Manager, or a request or response from a Participant. For more information, see "Setting up test scenarios" on page 55:

- Copy your VTP digital certificate to the file system:
  /opt/data/vcrouter/vms/security/vtp

  You can obtain this certificate from a CA, or it can be self-signed.

Edit the vtp values that appear in the bcg_console.properties file.

Edit the *bcg.certs.vtp.CertificateDir* location in the bcg_router.properties file.

Business Integration Connect automatically loads the VTP digital certificate for every Participant in the database, allowing you to post to any Participant. These certificates are not visible on the console.

- Verify that your gateways and connections are configured and that they are working properly.
- Verify that your targets are enabled and configured with the appropriate URL for incoming messages. Different traffic occurs on different targets. If the target's URLs are not correct, documents will not be processed.

  This requirement only applies when you are testing a document that requires a response.

  For more information about targets, see the *Hub Configuration Guide*.
- Verify the Business IDs that appear in the header of your test document. The Business IDs drive the routing process. They control where the document is sent.

  For example, if you are sending your document to yourself, the Community Manager, the "to" Business ID in the document header must be your own Business ID. The system uses the "to" Business ID to find the correct connection.

The following is an example of the "from" and "to" Business IDs in a test document (lines that are not relevant have been removed):

```
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE Preamble SYSTEM "3A4_MS_V02_02_PurchaseOrderRequest.dtd">
<Pip3A4PurchaseOrderRequest>
   <fromRole>
      <GlobalBusinessIdentifier>987654321</GlobalBusinessIdentifier>
   <toRole>
      <GlobalBusinessIdentifier>567890123</GlobalBusinessIdentifier>
```

Setting up test scenarios

You can use the CPS to test the following scenarios between you and your Participants:

Table 32. Test scenarios

Scenario	Destination for Connection	URL
One way outbound from Community Manager to Participant. Simulating Community Manager.	VTP_Owner	VTP_OWNER
One way inbound from Participant to Community Manager. Simulating Participant.	VTP_TP	Not applicable in this scenario.
Two way outbound from Community Manager to Participant (Upload Request). Simulating Community Manager.	VTP_Owner	VTP_OWNER
Two way inbound from Participant to Community Manager (Upload Request). Simulating Participant.	VTP_TP	VTP_TP
Two way outbound from Community Manager to Participant (Upload Response). Simulating Participant.	VTP_TP	VTP_TP
Two way inbound from Participant to Community Manager (Upload Response). Simulating Owner.	VTP_Owner	VTP_Owner

Sample scenarios

This section describes the steps involved in configuring the CPS to simulate two one-way RosettaNet (RN) interactions. The steps are not fully described here. They are described with more detail in the *Hub Configuration Guide*.

You will see the directories and hub configuration settings that are used by the CPS, and you will have a better understanding of how the CPS can be helpful in debugging routing between participants.

Community Manager:

Set up an HTTP sink gateway for the manager. This is an HTTP gateway that sends to URL `http://<console-ip>:<console-port>/console/sink`.

The sink gateway should be specified as the default CPS Participant and CPS Manager gateway for the community manager.

Community Participant:

Set up an HTTP sink gateway for the participant just as you did for the manager.

RosettaNet PIP XML files:

The 3A4 interaction is the scenario described here. The participant-to-manager simulation uses XML that contains the 3A4 Purchase Order Request content.

The manager-to-the participant simulation uses XML that complies with the 3A4 Purchase Order Confirmation RNSC content. These XML files reside on your local file system.

Please refer to the *Hub Configuration Guide* for related information. When you create the files, remember that the to and from Ids must match those of the manager and the participant in the appropriate places in these files.

Configuring the Console and Router Servers:

If you plan to use encryption or signing in your simulation, you need a pair of public-key and private-key certificates. Use p8 format for the private keystore and der format for the public certificate.

1. Copy your p8 and der files to the `common/security/vtp` directory.
2. Copy the der file to the `common/security/ca` directory.
3. With the console started and logged in as hubadmin, upload the der file as a Root Certificate.
4. Modify the console configuration to point to the certificate and keystore files.
5. Open the `<console-root>/was/wbic/bcg_console.properties` file in an editor.
6. Locate the VTP (Virtual Test Participant) section in the `bcg_console.properties` file and fill in the following values with values that are appropriate for your system. You must use der and p8 file formats as shown.

   ```
   ## VTP
   ibm.bcg.certs.vtp.CertificateDir=C:/WBIConnect/common/security/vtp
   ibm.bcg.certs.vtp.Certificate=testcert.der
   ibm.bcg.certs.vtp.PrivateKey=testkey.p8
   ibm.bcg.certs.vtp.Passwd=password
   ibm.bcg.certs.vtp.VerifySig=false
   ibm.bcg.vtp.RouterIn=C:/WBIConnect/common/router_in
   ```
7. Save the bcg_console.properties file.
8. If the console server is running, restart it. Otherwise, start it now.
9. Check to be sure that the router configuration is set up correctly.
10. Open the `<console-root>/was/wbic/bcg.properties` file in an editor.
11. Locate the VTP section and verify that the `vtp.CertificateDir` property points to the same directory as the console.
12. Change it if necessary and save the file.
13. If the router server is running, restart it. Otherwise, start it now.

Configuring 3A4 Connectivity:

If you are familiar with RosettaNet routing, configure RosettaNet connectivity between a Community Participant and the Community Manager using the following steps.

If you are not familiar with RosettaNet routing, refer to the *Hub Configuration Guide* for assistance when performing the following tasks:

1. Import the RN and RNSC files that support the 3A4 interactions.

Upload the following files in the order shown. The files are located in the /B2Bintegrate/rosettanet directory of the installation CD:

- Package_RNIF_V02.00.zip
- BCG_Package_RNIFV02.00_3A4V02.02.zip
- Package_RNSC_1.0_RNIF_V02.00.zip
- BCG_Package_RNSC1.0_RNIFV02.00_3A4V02.02.zip

2. Define the capabilities (called interactions) for 3A4 purchase order requests and confirmations to be routed through the hub.
3. Configure the Community Manager and Community Participant to be the source and target of Participant 3A4 requests and confirmations that use RNSC content.
4. Establish the Participant Connections between the Manager and the Participant to support the scenario you want to simulate.
5. Set the attributes of the connection to optionally specify signing and encryption using the security artifacts that you have placed on your system.

If you have sample 3A4 Request XML and 3A4 RNSC XML files in your file system, you can use the Community Participant Simulator to exercise all of the internal routing function. Click on the Community Participant Simulator tab and then click the Browse button. Select a file from the file system containing the content that you want to route, and then click the Route button.

The document will be read from the file system and uploaded to the hub. It is passed to the Document Manager for routing, and the routing that you have configured in the hub will be used.

Uploading and viewing your requests and responses

You must test your system's ability to send requests and responses. The Upload Document screen is used to upload both types of documents.

When you send a request, use the feature's second screen, View Document Flows, to examine the document to verify that it was processed correctly (it is an open document pending response). Examine your internal application to verify that the document was received and processed correctly. Use a text editor to edit the "to" and destination sections of the request to create a response. Then upload the response.

When you send a response, you can also use the View Document Flows screen to examine the document. It is not necessary to edit a response.

The View Document Flows does not show documents that are pending acknowledgment.

The CPS view changes after the upload is finished to give you an opportunity to view the routing trail left in the hub. See Figure 5.

Figure 5. Routing results screen

These two links are for your convenience. They take you to the two viewers that you will check see the routing results. You should wait a few seconds to allow the Document Manager time to handle the message before attempting to view the results.

Initiate and view document flow

1. Click **Community Participant Simulator** > **Initiate Document Flow**. The system displays the Upload Document screen.
2. Click **Browse** to locate the RosettaNet Service Content document that you want to upload. The document must be signed with a digital signature.
3. Click **Route** to start the test process. The document is routed through the system to the appropriate destination based on routing information in the document.
   - If the document is successfully routed, the system displays a message with links to the RosettaNet and Document Viewers. Use these links to track the routing progress of the document.
   - If an error occurs during document routing, the system displays an error message that includes a list of system generated events. Use this information to correct errors in the document, then resubmit the document through the CPS.
4. If you are simulating a one-way scenario, the test is complete.

Searching for an open document

1. Click **Community Participant Simulator** > **View Document Flows**.
2. Click  to view an open document flow. The system displays the Open CPS Document Flow screen.
3. Click  to view the raw document.

Responding to an open document

1. Use a text editor to edit the to and destination sections of the process requiring a response document (change VTP_OWNER to VTP_TP, or change VTP_TP to VTP_OWNER), and make the appropriate changes to the target's URL.

Table 33. Test scenarios

Scenario	Destination for Connection	URL
Two way outbound from Community Manager to Participant (Upload Request).	VTP_TP	VTP_TP
Simulating Community Manager. One way inbound from Participant to Community Manager.	VTP_OWNER	VTP_OWNER
Simulating Participant. Two way outbound from Community Manager to Participant (Upload Response).	VTP_OWNER	VTP_OWNER
Simulating Participant. Two way inbound from Participant to Community Manager (Upload Response).	VTP_TP	VTP_TP
Simulating Community Manager.		

2. Click **Community Participant Simulator** > **View Document Flows**.
3. Click **Respond** adjacent to the document requiring a response document.
4. Click **Browse** and select the edited document.
5. Click **Route**. The document is routed through the system to the appropriate destination based on routing information in the document.
6. Click **View Document Flows** to view the document.

Removing an open document

1. Click **Community Participant Simulator** > **View Document Flows**.
2. Click **Remove** next to the displayed document. The document is deleted from the system.

Chapter 8. Archiving

This chapter contains data archive management information for WebSphere Business Integration Connect users. Please read this entire chapter before performing any of the tasks.

Archiving data

In Business Integration Connect, archiving is used to move the inactive (non-repudiation) content to a safe media. Archiving consists of removing old data from the LG_MSG_ARCHIVE and LG_CERT_ARCHIVE tables. It also moves the payload datafiles from the non-repudiation store on the file system to the archive. The archived files can be restored if the non-repudiation data is needed.

Caution: Purging certain database tables will remove information about files stored in the system. Before purging database tables, review "Removing old files" on page 67.

1. Run the export script to copy the data from the tables to the archive:

   Oracle:

   For Oracle, the catexp.sql or catalog.sql script needs to be run to allow the database to be exported. Refer to the Oracle documentation for details. The catexp.sql or catalog.sql script only needs to be run once on a database. You do not need to run it again before you perform the export.

   Note: The actual names of the script files depend on your operating system. The script filenames and the method for running them are described in your Oracle operating system-specific documentation.

