

IBM WebSphere Business Integration Connect
Enterprise and Advanced Editions



Administrator Guide

Version 4.2.1

Note!

Before using this information and the product it supports, be sure to read the general information under Notices and Trademarks on page 207.

19December2003

This edition applies to Version 4, Release 2, Modification 1, 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.

IBM welcomes your comments. You can send to the following address:

IBM Burlingame Laboratory
Information Development
577 Airport Blvd., Suite 800
Burlingame, CA 94010
U.S.A

Include the title and order number of this book, and the page number or topic related to your comment.

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

© Copyright IBM Corp. 2003. All rights reserved.

US Government Users Restricted Rights – Use, duplication or disclosure restricted by GSA ADP Schedule Contract with IBM Corp.

Table of Contents

About this book - - - - -	7	Provided Document Flow Definitions - -	31
Who should read this book - - - - -	7	About Document Flow Definition contexts	32
Related documents - - - - -	8	Creating Document Flow Definitions - -	32
Conventions and terminology used in this		Creating content filters- - - - -	34
book - - - - -	9	Uploading RNIF packages - - - - -	35
Terms - - - - -	9	About Document Flow Definition attributes	36
Getting help - - - - -	10	Creating interactions- - - - -	42
Online Help- - - - -	10	Enabling, disabling, or editing interactions	42
Customer service - - - - -	11	About validation maps - - - - -	43
Chapter 1. Logging in to the Community		Updating validation maps - - - - -	43
Console - - - - -	13	Associating maps to Document Flow	
Starting Business Integration Connect		Definitions- - - - -	44
Console - - - - -	13	Configuring RosettaNet support - - - - -	44
Logging in to the Community Console - -	13	RNIF and PIP document flow packages	45
Navigating through the Community Console	15	RosettaNet end-to-end flows- - - - -	47
Community Console icons - - - - -	16	Setting up RosettaNet support - - - - -	54
Logging out of the Community Console -	18	Creating PIP channels to Community	
Stopping the Community Console - - - -	18	Participants - - - - -	54
Stopping the Business Integration Connect		Editing RosettaNet attribute values- -	57
Document Manager and Receiver - - - -	18	Configuring attribute values - - - - -	58
Chapter 2. Hub Admin Activities - -	19	Deactivating PIPs - - - - -	59
Configuring Community Console Locale		Providing failure notification - - - - -	59
information - - - - -	19	Creating PIP document flow packages -	60
Branding the Community Console - - -	21	About validation - - - - -	73
Downloading sample images - - - - -	21	PIP document flow package contents -	75
Uploading a header/banner and company		Updating alert mail addresses - - - - -	92
logo - - - - -	22	Managing XML formats - - - - -	93
Managing password policy - - - - -	22	Creating an XML format - - - - -	93
Viewing and editing password policy details	22	Editing XML format values - - - - -	94
Configuring permissions - - - - -	23	Deleting an XML format - - - - -	95
Viewing and editing permission details-	23	Enabling or disabling Actions - - - - -	96
Enabling or disabling permissions quickly	24	Managing event codes - - - - -	96
Configuring targets - - - - -	25	Viewing and editing permission details -	97
Creating a new target - - - - -	25	Saving event code names - - - - -	97
Viewing and editing target details - - -	29	Sending and receiving large files - - - -	98
Enabling or disabling targets - - - - -	30	Changing the database, database user, and	
Deleting targets- - - - -	30	password - - - - -	98
Implementing Document Flow Definitions	30	Chapter 3. Account Admin Activities	101
About Document Flow Definition types-	30		

Managing Participant profiles - - - - -	101	Activating the Participant Connection -	134
Creating Participants - - - - -	101	Restrictions and Limitations of Web Service support - - - - -	134
Viewing and editing Participant profiles	103	Chapter 5. cXML Support - - - - -	135
Searching for Participants - - - - -	104	cXML support overview - - - - -	135
Viewing your profile - - - - -	104	cXML document types - - - - -	136
Managing gateway configurations - - -	105	Content-type headers and attached documents - - - - -	138
Viewing and editing gateways - - -	105	Valid cXML interactions - - - - -	138
Viewing default gateways - - - - -	106	Creating a cXML document flow definition -	139
Creating gateways - - - - -	106		
Deleting gateway configurations- - -	107	Chapter 6. Using the Gateway Queue	143
Information required for gateway configuration - - - - -	107	Viewing the gateway list - - - - -	143
Managing FTP - - - - -	108	Viewing queued documents - - - - -	144
Community Console FTP configuration	108	Removing documents from the queue -	145
Setting up FTP - - - - -	110	Viewing gateway details - - - - -	145
Creating an FTP account - - - - -	113	Changing gateway status - - - - -	145
Specifying an FTP server - - - - -	113	Chapter 7. Troubleshooting - - - - -	147
Editing FTP details - - - - -	114	Optimizing database query performance	147
Managing certificates - - - - -	114	Increasing the Receiver timeout setting	147
Certificates not loaded - - - - -	114	Avoiding out-of-memory errors - - - - -	148
Viewing and editing digital certificates	115	Avoiding long processing time on large encrypted AS documents - - - - -	148
Creating digital certificates - - - - -	115	Reprocessing events and business documents that fail to log to the database -	148
Disabling a digital certificate- - - - -	116	Archiving and purging filesystem and database logs - - - - -	149
Managing B2B capabilities - - - - -	117	Purging application log files - - - - -	149
Changing B2B attribute values - - -	119	Purging non-repudiation directories -	149
Managing Participant connections - - -	120	Purging database tables - - - - -	150
Connection components - - - - -	121	Poor performance and system events are not working - - - - -	153
Connection duplication - - - - -	121	Shutting down - - - - -	154
Searching for connections- - - - -	123	Starting the system after a machine shutdown	154
Changing connection configurations- -	125	Starting DB2- - - - -	154
Managing Exclusion Lists - - - - -	126	Starting WebSphere MQ- - - - -	154
Adding Participants to the Exclusion List-	126	Starting the Community Console, Receiver, and Document Manager - - - - -	154
Editing the Exclusion List - - - - -	126	Restarting the router after a crash - - -	155
Chapter 4. Web Services Support - -	129	Appendix A. Administering Certificates	157
Identifying the participants for a Web Service	129		
Setting up Document Flow Definitions for a Web Service - - - - -	130		
Uploading the WSDL files for a Web Service	131		
Setting up a Valid Interaction for a new Web Service - - - - -	133		
Adding Document Flows to Participants B2B Capabilities - - - - -	133		
Setting up Source and Target Gateways for the Web Service participants - - - - -	134		

Certificate Overview - - - - -158
 Understanding terms and concepts - -159
 Creating and installing certificates - - - -159
 Inbound SSL certificates - - - - -159
 Outbound SSL certificate - - - - -161
 Adding a Certificate Revocation List (CRL)
 162
 Inbound signature certificate - - - -163
 Outbound signature certificate- - - -163
 Inbound encryption certificate - - - -164
 Outbound encryption certificate - - - -165

Configuring Inbound SSL for the Console and
 Receiver - - - - - 166

Appendix B. Failed Events 167

Appendix C. BCG.Properties 175

Appendix D. Transport and gateway re-tries 199

Notices and Trademarks - - - - 207

Programming interface information - - - - 208

Trademarks and service marks- - - - 209

About this book

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

Who should read this book

The parties involved with maintaining Business Integration Connect are the administrators. Business Integration Connect assumes two types of administrators:

- Hub Admin
- Operator 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. Only the Hub Admin can access the Hub Admin features.

The following table identifies the Console module activities available to Hub Admin and Operator Admin personnel. An “x” indicates that the individual has access to the module activity. When a Hub Admin or Operator Admin logs on to the Console, the Console only displays features that the Hub Admin or Operator Admin can access.

Modules and Activities	Hub Admin	Operator Admin
Hub Admin Activities (available to Hub Admin users only — see Chapter 2, page 19)		
Configuring Permissions	x	
Managing Password Policy	x	
Managing Event Codes	x	
Enabling or Disabling Actions	x	
Configuring Document Flow Definitions and Download Packages	x	
Configuring Validation Maps	x	
Configuring Targets	x	
Branding the Console	x	
Managing XML Formats	x	
Account Admin Activities (see Chapter 3, page 101)		
Managing Participant Profiles	x	x
Managing Gateway Configurations	x	x
Managing Users (see Note)	x	x
Managing Groups (see Note)	x	x
Managing Contacts (see Note)	x	x
Managing Addresses (see Note)	x	x
Managing Participant Connections	x	

Modules and Activities	Hub Admin	Operator Admin
Managing Exclusion Lists	x	
Managing Alerts (see Note)	x	x
Managing B2B Capabilities	x	x
Managing Certificates	x	x
Managing FTP	x	x
Viewers		
Event Viewer (see Note)	x	x
RosettaNet Viewer (see Note)	x	x
AS1/AS2 Viewer (see Note)	x	x
Document Viewer (see Note)	x	x
Gateway Queue (see Chapter 6, page 143)	x	
Tools (see Note)		
Document Analysis	x	x
Document Volume Report	x	x
Test Participant Connection	x	x
Community Participant Simulator Features (see Note)		
Initiate View Processes	x	x

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. For information about these shared features, see the WebSphere Business Integration Connect Community Console User Guide.

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/>

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.
<i>italics</i>	Indicates a variable.
/	In this document, forwardslashes (/) are used as the convention for directory paths. For Windows installations, substitute backslashes (\) for forwardslashes. 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 known as a business action. A message with content of a business nature such as a Purchase Order Request or a Request For Quote. The exchange of business actions and business signals comprise the message choreography necessary to complete a business activity specified by a given PIP.

Business action - see Action.

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

Participant connection: A Participant connection defines the connection between two specific community members' environments by which one unique process is executed according to the associated action.

Community Console: The Community Console is a Web based tool used to configure Business Integration Connect and to manage the flow of your company's business documents to and from your Community Manager and Participants.

Document: A collection of information adhering to an organizational convention. In this context, there are multiple documents in a process.

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

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.

Packages: Identify document packaging formats used to transmit documents over the internet. For example, RNIF, AS1, and AS2.

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.

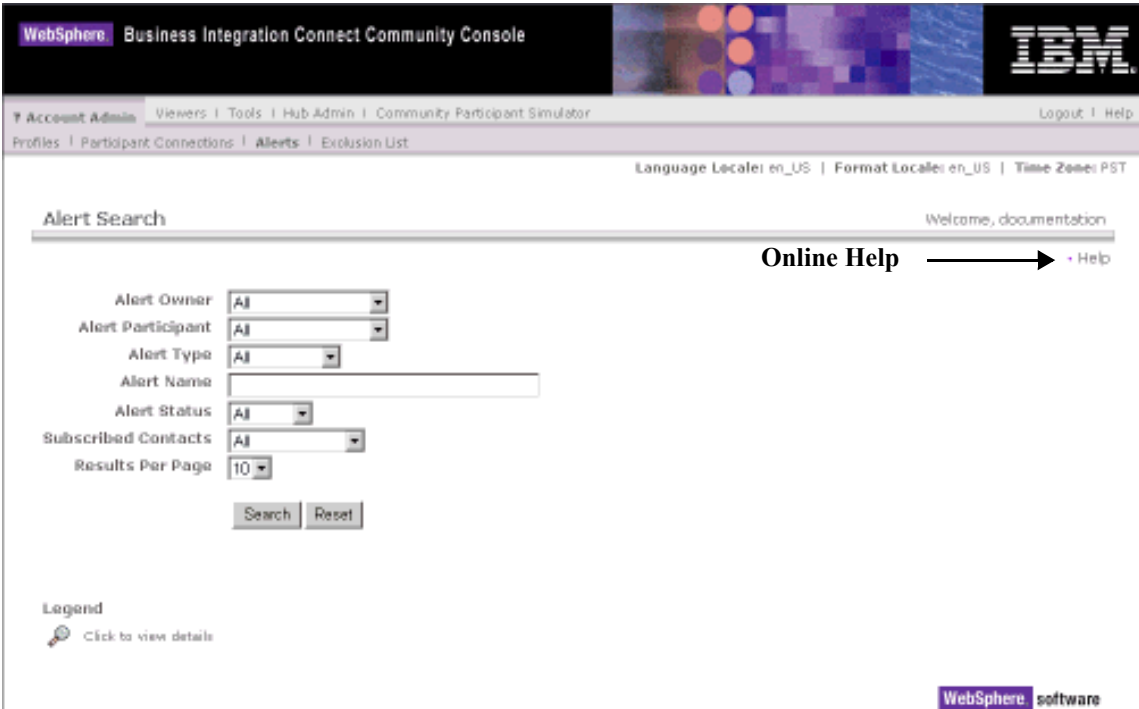
RosettaNet PIP (Partner Interface Process): A model that depicts the activities, decisions, and Partner Role Interactions that fulfill a business transaction between two partners in a given supply chain. (In Business Integration Connect, partners are called Participants.) Each Participant involved in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

Process: A process is a series of documents or messages executed between Community Managers and Participants. Taken as a whole, the documents make up a complete business process.

Getting help

Online Help

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



Customer service

Software support

www.ibm.com/software/support

Passport Advantage

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

Company web site

www.ibm.com/websphere/wbiconnect/

Chapter 1. Logging in to the Community Console

The administrator activities described in this guide are performed through the WebSphere Business Integration Connect Community Console. The Community Console is a Web-based facility that provides a secure Console access point. It features a friendly graphical user interface and convenient Web-based access capabilities.

Topics covered in this chapter include:

- [“Starting Business Integration Connect Console” on page 13](#)
- [“Logging in to the Community Console” on page 13](#)
- [“Navigating through the Community Console” on page 15](#)
- [“Community Console icons” on page 16](#)
- [“Logging out of the Community Console” on page 18](#)
- [“Stopping the Community Console” on page 18](#)
- [“Stopping the Business Integration Connect Document Manager and Receiver” on page 18](#)

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. This can be safely ignored.