   Before you begin using Export, confirm the following:

   - Run the catexp.sql or catalog.sql script
   - Ensure there is sufficient disk or tape storage to write the export file
   - Verify that you have the required access privileges

   The export script needs to be run from a system which has the Oracle client installed. Also, the ORACLE HOME, ORACLE SID, and ORACLE PATH environment variables must be defined. The script is located in:

   ```
   UNIX: /opt/IBM/WBIConnect/DBLoader/scripts/Oracle/export.sh
   Windows: \WBIConnect_Install_Dir\DBLoader\scripts\Oracle\export.bat
   ```

   The export script takes the following parameters for Oracle:

   - system password
   - connect string
   - destination directory

- schema name
- cut off date YYYYMMDD

Syntax: `./export <system password> <connect string> <destination directory> <schema name> <cut off date YYYYMMDD>`

Example: `./export password connectstring /tmp bcgapps 20030101`

The archive, named `export.dmp`, and the `export.log` file will be added to the `/tmp/20030101` folder.

DB2:

The `export` script needs to be run from the db2 command window after establishing a connection with the database. The script is located in:

`UNIX: /opt/IBM/WBIConnect/DBLoader/scripts/DB2/export.sh`

`Windows: \WBIConnect_Install_Dir\DBLoader\scripts\DB2\export.bat`

The `export` script takes the following parameters for DB2:

- cutoff date YYYY-MM-DD
- archive location
- database name
- database user name
- database password

Syntax: `./export <cutoff date YYYY-MM-DD> <archive location> <database name> <database user name> <database password>`

Example: `./export 2003-01-01 /tmp bcgapps bcgapps db2inst1 pa55word`

Note: `export` gives a SQL3100W warning which can be safely ignored.

The archive and the `msgarchive.txt` log file will be added to the `/tmp/2003-01-01` folder.

2. Run the `archive` script to copy the payload datafiles from the non-repudiation store on filesystem to the archive. This script needs to be run on the machines which have the non-repudiation file storage system. The script can be found in:

   `UNIX: /opt/IBM/WBIConnect/bin`

   `Windows: \WBIConnect_Install_Dir\bin`

   a. Execute the `setenv` script to ensure that the PATH and CLASSPATH variables are set properly.

   b. The `DBArchiveParams.properties` file is used by the `archive` script to get all of the required information. Edit the `DBArchiveParams.properties` file to ensure that the correct parameters are being passed. Refer to the sample entries for more details. Make sure that the entries correspond to the correct database type. The cut-off date should be the same as in Step 1.e. The DB_ARCHIVE_TASK parameter should be kept as 1.

   c. Run the `archive` script. The results of the copying will be kept in the destination directory, as specified in the file `DBOutput.txt`.

   IMPORTANT: STEPS 1 AND 2 ABOVE COPY THE DATA FROM DATASTORES TO THE ARCHIVE LOCATION. ONLY EXECUTE THE NEXT TWO STEPS AS THEY REMOVE DATA FROM DATASTORES ONCE THESE STEPS HAVE BEEN COMPLETED SUCCESSFULLY.

3. Set the DB_ARCHIVE_TASK parameter in the `DBArchiveParams.properties` to 0.
4. Run the `archive` script again to purge the payload datafiles from the non-repudiation store on the filesystem.

This script needs to be run on the machines which have the non-repudiation file storage system. Also, this script must be run with administrator/root privileges.

5. Run the AR_NONREP_MAINTENANCE stored procedure to purge the archived data from the LG_MSG_ARCHIVE and LG_CERT_ARCHIVE tables. It takes the cut-off date as the input parameter. This stored procedure is available in the database and is added during installation.

   ```
   Oracle: execute AR_NONREP_MAINTENANCE(YYYY-MM-DD)
   DB2: call AR_NONREP_MAINTENANCE(YYYY-MM-DD)
   ```

Archiving and purging filesystem and database logs

To maintain the operating efficiency of WebSphere Business Integration Connect, the following procedures can be used to archive or purge the file system and database log files.

Purging application log files

Application log files are located in three areas: $INSTALLATION_DIRECTORY/<*receiver, console, and router*>/was/logs/server1.

1. Stop the appropriate application first by running the stop script located under $INSTALLATION_DIRECTORY/<receiver, console and router>/was/bin/stopServer.sh server1.
2. Remove the log files as needed.

Purging non-repudiation directories

Non-repudiation files and directories are located in: $COMMON_DIRECTORY/non_rep/. Start with archiving the oldest files located in directories starting at 0, and increasing in number for newer files.

1. Stop the router service using the script: $INSTALLATION_DIRECTORY/router/was/bin/stopServer.sh server1.
2. Compress the files using the UNIX tar command or WinZip.
3. Move the files to an external media source for offsite storage as needed.

Purging database tables

Certain database tables may be purged when necessary, but other tables must not be modified in order to maintain proper system functionality. Tables starting with BP_ and LG_ may be purged with two exceptions: BP_ tables ending with _QUE and _HIST are continuously maintained by the RosettaNet engine and must not be changed. The BP_ tables ending with _QUE are queue tables, and the BP_ tables ending with _HIST are history tables which are used for archiving. For example, the BP_RNSTATEHDR_QUE table is archived in the BP_RNSTATEHDR_HIST table.

Tables starting with CG_ and PR_ contain configuration or profile data and must also remain unchanged in order to maintain proper system functionality.

Archive and purge functionality for RosettaNet and AS1/AS2 state engines

The criterion for purging table data is based upon the number of days that data must be kept online. Data in tables that end with _HIST are archived and purged on a daily basis. Also, any log information is truncated daily.

The purge criterion contains only one input parameter, p_days, which is the number of days that data should be kept online. Once the DBA sets the input parameter, the procedure works as follows:

Table	History table	Action
RosettaNet		
BP_rnStateHdr	BP_rnStateHdr_Hist	Purge
BP_rnStateDtl	BP_rnStateDtl_Hist	Purge
BP_Sponsor_State	BP_Sponsor_State_Hist	Purge
BP_rnStateHdrAuditLog	none	Truncate
AS1/AS2		
BP_State_Hdr	BP_State_Hdr_Hist	Purge
BP_AS_State_Hdr	BP_AS_State_Hdr_Hist	Purge
BP_AS_State_Dtl	BP_AS_State_Dtl_Hist	Purge

Data retention time

The procedure purges data based upon the combination of the record creation date in the header and the *p_days* input parameter. The Time to perform TPA stored in the header is not considered. It is the responsibility of the DBA to make sure that p_days is larger than the maximum value of (*Time to perform/1440*). Time to perform is stored in minutes.

It is recommended that data in the *BP_* tables be retained online for *p_days* or ((*TimeToPerform/1440*) +1 day), whichever is greater. Data in tables *BP_DupCheck* and *BP_RnMsgDigest* should be retained for seven days. Data in *BP_Process_Log* should be retained for two days.

Tables with names starting with DB are metadata tables except *DB_ProcAuditLog*. If *DB_ProcAuditLog* is on, it should be purged or truncated daily, or done based on the needs of the user. This log is normally turned off for production since it is primarily used in development and QA environments.

Log and summary tables

Tables with names starting with LG_ are log and summary tables with the exception of: LG_EventCd, LG_Media, and LG_media_Cfg. These are metadata tables and must remain unchanged in order to maintain proper system functionality. Tables starting with *LG_Access_* are not used in 4.2.1 and 4.2.2.

The following log tables can be archived and purged based upon Activity ID, and the driving table should be *LG_Activity*. The createdate or *RcvDocTS* can be used to determine the number of days that data should be retained online. *RcvDocTS* may be a better option because it is an indexed column. Data can remain online for seven days or ((*TimeToPerform*/1440) +1 day), whichever is greater.

Table	Notes
LG_ACTIVITY	
LG_ACTIVITY_DTL	
LG_ACTIVITY_ENDSTATE	
LG_ACTIVITY_RNDTL	
LG_ACTIVITY_RNHDR	

LG_AS_DTL	
LG_AS_HDR	
LG_ACTIVITY_EVENT	Links LG_Activity to LG_event
LG_EVENT	
LG_EVENT_EVENTSUMMARY	Links LG_Event to LG_EventSummary and LG_EventSummary. DRILLDOWNFLG can be used to indicate that drilldown is not available(Not implemented in 4.2.1 and 4.2.2 procedures).
LG_ACTIVITY_SUMMARY	Links LG_Activity to LG_Summary and LG_Summary. DRILLDOWNFLG can be used to indicate that drilldown is not available(Not implemented in 4.2.1 and 4.2.2 procedures).

The following log tables can be purged based on creation date.

Table	Notes
LG_Delivery_Log	Any record older than 1 day from createdate can be purged.
LG_DM_Doc_Lock	Any record older than 1 day from createdate can be purged.
LG_Msg_Archive	Any record older than 7 days from createdate can be purged.
LG_STACKTRACE	Any record older than 7 days from createdate can be purged.
LG_SYNCH_REQ_RESP	Any record older than seven days from createdate or (TimeToPerform/1440) +1 day), whichever is greater, can be purged.
LG_VALIDATION	Any record older than 7 days from createdate can be purged.
LG_VTP_STATUS	Any record older than 7 days from createdate can be purged.

The following summary tables must remain unchanged in order to maintain proper system functionality.

Table	Notes
Event Summary Tables	
LG_EVENTSUMMARY	
LG_EVENTSUMMARY_XREF	
Process Summary Tables	
LG_PROCESSSUMMARY_AS	
LG_PROCESSSUMMARY_AS_MI	
LG_PROCESSSUMMARY_AS_XREF	
LG_PROCESSSUMMARY_RN	
LG_PROCESSSUMMARY_RN_MI	

LG_PROCESSSUMMARY_XREF	
Document Summary Tables	
LG_DOCPROCESSING_SUMLG_MSGLENGTH_SUMMARY	
LG_SUMMARY	
LG_SUMMARY_MI	
LG_SUMMARY_PROCESSSUMMARY	Links LG_Sum_Xref_Lnk to LG_ProcessSummary_Xref
LG_SUMMARY_RN	
LG_SUMMARY_RN_MI	
LG_SUM_XREF_LNK	Links LG_SUM_XREF_PART and LG_SUM_XREF_PRCS to LG_Summary
LG_SUM_XREF_PART	
LG_SUM_XREF_PRCS	
Message Length Summary	
LG_MSGLENGTH_SUMMARY	

Restoring data

Use the following steps to restore data back to the database.

1. Run the `import` script to copy the data back to the database.

   Oracle:

   This script needs to be run from a machine running Oracle client. The script can be found in:

   ```
   UNIX: /WBIConnect_Install_Dir/opt/IBM/WBIConnect/DBLoader/scripts
   /Oracle/import.sh
   Windows: \WBIConnect_Install_Dir\DBLoader\scripts\Oracle\import.bat
   ```

   The `import` script takes the following parameters for Oracle:

   - Oracle user system password
   - Connect string
   - Archive location

   DB2:

   This script needs to be run from DB2 command prompt after connecting to the database. The script can be found in:

   ```
   UNIX: /WBIConnect_Install_Dir/opt/IBM/WBIConnect/DBLoader/scripts
   /DB2/import.sh
   Windows: \WBIConnect_Install_Dir\DBLoader\scripts\DB2\import.bat
   ```

   The `import` script takes the following parameters for DB2:

   - Archive location
   - Schema name
   - Database name
   - Database user name
   - Database user password

Syntax: `./import.sh <archive location> <schema name> <database name> <database user name> <database password>`

Example: `./import.sh /tmp/2003-01-01 db2inst1 bcgapps db2inst1 pa55word`

2. Run the `Restore` script to restore the payload files. The script can be found in:

   `UNIX: /WBIConnect_Install_Dir/opt/IBM/WBIConnect/bin`

   `Windows: \WBIConnect_Install_Dir\bin`

   The `Restore` script takes the following parameters:

   - The location of the archives e.g C:\tmp
   - The location of the log file DBOutput.txt from "Archiving data" on page 61, step 2. For example,

     `C:\Installers\DBOutput.txt`

   This program needs to be run on the machines which have the non-repudiation file storage system with admin/root privileges.

Removing old files

Use the `archive` script with DB_MODULE set as MSGSTORE. This will remove the old files from the message store. This script needs to be run on the machines which have the message store file storage system.

CAUTION: If the LG_MSG_ARCHIVE has already been purged, the locations of the file will be lost from the database. It is advisable to purge the message store before Archival.

Removing data from State Engine tables

Use the stored procedure AR_STATEENGINE_MAINTENANCE. It takes the number of days for which you want to retain the data. All records before that number of days are removed from the database.

Removing data from Summary tables

Use the stored procedure AR_SUMMARY_MAINTENANCE. It takes the cut-off date as the input parameter.

Removing data from Logging tables

Use the stored procedure AR_PURGE_HEADERS. It takes the cut-off date as the input parameter.

Chapter 9. Troubleshooting

This chapter provides troubleshooting information you can use to identify and resolve problems. Refer to Appendix B for a list of failed events and their corresponding descriptions.

Topics in this chapter include:

Optimizing database query performance

The RUNSTATS command updates the database query access plan for each table and index. To optimize database query performance, run RUNSTATS at least once a week when IBM WebSphere Business Integration Connect application and database activity is at a minimum. As database traffic increases, run RUNSTATS more frequently - up to once a day.

Note:

- Since RUNSTATS updates database system information, lock timeouts potentially can occur under specific circumstances. It is recommended that the WebSphere Business Integration Connect application be quiesced and database access be limited to running RUNSTATS.
- A lock timeout may occur when running RUNSTATS and db2rbind simultaneously. It is recommended that these commands be run daily at different times.

Increasing the Receiver timeout setting

If a Participant opens a connection to Business Integration Connect and receives the following error message: "Connection aborted by peer: socket write error", the Business Integration Connect Receiver is initiating a timeout due to the slow transmission rate from the Participant.

To correct this problem, the Receiver's default five second timeout can be increased to thirty seconds by running the `bcgHttp.jacl` script in the Receiver installation directory. To execute the `bcgHttp.jacl` script, run the following command:

```
$INSTALL_DIR/was/bin/wsadmin.sh -conntype NONE -f
$INSTALL_DIR/scripts/bcgHttp.jacl
```

Insufficient virtual memory for DB2 agents

The following error, located in the Business Integration Connect logs, indicates that there is insufficient virtual memory available to the database agent for sort processing. Decrease the value of the SORTHEAP parameter for the database that you created for Business Integration Connect. Contact your database administrator for specifics on how to set that parameter in your environment.

```
Error[DBChannelCheck] [main Thread 2] - Error in channel check for
com.ibm.bcg.channel.CheckChannelParameters@ebda9664
com.ibm.ejs.cm.portability.ResourceAllocationException: DB2 SQL error:
SQLCODE: -955, SQLSTATE:57011, SQLERRMC: null

ERROR [BPEEngine] [main Thread 2] - BPE:

ERROR [BPEEngine] [main Thread 2] -
java.lang.ArrayIndexOutOfBoundsException: 0

ERROR [BPEEngine] [main Thread 2] - Error closing
transConn.com.ibm.ejs.cm.exception. WorkRolledbackException: Outstanding
work on this connection which was not comitted or rolledback by the user
has been rolledback.
```

Avoiding out-of-memory errors

To improve routing performance and avoid out-of-memory errors, use the following scripts to change the initial and maximum heap size:

Query current heap size:

- `/WBIConnect_Install_Dir/console/was/bin/wsadmin.sh -conntype NONE -f $LOCATION_OF_SCRIPTS$/queryJVMAttrs.jacl`

Set min/max heap size:

- `/WBIConnect_Install_Dir/console/was/bin/wsadmin.sh -conntype NONE -f $LOCATION_OF_SCRIPTS$/setJVMAttrs.jacl`

Change the heap size to the recommended values by editing setJVMAttrs.jacl.

Default:

- Xms=50
- Xmx=256

First recommendation:

- Xms=256
- Xmx=512

Second recommendation:

- Xms=256
- Xmx=1024

Avoiding long processing time on large encrypted AS documents

Large encrypted AS documents may take a long time to process on some lower end hardware configurations. To avoid delays:

1. Select compression on the AS protocol configuration to decrease the size of the document sent.
2. Follow the steps in the Avoiding out-of-memory errors section above to increase memory size and speed up processing of encrypted documents.

Reprocessing events and business documents that fail to log to the database

If an event or doc in the DATALOGQ JMS queue fails three attempts to log to the database, it is inserted into the DATALOGERRORQ JMS queue to allow for later reprocessing when the problem has been resolved.

To reprocess these failed events and documents, use the manual utility reprocessDbLoggingErrors.sh. This utility dequeues all the events and docs from DATALOGERRORQ and re-queues them into DATALOGQ, so the normal DocumentLogReceiver will log them to the database again.

The utility stops after it processes all the existing events and documents in DATALOGERRORQ. Any events and document that fails to log ends up in DATALOGERRORQ again; however, this time, the utility ensures that the event or document is reprocessed only once (that is, the utility does not enter an endless loop with failing events and documents).

To run the reprocessDbLoggingErrors.sh utility:

1. Verify that the env variables are correctly defined in reprocessDbLoggingErrors.sh on any router machine:

   ```
   REPROCESSOR_HOME=Document Manager installation root
   JAVA_HOME=$REPROCESSOR_HOME/java
   LOG_REPROCESSOR_CLASSES=$REPROCESSOR_HOME/classes
   ```

2. Run the utility from the command line:

   ```
   ./reprocessDbLoggingErrors.sh
   ```

0A1 generated with data validation errors

0A1 mandates that GlobalSupplyChainCode be present in the xml.If the incoming 3A7 does not contain this value, it must be added as an attribute to 0A1. GlobalSupplyChainCode must be either in the 3A7 document or added as attribute to 0A1 in Document Flow Definition.

To add the attribute:

1. Click **Hub Admin** > **Hub Configuration** > **Document Flow Definition**. The Console displays the Manage Document Flow Definitions screen.
2. Click **Package: RNIF** > **Protocol: Rosettanet** > **DocumentFlow: 0A1**, and select the Actions (blue arrow).
3. If the Global Supply Chain Code attribute is not there, click **Add Attributes** to add it.
4. Select a value from the drop down list.
5. Click **Save**.

Poor performance and system events are not working

If the system is performing very slowly and system events are not working, there may be a problem with the WebSphere MQ publish/subscribe broker.

1. Open the file /var/mqm/qmgrs/<*queue manager name*>/qm.ini and look for the following:

   ```
   MaxActiveChannels=1000Broker:
   ```

   If you see this entry, replace the Channels and Broker parameters with the following:

Channels:

```
MaxChannels=1000
MaxActiveChannels=1000
SyncPointIfPersistent=yes
```

2. Save your changes
3. Shut down Business Integration Connect (see "Shutting down" below).
4. Stop WebSphere MQ by:
   a. Stopping the publish/subscribe broker:
      `endmqbrk -m <hostname>.queue.manager`
   b. Stopping the listener:
      `endmqlsr -m <hostname>.queue.manager`
   c. Stopping the queue manager:
      `endmqm <hostname>.queue.manager`
5. Create and start WebSphere MQ, using the instructions in the WebSphere Business Integration Connect Installation Guide. However, do not perform steps 2 through 4 in the procedure.
6. Restart Business Integration Connect, using the instructions in the WebSphere Business Integration Connect Installation Guide.

Shutting down

When shutting down the system, shut down the receiver before shutting down the router. This safeguard prevents documents from entering the system while the router is shutting down. A shutdown can take up to 15 minutes if there is a large number of documents being processed.

Starting the system after a machine shutdown

The following sections describe how to start the system components if the machine where they reside has been out of service. You must first start DB2 and WebSphere MQ before you can start the Business Integration Connect components.

Starting DB2

To start DB2, use the following procedure.

1. Change to the database owner (db2inst1 if the default was used):
   `su - db2inst1`
2. Start the database instance:
   `db2start`

Starting WebSphere MQ

To start WebSphere MQ, use the following procedure.

1. Change to the WebSphere MQ user:
   `su - mqm`
2. Start the queue manager:
   `strmqm <hostname>.queue.manager`
3. Start the listener:
   `runmqlsr -t tcp -p <port number> -m <hostname>.queue.manager &`
4. Wait about 10 seconds and press Enter to return to the command prompt.

5. Start the JMS Broker (the publish-subscribe broker):
   `strmqbrk -m <hostname>.queue.manager`

Starting Community Console, Receiver, and Document Manager

To start Community Console, Receiver, and Document Manager, use the following procedure.

1. Change to the general Business Integration Connect user:
   `su - bcguser`
2. Navigate to the Community Console script directory:
   `cd <installation location>/console/was/bin`
   where *<installation location>* is where Business Integration Connect is installed.
3. Start Community Console:
   `./startServer.sh server1`
4. Navigate to the Receiver script directory:
   `cd <installation location>/receiver/was/bin`
5. Start the Receiver:
   `./startServer.sh server1`
6. Navigate to the Document Manager script directory:
   `cd <installation location>/router/was/bin`
7. Start the Document Manager:
   `./startServer.sh server1`

Restarting the router after a crash

If the router should crash, use the following procedure to restart it. This procedure ensures that all documents that have been received will be processed.