Logging in to the Community Console

The following procedure describes how to log in to the Community Console. To log in, you need one of the following Web browsers:

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

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

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

1. Enter the following URL in the location field of any Web browser:

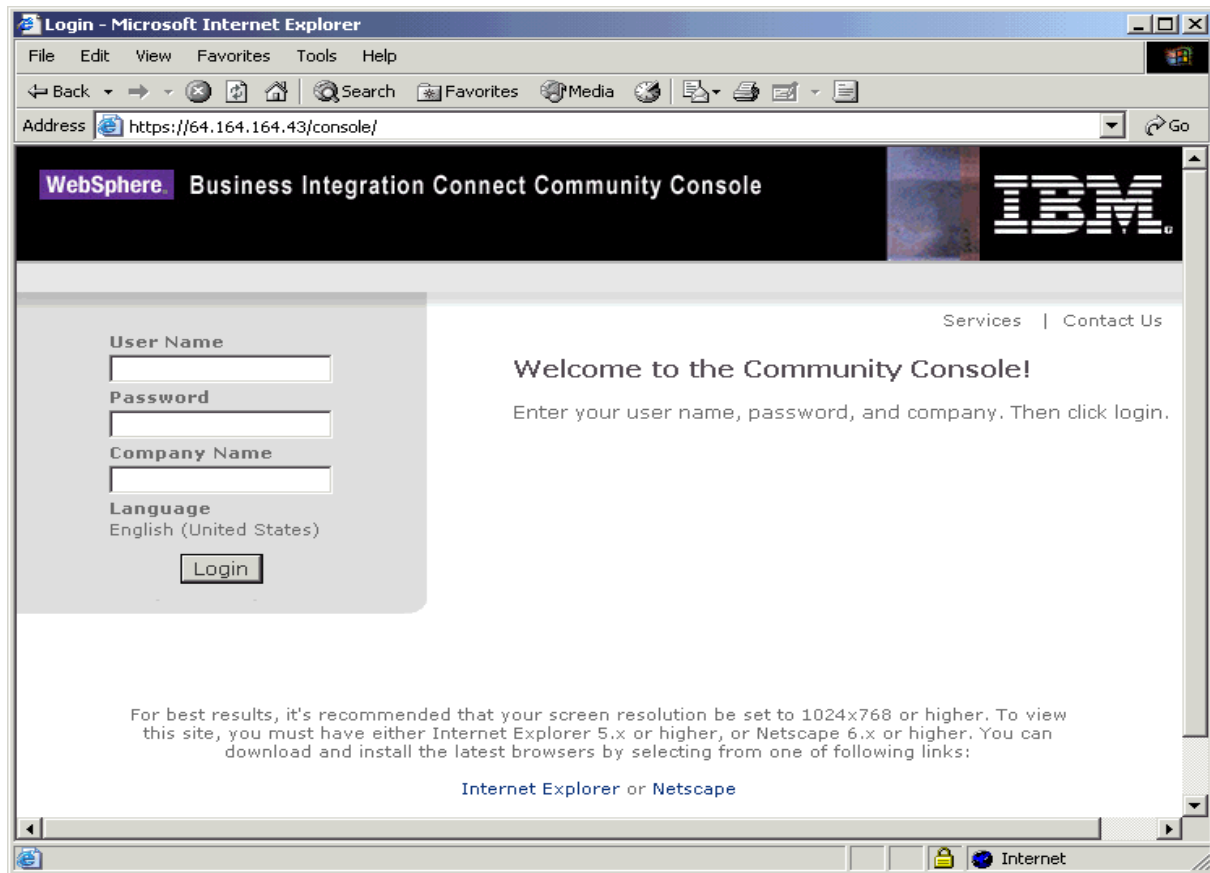
`http://<hostname>.<domain>:58080/console (unsecure)`

`http://<hostname>.<domain>:58443/console (secure)`

Where `<hostname>` and `<domain>` are the name and location of the computer hosting the Community Console component.

The Community Console login screen is displayed.

Figure 1-1. Community Console Login Screen



2. Next to **User Name**, enter the appropriate user name.
 - For the Hub Admin, the default user name is **hubadmin**
 - For the Operator Admin, the default user name is **Admin**
3. Next to **Password**, enter the password for your company. The default password is **Pa55word**
4. Next to **Company Name**, enter the Admin login name. The default Admin 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** text box.
7. Click **Save**. The system displays the Console's initial entry screen.

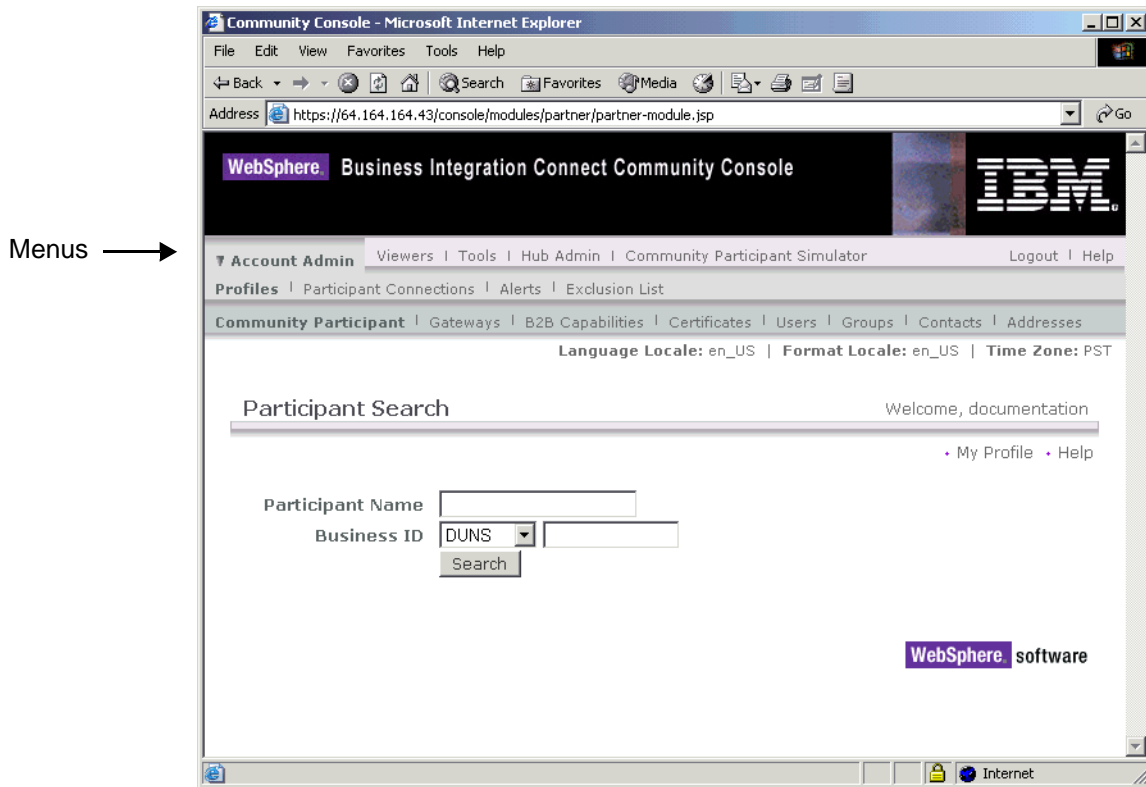
Navigating through the Community Console

The Community Console consists of various menus used to configure Business Integration Connect. Click **Account Admin** > **Profiles** in the menu. The screen in [Figure 1-2](#) is displayed.

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

- **Logout** allows you to log out from the current WebSphere Business Integration Connect session. The application continues to run in the background. To log in again, use the procedure under “[Logging in to the Community Console](#)” on page 13.
- **Help** allows you to access the online help for WebSphere Business Integration Connect.

Figure 1-2. User Interface Controls



Community Console icons

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

Table 1-1. Community Console Icons



















Icon	Description
Clickable icons	
	Click to view detailed information.
	Click to modify a selected item.
	Click to delete one or more selected items or to activate the associated inactive item.
	Click to display a raw document.
	Click to view validation errors.
	Click to continue.
	Click to pause.
	Click to print a document or report.
	Click to export a report.
	Click to select calendar dates.
	Click to view greater details.
	Click to close the detailed view.
	Click to view the groups to which a user belongs.
	Click to view users in a group.
	Click to export information from the system.
	Click to deactivate the associated active item.
	Click to edit a Document Flow Definition.
	Click to view Document Flow Definition attribute setup.

Table 1-1. Community Console Icons (continued)






















Icon	Description
	Click to upload a new map.
	Click to download a map.
	Click to edit attribute values.
	Click to edit RosettaNet attribute values.
	Click to view a previously sent original document when there is a duplicate document event.
	Click to hide search criteria.
	Click to view permissions.
	Roll is not active; click to create role.
	Click to view the Help system.
Icons that show information	
	Indicates that the field requires input from the user.
	Indicates that a Trade Participant Agreement (TPA) has been entered.
	Indicates that a Participant or gateway is disabled.
	Indicates that a document contains an attachment.
	Indicates that document currently in progress.
	Indicates that document processing was successful.
	Indicates that document processing failed.
	Indicates synchronous data flow. No icon is displayed for asynchronous transactions.
	Indicates that data is contained.
	Indicates that no data is contained.

Table 1-1. Community Console Icons (continued)

Icon	Description
	Indicates that a hierarchical tree is in the “collapsed” view.
	Indicates that a hierarchical tree is in the “expanded” view.

Logging out of the Community Console

When you finish using the Business Integration Connect Community Console, click **Logout** at the top-right side of any Console screen (see [Figure 1-2 on page 15](#)). The system logs you out and returns you to the Console Login screen.

Stopping the Community Console

To stop the 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. This can be safely ignored.

Stopping the Business Integration Connect Document Manager and Receiver

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

- UNIX - `INSTALLATION_DIRECTORY/console/was/bin/shutdown_bcg.sh`
- Windows - `INSTALLATION_DIRECTORY/console/was/bin/shutdown_bcg.bat`

NOTE: When running this command, a warning message appears. This can be safely ignored.

Chapter 2. Hub Admin Activities

This chapter describes the tasks that a Hub Admin user can perform. These tasks are:

- “Configuring Community Console Locale information” on page 19
- “Managing password policy” on page 22
- “Configuring permissions” on page 23
- “Configuring targets” on page 25
- “Implementing Document Flow Definitions” on page 30
- “Configuring RosettaNet support” on page 44
- “Updating alert mail addresses” on page 92
- “Managing XML formats” on page 93
- “Enabling or disabling Actions” on page 96
- “Managing event codes” on page 96
- “Sending and receiving large files” on page 98
- “Changing the database, database user, and password” on page 98

Configuring Community Console Locale information

Locale Configuration allows the user to customize how Community Console data is presented based on the language and form that is best understood by the user.

To configure the Community Console Locale information, use the following procedure.

1. Click **Hub Admin > Console Configuration > Locale Configuration** on the menu bar and select the desired locale. The Console displays the Locale Upload screen (see [Figure 2-1](#)).

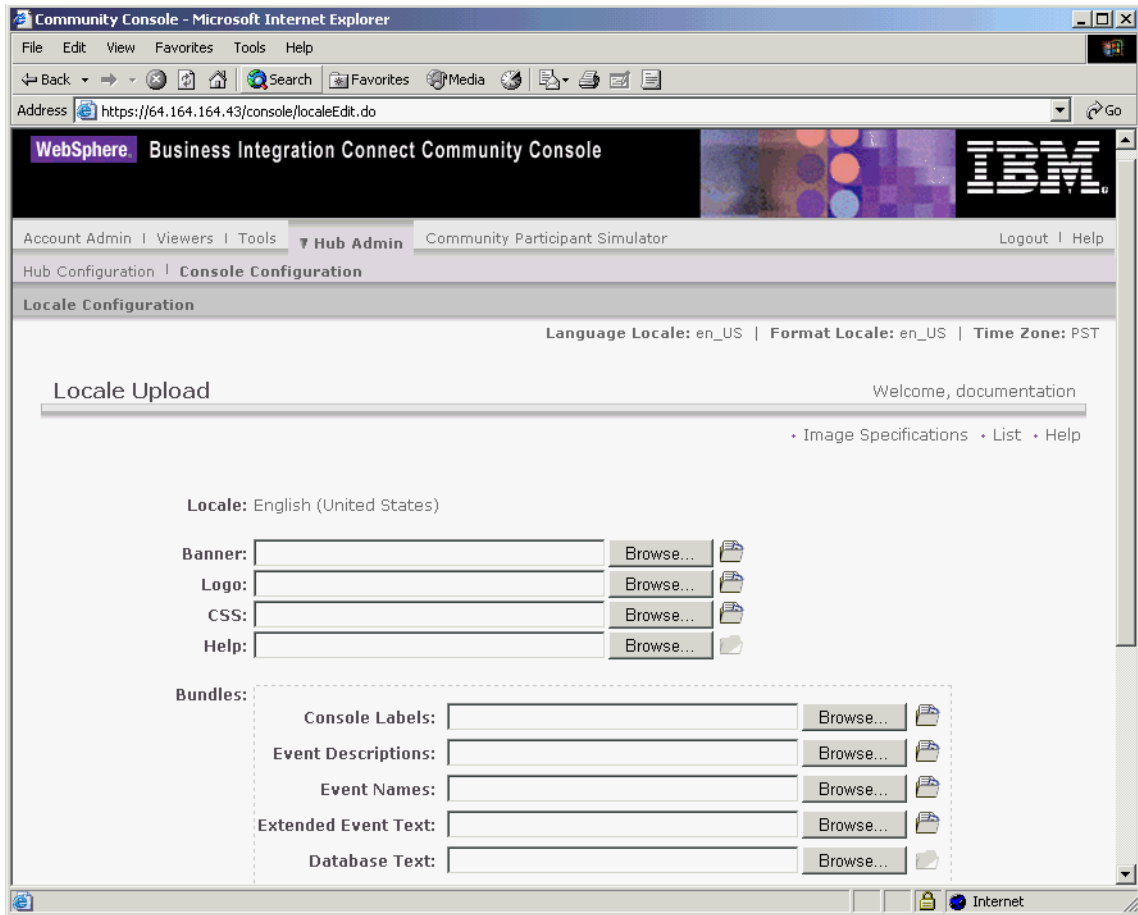


Figure 2-1. Console Branding Screen

2. Upload the following console elements into the system for locale customization:
 - **Banner** - Spans the top of the Community Console. See [“Uploading a header/banner and company logo” on page 22](#) for details.
 - **Logo** - Appears at the top right of the Community Console. See [“Uploading a header/banner and company logo” on page 22](#) for details.
 - **CSS** - Cascading Style Sheets (CSS) are used for customizing the style (e.g., fonts, colors, spacing) of the Community Console. The style sheet must be a proper style sheet document; otherwise, the Community Console will be displayed using the browser's default settings.
 - **Help** - A Web-based, language specific help can be uploaded and displayed in the Community Console. The system currently supports eHelp Corporation's WebHelp output format. The WebHelp generated help files must be contained within a ZIP archive for uploading.
 - **Bundles** - Resource bundles are used to localize the data displayed in the Community Console. The resource bundles in [Table 2-1](#) can be uploaded into the system:

Table 2-1. Resource bundles

Bundle	Description
Console	Static text, headers, and links.
Event Text	Text used to display event details.
Event Name	Text used to display event name.
Global Search	Text used for providing additional information on events—event cause, troubleshooting, etc.
Database Labels	Text used for displaying participant specific data stored in the database. Examples include: participant name, package, protocol, message ID, etc.

Branding the Community Console

You can customize the look and feel of the Community Console by changing the branding images. Branding of the Community Console consists of importing two images: header background and company logo.

- The header background spans across the top of the Community Console.
- The company logo is displayed at the top right of the Community Console.