1. Check the `router_in` directory for any files that have the extension `vmd_locked`.
2. If there are files that have the extension `vmd_locked` that are more than two minutes old, rename them to the extension `vmd_restart`.

   Note: If there are multiple instances of the router running, there will be files with the `vmd_locked` extension that are being actively processed by the other instances of the router. Do not rename those files.
3. Depending on the state of processing a document, it is possible that a document will fail with an event 210031 "Unable to nonrep document." If this occurs, the files for the document will reside in the directory `router_in/reject`. If this happens, rename the file with the extension vmd with the extension `vmd_restart`. Then move the files for the document to the directory `router_in dir` for processing.

Appendix A. Performance considerations

This appendix contains information to assist you in achieving the best performance for your specific environment.

Events filtering

The `bcg.event_log_exclude` property allows the user to exclude the recording of selected events within the event log (DataLogQ). By default, normal and successful processing of documents will produce several events which are recorded in the event log. It may be useful to decrease the number of events that are recorded for successful document processing. Reducing this number may increase the performance or transaction capacity of the system. Some messages may not be excluded with this parameter. The format of the `bcg.event_log_exclude` property is a comma delimited list of message numbers to exclude. For example:

```
bcg.event_log_exclude=210060,210062,230011,250004
```

Messages that may be useful to exclude:

```
210060 Passed destination parse.
210062 Destination process successful.
210100 Timing start event
210101 Timing end event
230011 Sequence validation successful
250004 Document delivery successful
```

Summary data generation

WebSphere Business Integration Connect periodically summarizes data about system activity. This summary-service data is the information you see when you use the Document Analysis or Document Volume Report functions.

The Summary Service Properties screen allows you to view and edit how often the summary data is generated. This screen also displays the date and time that the summary data was last updated.

To change the time interval:

1. Click **System Administration** > **Event Processing** > **Summary Service**. The Console displays the Summary Service Properties screen.
2. Click the  icon next to Processing Interval (in Minutes).
3. Enter a value (from 1 through 60) indicating the number of seconds that should occur before data is summarized again. The default value is 15.
4. Click Save.

Appendix B. Failed Events

When a document fails processing, the WebSphere Business Integration Connect system generates an event. Table 34 provides a list of failed events and their corresponding descriptions.

Note: The HTTP Receiver component will return an HTTP error code if it is unable to persist the document, but the document content will not be persisted. For all other Receiver component types, the document content will be persisted at its current location at the time of failure.

Table 34. Failed Events

Event	Event Name	Internal Description	Severity	Extended Description
BCG103201	Hub Owner State Engine Error	Error Reason:{0}	Error	This event is generated when a fatal system occurs causing a document to fail processing. An example can be a database write error.
BCG103203	Receiver Processing Error	Receiver '{0},{1}' failed to processing document, error: {2}.	Error	This event is generated when the receiver is unable to process a document due to document or system errors.
BCG200001	Get Protocol Transformer Business Process Failed	Factory failed to get an instance of the protocol transformer business process because {0}	Critical	This event is generated due to system failure when attempting to locate an instance of the protocol transformer business process.
BCG200005	Document Transformation Failure	Document failed transformation due to {0}	Error	This event is generated due to a failure during document transformation.
BCG200006	Protocol Transformer Input File Failure	Protocol transformer input file error: {0}	Critical	This event is generated due to a failure with the input file during action processing. For example, the file is corrupted.
BCG200007	Protocol Transformer Output File Failure	Protocol transformer output file error: {0}	Critical	This event is generated due to a failure when attempting to write to the output file directory.
BCG200009	Failed to Parse Document	Failed to parse: {0}	Error	This event is generated due to failure when attempting to parse the document.
BCG200013	Community Manager Provided RN Process-Instance-ID Error	{0}	Error	This event is generated when an invalid Process Instance ID is received and the configuration property indicates that the system will not generate a new Process Instance ID.
BCG200015	Community Manager Provided RosettaNet GlobalUsageCode Error	{0}	Error	This event is generated when the x-aux-production header value is invalid and the configuration property indicates that the system will not use the default value on error.

Table 34. Failed Events (continued)

Event	Event Name	Internal Description	Severity	Extended Description
BCG210000	Check Channel Error	Check Channel Error	Error	This event is generated when there is a check channel related error.
BCG210001	Check Channel Error	Check Channel Error	Error	This event is generated when data required to lookup a connection is available but the matching connection is not found.
BCG210002	Connection Lookup Failed	Connection lookup failed {0}	Error	This event is generated when data required to lookup a connection is not available.
BCG210007	Outbound Document Cannot be Packaged	Error in Outbound Processor	Critical	This event is generated when a packager is not available for an outbound document.
BCG210008	IP Address Validation Failure	From IP address is not in the participant profile {0}	Error	This event is generated when a document is posted from an unapproved IP Address for that participant.
BCG210009	SSL Certificate Validation Failure	Client SSL certificate name is not in the participant profile {0}	Error	This event is generated when the SSL Certificate used to post the document is not in the approved certificate list for that participant.
BCG210010	Document Too Large	Document too large: {0} bytes	Error	This event is generated when the document received is too large to be processed.
BCG210011	Community Manager Transport Unpackage Failure	Insufficient Community Manager transport information provided: {0}	Error	This event is generated when insufficient transport information is provided.
BCG210012	B2B Capability Not Found	B2B capability not found {0}	Error	This event is generated when the B2B capability required to route the document is not enabled.
BCG210013	Connection Not Fully Configured	Connection not fully configured {0}	Error	This event is generated when the connection for the document is not fully configured. Most likely the destination for the document does not have a configured gateway.
BCG210014	MIME Multipart Unpackaging Failure	Failed to unpackage a MIME multipart document: {0}	Error	This event is generated when the system failed to unpackage a MIME multipart document.
BCG210017	EDI Connection Parse Failure	Failed to parse EDI routing information: {0}	Error	This event is generated when the system failed to parse EDI routing information.
BCG210019	Synchronous Operation not Supported on this Connection	Synchronous Operation not Supported on this Connection	Error	This event is generated when the document requests synchronous operation but the connection does not support synchronous operations.

Table 34. Failed Events (continued)

Event	Event Name	Internal Description	Severity	Extended Description
BCG210031	Unable to Non-Rep document	Unable to Non-Rep document {0}	Critical	This event is generated when the system is unable to non-repudiate the document. Insure that the system has sufficient disk space, and that the following directories contain system-only files: • /<*common information directory*>/non_rep/ • /<*common information directory*>/msg_store/ If these two directories contain user generated files, document processing will fail.
BCG210032	System Error in the Inbound Processor	System error in the Inbound Processor for document: {0}	Critical	This event is generated when the system encounters an error in the inbound processor.
BCG210033	Message Store Failed	Unable to store document plain text	Error	This event is generated when the system is unable to store the document in plain text. Insure that the system has sufficient disk space, and that the following directories contain system-only files: • /<*common information directory*>/non_rep/ • /<*common information directory*>/msg_store/ If these two directories contain user generated files, document processing will fail.
BCG210034	System Error in the document manager	System error in the document manager for document: {0}	Critical	This event is generated when the system encounters an error in the document manager.
BCG210051	Duplicate Processing Failure	System error - failure in duplicate process	Critical	This event is generated when the system is unable to contact the database server during duplicate processing.
BCG210052	Duplicate Document Received	This document appears to be a duplication of a document sent on {2}	Error	This event is generated when a document received is a duplicate and rejected.
BCG210061	Destination Parse Failure	Error in destination Parse	Critical	This event is generated when destination parse fails. Usually due to a database problem.
BCG210063	Destination Process Failure	Destination Process failed	Critical	This event is generated when destination processing fails. Usually due to a database problem.

Table 34. Failed Events (continued)

Event	Event Name	Internal Description	Severity	Extended Description
BCG210065	Destination Determination Failure	{0}	Error	This event is generated when there are conflicting inputs when processing the destination.
BCG210066	Package and Content Business Id's map to different partners	From Partner ID = {0}, To Partner ID = {1}, From Package Partner ID = {2}, To Package Partner ID = {3}	Error	This event is generated when there is a mismatch between the content and package routing information
BCG210201	PIP Load During Doctype Processing Failure	Unable to load PIP for a document during Doctype processing	Critical	This event is generated when a spec for the PIP cannot be found. Should not occur unless there is a configuration problem.
BCG210202	Exception in Doctype Processing	Exception during Doctype Processing: {0}	Critical	This event is generated when the system fails when attempting to insert the DocType tag.
BCG210203	DoctypeProcess Error - No Action Found	DoctypeProcess Error - No action found	Critical	This event is generated when a spec for the PIP DocType cannot be found.
BCG230004	Validation Internal Error	{0}	Critical	This event is generated due to internal system failure during validation processing.
BCG230006	Validation Database Error	{0}	Critical	This event is generated due to a database error during validation processing.
BCG230007	Validation Business Process Factory Error	{0}	Critical	This event is generated when the system is unable to determine the process to send to the validation engine.
BCG230009	RosettaNet Validation Error	{0}	Error	This event is generated when a document fails to complete RosettaNet process validation.
BCG230010	Data Validation Error	Document failed data validation: {0}	Error	This event is generated when a document fails data validation and is rejected.
BCG230012	AS Sequence Validation Error	{0}	Error	This event is generated when a document fails to complete EDIINT process validation.
BCG240003	RosettaNet Unpackaging Error	RosettaNet Unpackaging Error	Error	This event is generated when the system is unable to parse the RosettaNet preamble during unpackaging.
BCG240005	RNPackager Delivery Header Parser Failure	Delivery Header Parser Error: {0}	Error	This event is generated when the system is unable to parse the RosettaNet delivery header during unpackaging.
BCG240007	RNPackager Service Header Failure	Service Header parser error: {0}	Error	This event is generated when the system is unable to parse the RosettaNet service header during unpackaging.