The images must be .JPG format files and must conform to the following size restrictions:

Table 2-2. Header Background and Company Logo Size Restrictions

Specification	Header Background	Company Logo
Height	80 pixels	80 pixels
Width	1100 pixels minimum (including the company logo image)	200 pixels maximum
Size	32k maximum	32k maximum



Figure 2-2. Image Specifications

Downloading sample images

To download sample header/banner and company logo images, use the following procedure.

1. Click **Hub Admin > Console Configuration > Locale Configuration** on the menu bar and select the desired locale. The Console displays the Locale Upload screen (see [Figure 2-1](#)).
2. Click on the **Image Specification** option in the upper right corner of the screen.
3. Scroll down to the **Sample Images** portion of the screen.
4. To view a sample header background image, click the **sample_headerback.jpg** link.
5. To view a sample company logo, click the **sample_logo.jpg** link.
6. To view a sample image, click the **Click for Sample** link or the graphic above it.
7. To download sample images (header background and company logo) in a zip file, click the **Sample Images (header background and company logo)** link.

Uploading a header/banner and company logo

To upload header/banner and company logo images, use the following procedure.

1. Click **Hub Admin > Console Configuration > Locale Configuration** on the menu bar and select the desired locale. The Console displays the Locale Upload screen (see [Figure 2-1 on page 20](#)).
2. In the **Banner** field, type the path and name of the image file you want to use for the header/banner or browse and select the file.
3. Next to **Logo**, type the path and name of the logo file you want to use for the company logo or browse and select the file.
4. Click **Upload**.


NOTE: Replacing the header background and company logo require that the Community Console be restarted for the changes to take effect. See your system administrator to restart the Community Console.

Managing password policy

The Password Policy screen lets you set up the password policy for the Hub community. Using this screen, you can implement a strong password policy that includes limiting a password's life span. The Password Policy screen also allows you to use special characters in the password to prevent susceptibility to dictionary attack. It also lets you prevent the use of passwords that resemble those previously used or passwords that are similar to a user's login or full name.

Viewing and editing password policy details

The following procedure describes how to view password policy details. As part of this procedure, you can change the maximum length, expire time, uniqueness, special character, and name variation checking parameters.

1. Click **Hub Admin > Console Configuration > Password Policy**. The Console displays the Password Policy screen.
2. Click the  icon to edit the contents.

3. Complete the following parameters in the screen:

Table 2-3. Password Policy Details

Parameter	Description
Minimum Length	Minimum number of characters used for the password.
Expire Time	Number of days until the password expires.
Uniqueness	Retains a numeric history of previously used passwords. An old password cannot be reused if it exists in the history file.
Special Characters	When checked, passwords must contain at least three of the following types of special characters: <ul style="list-style-type: none">• Upper-case characters• Lower-case 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. It is recommended that Special Characters remain Off when using passwords composed of international characters. Non-english character sets may not contain the required three out of four character types. The special characters supported by the system are as follows: '#', '@', '\$', '&', '+'.
Name Variation Checking	When checked, prevents the use of passwords that comprise an easily guessed variation of the user's login or full name.

4. Click **Save**.

Configuring permissions

Permissions represent privileges required for accessing various Console modules. The Community Console provides the Permission List screen to display the following information for each module:

- The name of the module
- The description of the permission
- The status (Enabled or Disabled) of each permission

From the Permission List screen, you can set whether users must have permission to use a module and change the description of the permission descriptions. You cannot, however, define new permissions.

Viewing and editing permission details

The following procedure describes how to view details for a permission. As part of this procedure, you can edit the permission description that is displayed on the Permission List screen and enable or disable the permission.

1. Click **Hub Admin > Console Configuration > Permissions**. The Console displays the Permission List screen.



2. Click the  icon next to the permission whose details you want to view. The Console displays the Permission Detail screen.
3. Click the  icon to edit the description of the permission you are viewing.
4. Complete the following parameters in the screen:

Table 2-4. Permission Details

Parameter	Description
Module Name	Read-only field that shows the name of the module that corresponds to the permission.
Description	A description of the permission, which is displayed on the Permission List screen.
Status	<p>Enables or disables the permission.</p> <ul style="list-style-type: none"> • If enabled, a module can be viewed and access rights controlled by the operator, manager, and participant admin users. • If disabled, the module will not be viewable in the console navigation, and will not appear as a selectable module within the Group Permission screen. <p>(Permissions can also be enabled or disabled directly from the Permission List – see “Enabling or disabling permissions quickly” on page 24).</p>

5. Click **Save**.

Enabling or disabling permissions quickly

You can change the permission status of a module from the Permission List screen by clicking Enabled or Disabled in the status column.

- If enabled, a module can be viewed and access rights controlled by the operator, manager, and participant admin users.
 - If disabled, the module will not be viewable in the console navigation, and will not appear as a selectable module within the Group Permission screen.
1. Click **Hub Admin > Console Configuration > Permissions**. The Console displays the Permission List screen.
 2. Click **Enabled** or **Disabled** under the **Status** column on the Permission List screen. If the status is **Enabled**, a dialog box asks whether you want to disable permissions. If the status is **Disabled**, a dialog asks whether you want to enable permissions,
 3. To change the module's permission status, click **OK**. If you click **OK**, the Permission List screen displays the module's new status.

Configuring targets

The Target List screen provides location information that enables the Document Manager to fetch documents from the appropriate system location based on the transport type of the incoming document. You can create separate target configurations based on transport type. The Document Manager can then poll the document repository locations of multiple Web, FTP, and POP mail servers — including internal directories and JMS queues — for incoming documents. Once the Document Manager retrieves a document from the location based on a pre-defined target, the routing infrastructure can process the document based on channel configuration.

Creating a new target

To create a new target for incoming documents, use the following procedure.

1. Click **Hub Admin > Hub Configuration > Targets**. The Console displays the Target List screen.
2. Click **Create** in the upper right corner of the screen. The Console displays the Target Details screen (see [Figure 2-3](#)).

The screenshot shows a web browser window with the address `https://64.164.164.43/console/receiverNew.do`. The page title is "WebSphere Business Integration Connect Community Console". The navigation menu includes "Account Admin", "Viewers", "Tools", "Hub Admin", and "Community Participant Simulator". The "Hub Admin" menu is expanded to show "Hub Configuration" and "Console Configuration". The "Hub Configuration" menu is further expanded to show "Event Codes", "Targets", "Document Flow Definition", "XML Formats", "Validation Maps", and "Actions". The "Targets" menu item is selected. The page displays the "Target Details" screen, which includes a "Welcome, Hub Administrator" message and a "List" link. The form fields are: "Target Name" (text input), "Status" (radio buttons for "Enabled" and "Disabled"), "Description" (text area), and "Transport" (dropdown menu with "Select Transport Type" selected). The page footer includes the "WebSphere software" logo and the "Done" button.

Figure 2-3. Target Details Screen

- Complete the following parameters in the screen:

Table 2-5. Target Details

Parameter	Description
Target Name	Name used to identify the target.
Status	Allow (Enabled) or deny (Disabled) the system to access this target.
Description	Text that describes the function or other characteristic of this target.
Transport	One of the following transport types: <ul style="list-style-type: none"> FTP Directory — see “FTP Directory” on page 26 JMS — see “JMS” on page 27 POP3 — see “POP3” on page 27 HTTP/S — see “HTTP/S” on page 28 File Directory — see “File Directory” on page 28

FTP Directory

If you selected **FTP Directory** as the transport, perform the following procedure.

- Complete the following parameters in the screen:

Table 2-6. FTP Directory

Parameter	Description
FTP Root Directory	Location of the root directory where you want the FTP receiver to poll. For example: <ul style="list-style-type: none"> UNIX - /data/router/ftp Windows - C:/data/router/ftp Note: Use forward slashes for both UNIX and Windows
File Unchanged Interval	Number of seconds the file size must remain unchanged before the Document Manager retrieves it for processing.
Thread Nbr	Number of documents the Document Manager will process simultaneously.
Exclude File Ext	File extension for documents the Document Manager will exclude from processing. Examples may include exe, txt, or doc.

- Click **Add**. The Document Manager ignores all documents with the displayed file extension. Click **Remove** to delete a file extension from the exclusion list.

NOTE: Do not type a dot in front of the file name extension (for example, .exe or .txt). Just type the characters that denote the file extension.

- (Optional) Configure the schedule the Document Manager uses to poll documents from the FTP directory.
- Click **Save**.

JMS

If you selected **JMS** as the transport, perform the following procedure.

1. Click **new** to create the required Gateway Type for this target. All incoming documents to this target will be assigned the displayed Gateway Type. To change an existing Gateway Type, click **edit**.
2. Complete the following parameters in the screen:

Table 2-7. JMS Values

Parameter	Description
JMS Provider URL	URL of name service used to find JMS queue. Examples: JMS MQ Series - file:/D:/JNDI-Directory JBoss - jnp://hplxdev2:1099
User Id	User ID required to access JMS queue. Leave blank if not used.
Password	Password associated to user ID above. Leave blank if not used.
JMS Queue Name	Name of JMS queue.
JMS Factory Name	Name of Java class the JMS provider will use to generate connection to JMS queue.
Provider URL Package	Name of classes (or JAR file) that Java uses to understand JMS Context URL.
JNDI Factory Name	Factory name used to connect to name service.
Time Out	Number of milliseconds that target will monitor JMS queue.
Thread Nbr	Number of documents the Document Manager will process simultaneously.

3. Click **Save**.

POP3

If you selected **POP3** as the transport, perform the following procedure.

1. Click **new** to create the required Gateway Type for this target. All incoming documents to this target will be assigned the displayed Gateway Type. To change an existing Gateway Type, click **edit**.
2. Complete the following parameters in the screen:

Table 2-8. POP3 Values

Parameter	Description
POP3 Server	The name of the POP3 server to be used.
Port Number	Port number assigned to POP3. The default value is recommended.
User Id	User ID required to access port. Leave blank if not used.
Password	Password associated to user ID above. Leave blank if not used.
Time Out	Number of milliseconds that target will monitor the URI.
Thread Nbr	Number of documents the Document Manager will process simultaneously.

3. (Optional) Configure the schedule the Document Manager uses to poll documents from the directory.
4. Click **Save**.

HTTP/S

If you selected **HTTP/S** as the transport, perform the following procedure.

1. Click **new** to create the required Gateway Type for this target. All incoming documents to this target will be assigned the displayed Gateway Type. To change an existing Gateway Type, click **edit**.
2. For **URI**, type the Web address for incoming documents. This address must start with /bcgreceiver. Example: /bcgreceiver/Receiver
3. For **Max Sync Timeout**, type the number of milliseconds a synchronous connection will remain open. For **Max Sync Sim Conn**, type the maximum number of synchronous connections the system will allow.

NOTE: Sync Routing values are global across all HTTP/S targets. Changing these values for a single HTTP/S target affects all HTTP/S targets in the system. Also, these settings on the Target override the Connection Timeout setting on the gateway for the post back to the trading partner for a synchronous document flow.

4. Click **Save**.

File Directory

If you selected **File Directory** as the transport, perform the following procedure.

1. Click **New** to create the required gateway type for this target. Note that you can change an existing gateway type by clicking **Edit**.

2. Complete the following parameters in the screen:



Table 2-9. File Directory Values

Parameter	Description
Document Root Path	Location of the root directory where the directory tree will be built.
Poll Interval	Number of seconds the document manager will use for polling documents from the directory.
File Unchanged Interval	Number of seconds the file size must remain unchanged before the Document Manager retrieves it for processing.
Thread Nbr	Number of documents the Document Manager will process simultaneously.

3. Click **Save**.

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**. The Console displays the Target List screen.
1. Click the  icon next to the target whose details you want to view. The Console displays the Target Details screen (see [Figure 2-3 on page 25](#)).
2. Click the  icon to edit the parameters of the target.
3. Complete the parameters in the screen (see [Table 2-5 on page 26](#)) and the appropriate target configuration screen ([Table 2-6 on page 26](#), [Table 2-7 on page 27](#), [Table 2-9 on page 29](#), or [Table 2-8 on page 28](#)).
4. 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:

1. Click **Hub Admin > Hub Configuration > Targets**. The Console displays the Target List screen.
2. 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 anymore. Note that the deletion occurs immediately. There is no warning message asking you to confirm this step.

1. Click **Hub Admin > Hub Configuration > Targets**. The Console displays the Target List screen.

NOTE: The target in the following step is immediately deleted without a warning message. Be sure that you want to delete the target.
2. Click the  icon next to the target you want to delete.

Implementing Document Flow Definitions

The core of Business Integration Connect is connectivity between disparate business processes, protocols, and delivery standards. The system handles this connectivity using Document Flow Definitions. A Document Flow Definition is a collection of metadata that defines how Business Integration Connect processes a specific set of documents. This information includes the name, version, type, attributes, and context to which the Document Flow Definition belongs.

Setting up B2B connectivity involves implementing Document Flow Definitions using the following steps:

1. [“Creating Document Flow Definitions” on page 32](#) or using definitions contained in packages (see [“Uploading RNIF packages” on page 35](#) for information).
2. [“Setting Document Flow Definition attributes” on page 37](#).
3. [“Editing attribute values” on page 38](#).
4. [“Enabling and disabling Document Flow Definitions” on page 38](#).
5. [“Creating interactions” on page 42](#)
6. [“Enabling, disabling, or editing interactions” on page 42](#)

About Document Flow Definition types

Each Document Flow Definition has a type. The type describes a particular aspect of the documents handled by the definition. The types are:

- **Package** - specifies the document format, packaging, encryption, and content-type of the documents.

- Protocol - specifies the structure and location of processing and routing information within the documents.
- Document Flow - specifies the business process or transaction to which the documents belong. For example, if the documents are part of a RosettaNet exchange, the Document Flow identifies the PIP.
- Activity - specifies the business function within the process or transaction.
- Action - specifies the actual electronic documents exchanged in the business process or transaction.
- Signal - specifies a document sent in response to the action.

The Manage Document Flow Definitions screen displays these Document Flow Definitions in a tree with Package type being topmost in the tree and the Signal type being the lowest. The following illustrates the hierarchical relationship of the Document Flow Definitions:



Provided Document Flow Definitions

Business Integration Connect has several Document Flow Definitions already installed and uploaded that you can use. These Document Flow Definitions are:

Package

- AS1 (Applicability Statement 1 standard)
- AS2 1.0 / 1.1 (Applicability Statement 2 standard)
- Backend Integration (a proprietary standard for custom back-end integration)

NOTE: When using the transport-envelope element in documents containing attachments, the following xmlns attribute must be used when sending outbound documents from the Community Manager to a Participant:

```
<transport-envelope xmlns http://www.ibm.com/websphere/bcg/2003/v1.0/wbipackaging.">
```

For documents containing attachments, the payload portion of the document must be base-64 encoded.