Table 34. Failed Events (continued)

Event	Event Name	Internal Description	Severity	Extended Description
BCG240009	RNPackager Mime Parsing Failure	Mime parsing error: {0}	Error	This event is generated when an error occurs in Mime parsing of the RosettaNet message during unpackaging.
BCG240011	RNPackager Signature Failed	Digital Signature validation failed: {0}	Error	This event is generated when digital signature validation fails during unpackaging.
BCG240012	RN Unpackaging State Update Error	Database access failure: Could not update the RosettaNet state	Critical	This event is generated when the unpackager encounters database communication errors when updating the RosettaNet state.
BCG240013	Participant Certificate Did Not Match Signer	Name/serial on signer certificate did not match database entry	Error	This event is generated when Certificate to DUNS check fails for digital signature.
BCG240014	Missing Signature in Document	Signature not found in document	Error	This event is generated when a signature is required by the TPA, but not found in the document.
BCG240015	RosettaNet Document Creation Failure	{0}	Critical	This event is generated when an attempt to construct a RosettaNet document fails.
BCG240016	RosettaNet Non-Repudiation Error	{0}	Error	This event is generated when the Receipt Ack does not contain correct digest of previous message, or the digest is missing.
BCG240031	Packaging Instance Error	Error: {0}	Critical	This event is generated when the system is unable to find a packager for the supplied document type.
BCG240036	Unpackaging Instance Error	Error: {0}	Error	This event is generated when the system cannot find an unpackager for a document.
BCG240065	Connection Parse XML Failure	XML connection parsing failed: {0}	Error	This event is generated when connection info for an XML message could not be found.
BCG240068	Connection Parser RosettaNet Failure	Connection Parse RosettaNet Failure	Error	This event is generated when connection info could not be found in a RosettaNet document.
BCG240070	XML Connection Parse Failure	XML connection parse failed	Error	This event is generated when the system is unable to find connection information for an XML file.
BCG240071	Flat File Connection Parse Failure	Flat File connection parse failed: {0}	Error	This event is generated when the system is unable to find connection information for a Flat File.
BCG240078	Web Service Connection Parse Failed	Web Service connection parse failed	Error	This event is generated when the system is unable to find connection information for a SOAP message.
BCG240409	AS Unpackager Failure	AS Unpackager Error: {0}	Error	This event is generated when the AS unpackager fails.

Table 34. Failed Events (continued)

Event	Event Name	Internal Description	Severity	Extended Description
BCG240411	AS Signature Failure	AS Signature Validation Error: {0}	Error	This event is generated when AS signature validation fails.
BCG240412	AS State Engine DB Failure	AS State Engine DB error: {0}	Critical	This event is generated when the AS state engine database fails.
BCG240415	AS Packager Failure	AS Packager Error: {0}	Critical	This event is generated when the AS packager fails.
BCG240416	AS Non-Repudiation Error	{0}	Error	This event is generated when AS Non-Repudiation fails.
BCG240417	Decryption Failed	{0}	Error	This event is generated when decryption fails.
BCG240418	Unable to Generate Message Digest	{0}	Error	This event is generated when the system is unable to generate a message digest.
BCG240419	Unsupported Signature Format	{0}	Error	This event is generated when the system receives an unsupported signature format.
BCG240420	Unsupported Signature Algorithm	{0}	Error	This event is generated when the system receives unsupported signature algorithm.
BCG240421	Unexpected Error	{0}	Critical	This event is generated when the system encounters an unexpected error.
BCG240422	AS document not found for this MDN	{0}	Error	This event is generated when a MDN is received and the system is unable to locate the corresponding document.
BCG240423	Input File Failure	Invalid input file passed in the document	Error	This event is generated when the system encounters an invalid input file.
BCG240424	Insufficient Message Security	{0}	Error	This event is generated when the system encounters insufficient message security.
BCG240500	RosettaNet State Engine Error	RosettaNet State Engine Error	Critical	This event is generated when the RosettaNet State Engine encounters a system error.
BCG240600	AS State Engine Error	AS State Engine Error: {0}	Critical	This event is generated when the RosettaNet State Engine encounters a system error.
BCG240601	AS Retry Failure	AS Attribute max retry limit reached	Error	This event is generated when the system fails AS retries. The maximum retry limit may have been reached.
BCG250001	Document Delivery Failed	Document delivery to participant gateway failed: {0}	Error	This event is generated when document delivery to a participant's gateway fails and the document is set to a failed state.

Table 34. Failed Events (continued)

Event	Event Name	Internal Description	Severity	Extended Description
BCG250002	Delivery Scheduler Failed	An internal error occurred in the Delivery Scheduler: {0}	Critical	This event is generated when an uncategorized internal error occurred within the Delivery Manager, due to bad gateway or document data, rather than failure to deliver.
BCG250005	FTP Delivery Failed	FTP delivery to participant gateway failed with exception: {0}	Error	This event is generated when the FTP protocol document delivery failed but more retries may be possible. Final failure will generate event 250001.
BCG260002	RosettaNet Pass Through Logging Failed	RosettaNet pass through process view logging failed: {0}	Error	This event is generated when a document fails RN pass through logging.
BCG800000	Get Community Manager Business Process Failed	Failed to get an instance of the Community Manager business process because {0}	Critical	This event is generated when the system fails to locate the Community Manager action for business processing.
BCG800001	Community Manager Business Process Entrance	Community Manager business process {0} entrance	Debug	
BCG800002	Community Manager Business Process Exit	Community Manager business process {0} exit	Debug	
BCG800003	Community Manager Business Process Successful	Community Manager business process successful	Info	
BCG800004	Community Manager Business Process Encounters Database Error	{0}	Critical	This event is generated due to database error while processing the Community Manager's action.
BCG800005	Community Manager Process Encounters Internal Error	{0}	Critical	This event is generated due to internal system error while processing the Community Manager's action.
BCG800006	Community Manger Business Process Warning	{0}	Warning	
BCG800007	Discard MSA File	Discard MSA file	Debug	
BCG900001	0A1 Service Content Received	0A1 service content received	Info	

Appendix C. BCG.Properties

The following tables contain all of the configurable parameters in the BCG.Properties file that controls the console, receiver, and router.

Table 35. Console-specific properties

Entry	Default value	Possible setting	Description
## DR Mode indicator property			
`console.environment`		Blank or DR	Text string that appears in the console indicating wether or not this is a DR environment
## Version indicator			
`console.version`	4.2.1	Version #	Text string used for informational purposes
## DB Proc Audit Debug level ## 0 = off, 1 = on			
`ibm.bcg.db.debugLevel`	0	0,1	Turns database debugging on and off
########## Start log4j Debug Properties ################## # Viacore Log4J Debug Properties # Possible Categories - debug/info/warn/error/fatal # Default Category "error", Output to: stdout and RollingFile			
`log4j.rootCategory`	error, stdout, RollingFile	debug, info, warn, error, fatal	Root logging setting for all containers
`log4j.appender.stdout`	org.apache.log4j.FileAppender		Logging java class using for Log4J libraries
`log4j.appender.stdout.File`	System.out		
`log4j.appender.stdout.layout`	org.apache.log4j.PatternLayout		Logging java class using for Log4J libraries
`log4j.appender.stdout.layout.ConversionPattern`	%d{ABSOLUTE} %c{1} [%t] - %m%n		Logging pattern for log file
`log4j.appender.RollingFile`	org.apache.log4j.RollingFile Appender		Logging java class using for Log4J libraries
`log4j.appender.RollingFile.File`	$CONSOLE_INSTALL_DIR$ /logs/server1 /wbic_console.log		Rolling log file name and path
`log4j.appender.RollingFile.MaxFileSize`	1000KB		Maximum size of log file before being rolled.
`log4j.appender.RollingFile.MaxBackupIndex`	5		Maximum number of rolled log files.

Table 35. Console-specific properties (continued)

Entry	Default value	Possible setting	Description
log4j.appender.RollingFile.layout	org.apache.log4j.PatternLayout		Logging java class using for Log4J libraries
log4j.appender.RollingFile.layout.ConversionPattern	%d{DATE} %c{2} [%t] - %m%n		Logging pattern for log file
ibm.bcg.appserver.loggerClass	com.viacore.shared.logging.Log4jLogger		Specifies the appropriate Logging class to use
## Console global appserver properties			
ibm.bcg.appserver.ejbEnabled	TRUE	true, false	Whether the management services use use EJBs or direct services
ibm.bcg.appserver.mgmt.pool.maxsize	20		The size of the EJB Pool
ibm.bcg.appserver.mgmt.ctx.instancepolicy	singleton		JNDI Init Context Policy
java.naming.security.principal	admin		JNDI Security Principal param.
## Websphere JNDI Settings			
ibm.bcg.appserver.jndiInitialContextFactory	com.ibm.websphere.naming.WsnInitialContextFactory		JNDI Context Factory
ibm.bcg.appserver.jndiContextProviderURL	corbaloc:iiop:localhost:52809		JNDI Provider URL
ibm.bcg.appserver.jdbcJndiPool	$CONSOLE.JNDI$	datasources/DB2DS,datasources/OraclePool	Datasource JNDI Prefix
# Database JDBC Schema			
ibm.bcg.db.product	$CONSOLE.DB.TYPE$	db2,oracle	Database type
bcg.co.db.schema	$CONSOLE.DB.SID$		schema information (DB2 - Database Owner, Oracle - Schema Owner)
## JMS Poster Instance ## Possible values are: ## com.ibm.bcg.shared.event.MQSeriesPoster			
ibm.bcg.jmsPosterInstance	com.ibm.bcg.shared.event.MQSeriesPoster		
## JMS Properties for Event Posting ## JNDI Provider URL			
ibm.bcg.jms_cntxt_url	file:$CONSOLE_INSTALL_DIR$/jndi		Location of .binding file, used for JMS information

Table 35. Console-specific properties (continued)

Entry	Default value	Possible setting	Description
ibm.bcg.jms_jndi_factory	com.sun.jndi.fscontext.RefFSContext Factory		
## Connection Factory Names			
ibm.bcg.jms.qconnFactory.name	WBIC/QCF		JMS Queue Connection Factory Name
ibm.bcg.jms.topicconnFactory.name	WBIC/TCF		JMS Topic Connection Factory Name
ibm.bcg.jms.queue.name	WBIC/datalogQ		JMS Queue Name
## Gateway Queue			
ibm.bcg.outbound.gatewayDirectory	$SHARED_DATA_DIR$/gateways		Gateway Directory
## VTP			
ibm.bcg.certs.vtp.CertificateDir	$SHARED_DATA_DIR$/security/certs		Location of Client Certificates for use w/ VTP
ibm.bcg.certs.vtp.Certificate			VTP Public Key (DER, binary format)
ibm.bcg.certs.vtp.PrivateKey			VTP Private Key (pkcs8, binary format)
ibm.bcg.certs.vtp.Passwd			VTP Private Key Password
ibm.bcg.certs.vtp.VerifySig	FALSE	true, false	Determine whether the VTP should verify signer or not (true, false)
ibm.bcg.vtp.RouterIn	$SHARED_DATA_DIR$/router_in		Router In directory
## EAI Directory Management			
ibm.bcg.EAIDocDir	Documents		This provides the console with the name of the EAI directory used by the router
## Special characters - used for validation of partnerLogin and Receiver and Destination Types (gateway types) ## Note: 2 keys are defined as one allows the / \ chars and the other does not ## For i18n purposes these values could change depending on the language of the OS and what is allowed for directory names.			
ibm.bcg.specialChars	!#:;\\& /?.,		
ibm.bcg.specialCharsDir	!#:;& ?.,		