Protocol

- Binary (a general use protocol used for pass-through routing of binary documents requiring no validation or transformation)
- XML Event (a general protocol for custom back-end integration)

Document Flow

- Binary (a document flow for pass-through routing of binary documents)
- XML Event (a document flow for routing status events for custom documents)

About Document Flow Definition contexts

Because of the many different business processes and protocols available for B2B communications to use, Business Integration Connect uses contexts to support their various combinations. A context provides the information that Business Integration Connect uses to receive or send documents of a particular process and protocol. It also provides Business Integration Connect with the information to transform and validate the documents. The collection of contexts describe the B2B capabilities of the Community Participant or Community Manager.

A context consists of a specific set of linked Document Flow Definitions. Each level of the context has a different Document Flow Definition type. The Package type is at the top of the context chain. The Protocol type is a child of the Package type and so on down the context chain to the Signal type. The following is an example of a context for handling a specific RosettaNet acknowledgement message:

Package: RNIF (V02.00)

Protocol: RosettaNet (V02.00)

Document Flow: 3A4 (V02.02) "Request Purchase Order"

Activity: Request Purchase Order

Action: Purchase Order Request Action

Signal: Receipt Acknowledgement

The Package, Protocol, and Document Flow types are mandatory in the context. The Document Flow may or may not have an Activity or its subtypes.

Creating Document Flow Definitions

Document Flow Definitions define how Business Integrate Connect handles specific documents. You can upload already defined Document Flow Definitions or you can create Document Flow Definitions. For information on how to upload preconfigured Document Flow Definitions, see [“Uploading RNIF packages” on page 35](#). The following procedure describes how to create Document Flow Definitions using the Community Console.

NOTE: When creating Document Flow Definitions to send EDI messages to a community participant, these definitions must be part of context that has the Backend Integration package rather than the None package. This is because EDI messages are binary data and Business Integration Connect requires the Backend Integration headers to route the message. For information on these headers and the Backend Integration package, see the Integration Overview document.

When a context has a custom XML protocol in a Backend Integration package, Business Integration Connect obtains the protocol, protocol version, process, and process version information from the Backend Integration headers rather than from the protocol in the context. When a context has a custom XML format combined with any other package such as AS1, AS2, None, or RNIF, Business Integration Connect obtains the protocol, protocol version, process, and process version from the element path defined in the XML format guideline.

To create Document Flow Definitions, use the following procedure:

1. Click **Hub Admin > Hub Configuration > Document Flow Definition**.

2. Click **Create Document Flow Definition**. The Console displays the Manage Document Flow Definitions screen.
3. In Manage Document Flow Definitions, set the following parameters in the screen:

Table 2-10. Document Flow Definition Parameters

Parameter	What to do
Document flow type	<p>Select one of the following types:</p> <ul style="list-style-type: none"> • Package - specifies the document format, packaging, encryption, and content-type identification. • Protocol - specifies the structure and location of information within the document needed for processing and routing. • Document Flow - specifies the process being used to perform the business transaction. • Activity - specifies the business function within the process. • Action - specifies the source document sent in the activity. <p>Note that you do not need to create Document Flow Definitions for Signals because they are a subtransaction in a RosettaNet process.</p>
Code	<p>If you selected Protocol in the Document flow type field above, identify the specific protocol in this field such as RNSC, RosettaNet, or Binary.</p> <p>If you selected Document Flow in the Document flow type field above, identify the specific process in this field. For example, if you are creating a Document Flow for RosettaNet, type the name of the PIP in this field.</p> <p>If you selected Activity or Action in the Document flow type field above, type the name of the Activity or Action in this field. For a RosettaNet Document Flow Definition, use the value specified for the Activity or Action in the PIP specification.</p> <p>For Package and Signal types, Business Integration Connect ignores the code.</p>
Name	Type the name of the Document Flow Definition. For Activity and Action types, the name must match the name in the Code field above.
Version	Type the version of Document Flow Definition.
Description	Type a description of the Document Flow Definition.
Document level	<p>Select Yes if the Document Flow Definition you are creating is the level at which Business Integration Connect exchanges documents. For example, with RosettaNet, Business Integration Connect exchanges documents at the Document Flow level but with a Binary interaction, it exchanges documents at the Protocol level.</p> <p>Select No if Business Integration Connect does not exchange documents at the level of this Document Flow Definition</p>

Table 2-10. Document Flow Definition Parameters

Parameter	What to do
Status	Select Enabled to make Document Flow Definition available to the system.
Visibility	Select which type of user and above can see this Document Flow Definition in the Community Console.

The Validation maps field displays the validation map associated to this definition or the "No maps found" message if a validation map has not been assigned.

4. In the Document Flow Definition tree, select the parent Document Flow Definition.
5. Click **Save**.

Once you have created a Document Flow Definition, set its attributes. See [“Setting Document Flow Definition attributes” on page 37](#) for information on how to do this.

NOTE: When using the transport-envelope element in documents containing attachments, the following xmlns attribute must be used when sending outbound documents from the Community Manager to a Participant:



```
<transport-envelope xmlns="http://www.ibm.com/websphere/bcg/2003/v1.0/wbipackaging">
```

Creating content filters

A content filter will either include or exclude the attachment of files to a document flow definition. This filter is set at the package level, and applies only to the Backend Integration package. The filter includes the following features:

- Inclusion - filter will allow attachments based on selected content type.
- Exclusion - system will strip an excluded attachment but continue to process and route document.
- All content types - select to either include or exclude all attachments.
- Only the content types in list - select if a particular MIME content type is either included or excluded based on the filter selection. Examples include: application/octet-stream, application/postscript, audio/basic, image/jpeg, etc.

To create a content filter

1. Click **Hub Admin > Hub Configuration > Document Flow Definition**.
2. Click  adjacent to **Package : Backend Integration**.
3. Click  to view package details.
4. Apply filter as needed.
5. Click **Save**.

Uploading RNIF packages

Business Integration Connect provides a way to import already defined RNIF Document Flow Definitions and maps. These definitions or maps are stored in ZIP archives called packages. For examples of packages, see the RNIF packages installed in the B2BIntegrate directory.

For information on exporting definitions, see [“Downloading packages” on page 36](#).

To upload a RNIF Document Flow Definition package, use the following procedure.

NOTE: When uploading a source package, target package, and their valid interaction within the same ZIP file, the interaction data will fail to upload. This is due to the system’s default behavior of storing the interaction data within the source package, and loading the source package into the database before the target package. However, the interaction data requires that the target package already exist in the database in order to load successfully.

To resolve the failed interaction upload, either repeat uploading the original ZIP file since the target package will already be in the database and previously loaded data is skipped during subsequent uploads. Or first upload the target package in a separate ZIP file, then upload the source package.

1. Click **Hub Admin > Hub Configuration > Document Flow Definition**.
2. Click **Upload/Download Packages**.
3. Ensure that WSDL Package is set to No.
4. Complete the following parameters in the screen:

Table 2-11. Upload/Download RNIF Package

Parameter	Description
File	Type the path and name of the package ZIP file or browse and select the file. IMPORTANT: The files within the ZIP archive must be within a directory titled Packages. For example: Packages/AS1.xml.
Commit to database	To test the importing of the package, select No . This option enables you to troubleshoot upload errors before committing the package contents to the Business Integration Connect database. To import the package, select Yes .
Overwrite data	To preserve any matching packages in the database, select No . You would choose this option, for example, if you are uploading Package_RNIF_V02.00.zip and Package_RNIF_1.1.zip has already been loaded. To replace any matching packages in the database, select Yes .

Note that you only use the Web Service Public URL field when you are uploading WSDL (Web Service Definition Language) files.

5. Click **Upload**. The package is installed into the system.

IMPORTANT: When uploading a source package, target package, and their valid interaction within the same ZIP file, the interaction data will fail to upload. This is due to the system's default behavior of storing the interaction data within the source package, and loading the source package into the database before the target package. However, the interaction data requires that the target package already exist in the database in order to load successfully.

To resolve the failed interaction upload, either repeat uploading the original ZIP file since the target package will already be in the database and previously loaded data is skipped during subsequent uploads. Or first upload the target package in a separate ZIP file, then upload the source package.

Validating packages using schema files

A set of XML schemas that describe the XML files that can be uploaded through the console is provided on the Business Integration Connect installation medium. Uploaded files are validated against these schemas. The schema files are a useful reference for determining the cause of an error when a file cannot be uploaded because of non-conforming XML. The files are: `packageConfig.xsd` and `packageConfigDbTables.xsd`, which contain the schema describing valid package (non-Web service) XML files.

The files are located in the following directory on the installation medium:

```
B2BIntegrate\packagingSchemas
```

Downloading packages

To download a package to a local computer, use the following procedure.

NOTE: When downloading a public WSDL file, Internet Explorer appends a ".1" to the end of the file. You must remove the ".1" and resave the file to avoid errors.

1. Click **Hub Admin > Hub Configuration > Document Flow Definition**.
2. Click **Upload/Download Packages**.
3. To download all packages, leave all boxes unchecked. To download a specific Package, Protocol or Document Flow level definition, select the closed folder icons to expand the Document Flow Definition tree until you can see the definition you want to download. Enable the box beside that definition. You can select more than one definition.
4. If you want to specify a name for the package, type a name in the File name field.
5. Click **Download**.

You may see a dialog in which you can specify where to download the ZIP file. If this happens, browse to where you want to save the file and then save it.

NOTE: If you extract files from the ZIP file, ensure that you preserve the directory structure contained in the ZIP file when you place the files back into the ZIP file. This guarantees that you can successfully upload the package after making any modifications.

About Document Flow Definition attributes

The attributes of a Document Flow Definition provide information on how to process the documents, validate the structure of the documents, check for encryption, and specify how many attempts Business Integration Connect makes to process the document before failing.

The highest level Document Flow Definition in the hierarchy is the Package, and attributes assigned to a package are global to all the other Document Flow Definitions that are below the package in the hierarchy.

A Document Flow Definition has inherited attributes and may have added attributes. Inherited attributes are attributes received from the parent Document Flow Definition in the hierarchy. Added attributes are attributes that you add specifically to this Document Flow definition using the Community Console. Note that any child Document Flow Definitions inherit these added attributes.

You can override inherited attributes by setting and adding values to the lower level definitions individually. For example, you can change an attribute set at the Package level at the lower level.

Setting Document Flow Definition attributes

Once you have created a Document Flow Definition, you should set it up by adding attributes. The following procedure describes how to add attributes based on the context of the new Document Flow Definition. You can also add them while editing the attribute values of the Document Flow Definition.

To set Document Flow Definition attributes, use the following procedure.

1. Click **Hub Admin > Hub Configuration > Document Flow Definition**.
2. Click the closed folder icon to individually expand a node to the appropriate Document Flow Definition level or select All to expand the entire tree.
3. Click the View Document Flow Definition Details icon to view the attributes for the selected Document Flow Definition.
4. In the **Document Flow Definition Contexts** section, you can either select attributes from a pre-defined list or clone attributes from a different Document Flow Definition of the same type within the same Package or from the same Document Flow Definition in another package. For example, say you are creating a RNSC protocol. You can clone its attributes from a RosettaNet protocol as long as the two protocols are in the same package or you can clone its attributes from another RNSC protocol that is in a different package.

NOTE: You can only clone attributes from enabled Document Flow Definitions.

NOTE: For two-action PIPS such as 3A4, Business Integration Connect only uses the following attributes for the confirmation action:

Time To Acknowledge
Retry Count
Signature Required
Encryption
Validation Map

To select attributes from a list:

1. In the Document Flow Definition Contexts section, select **Select attributes from a list** in one of the definitions.
2. Click the Setup of attributes icon to view the attribute list.
3. From the list, select the attributes for the Document Flow Definition. Note that some attributes may already be selected. The Document Flow Definition has inherited these attributes from higher level Document Flow Definitions.
4. Click **Save**.

To clone attributes from another Document Flow Definition:

1. In the Document Flow Definition Contexts section, select **Clone from an existing object in this context**.
2. Click the Setup of attributes icon to view the attribute list.
3. In the **Document Flow Definition Peers** section, beside the Document Flow Definition that you want to clone, click **Clone**.

Editing attribute values

After you define the attributes for a Document Flow Definition, use the following procedure to edit the values for each attribute.

1. Click **Hub > Hub Configuration > Document Flow Definition**.
2. Click the closed folder icon to individually expand a node to the appropriate Document Flow Definition level or select All to expand the entire tree.
3. In the Actions column, click the edit attribute values icon in the same row as the Document Flow Definition whose attributes you want to edit. The Console displays a list of defined attributes under **Document Flow Context Attributes**.
4. For each attribute you want to change, do one of the following:
 - a. To select or type a new value, use the field in the **Update** column.
 - b. To clear the attribute value, enable the box in the **Reset** column.

IMPORTANT: Resetting the attribute value at the Global Package level will result in a null value in the database for that attribute. Ensure an actual value is used for the attribute to avoid document failure.

5. Click **Save**.

Note that you can also add attributes by clicking **Add New Attribute** and selecting the attribute to add from the list.

Enabling and disabling Document Flow Definitions

If a Document Flow Definition is disabled, you cannot use it to create a connection. All existing connections continue to function. Note that if a Document Flow Definition is disabled, all of its child Document Flow Definitions and their descendants are also disabled regardless of whether they are individually set to enabled. The peers and parent of the disabled Document Flow Definition are not affected.

To enable or disable a Document Flow Definition, use the following procedure.

1. Click **Hub > Hub Configuration > Document Flow Definition**.
2. Click the closed folder icon to individually expand a node to the appropriate Document Flow Definition level or select All to expand the entire tree.
3. In the **Status** column, click **Enabled** to place the Document Flow Definition online or **Disabled** to place the Document Flow Definition offline.
4. In the confirmation dialog, click **OK**.

About interactions

To provide routing functionality, Business Integration Connect combines two contexts into an interaction. One context in the interaction receives the documents and the other sends them. Business Integration Connect automatically creates a connection between the backend application and the Community Participant based on the interaction.

You must create an interaction:

- For each individual document (or message) exchanged in a document flow. For example, for a two action PIP, you must create an interaction for the first action and create another interaction for the second action.
- For any transaction requiring a connection between a backend application and a Community Participant.

Each interaction that includes a transformation requires a transformation map (XSLT). This map converts data from one protocol format to another. The following table lists the supported Document Flow Definitions for messages going from the Community Participant to Business Integration Connect and the functionality supported by Business Integration Connect:

Table 2-12. Community Participant to Business Integration Connect supported Document Flow Definitions

From Package	To Package	From Protocol	To Protocol	Manage States	Pass Through	Duplicate Check	Validate	Translate
RNIF 1.1	Backend Integration	RN	RNSC	X			X	X
RNIF 1.1	Backend Integration	RN	XML	X			X	X
RNIF 1.1	Backend Integration	RN	RN		X			
RNIF 2.0	Backend Integration	RN	RNSC	X			X	
RNIF 2.0	Backend Integration	RN	XML	X			X	
RNIF 2.0	Backend Integration	RN	RN		X			
None	Backend Integration	Binary	Binary		X			
None	Backend Integration	XML	XML		X			
None	Backend Integration	XML	XML			X	X	X
None	Backend Integration	XML	XML			X	X	
None	Backend Integration	XML	XML			X		
None	Backend Integration	XML	XML				X	X

Table 2-12. Community Participant to Business Integration Connect supported Document Flow Definitions

From Package	To Package	From Protocol	To Protocol	Manage States	Pass Through	Duplicate Check	Validate	Translate
None	Backend Integration	XML	XML					X
None	Backend Integration	XML	XML				X	
AS2	Backend Integration	Binary	Binary	X	X			
AS2	Backend Integration	XML	XML	X	X			
AS2	Backend Integration	XML	XML	X		X	X	X
AS2	Backend Integration	XML	XML	X		X	X	
AS2	Backend Integration	XML	XML	X		X		
AS2	Backend Integration	XML	XML	X			X	X
AS2	Backend Integration	XML	XML	X				X
AS2	Backend Integration	XML	XML	X			X	
None	None	Web Service (SOAP)	Web Service (SOAP)		X			
None	None	cXML	cXML		X		X	

The following table lists the supported Document Flow Definitions for messages going from Business Integration Connect to a Community Participant and the functionality supported by Business Integration Connect: .

Table 2-13. Business Integration Connect to Community Participant supported Document Flow Definitions

From Package	To Package	From Protocol	To Protocol	Manage States	Pass Through	Content-level Duplicate Check	Validate	Translate
Backend Integration	RNIF 1.1	RNSC	RN	X			X	
Backend Integration	RNIF 1.1	XML	RN	X		X	X	X
Backend Integration	RNIF 1.1	XML	RN				X	X
Backend Integration	RNIF 2.0	RNSC	RN	X			X	

Table 2-13. Business Integration Connect to Community Participant supported Document Flow Definitions (continued)

From Package	To Package	From Protocol	To Protocol	Manage States	Pass Through	Content-level Duplicate Check	Validate	Translate
Backend Integration	RNIF 2.0	XML	RN	X		X	X	X
Backend Integration	RNIF 2.0	XML	RN				X	X
Backend Integration	AS2	Binary	Binary	X	X			
Backend Integration	AS2	XML	XML	X	X			
Backend Integration	AS2	XML	XML	X		X	X	X
Backend Integration	AS2	XML	XML	X		X	X	
Backend Integration	AS2	XML	XML	X		X		
Backend Integration	AS2	XML	XML	X			X	X
Backend Integration	AS2	XML	XML					X
Backend Integration	AS2	XML	XML	X			X	
Backend Integration	None	Binary	Binary		X			
Backend Integration	None	XML	XML		X			
Backend Integration	None	XML	XML			X	X	X
Backend Integration	None	XML	XML			X	X	
Backend Integration	None	XML	XML			X		
Backend Integration	None	XML	XML				X	X
Backend Integration	None	XML	XML					X
Backend Integration	None	XML	XML				X	
Backend Integration	None	XML	cXML		X		X	

Table 2-13. Business Integration Connect to Community Participant supported Document Flow Definitions (continued)

From Package	To Package	From Protocol	To Protocol	Manage States	Pass Through	Content-level Duplicate Check	Validate	Translate
None	None	Web Service (SOAP)	Web Service (SOAP)		X			
None	None	cXML	cXML		X		X	

Creating interactions

To create interactions, use the following procedure.

1. Click **Hub Admin > Hub Configuration > Document Flow Definition**.
2. Click **Manage Interactions**.
3. Click **Create a Valid Interaction**.
4. In the Source Document Flow Definition tree, click the closed folder icon to individually expand a node to the appropriate Document Flow Definition level or select All to expand the entire tree.
5. Select the Document Flow Definition you want as the source of the interaction.
6. In the Target Document Flow Definition tree, click the closed folder icon to individually expand a node to the appropriate Document Flow Definition level or select All to expand the entire tree.
7. Select the Document Flow Definition you want as the destination of the interaction.
8. If you need to translate data from one protocol to another, in the **Transform Map Document** field type the name of the transformation map file or click **Browse** to navigate to the file.
9. Optionally, in the Transform Map Description field, type a description.
10. In the **Action** field, select the action that Business Integration Connect is to perform in this interaction.
11. Click **Save**.

Enabling, disabling, or editing interactions

To enable, disable or edit interactions, use the following procedure.

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 red X 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 red X icon with a green checkmark icon to show that you have enabled the interaction.
6. To disable an interaction, click the green checkmark 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 green checkmark icon with a red X icon to show that you have enabled the interaction.
7. To edit an interaction, click the edit icon next to the interaction. A window appears with controls for editing the interaction. Perform your edits and click **Save**.

About validation maps

Business Integration Connect uses validation maps to validate the structure of documents. An Action can have an associated validation map to ensure that the destination Community Participant or backend application can parse the document. Note that a validation map only validates the structure of the document. It does not validate the contents of the message.

NOTE: Once you associate a validation map to a Document Flow Definition, you cannot disassociate them. This prevents Business Integration Connect from deactivating existing connections based on the Document Flow Definition.

Adding validation maps

To add a new validation map to a Business Integration Connect, use the following procedure.

1. Save the validation map file to the Business Integration Connect server or to a location from which Business Integration Connect can read files
2. Click **Hub Admin > Hub Configuration > Validation Maps**.
3. Click **Create**.
4. Complete the following parameters in the map update screen:

Table 2-14. Manage Maps Screen

Parameter	Description
Description	Type a description of the validation map.
Choose A File	Type the path and name of the schema file you want to use to validate documents.

5. Click **Save**.

Updating validation maps

To update a validation map currently in the system, use the following procedure.

1. Click **Hub Admin > Hub Configuration > Validation Maps**.
2. Click the download icon to save the validation map to your local computer.
3. You may see a dialog in which you can specify where to download the ZIP file. If this happens, browse to where you want to save the file and then save it.

4. Update the map file as needed.
5. Click the upload icon.
6. Type the path to the updated map file or browse and select it.

Associating maps to Document Flow Definitions

To associate a validation map to a Document Flow Definition, use the following procedure.

1. Click **Hub Admin > Hub Configuration > Validation Maps**. The Console displays the Manage Maps screen.
2. Click the edit icon next to the validation map you want to associate to the Document Flow Definition.
3. Click the closed folder icon to individually expand a node to the Action Document Flow Definition level or select All to expand the entire tree.
4. Select the Document Flow Definition you want associated with the validation map.
5. Click **Save**.
6. When prompted, save the exported file.

Configuring RosettaNet support

RosettaNet is an organization that provides open standards to support the exchange of business messages between trading partners. For more information on RosettaNet, see <http://www.rosettanet.org>. The standards include RosettaNet Implementation Framework (RNIF) and Partner Interface Process (PIP) specifications. RNIF defines how trading partners exchange messages by providing a framework of message packaging, transfer protocols, and security. There are two released versions: 1.1 and 2.0. A PIP defines a public business process and the XML-based message formats to support the process.

Business Integration Connect supports RosettaNet messaging using RNIF 1.1 and 2.0. Once Business Integration Connect receives a PIP message, it validates and transforms the message to send it to the appropriate backend application. Business Integration Connect provides a protocol for packaging the transformed message into a RosettaNet Service Content (RNSC) message that the backend application can handle. See the Integration Overview for information on packaging used on these messages to provide routing information. Business Integration Connect can also receive RNSC messages from backend applications and create the appropriate PIP message and send the message to the appropriate trading partner (a Community Participant). To provide this functionality, all Business Integration Connect requires are the Document Flow Definitions for the RNIF version and the PIPs you want to use.

In addition to providing routing capability for RosettaNet messages, Business Integration Connect maintains a state for each message it handles. This enables it to resend any messages that fail until the number of attempts reaches a specified threshold. Business Integration Connect also provides Event Notification mechanism to alert backend applications if it is unable to deliver a PIP message. Additionally, Business Integration Connect can automatically generate 0A1 PIPs to send to appropriate Community Participants if it receives certain Event Notification messages from backend applications. See the Integration Overview for more information on Event Notification.

RNIF and PIP document flow packages

To support RosettaNet messaging, Business Integration Connect provides two sets of ZIP files called packages. The *RNIF packages* consist of Document Flow Definitions required to support the RNIF protocol. These packages are in the B2BIntegrate directory.

For RNIF V1.1

- Package_RNIF_1.1.zip
- Package_RNSC_1.0_RNIF_1.1.zip

For RNIF V02.00

- Package_RNIF_V02.00.zip
- Package_RNSC_1.0_RNIF_V02.00.zip

The first package in each pair provides the Document Flow Definitions required to support RosettaNet communications with Community Participants and the second package provides the Document Flow Definitions required to support RosettaNet communications with backend applications.

The second set of packages is PIP document flow packages. Each PIP document flow package has a Packages directory containing an XML file and a GuidelineMaps directory containing XSD files. The XML file specifies the Document Flow Definitions that define how Business Integration Connect handles the PIP and define the exchanged messages and signals. The XSD files specify the format of the PIP's messages and define acceptable values for XML elements in the messages. The ZIP files for 0A1 PIPs also have an XML file that Business Integration Connect uses as template to create 0A1 documents.

The PIPs for which Business Integration Connect provides PIP document flow packages are:

- PIP 0A1 Notification of Failure v1.0
- PIP 0A1 Notification of Failure V02.00.00
- PIP 2A12 Distribute Product Master V01.03.00
- PIP 3A1 Request Quote V02.00.00
- PIP 3A2 Request Price and Availability R02.01.00B
- PIP 3A4 Request Purchase Order V02.02.00
- PIP 3A5 Query Order Status R02.00.00
- PIP 3A6 Distribute Order Status V02.02.00
- PIP 3A7 Notify of Purchase Order Update V02.02.00
- PIP 3A8 Request Purchase Order Change V01.02.00
- PIP 3A9 Request Purchase Order Cancellation V01.01.00
- PIP 3B2 Notify of Advance Shipment V01.01.00
- PIP 3C3 Notify of Invoice V01.01.00
- PIP 3C4 Notify of Invoice Reject V01.00.00

- PIP 3C6 Notify of Remittance Advice V01.00.00
- PIP 3D8 Distribute Work in Process V01.00.00
- PIP 4A1 Notify of Strategic Forecast V02.00.00
- PIP 4A3 Notify of Threshold Release Forecast V02.00.00
- PIP 4A5 Notify of Forecast Reply V02.00.00
- PIP 4B2 Notify of Shipment Receipt V01.00.00
- PIP 4C1 Distribute Inventory Report V02.03.00
- PIP 5C1 Distribute Product List V01.00.00
- PIP 5C4 Distribute Registration Status V01.02.00
- PIP 5D1 Request Ship From Stock And Debit Authorization V01.00.00
- PIP 7B1 Distribute Work in Process V01.00.00

For each PIP, there are four PIP document flow packages:

- For RNIF 1.1 messaging with Community Participants
- For RNIF 1.1 messaging with backend applications
- For RNIF 2.0 messaging with Community Participants
- For RNIF 2.0 messaging with backend applications

Each PIP document flow package follows a specific naming convention so that you can identify the whether the package is for messages between Business Integration Connect and Community Participants or between Business Integration Connect and backend applications. The naming convention also identifies the RNIF version, PIP, and PIP version that the package supports. For PIP document flow packages used for messaging between Business Integration Connect and Community Participants, the format is:

`BCG_Package_RNIF<RNIF version>_<PIP><PIP version>.zip`

For PIP document flow packages used for messaging between Business Integration Connect and backend applications, the format is:

`BCG_Package_RNSC<Backend Integration version>_RNIF<RNIF version>_<PIP><PIP version>.zip`

For example, the `BCG_Package_RNIF1.1_3A4V02.02.zip` is for validating documents for version 02.02 of the 3A4 PIP sent between Community Participants and Business Integration Connect using the RNIF 1.1 protocol. For PIP document flow packages for communicating with backend applications, the name of the package must also identify the protocol used to send the RosettaNet contents to the backend applications. See the Integration Overview for information on the packaging used for these messages.

RosettaNet end-to-end flows

To support RosettaNet PIPs, Business Integration Connect must support the request, response, and acknowledgement messages required by the PIP. The end-to-end flows follow a single PIP as it enters Business Integration Connect. The end-to-end flows finish when Business Integration Connect has sent or received the final message required by the PIP and any resulting transport messages.

The flows shown in this section are for asynchronous Rosettanet processing. Differences in the flows do exist for synchronous RosettaNet processing. These differences called out in each section.

Two action PIP initiated by a community participant

This end-to-end flow describes how Business Integration Connect handles a two action PIP that a Community Participant has initiated. In particular, it describes the messaging that occurs between the Community Participant, Business Integration Connect, and a backend application. It starts from when the Community Participant sends the PIP request message. It ends when Business Integration Connect has sent the response from the backend application to the Community Participant's request and sent an event notification message to the backend application. It also describes how Business Integration Connect handles problems when the end-to-end flow breaks.

In this particular end-to-end flow, Business Integration Connect wraps a PIP message with RosettaNet Service Content (RNSC) headers (Backend Integration packaging) to deliver it to a backend application and then unwraps the PIP response and delivers this message to the Community Participant using RNIF. The description uses HTTP as the transport mechanism between Business Integration Connect and the backend application but the flow can also use JMS.

End-to-end flow

The following process describes what happens when a Community Participant sends a two action PIP message to Business Integration Connect. Note that this flow concentrates on the messaging in and out of Business Integration Connect. It does not contain internal steps that are not part of creating, processing, or sending messages. An example of an internal step is saving a message to the non-repudiation database.

1. The Receiver component receives the RNIF PIP request message through an HTTP POST from the Community Participant. The Receiver then persists the request message.
2. The Document Manager retrieves the request message from where the Receiver persisted it.
3. The Document Manager unpacks and decrypts (if necessary) the RNIF message and performs structure-level validation, authentication, and authorization checks. The Document Flow Definitions in the source side of the interaction provide the information that the Document Manager needs to process the message. For example, the validation maps provide the XSD files used to validate the message structure. Depending on which Action is associated with the interaction, the Document Manager performs content-level validation.
4. The Document Manager sets the state of the PIP to indicate that the PIP has been initiated.
5. The Document Manager sends the acknowledgement receipt message to the Community Participant.

NOTE: For synchronous processing in a two way PIP, a separate acknowledgement message is not used.