Table 36. Receiver-specific properties

Entry	Default value	Possible settings	Description
###### Set this so bcg.prperties logging settings are ignored!!			
bcg.use_container_logging	TRUE	true, false	
############ BCG DB ##			
bcg.co.db.DBType	$RECEIVER. DB.TYPE$	db2,oracle	Database type
bcg.co.db.DBPoolName	$RECEIVER. JNDI$	datasources/DB2DS, datasources/Oracle Pool	Datasource JNDI Prefix
bcg.co.jndiContextURL	corbaloc:iiop: localhost:57809		JNDI Provider URL
bcg.co.jndiFactory	com.ibm. websphere. naming. WsnInitial ContextFactory		JNDI Context Factory
bcg.co.db.schema	$RECEIVER. DB.SID$		schema information (DB2 - Database Owner, Oracle - Schema Owner)
############ MQ PROPS			
bcg.use_oaq	FALSE	true, false	
bcg.jms.queue.factory	WBIC/QCF		JMS Queue Connection Factory Name
bcg.jms.topic.factory	WBIC/TCF		JMS Topic Connection Factory Name
bcg.jms.jndi_factory	com.sun.jndi. fscontext.RefFS ContextFactory		Class used to connect to the JNDI server
bcg.jms.context_url	file:$RECEIVER _INSTALL_DIR$ /jndi		Location of .binding file, used for JMS information
########## BPE			
bcg.oaq_log_q	WBIC/datalogQ		JMS Queue Name
########## RECEIVER MBEAN			
bcg.vms_receiver_reject_dir	$SHARED_DATA _DIR$/receiver /reject		File system path where the Receiver puts rejected messages
bcg.vms_receiver_tmp_dir	$SHARED_DATA _DIR$/receiver /tmp		File system path where the Receiver puts temporary messages
########## END RECEIVER MBEAN			
bcg.receiver.persistpath	$SHARED_DATA _DIR$/router_in/		File system path where the Receiver persists inbound RosettaNet signals.
bcg.receiver.sync.persistpath	$SHARED_DATA _DIR$/sync_in		File system path where the Receiver persists Synchronous RosettaNet signals.

Table 36. Receiver-specific properties (continued)

Entry	Default value	Possible settings	Description
bcg.receiver.sync.sync CheckClasses	com.ibm.bcg. server.sync. SyncRosettaNet Request|com.ibm .bcg.server.sync. SyncAS2Request| com.ibm.bcg. server.sync.Sync SOAPRequest| com.ibm.bcg. server.sync.Sync cXMLRequest		
bcg.receiver.sync.responseURL	/bcgreceiver/ SyncResponse		URI to post Synchronous Responses
bcg.receiver.sync. responseURL.port	$RECEIVER _HTTP_PORT$		HTTP Port for Receiver
## Servlet properties ## HTTP headers to be persisted as meta-data by the receiver servlet. ## All properties beginning with "viacore.http.hdrdef" will be ## interpreted as headers to be persisted.			
bcg.http.hdrdef.fromID	x-aux-sender-id		HTTP header persisted in metadata file for the BPE to process
bcg.http.hdrdef.toID	x-aux-receiver-id		HTTP header persisted in metadata file for the BPE to process
bcg.http.hdrdef.protocol	x-aux-protocol		HTTP header persisted in metadata file for the BPE to process
bcg.http.hdrdef.protocolVersion	x-aux-protocol -version		HTTP header persisted in metadata file for the BPE to process
bcg.http.hdrdef.process	x-aux-process -type		HTTP header persisted in metadata file for the BPE to process
bcg.http.hdrdef.processVersion	x-aux-process -version		HTTP header persisted in metadata file for the BPE to process
bcg.http.hdrdef.msgid	x-aux-msg-id		HTTP header persisted in metadata file for the BPE to process
bcg.http.hdrdef. contentType	content-type		HTTP header persisted in metadata file for the BPE to process
bcg.http.hdrdef. systemMsgId	x-aux-system -msg-id		HTTP header persisted in metadata file for the BPE to process

Table 36. Receiver-specific properties (continued)

Entry	Default value	Possible settings	Description
bcg.http.hdrdef. RNResponseType	x-rn-response -type		HTTP header persisted in metadata file for the BPE to process
bcg.http.hdrdef. RNVersion	x-rn-version		HTTP header persisted in metadata file for the BPE to process
bcg.http.hdrdef. productionFlag	x-aux-production		HTTP header persisted in metadata file for the BPE to process
bcg.http.hdrdef. provSessionId	x-aux-prov -session-id		HTTP header persisted in metadata file for the BPE to process
bcg.http.hdrdef. processInstanceId	x-aux-process -instance-id		HTTP header persisted in metadata file for the BPE to process
bcg.http.hdrdef. contentLength	Content-Length		HTTP header persisted in metadata file for the BPE to process
bcg.http.hdrdef. as2From	AS2-From		HTTP header persisted in metadata file for the BPE to process
bcg.http.hdrdef. as2To	AS2-To		HTTP header persisted in metadata file for the BPE to process
bcg.http.hdrdef. as2Version	AS2-Version		HTTP header persisted in metadata file for the BPE to process
bcg.http.hdrdef. mimeVersion	Mime-Version		HTTP header persisted in metadata file for the BPE to process
bcg.http.hdrdef. messageId	Message-ID		HTTP header persisted in metadata file for the BPE to process
bcg.http.hdrdef.date	Date		HTTP header persisted in metadata file for the BPE to process
bcg.http.hdrdef.from	From		HTTP header persisted in metadata file for the BPE to process
bcg.http.hdrdef. subject	Subject		HTTP header persisted in metadata file for the BPE to process
bcg.http.hdrdef. contentTransferEncoding	Content-Transfer -Encoding		HTTP header persisted in metadata file for the BPE to process
bcg.http.hdrdef. contentDisposition	Content- Disposition		HTTP header persisted in metadata file for the BPE to process

Table 36. Receiver-specific properties (continued)

Entry	Default value	Possible settings	Description
bcg.http.hdrdef. dispositionNotificationTo	Disposition-Notification-To		HTTP header persisted in metadata file for the BPE to process
bcg.http.hdrdef. dispositionNotificationOptions	Disposition-Notification-Options		HTTP header persisted in metadata file for the BPE to process
bcg.http.hdrdef. receiptDeliveryOption	Receipt-Delivery -Option		HTTP header persisted in metadata file for the BPE to process
bcg.http.hdrdef. toPackagingName	ToPackaging Name		HTTP header persisted in metadata file for the BPE to process
bcg.http.hdrdef. asDocType	ASDocType		HTTP header persisted in metadata file for the BPE to process
bcg.http.hdrdef. recipientAddress	Recipient -Address		HTTP header persisted in metadata file for the BPE to process
bcg.http.hdrdef. authorization	Authorization		HTTP header persisted in metadata file for the BPE to process
bcg.http.hdrdef. soapAction	SOAPAction		HTTP header persisted in metadata file for the BPE to process

Table 37. Router-specific properties

Entry	Default value	Possible settings	Description
###### Set this so viacore.prperties logging settings are ignored!!			
bcg.use_container_ logging	TRUE	true, false	
############ Third party duns #####	105217165		
bcg.duns			
############ BCG DB ##			
bcg.co.db.DBType	$ROUTER.DB. TYPE$	db2,oracle	Database type
bcg.co.db.DBPoolName	$ROUTER.JNDI$	datasources/DB2 DS,datasources /OraclePool	Datasource JNDI Prefix
bcg.co.jndiContextURL	corbaloc:iiop: localhost:56809		JNDI Provider URL
bcg.co.jndiFactory	com.ibm. websphere. naming. WsnInitialContext Factory		JNDI Context Factory
bcg.co.db.schema	$ROUTER.DB. SID$		schema information (DB2 - Database Owner, Oracle - Schema Owner)

Table 37. Router-specific properties (continued)

Entry	Default value	Possible settings	Description
############ MQ PROPS			
bcg.use_oaq	FALSE	true, false	
bcg.jms.queue.factory	WBIC/QCF		JMS Queue Connection Factory Name
bcg.jms.topic.factory	WBIC/TCF		JMS Topic Connection Factory Name
bcg.jms.jndi_factory	com.sun.jndi.fscontext.RefFS ContextFactory		Class used to connect to the JNDI server
bcg.jms.context_url	file:$ROUTER_INSTALL_DIR$/jndi		Location of .binding file, used for JMS information
########## BPE ##########			
bcg.oaq_log_q	WBIC/datalogQ		JMS Log Receiver Queue Name
# Maximum File Size Supported by Document Manager # in bytes. ex. 52000000 = 52MB. 0 = no limit.			
bcg.bpe_max_file_size	0		Max filesize (in bytes)
bcg.bpe_in_workflow	com.ibm.bcg.server.transport.TransportUnPackagingFactory | com.ibm.bcg.server.ChannelParseFactory | com.ibm.bcg.destination.DestinationParseFactory | com.ibm.bcg.destination.DestinationProcessFactory | com.ibm.bcg.server.ChannelCheckFactory | com.ibm.bcg.server.transport.TransportLoggingFactory | com.ibm.bcg.duplicate.DuplicateProcessFactory		
bcg.bpe_out_workflow	com.ibm.bcg.server.pkg.PackagingFactory | com.ibm.bcg.server.transport.TransportPackagingFactory		

Table 37. Router-specific properties (continued)