6. The Document Manager wraps the message according to the Package and Protocol Document Flow Definitions on the target side of the interaction. Note that if the Action is to pass through the message, the Document Manager does not perform the wrapping. For the purpose of describing this flow, the Document Manager wraps the message with Backend Integration packaging to form an RNSC message.
7. The Document Manager sends the RNSC request message to the backend application.
8. The Receiver receives the RNSC response from the backend application and persists it.
9. The Document Manager retrieves the RNSC message and removes the Backend Integration packaging. It creates the RNIF message, validates the structure and contents of the message and, if required, digitally signs and encrypts it.
10. The Document Manager updates the state of the PIP to reflect that it has received the response.
11. The Document Manager sends the RNIF PIP response message.
12. The Receiver receives the receipt acknowledgement message for the PIP response and persists it.
NOTE: For synchronous processing, a separate acknowledgement message is not used.
13. The Document Manager retrieves the response receipt acknowledgement message.
14. The Document Manager updates the state of the PIP to indicate that it has received the response acknowledgement.
15. Because this message is a receipt acknowledgement message, the Document Manager creates an event notification message with a statusCode of 100 to indicate that the Community Participant successfully processed the message and sends it to the backend application.

If a problem occurs in step 1, the receiver does not generate an HTTP 202 message. In effect, the message has not been delivered.

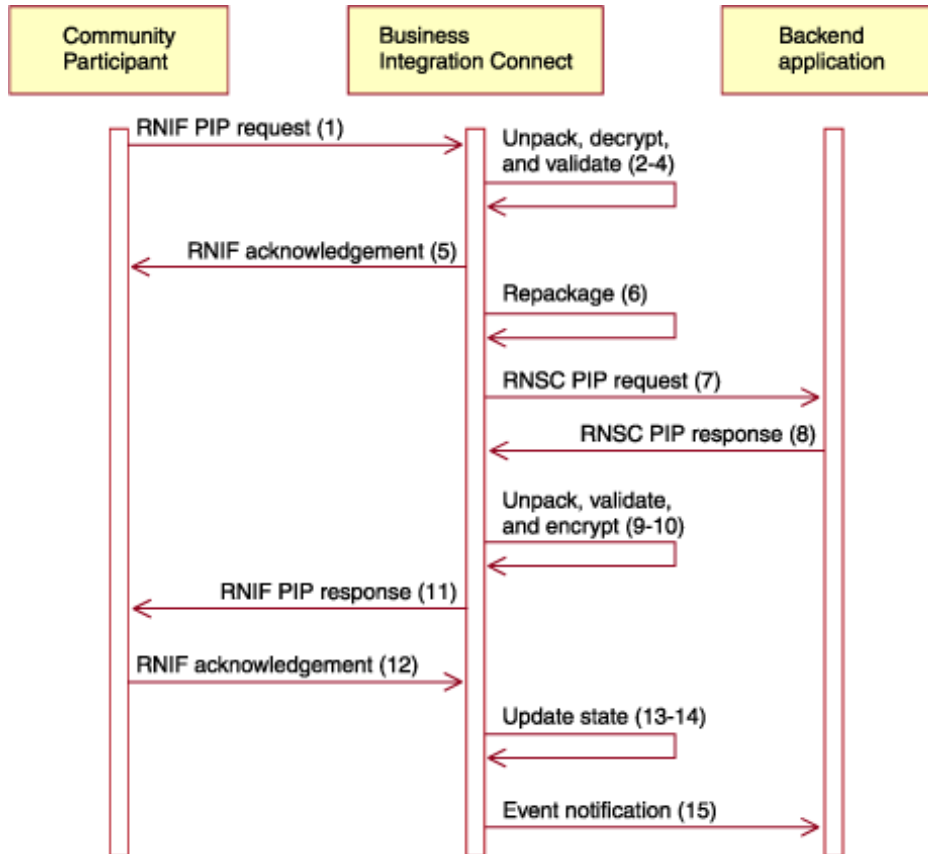
If a problem occurs in steps 2 to 5, Document Manager sends the receipt acknowledgement exception message to the Community Participant to indicate the failure of the PIP.

If a problem occurs at the backend application, the application either sends an event notification to Business Integration Connect with a statusCode of 800 or it ignores the request. When Business Integration Connect receives event notification with the status code 800, the Document Manager creates a 0A1 PIP and sends it to the Community Participant to cancel the request. If the backend application does not send any response to the request, Business Integration Connect waits for the Community Participant to cancel the PIP.

If a problem occurs in steps 12 to 15, the Document Manager creates an event notification message with a statusCode of 900 and sends it to the backend application to roll back the changes made when processing the RNSC content. This also applies if the receipt acknowledgement message contains an exception indicating that the Community Participant could not process the response message.

Sequence diagram

The following sequence diagram shows the messaging that occurs between the Community Participant, Business Integration Connect, and a backend application when the Community Participant initiates a two action PIP.



NOTE: Flows (5) and (12) do not exist for RosettaNet synchronous processing.

For information on what processing is occurring with the messages, see the end-to-end flow description.

Two action PIP initiated by a backend application

This end-to-end flow describes how Business Integration Connect handles a two action PIP that a backend application has initiated. The flow starts when the backend application sends an RNSC message and ends when Business Integration Connect sends an RNSC response message to the backend application. Between these two events, Business Integration Connect sends a RNIF message to the Community Participant and receives a response to that message. The description uses HTTP as the transport mechanism between Business Integration Connect and the backend application but the flow can also use JMS.

End-to-end flow

The following process describes what happens when a backend application sends a two action PIP to a Community Participant through Business Integration Connect. Note that this flow concentrates on the messaging in and out of Business Integration Connect. It does not contain internal steps that are not part of creating, processing, or sending messages. An example of an internal step is saving a message to the non-repudiation database.

1. The Receiver component receives the RNSC request message through an HTTP POST from the backend application. The Receiver then persists the request message.
2. The Document Manager retrieves the request message from where the Receiver persisted it.
3. The Document Manager unpacks the message from its Backend Integration packaging and creates an RNIF PIP request message.
4. The Document Manager performs structure-level validation on the RNIF message using the Document Flow Definitions in the source side of the interaction. Depending on which Action is associated with the interaction, the Document Manager performs content-level validation. The Document Manager then encrypts or signs the RNIF message if required by the PIP configuration.
5. The Document Manager updates the state of the PIP to indicate that the PIP has been initiated.
6. The Document Manager sends the PIP request message to the Community Participant.
7. The Receiver receives the acknowledgement receipt message from the Community Participant and persists it.

NOTE: For synchronous processing in a two-way PIP, a separate acknowledgement message is not used.
8. The Document Manager retrieves the acknowledgement receipt message and updates the state of the PIP to indicate that the Community Participant has received the request message.
9. The Document Manager generates an event notification message with a statusCode of 100. It sends this message to the backend application.
10. The Receiver receives the RNIF PIP response message from the Community Participant and persists it.
11. The Document Manager retrieves the RNIF PIP response message.
12. The Document Manager decrypts the message if it was encrypted and verifies the signature if it was signed. The Document Manager then performs structure-level validation on the message using the Document Flow Definitions in the source side of the interaction. Depending on which Action is associated with the interaction, the Document Manager performs content-level validation.
13. The Document Manager updates the state of the PIP to indicate that the response message has been successfully received.
14. The Document Manager prepares the receipt acknowledgement message for the RNIF PIP response and sends it to the Community Participant.

NOTE: For synchronous processing in a two-way PIP, an acknowledgement message is not used.
15. The Document Manager wraps the PIP response message in Backend Integration Packaging to create an RNSC response message. The Delivery Manager sends the RNSC response message to the backend application.

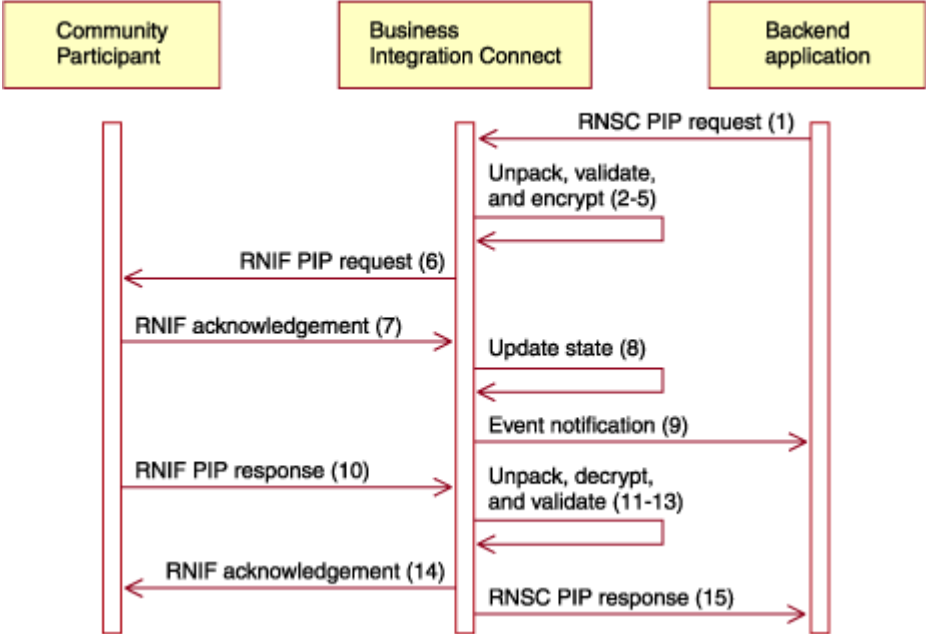
If a problem occurs in step 1, the receiver does not generate an HTTP 202 message. In effect, the message has not been delivered.

If a problem occurs in steps 2 to 7, Document Manager sends an event notification message with a statusCode of 900 to the backend application to indicate a problem with creating, sending, or retrieving the PIP messages from the Community Participant. If Business Integration Connect does not receive the receipt acknowledgement sent in step 6 by a specified time, it checks whether it should resend the PIP request message. If it is under the retry limit, it sends the message again. If it has reached the retry limit, Business Integration Connect generates a 0A1 message and sends it to the Community Participant. Business Integration Connect also sends an event notification message with a statusCode of 900 to the backend application. If Business Integration Connect receives a receipt acknowledgement exception from the Community Participant, it updates the PIP state and sends an event notification message with a statusCode of 900 to the backend application.

If a problem occurs in the Community Participant and the request times out (steps 8 to 15), the Document Manager creates a 0A1 PIP and sends it to the Community Participant to cancel the PIP.

Sequence diagram

The following sequence diagram shows the messaging that occurs between the Community Participant, Business Integration Connect, and a backend application when the backend application initiates a two action PIP.



NOTE: Flows (7) and (14) do not exist for RosettaNet synchronous processing.

For information on what processing is occurring with the messages, see the end-to-end flow description.

One action PIP initiated by a community participant

The end-to-end flow of a one action PIP initiated by a community participant resembles the end-to-end flow a two action PIP. The difference is that the end-to-end flow for a one action PIP does not have steps 8 to 15. These are the steps that process the second action of the two action PIP.

End-to-end flow

1. The Receiver component receives the RNIF PIP request message through an HTTP POST from the Community Participant. The Receiver then persists the request message.

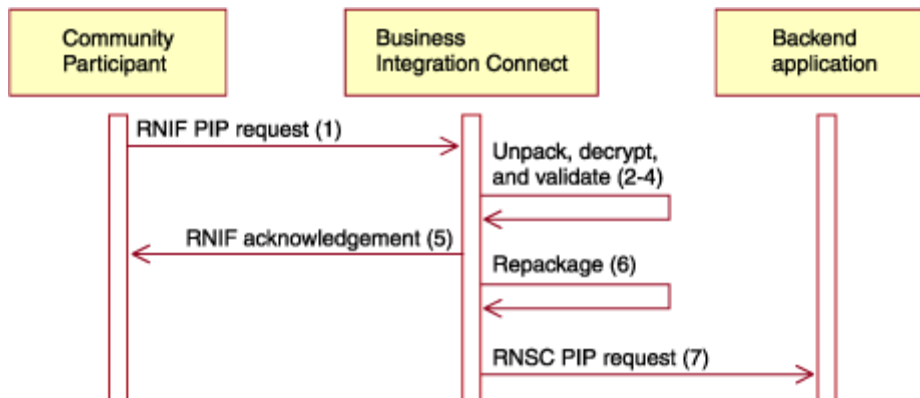
2. The Document Manager retrieves the request message from where the Receiver persisted it.
3. The Document Manager unpacks and decrypts (if necessary) the RNIF message and performs structure-level validation, authentication, and authorization checks. The Document Flow Definitions in the source side of the interaction provide the information that the Document Manager needs to process the message. For example, the validation maps provide the XSD files used to validate the message structure. Depending on which Action is associated with the interaction, the Document Manager performs a content-level validation.
4. The Document Manager sets the state of the PIP to indicate that the PIP has been initiated.
5. The Document Manager sends the acknowledgement receipt message to the Community Participant.

NOTE: For synchronous processing in a one-way PIP, a separate acknowledgement message is not used. The acknowledgement is contained within the http 200 response if it is requested in the TPA, or the option exists to not include the acknowledgement at all in the 200 response (an empty http response).

6. The Document Manager wraps the message according to the Package and Protocol Document Flow Definitions on the target side of the interaction. Note that if the Action is to pass through the message, the Document Manager does not perform the wrapping. For the purpose of describing this flow, the Document Manager wraps the message with Backend Integration packaging to form an RNSC message.
7. The Document Manager sends the RNSC request message to the backend application.

Sequence diagram

The following sequence diagram shows the messaging that occurs between the Community Participant, Business Integration Connect, and a backend application when the Community Participant initiates a one action PIP.



NOTE: Flow (5) exists for HTTP 200 with or without an acknowledgement for RosettaNet synchronous processing.

One action PIP initiated by a backend application

The end-to-end flow of a one action PIP initiated by a community participant resembles the end-to-end flow a two action PIP. The difference is that the end-to-end flow for a one action PIP does not have steps 10 to 15. These are the steps that process the second action of the two action PIP.

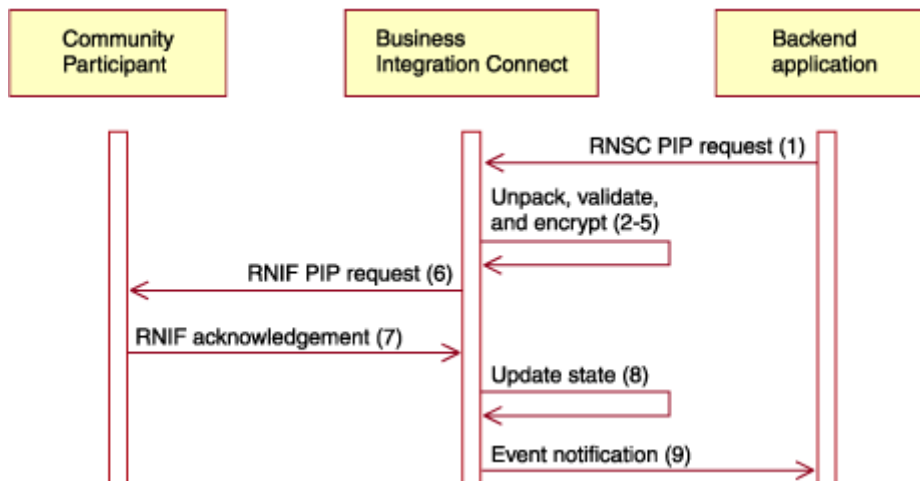
End-to-end flow

The following process describes what happens when a backend application sends a one action PIP to a Community Participant through Business Integration Connect. Note that this flow concentrates on the messaging in and out of Business Integration Connect. It does not contain internal steps that are not part of creating, processing, or sending messages. An example of an internal step is saving a message to the non-repudiation database.

1. The Receiver component receives the RNSC request message through an HTTP POST from the backend application. The Receiver then persists the request message.
2. The Document Manager retrieves the request message from where the Receiver persisted it.
3. The Document Manager unpacks the message from its Backend Integration packaging and creates an RNIF PIP request message.
4. The Document Manager performs structure-level validation on the RNIF message using the Document Flow Definitions in the source side of the interaction. Depending on which Action is associated with the interaction, the Document Manager performs a content-level validation. The Document Manager then encrypts or signs the RNIF message if required by the PIP configuration.
5. The Document Manager updates the state of the PIP to indicate that the PIP has been initiated.
6. The Document Manager sends the PIP request message to the Community Participant.
7. The Receiver receives the acknowledgement receipt message from the Community Participant and persists it.
8. The Document Manager retrieves the acknowledgement receipt message and updates the state of the PIP to indicate that the Community Participant has received the request message.
9. The Document Manager sends an event notification message with a statusCode of 100 to the backend application.

Sequence diagram

The following sequence diagram shows the messaging that occurs between the Community Participant, Business Integration Connect, and a backend application when the backend application initiates a one action PIP.



NOTE: Flow (7) exists for HTTP 200 with or without an acknowledgement for RosettaNet synchronous processing.

Setting up RosettaNet support

For RosettaNet messaging, Business Integration Connect requires the RNIF packages for the version of RNIF used to send the messages. For each PIP that Business Integration Connect supports, it requires the PIP's two PIP document flow packages for the RNIF version. For example, to support the 3A4 PIP over RNIF 2.0, Business Integration Connect requires the following packages:

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

The first package supports RosettaNet messaging with Community Participants and the second package supports RosettaNet messaging with backend applications. The third package and fourth packages enable Business Integration Connect to pass 3A4 messages between Community Participants and backend applications using RNIF 2.0.

To support RosettaNet messaging:

1. If Business Integration Connect does not have the RNIF packages loaded for the version of RNIF you want to use, import them. See [“Uploading RNIF packages” on page 35](#) for information on how to import the packages into Business Integration Connect.
2. For each PIP you want to support, upload the PIP document flow package for the PIP and for the RNIF version you are supporting. For information on the convention used to name these packages, see [“RNIF and PIP document flow packages” on page 45](#). If Business Integration Connect does not provide a package for the PIP or PIP version you want to use, you can create your own and upload it. See [“Creating PIP document flow packages” on page 60](#) for more information.

Creating PIP channels to Community Participants

The following process describes how to create a channel between a backend application and a Community Participant. Note that you must create a channel for each PIP that you want to send and one for each PIP that you want to receive.

Before you begin, ensure that the following conditions apply:

- You are logged in as a Hub Admin.
- The appropriate RNIF Document Flow Definitions have been uploaded and that the packages for the PIP you want to use have been uploaded. See [“Setting up RosettaNet support” on page 54](#) for the names of these packages.

To create a channel for a particular PIP, do the following:

1. Create the interaction for the channel:
 - a. Click **Hub Admin > Hub Configuration > Document Flow Definition**.
 - b. Click **Manage Interactions**.
 - c. Click **Create a Valid Interaction**.

- d. Expand the source Document Flow Definition tree to the Action level and expand the target Document Flow Definition tree to the Action level.
- e. In the trees, select the Document Flow Definitions to use for the source context and the target context. For example, if the community participant is the initiator of a 3C6 PIP (a one action PIP), select the following Document Flow Definitions in the trees:

Table 2-15. 3C6 PIP initiated by a Community Participant

Source	Target
Package: RNIF (V02.00)	Package: Backend Integration (1.0)
Protocol: RosettaNet (V02.00)	Protocol: RNSC (1.0)
Document Flow: 3C6 (V01.00)	Document Flow: 3C6 (V01.00)
Activity: Notify of Remittance Advice	Activity: Notify of Remittance Advice
Action: Remittance Advice Notification Action	Action: Remittance Advice Notification Action

If the backend application is the initiator of the 3C6 PIP, select the following Document Flow Definitions from the trees:

Table 2-16. 3C6 PIP initiated by a backend application

Source	Target
Package: Backend Integration (1.0)	Package: RNIF (V02.00)
Protocol: RNSC (1.0)	Protocol: RosettaNet (V02.00)
Document Flow: 3C6 (V01.00)	Document Flow: 3C6 (V01.00)
Activity: Notify of Remittance Advice	Activity: Notify of Remittance Advice
Action: Remittance Advice Notification Action	Action: Remittance Advice Notification Action

For a two action PIP such as 3A4 initiated by a Community Participant, select the following Document Flow Definitions for the first action:

Table 2-17. 3A4 PIP initiated by a Community Participant

Source	Target
Package: RNIF (V02.00)	Package: Backend Integration (1.0)
Protocol: RosettaNet (V02.00)	Protocol: RNSC (1.0)
Document Flow: 3A4 (V02.02)	Document Flow: 3A4 (V02.02)
Activity: Request Purchase Order	Activity: Request Purchase Order
Action: Purchase Order Request Action	Action: Purchase Order Request Action

If a backend application initiates the two action 3A4 PIP, select the following Document Flow Definitions for the first action:

Table 2-18. 3A4 PIP initiated by a backend application

Source	Target
Package: Backend Integration (1.0)	Package: RNIF (V02.00)
Protocol: RNSC (1.0)	Protocol: RosettaNet (V02.00)
Document Flow: 3A4 (V02.02)	Document Flow: 3A4 (V02.02)
Activity: Request Purchase Order	Activity: Request Purchase Order
Action: Purchase Order Request Action	Action: Purchase Order Request Action

- f. In the Action field, select **Bi-Directional Translation of RosettaNet and RosettaNet Service Content with Validation**.

- g. Click **Save**.
- h. If you are setting up a two action PIP, repeat steps c-g to create the interaction for the second action. For example, select the following Document Flow Definitions for the second action for a 3A4 PIP initiated by a Community Participant. This is the action in which the backend application sends the response.

Table 2-19. 3A4 PIP initiated by a Community Participant (second action)

Source	Target
Package: Backend Integration (1.0)	Package: RNIF (V02.00)
Protocol: RNSC (1.0)	Protocol: RosettaNet (V02.00)
Document Flow: 3A4 (V02.02)	Document Flow: 3A4 (V02.02)
Activity: Request Purchase Order	Activity: Request Purchase Order
Action: Purchase Order Confirmation Action	Action: Purchase Order Confirmation Action

For the second action for a backend application initiated 3A4 PIP, select the following Document Flow Definitions:

Table 2-20. 3A4 PIP initiated by a backend application (second action)

Source	Target
Package: RNIF (V02.00)	Package: Backend Integration (1.0)
Protocol: RosettaNet (V02.00)	Protocol: RNSC (1.0)
Document Flow: 3A4 (V02.02)	Document Flow: 3A4 (V02.02)
Activity: Request Purchase Order	Activity: Request Purchase Order
Action: Purchase Order Confirmation Action	Action: Purchase Order Confirmation Action

2. If a participant profile does not exist for the community participant, create it. See [“Managing Participant profiles” on page 101](#) for information on how to do this. There must also be a participant profile of the Community Manager type for the backend application.
3. If a gateway with the supported protocol does not exist between the community participant and Business Integration Connect or between a backend application and Business Integration Connect, create it. See [“Managing gateway configurations” on page 105](#) for information on how to do this. The supported protocols for RosettaNet messages between a community participant and Business Integration Connect are HTTP and HTTPS. The supported protocols for RosettaNet messages between a backend application and Business Integration Connect are HTTP, HTTPS, and JMS.
4. Activate the Document Flow Definitions that Business Integration Connect uses to process the PIP. To do this, activate the Community Participant's and backend application's definitions for the Package, Protocol, and Document Flow for the PIP. The direction of the message determines which one is the source and which one is the target. Business Integration Connect automatically activates the Activity, Actions, and Signals when you activate the parent Document Flow. For information on how to activate the Document Flow Definitions, see [“Managing B2B capabilities” on page 117](#).

Community Participant

- Package: RNIF (1.1 or V02.00 depending on which RNIF version you are using)
- Protocol: RosettaNet (1.1 or V02.00 depending on which RNIF version you are using)
- Document Flows: *<PIP name and version>*

Backend application

- Package: Backend Integration (1.0)
 - Protocol: RNSC (1.0)
 - Document Flows: *<PIP name and version>*
5. Activate the channel by setting the source and target in the Participant Connections screen. If the community participant is the initiator of the PIP, set the source to the community participant's profile and the target to the community manager profile. If the initiator is a backend application, set the source to the community manager profile and set the target to the community participant's profile. See [“Managing Participant connections” on page 120](#) for information on searching for connections and activating them as a channel. If the PIP is a two action PIP, you must also activate the channel in the other direction to support the second action of the PIP. To do this, the source and target of the second action are the opposite of the source and target of the first action.
 6. If Business Integration Connect does not have a target defined for each of the protocols, create it. See [“Configuring targets” on page 25](#) for information on how to do this.

Editing RosettaNet attribute values

For RosettaNet support, an Action type Document Flow Definition has a specific set of attributes. These attributes provide information used to validate the PIP message, to define the roles and services used in the PIP, and to define the response to the Action. The PIP packages provided by Business Integration Connect automatically define values for these attributes and you usually do not need to change them.

To edit the RosettaNet attributes of an Action Document Flow Definition, do the following:

1. Click **Hub Admin > Hub Configuration > Document Flow Definition**.
2. Click folder icons to individually expand a node to the appropriate Document Flow Definition level or select All to expand the entire tree.
3. The Actions column for each Action Document Flow Definition contains a RosettaNet attributes icon. Click this icon to edit the RosettaNet attributes of the Action. The Console displays a list of defined attributes under RosettaNet Attributes.
4. Complete the following parameters under RosettaNet Attributes. (These attributes are defined automatically when a PIP is uploaded to the system.)

Table 2-21. RosettaNet attributes

RosettaNet Attribute	Description
DTD Name	Identifies the name of the action of the PIP in the DTD provided by RosettaNet
From Service	Contains the network component service name of the community participant or backend application that is sending the message
To Service	Contains the network component service name of the community participant or backend application that is receiving the message
From Role	Contains role name of community participant or backend application that is sending the message

Table 2-21. RosettaNet attributes

To Role	Contains role name of community participant or backend application that is receiving the message
Root Tag	Contains the name of the root element in the PIP message's XML document
Response From Action Name	Identifies the next Action to perform in the PIP

NOTE: If the Console displays the "No attributes were found" message, the attributes have not been defined. See [“Setting Document Flow Definition attributes” on page 37](#) for information about how to define the attributes.

5. If the Console displays this message for a lower-level definition, the definition may still work, since it inherits the attributes of the higher-level definition. Adding attributes and their values overrides the inherited attributes and changes the functionality of the Document Flow Definition.
6. Click **Save**.

Configuring attribute values

For PIP Document Flow Definitions, most of the values of the attributes are already set and do not need configuring. However, you do need to set the following attributes:

RNIF (1.0) package

- **GlobalSupplyChainCode** - Identify the type of supply chain used by the Community Participant. The types are Electronic Components, Information Technology, and Semiconductor manufacturing. This attribute does not have a default value.

RNIF (V02.00) package

- **Encryption** - Set whether the PIPs must have an encrypted payload, an encrypted container and payload, or no encryption. The default value is None.
- **Sync Ack Required** - Set to yes if the trading partner wants to receive the receipt acknowledgement. Set to No if a 200 is requested.
- **Sync Supported** - Set whether the PIP supports synchronous message exchanges. The default value is No.

Note that for the PIPs for which Business Integration Connect provides PIP document flow packages are not synchronous. As a result, you do not need to change the Sync Ack Required and Sync Supported attributes for these PIPs.

If you want to set the attributes using the Document Flow Definition context, do the following.

1. Click **Hub Admin > Hub Configuration > Document Flow Definition**.
2. Click folder icons to individually expand a node to the appropriate Document Flow Definition level or select All to expand all displayed Document Flow Definition nodes.
3. In the Actions column, click the Edit attribute values icon for the package you want to edit such as Package:RNIF (1.1) or Package:RNIF (V02.00).
4. In the Document Flow Context Attributes section, go to the Update column of the attribute you want to set and select or type the new value in the update field. Repeat for each attribute that you want to set.

5. Click **Save**.

If you want to set the value of the attributes for each connection, do the following:

1. Click **Account Admin > Participant Connections**.
2. Select the source and the target of the connection you want to change and then click **Search**.
3. The Console displays a list of connections that match the source and target criteria. Each connection displays two sets of Document Flow Definitions (Source and Target) and a set of buttons including two **Attributes** buttons. To edit Document Flow Definition attributes for the source or target, click the **Attributes** button closest to source or target you want to edit.
4. In the Connection Attributes window, expand the Package node.
5. Go to the Update column of the attribute you want to set and select or type the new value in the update field. Repeat for each attribute that you want to set.
6. Click **Save**.

Deactivating PIPs

Once a PIP package has been uploaded into Business Integration Connect, it cannot be removed. However, you can deactivate the PIP so that it cannot be used.

To deactivate a PIP for all communications with Community Participants, do the following:

1. Click **Hub Admin > Hub Configuration > Document Flow Definition**.
2. Expand the Document Flow Definitions tree to reveal the Document Flow Definition of the PIP you want to disable.
3. In the Status column of the package, click **Enabled**. The Status column now displays "Disabled" and Business Integration Connect cannot use the Document Flow Definition for the PIP.

To deactivate a PIP communication with a specific Community Participant, deactivate the channel to the Community Participant defined for the PIP. See [“Enabling, disabling, or editing interactions” on page 42](#) for information.

Providing failure notification

If a failure occurs during the processing of a PIP message, Business Integration Connect uses the 0A1 PIP as the mechanism to broadcast the failure to the community participant or backend application that sent the message. For example, say a backend application initiates a 3A4 PIP. Business Integration Connect processes the RNSC message and sends a RosettaNet message to a community participant. Business Integration Connect waits for the response to the RosettaNet message until the waiting time reaches the timeout limit. Once this occurs, Business Integration Connect creates a 0A1 PIP and sends it to the community participant. The 0A1 PIP identifies the exception condition so that the community participant can then compensate for the failure of the 3A4 PIP.