Entry	Default value	Possible settings	Description
## MAIN RTR ##			
bcg.oaq_bpe_in.main	WBIC/main_ InboundQ		JMS Main In Queue Name
bcg.oaq_bpe_out.main	WBIC/delivery ManagerQ		JMS Delivery Manager Queue Name
bcg.inbound_poll_interval.main	1000		Time in milliseconds for each directory scan
bcg.inbound_files_per _pass.main	5		Max files to pick up per scan
bcg.in_thread_count.main	2		Number of Inbound threads for Main Router
bcg.bpe_thread_count.main	2		Number of BPE threads for Main Router
bcg.vms_inbound_directory.main	$SHARED_DATA _DIR$/router_in		Main Router inbound directory
bcg.bpe_temp_directory.main	$SHARED_DATA _DIR$/dat		Main Router data directory
## SIGNAL RTR ##			
bcg.oaq_bpe_in.signal	WBIC/signal _InboundQ		JMS Signal In Queue Name
bcg.oaq_bpe_out.signal	WBIC/delivery ManagerQ		JMS Delivery Manager Queue Name
bcg.inbound_poll_interval.signal	1000		Time in milliseconds for each directory scan
bcg.inbound_files_per_pass.signal	5		Max files to pick up per scan
bcg.in_thread_count.signal	2		Number of Inbound threads for Signal Router
bcg.bpe_thread_count.signal	2		Number of BPE threads for Signal Router
bcg.vms_inbound_directory.signal	$SHARED_DATA _DIR$/signal_in		Signal Router inbound directory
bcg.bpe_temp_directory.signal	$SHARED_DATA _DIR$/data		Signal Router data directory
## SYNCHRONOUS RTR ##			
bcg.oaq_bpe_in.synchronous	WBIC/sync _InboundQ		JMS Synchronous In Queue Name
bcg.oaq_bpe_out.synchronous	WBIC/delivery ManagerQ		JMS Delivery Manager Queue Name
bcg.inbound_poll_interval. synchronous	1000		Time in milliseconds for each directory scan
bcg.inbound_files_per_pass. synchronous	5		Max files to pick up per scan
bcg.in_thread_count.synchronous	2		Number of Inbound threads for Synchronous Router
bcg.bpe_thread_count.synchronous	2		Number of BPE threads for Synchronous Router

Table 37. Router-specific properties (continued)

Entry	Default value	Possible settings	Description
bcg.vms_inbound_directory.synchronous	$SHARED_DATA_DIR$/sync_in		Synchronous Router inbound directory
bcg.bpe_temp_directory.synchronous	$SHARED_DATA_DIR$/data		Synchronous Router data directory
## DESTINATION ##			
bcg.destination.destination_class	com.ibm.bcg.destination.H2 Destination Process		Destination Class
### RECEIVER MBEAN ###			
bcg.vms_receiver_reject_dir	$SHARED_DATA_DIR$/receiver/reject		File system path where the Receiver puts rejected messages
bcg.vms_receiver_tmp_dir	$SHARED_DATA_DIR$/receiver/tmp		File system path where the Receiver puts temporary messages
### DUPLICATE ###			
bcg.duplicate.DupField1	x-aux-system -msg-id		
bcg.duplicate.DupField2	none		
bcg.duplicate.DupField3	none		
bcg.duplicate.DupField4	none		
bcg.duplicate.DupField5	none		
bcg.duplicate.DupField6	none		
bcg.duplicate.DupField7	none		
bcg.duplicate.DupField8	none		
bcg.duplicate.DupField9	none		
bcg.duplicate.DupField10	none		
### LogReceiver ###			
bcg.logReceiver.queue	WBIC/datalogQ		JMS Log Receiver Queue Name
bcg.logReceiver.initial NumberOfReceivers	4		Number of Log Receivers
bcg.dberrors.queue	WBIC/datalog ErrorQ		JMS Log Receiver Errors Queue Name
### Alert Engine ###			
bcg.alertQueue.queue	WBIC/alertQ		JMS Alert Queue Name
bcg.alertQReceiver.initial NumberOfReceivers	1		Number of Alert Receivers
bcg.alertQReceiver.maxRetries	100		Max Alert Retries
bcg.alertQReceiver.retryInterval	60000		Alert retry interval in milliseconds
bcg.eventAlertQReceiver.queue	WBIC/alert EventQ		JMS Alert Event Queue Name
bcg.eventAlertQReceiver. initialNumberOfReceivers\	1		Number of Alert Event Receivers

Table 37. Router-specific properties (continued)

Entry	Default value	Possible settings	Description
# Allow this much time after the volume alert end time to record that the doc # was received in our system, before evaluating the alert:			
bcg.volumeAlertScheduler.allowance ForProcessingReceivedDocInMins	10		
# These parameters avoid excessive email notifications. If there are more than 'maxNotificationsInInterval' # in the time interval 'maxNotificationIntervalInMins' for the same alert, alerts are held and batched every # 'heldAlertsBatchTimeInMins' until no alerts of that type are received for 'minNotificationQuietInterval InMins':			
bcg.alertNotifications. maxNotificationsInInterval	10		
bcg.alertNotifications. maxNotificationIntervalInMins	30		
bcg.alertNotifications. minNotificationQuietInterval InMins	30		
bcg.alertNotifications. heldAlertsBatchTimeInMin	30		
# Notifications that are returned because of e.g. invalid partner email addresses will go # to bcg.alertNotifications. mailEnvelopeFrom.			
bcg.alertNotifications. mailHost	$ROUTER.ALERTS.SMTP_RELAY$		SMTP Relay Host
bcg.alertNotifications. mailFrom	$ROUTER.ALERTS.MAIL_FROM$		Alerts ″from″ mail address
bcg.alertNotifications. mailReplyTo	$ROUTER.ALERTS.MAIL_FROM$		Alerts ″from″ mail address
bcg.alertNotifications. mailEnvelopeFrom	$ROUTER.ALERTS.MAIL_FROM$		Alerts ″from″ mail address
# time for running cert expiration event generator # <minutes> <hour> <class name> # this runs at 1:13 am:			
alert.eventGenerator.schedule	13 1 Certificate Expiration		

Table 37. Router-specific properties (continued)

Entry	Default value	Possible settings	Description
### Delivery Manager ###			
bcg.delivery.gatewayDirectory	$SHARED_DATA _DIR$/gateways		Location of Gateways directory
bcg.delivery.smtpHost	$ROUTER.DM. SMTP_RELAY$		SMTP Mail host
bcg.delivery.smtpHostPort	$ROUTER.DM. SMTP_RELAY. PORT$		SMTP Mail port
bcg.delivery.responseDir	$SHARED_DATA _DIR$/sync_in		Location of Synchronous directory
bcg.delivery.msMaxFileLockLife	180000		Max time for a file to be locked in milliseconds
bcg.delivery.threadPoolMaxThreads	50		
bcg.delivery.gatewayMaxThreads	20		Max Gateway threads
bcg.delivery.gwTransportMaxRetries	3		Number of Retries per gateway
# in millisecs, applies to all gateways			
bcg.delivery.gwTransport RetryInterval	3000		Gateway retry interval in milliseconds
bcg.delivery.queue	WBIC/delivery ManagerQ		JMS Delivery Manager Queue Name
bcg.deliveryQReceiver. initialNumberOfReceivers	10		Number of Gateway receivers
bcg.delivery.numberOfLoggers	10		
# sync response delivery to Response Servlet			
bcg.syncdelivery.queue	WBIC/sync DeliveryManagerQ		JMS Synchronous Delivery Manager Queue Name
bcg.syncdeliveryQReceiver. initialNumberOfReceivers	3		Number of Synchronous Delivery Manager receivers
#bcg.deliveryQReceiver.jmsLog	jms.log		
bcg.delivery.jmstimeout	60000		
# socket timeout for posting in ms			
bcg.http.socketTimeout	120000		HTTP Socket Timeout
bcg.http.version	1.1	1.0,1.1	HTTP Version
### RosettaNet ###			
bcg.rosettanet.retryWaitTmMS	5000		
bcg.rosettanet.strictBoundaryParse	FALSE	true,false	
bcg.rosettanet.mimeBoundaryValidate	FALSE	true,false	

Table 37. Router-specific properties (continued)

Entry	Default value	Possible settings	Description
## If property exists and = ″Literal″, we expect the x-aux-production to ## literally be ″Production″, ″Test″. If property doesn't exist or not ## equal to ″Literal″, we expect the x-aux-production to be ″True″ or ″False″. ## All values are case insensitive.			
bcg.rosettanet.globalUsageCode	Literal	Literal, Production,Test	
## If x-aux-production header is not ″Production″, ″Test″, ″True″, or ″False″, ## and if this property is set to '1', then we will default to the value set ## in property viacore.rosettanet.defaultGlbUsageCd.			
bcg.rosettanet.default UsageCdOnErr	1		
bcg.rosettanet.defaultGlbUsageCd	Production	Production,Test	
## If property exist and equals '1', we expect the builder to provide ## x-aux-process-instance-id to be used as the process instance id an ## outbound request.			
bcg.rosettanet.useBuilder ProcessInstanceId	1		
## If builder provided process-instance-id is invalid (for whatever reason), we ## can generate a new process-instance-id.			
bcg.rosettanet.genProcess InstanceIdOnError	1		
################			
bcg.receiver.persistpath	$SHARED_DATA _DIR$/router_in/		
### RNE ###			
bcg.rne.inbound_poll_interval	1000		RosettaNet Engine poll interval in milliseconds
bcg.rne.in_thread_count	2		RosettaNet Engine Threadcount
bcg.rne.work_size	50		
bcg.0A1.fromContactName	$ROUTER. CONTACT_ NAME$		0A1 Contact Name

Table 37. Router-specific properties (continued)

Entry	Default value	Possible settings	Description
bcg.0A1.fromEMailAddr	$ROUTER. CONTACT. MAIL_FROM$		0A1 E-Mail address
bcg.0A1.fromPhoneNbr	$ROUTER. CONTACT. PHONE_NO$		0A1 Phone Number
bcg.0A1.fromFaxNbr	$ROUTER. CONTACT. FAX_NO$		0A1 Fax Number
## HTTP/S related properties			
bcg.http.CRLDir	$SHARED_DATA _DIR$/security /crl/		Path to CRL directory
bcg.http.SSLDebug	FALSE	true,false	
## Digital signature related properties			
bcg.rosettanet.signature.CRLDir	$SHARED_DATA _DIR$/security /crl/		Path to CRL directory
# Possible values: SHA1,MD5			
bcg.rosettanet.signature. DigestAlgorithm	SHA1	sha1,md5	
# Possible values: true, false			
bcg.rosettanet.signature. RejectIfFailVal	TRUE	true, false	
# Possible values: true, false			
bcg.rosettanet.signature. VerifySigner	TRUE	true, false	
## Encryption properties			
bcg.rosettanet.encrypt.CRLDir	$SHARED_DATA _DIR$/security /crl/		Path to CRL directory
bcg.rosettanet.encrypt. CertDbRefreshInterval	600000		
# valid values: 3des, rc5, rc2-40			
bcg.rosettanet.encrypt.Algorithm	3des	3des,rc5	Encryption Algorithm
# Load certificates for validating signatures - used for VTP signature validation			
bcg.certs.vtp.CertificateDir	$SHARED_DATA _DIR$/security /vtp		

Table 37. Router-specific properties (continued)

Entry	Default value	Possible settings	Description
## Servlet properties ## HTTP headers to be persisted as meta-data by the receiver servlet. ## All properties beginning with ″viacore.http.hdrdef″ will be ## interpreted as headers to be persisted.			
bcg.http.hdrdef.fromID	x-aux-sender-id		HTTP header persisted in metadata file for the BPE to process
bcg.http.hdrdef.toID	x-aux-receiver-id		HTTP header persisted in metadata file for the BPE to process
bcg.http.hdrdef.protocol	x-aux-protocol		HTTP header persisted in metadata file for the BPE to process
bcg.http.hdrdef.protocolVersion	x-aux-protocol -version		HTTP header persisted in metadata file for the BPE to process
bcg.http.hdrdef.process	x-aux-process -type		HTTP header persisted in metadata file for the BPE to process
bcg.http.hdrdef.processVersion	x-aux-process -version		HTTP header persisted in metadata file for the BPE to process
bcg.http.hdrdef.msgid	x-aux-msg-id		HTTP header persisted in metadata file for the BPE to process
bcg.http.hdrdef.contentType	content-type		HTTP header persisted in metadata file for the BPE to process
bcg.http.hdrdef.systemMsgId	x-aux-system -msg-id		HTTP header persisted in metadata file for the BPE to process
bcg.http.hdrdef.RNResponseType	x-rn-response -type		HTTP header persisted in metadata file for the BPE to process
bcg.http.hdrdef.RNVersion	x-rn-version		HTTP header persisted in metadata file for the BPE to process
bcg.http.hdrdef.productionFlag	x-aux-production		HTTP header persisted in metadata file for the BPE to process
bcg.http.hdrdef.provSessionId	x-aux-prov -session-id		HTTP header persisted in metadata file for the BPE to process
bcg.http.hdrdef.processInstanceId	x-aux-process-instance-id		HTTP header persisted in metadata file for the BPE to process

Table 37. Router-specific properties (continued)

Entry	Default value	Possible settings	Description
bcg.http.hdrdef.contentLength	Content-Length		HTTP header persisted in metadata file for the BPE to process
bcg.http.hdrdef.as2From	AS2-From		HTTP header persisted in metadata file for the BPE to process
bcg.http.hdrdef.as2To	AS2-To		HTTP header persisted in metadata file for the BPE to process
bcg.http.hdrdef.as2Version	AS2-Version		HTTP header persisted in metadata file for the BPE to process
bcg.http.hdrdef.mimeVersion	Mime-Version		HTTP header persisted in metadata file for the BPE to process
bcg.http.hdrdef.messageId	Message-ID		HTTP header persisted in metadata file for the BPE to process
bcg.http.hdrdef.date	Date		HTTP header persisted in metadata file for the BPE to process
bcg.http.hdrdef.from	From		HTTP header persisted in metadata file for the BPE to process
bcg.http.hdrdef.subject	Subject		HTTP header persisted in metadata file for the BPE to process
bcg.http.hdrdef.content TransferEncoding	Content-Transfer-Encoding		HTTP header persisted in metadata file for the BPE to process
bcg.http.hdrdef.contentDisposition	Content-Disposition		HTTP header persisted in metadata file for the BPE to process
bcg.http.hdrdef.disposition NotificationTo	Disposition-Notification-To		HTTP header persisted in metadata file for the BPE to process
bcg.http.hdrdef.disposition NotificationOptions	Disposition-Notification-Options		HTTP header persisted in metadata file for the BPE to process
bcg.http.hdrdef.receipt DeliveryOption	Receipt-Delivery-Option		HTTP header persisted in metadata file for the BPE to process
bcg.http.hdrdef.toPackagingName	ToPackaging Name		HTTP header persisted in metadata file for the BPE to process
bcg.http.hdrdef.asDocType	ASDocType		HTTP header persisted in metadata file for the BPE to process

Table 37. Router-specific properties (continued)

Entry	Default value	Possible settings	Description
# Packaging related properties # Attachments with one of the following content types will not be base64 encoded			
bcg.pkg.sponsor.contenttypes	bcg.pkg.sponsor.contenttypes		
### START of SPONSOR ENGINE ###			
bcg.sponsor.inbound_poll_interval	10000		
bcg.sponsor.in_thread_count	2		Number of Inbound threads for Sponsor Engine
bcg.sponsor.work_size	10		
bcg.delivery.sponsor.eventMsgClass	com.ibm.bcg.delivery.sponsor.SponsorEvent Message		
### DB proc debug properties###			
DBProcDebug	1		Database debugging flag
# Global State engines instance ID			
GlobalStateEngInstanceId	bcg		
# EDIINT defaults			
bcg.ediint.reportingUA	WBI_Connect		
bcg.ediint.retry WaitTmMS	5000		

Notices

IBM may not offer the products, services, or features discussed in this document in all countries. Consult your local IBM representative for information on the products and services currently available in your area. Any reference to an IBM product, program, or service is not intended to state or imply that only that IBM product, program, or service may be used. Any functionally equivalent product, program, or service that does not infringe any IBM intellectual property right may be used instead. However, it is the user's responsibility to evaluate and verify the operation of any non-IBM product, program, or service.

IBM may have patents or pending patent applications covering subject matter described in this document. The furnishing of this document does not give you any license to these patents. You can send license inquiries, in writing, to:

IBM Director of Licensing
IBM Corporation
North Castle Drive
Armonk, NY 10504-1785
U.S.A.

The following paragraph does not apply to the United Kingdom or any other country where such provisions are inconsistent with local law:

INTERNATIONAL BUSINESS MACHINES CORPORATION PROVIDES THIS PUBLICATION "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF NON-INFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. Some states do not allow disclaimer of express or implied warranties in certain transactions, therefore, this statement may not apply to you.

This information could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein; these changes will be incorporated in new editions of the publication. IBM may make improvements and/or changes in the product(s) and/or program(s) described in this publication at any time without notice.

Any references in this information to non-IBM Web sites are provided for convenience only and do not in any manner serve as an endorsement of those Web sites. The materials at those Web sites are not part of the materials for this IBM product and use of those Web sites is at your own risk.

IBM may use or distribute any of the information you supply in any way it believes appropriate without incurring any obligation to you.

Licensees of this program who wish to have information about it for the purpose of enabling: (i) the exchange of information between independently created programs and other programs (including this one) and (ii) the mutual use of the information which has been exchanged, should contact:

IBM Burlingame Laboratory Director
IBM Burlingame Laboratory
577 Airport Blvd., Suite 800

Burlingame, CA 94010
U.S.A

Such information may be available, subject to appropriate terms and conditions, including in some cases, payment of a fee.

The licensed program described in this document and all licensed material available for it are provided by IBM under terms of the IBM Customer Agreement, IBM International Program License Agreement, or any equivalent agreement between us.

Any performance data contained herein was determined in a controlled environment. Therefore, the results obtained in other operating environments may vary significantly. Some measurements may have been made on development-level systems and there is no guarantee that these measurements will be the same on generally available systems. Furthermore, some measurement may have been estimated through extrapolation. Actual results may vary. Users of this document should verify the applicable data for their specific environment.

Information concerning non-IBM products was obtained from the suppliers of those products, their published announcements or other publicly available sources. IBM has not necessarily tested those products and cannot confirm the accuracy of performance, compatibility or any other claims related to non-IBM products. Questions on the capabilities of non-IBM products should be addressed to the suppliers of those products.

This information may contain examples of data and reports used in daily business operations. To illustrate them as completely as possible, the examples may include the names of individuals, companies, brands, and products. All of these names are fictitious and any similarity to the names and addresses used by an actual business enterprise is entirely coincidental.

All statements regarding IBM's future direction or intent are subject to change or withdrawal without notice, and represent goals and objectives only.

COPYRIGHT LICENSE

This information may contain sample application programs in source language, which illustrates programming techniques on various operating platforms. You may copy, modify, and distribute these sample programs in any form without payment to IBM, for the purposes of developing, using, marketing or distributing application programs conforming to the application programming interface for the operating platform for which the sample programs are written. These examples have not been thoroughly tested under all conditions. IBM, therefore, cannot guarantee or imply reliability, serviceability, or function of these programs.

Websphere Business Integration Connect contains code named ICU4J which is licensed to you by IBM under the terms of the International Program License Agreement, subject to its Excluded Components terms. However, IBM is required to provide the following language to you as a notice:

COPYRIGHT AND PERMISSION NOTICE

Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the ″Software″), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, provided that the above copyright notice(s) and this permission notice appear in all copies of the Software and that both the above copyright notice(s) and this permission notice appear in supporting documentation.

THE SOFTWARE IS PROVIDED ″AS IS″, WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OF THIRD PARTY RIGHTS. IN NO EVENT SHALL THE COPYRIGHT HOLDER OR HOLDERS INCLUDED IN THIS NOTICE BE LIABLE FOR ANY CLAIM, OR ANY SPECIAL INDIRECT OR CONSEQUENTIAL DAMAGES, OR ANY DAMAGES WHATSOEVER RESULTING FROM LOSS OF USE, DATA OR PROFITS, WHETHER IN AN ACTION OF CONTRACT, NEGLIGENCE OR OTHER TORTIOUS ACTION, ARISING OUT OF OR IN CONNECTION WITH THE USE OR PERFORMANCE OF THIS SOFTWARE.

Except as contained in this notice, the name of a copyright holder shall not be used in advertising or otherwise to promote the sale, use or other dealings in this Software without prior written authorization of the copyright holder.

Programming interface information

Programming interface information, if provided, is intended to help you create application software using this program.

General-use programming interfaces allow you to write application software that obtain the services of this program's tools.

However, this information may also contain diagnosis, modification, and tuning information. Diagnosis, modification and tuning information is provided to help you debug your application software.

Warning: Do not use this diagnosis, modification, and tuning information as a programming interface because it is subject to change.

Trademarks and service marks

The following terms are trademarks or registered trademarks of International Business Machines Corporation in the United States or other countries, or both:

IBM
the IBM logo
AIX
CrossWorlds
DB2
DB2 Universal Database
Domino
Lotus
Lotus Notes
MQIntegrator

MQSeries
Tivoli
WebSphere

Microsoft, Windows, Windows NT, and the Windows logo are trademarks of Microsoft Corporation in the United States, other countries, or both.

MMX, Pentium, and ProShare are trademarks or registered trademarks of Intel Corporation in the United States, other countries, or both.

Java and all Java-based trademarks are trademarks of Sun Microsystems, Inc. in the United States, other countries, or both.

Other company, product or service names may be trademarks or service marks of others.

WebSphere Business Integration Connect Enterprise and Advanced Editions Version 4.2.2.

Index

A

B

C

D

E

F

G

H

I

L

M

N

O

P

Q

R

S

T

U

V

W

X

Printed in USA