To provide failure notification, upload a 0A1 package and create a PIP channel to the Community Participant using this package. See [“Setting up RosettaNet support” on page 54](#), [“Creating PIP channels to Community Participants” on page 54](#), and [“Configuring attribute values” on page 58](#) for information on how to do this.

Updating contact information

To change the RosettaNet contact information with the 0A1 PIP, you must edit the BCG.Properties file, located in the <install_root>/wbic/config directory.

These fields populate the contact information within the 0A1 PIP. Fax is optional (value can be empty), but the rest are required.

- `bcg.0A1.fromContactName=VQA`
- `bcg.0A1.fromEMailAddr=vqa@viacore.net`
- `bcg.0A1.fromPhoneNbr=949-725-1200`
- `bcg.0A1.fromFaxNbr=949-725-1201`

The phone numbers are limited to 30 bytes in length. The other fields are unlimited in length. When they are changed, the router will need to be restarted.

Creating PIP document flow packages

Because RosettaNet adds PIPs from time to time, you may need to create your own PIP packages to support these new PIPs or to support upgrades to PIPs. Except where noted, the procedures in this section describe how to create the PIP document flow package for PIP 5C4 V01.03.00. Business Integration Connect supplies a PIP document flow package for PIP 5C4 V01.02.00 so the procedures actually document how to perform an upgrade. However, creating a PIP document flow package is similar and the procedures identify any additional steps.

Before you begin, download the PIP specifications from www.rosettanet.org for the new version, and if you are performing an upgrade, the old version. For example, if you are performing the upgrade described in the procedures, download `5C4_DistributeRegistrationStatus_V01_03_00.zip` and `5C4_DistributeRegistrationStatus_V01_02_00.zip`. The specification includes the following file types:

- RosettaNet XML Message Guidelines - HTML files such as `5C4_MG_V01_03_00_RegistrationStatusNotification.htm` that define the PIP's cardinality, vocabulary, structure, and allowable data element values and value types.
- RosettaNet XML Message Schema - DTD files such as `5C4_MS_V01_03_RegistrationStatusNotification.dtd` that define the PIP's order or sequence, element naming, composition and attributes
- PIP Specification - DOC file such as `5C4_Spec_V01_03_00.doc` that provides the PIP's business performance controls.
- PIP Release Notes - DOC file such as `5C4_V01_03_00_ReleaseNotes.doc` that describes the difference between this version and the previous version.

Creating or upgrading a PIP document flow package involves the following procedures:

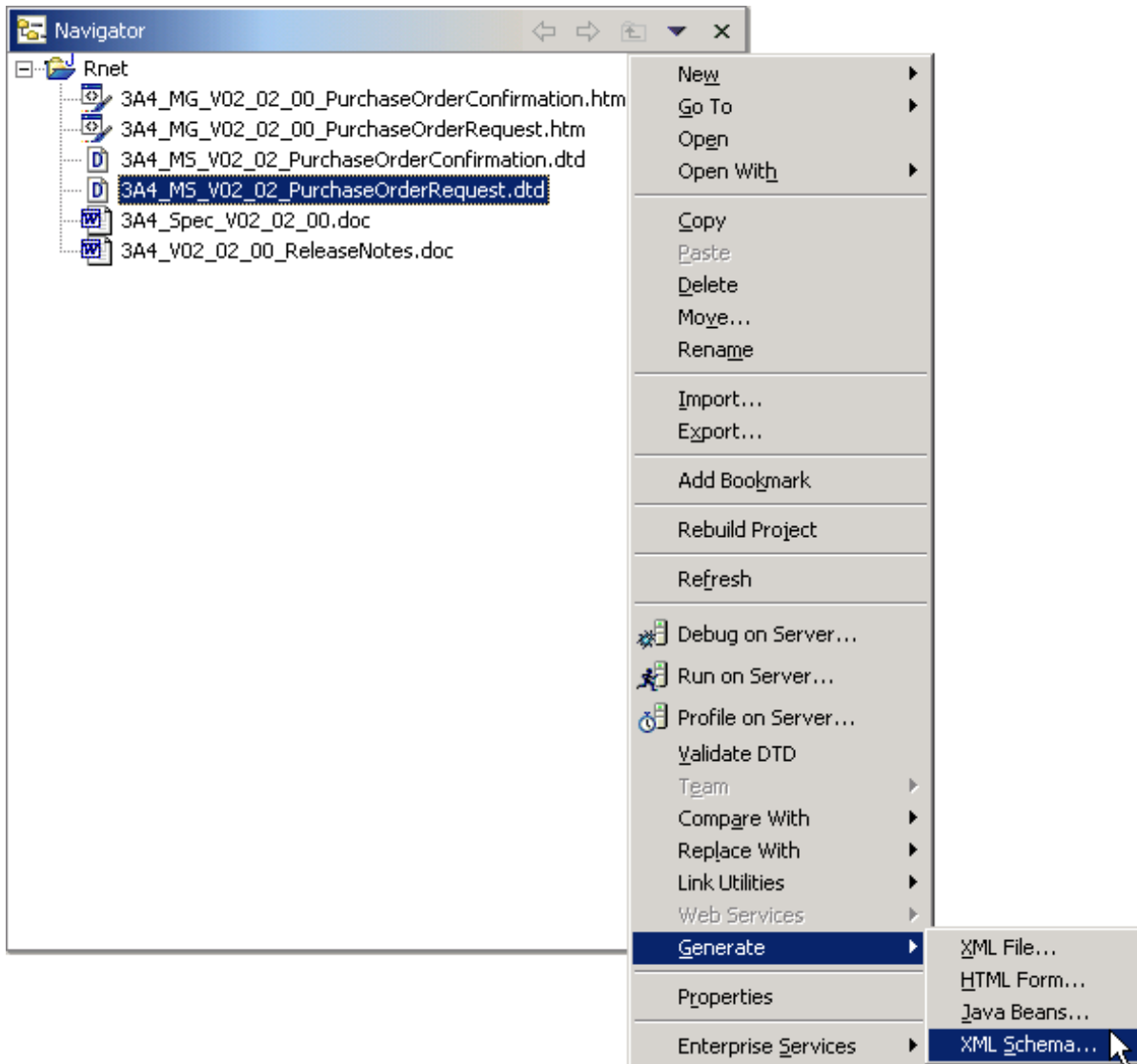
- [“Creating the XSD files” on page 61](#)
- [“Creating the XML file” on page 70](#)
- [“Creating the package” on page 72](#)

Creating the XSD files

A PIP document flow package contains XML schema files that define message formats and acceptable values for elements. The following procedure describes how to create these files based on the contents of the PIP specification file. You create at least one XSD file for each DTD file in the PIP specification file. For the example of upgrading to PIP 5C4 V01.03.00, because the message format changed, the procedure describes how to create the BCG_5C4RegistrationStatusNotification_V01.03.xsd file as an example. For information on the XSD files, see [“About validation” on page 73](#).

To create the XSD files for the PIP document flow package, do the following:

1. Import or load the DTD file into an XML editor such as WebSphere Studio Application Developer. For example, load the 5C4_MS_V01_03_RegistrationStatusNotification.dtd file.
2. Using the XML editor, convert the DTD into an XML schema. The following steps describe how to do this using Application Developer:
 - a. In the Navigation pane of the XML perspective, open the project containing the imported DTD file
 - b. Right click the DTD file and select **Generate > XML Schema**.



- c. In the Generate panel, type or select where you want to save the new XSD file. In the File name field, type the name of the new XSD file. In the case of the example, you would type a name such as BCG_5C4RegistrationStatusNotification_V01.03.xsd. Click **Finish**.
3. Compensate for elements that have multiple cardinality values in the RosettaNet XML guidelines by adding specifications to the new XSD file. The guidelines show the elements in the message using a tree and displaying the cardinality of each element to the left of the element:

1	1..n	<u>DesignRegistrationInformation</u>
2	0..1	-- <u>designEngagementDate.DatePeriod</u>
3	1	-- <u>beginDate.DateStamp</u>
4	1	-- <u>endDate.DateStamp</u>
5	1	-- <u>DesignProjectInformation</u>
6	0..n	-- <u>DesignAssemblyInformation</u>
7	0..1	-- <u>assemblyComments.FreeFormText</u>
8	0..1	-- <u>demandCreatorTrackingIdentifier.ProprietaryReferenceIdentifier</u>
9	0..n	-- <u>DesignPartInformation</u>
10	1	-- <u>demandCreatorTrackingIdentifier.ProprietaryReferenceIdentifier</u>
11	0..1	-- <u>GeographicRegion</u>

Generally, the elements in the guidelines match the definitions of the elements in the DTD file. However, the guidelines many contain some elements that have same name but different cardinalities. Because the DTD cannot provide the cardinality in this case, you need to modify the XSD. For example, the 5C4_MG_V01_03_00_RegistrationStatusNotification.htm guidelines file has a definition for ContactInformation on line 15 that has five child elements with the following cardinalities:

- 1 contactName
- 0..1 EmailAddress
- 0..1 facsimileNumber
- 0..1 PhysicalLocation
- 0..1 telephoneNumber

The ContactInformation definition on the line 150 has four child elements with the following cardinalities:

- 1 contactName
- 1 EmailAddress
- 0..1 facsimileNumber
- 1 telephoneNumber

In the XSD file, however, each child of ContactInformation has a cardinality that complies with both definitions:

```
<xsd:element name="ContactInformation">
  <xsd:complexType>
    <xsd:sequence>
      <xsd:element ref="contactName"/>
      <xsd:element maxOccurs="1" minOccurs="0" ref="EmailAddress"/>
      <xsd:element maxOccurs="1" minOccurs="0" ref="facsimileNumber"/>
      <xsd:element maxOccurs="1" minOccurs="0" ref="PhysicalLocation"/>
      <xsd:element maxOccurs="1" minOccurs="0" ref="telephoneNumber"/>
    </xsd:sequence>
  </xsd:complexType>
</xsd:element>
```

If you are updating the PIP document flow package based of another version of the package and want to reuse a definition from the other version, do the following for each of these definitions:

- a. Delete the definition of the element. For example, delete the ContactInformation element.
- b. Open the PIP document flow package of the version being replaced. For example, open the BCG_Package_RNIFV02.00_5C4V01.02.zip file.
- c. Find the definition you want to reuse. For example, the ContactInformation_type7 definition in the BCG_ContactInformation_Types.xsd file matches the definition you need for line 15 of the guidelines.

```
<xsd:complexType name="ContactInformation_type7">
  <xsd:sequence>
    <xsd:element name="contactName" type="common_FreeFormText_R"/>
    <xsd:element name="EmailAddress" type="common_EmailAddress_R"
      minOccurs="0"/>
    <xsd:element name="facsimileNumber"
      type="common_CommunicationsNumber_R" minOccurs="0"/>
    <xsd:element name="PhysicalLocation"
      type="PhysicalLocation_type1" minOccurs="0" />
    <xsd:element name="telephoneNumber"
      type="common_CommunicationsNumber_R" minOccurs="0" />
  </xsd:sequence>
</xsd:complexType>
```

- d. In the new XSD file you are creating for the updated PIP document flow package, create a reference to the XSD file containing the definition you want to reuse. For example, create a reference to BCG_ContactInformation_Types.xsd in the BCG_5C4RegistrationStatusNotification_V01.03.xsd file as follows:

```
<xsd:include schemaLocation="BCG_ContactInformation_Types.xsd"/>
```

- e. In the new XSD file, delete the ref attribute of any elements that refer to the element you deleted. Add a type attribute that refers to the definition you are reusing. For example, in the productProviderFieldApplicationEngineer element, delete *ref="ContactInformation"* and add the following:

```
name="ContactInformation
type="ContactInformation_type7"
```

If you are creating a PIP document flow package, or are upgrading a PIP document flow package but the definition you need does not exist in the other version, do the following for each instance of the element you found in the guidelines:

- a. Delete the definition of the element. For example, delete the ContactInformation element.
- b. Create the replacement definition. For example, create the ContactInformation_localType1 definition to match the definition in line 15 of the guidelines.


```

<xsd:complexType name="ContactInformation_localType1">
  <xsd:sequence>
    <xsd:element ref="contactName"/>
    <xsd:element maxOccurs="1" minOccurs="0" ref="EmailAddress"/>
    <xsd:element maxOccurs="1" minOccurs="0"
      ref="facsimileNumber"/>
    <xsd:element maxOccurs="1" minOccurs="0"
      ref="PhysicalLocation"/>
    <xsd:element maxOccurs="1" minOccurs="0"
      ref="telephoneNumber"/>
  </xsd:sequence>
</xsd:complexType>

```

- c. For any elements that refer to the element you deleted, delete its ref attribute and add a type attribute that refers to the appropriate complex type you defined in the previous step. For example, in the productProviderFieldApplicationEngineer element, delete *ref="Contact Information"* and add the following:

```

name="ContactInformation
type="ContactInformation_localType1"

```

Element productProviderFieldApplicationEngineer before modification

```

<xsd:element name="productProviderFieldApplicationEngineer">
  <xsd:complexType>
    <xsd:sequence>
      <xsd:element ref="ContactInformation"/>
    </xsd:sequence>
  </xsd:complexType>
</xsd:element>

```

Element productProviderFieldApplicationEngineer after modification

```

<xsd:element name="productProviderFieldApplicationEngineer">
  <xsd:complexType>
    <xsd:sequence>
      <xsd:element name="ContactInformation"
        type="ContactInformation_localType1"/>
    </xsd:sequence>
  </xsd:complexType>
</xsd:element>

```

4. Specify the enumeration values for elements that can only have specific values. The guidelines define the enumeration values in the tables in the Guideline Information section. For example, GlobalRegistrationComplexityLevelCode has the following table:

GlobalRegistrationComplexityLevelCode lines 139	
Entity Instances	
Above average	Above average complexity
Average	Average complexity
Maximum	Maximum complexity
Minimum	Minimal complexity
None	No complexity
Some	Some complexity

Therefore, in a PIP 5C4 V01.03.00 message, the GlobalRegistrationComplexityLevelCode can only have the following values: Above average, Average, Maximum, Minimum, None and Some.

If you are updating the PIP document flow package based of another version of the package and want to reuse a set of enumeration values from the other version, do the following for each set:

- a. Delete the definition for the element. For example, delete the `GlobalRegistrationComplexityLevelCode` element:
- b. Open the PIP document flow package of the version being replaced. For example, open the `BCG_Package_RNIFV02.00_5C4V01.02.zip` file.
- c. Find the definition containing the enumeration values you want to reuse. For example, the `_GlobalRegistrationComplexityLevelCode` definition in the `BCG_GlobalRegistrationComplexityLevelCode.xsd` file contains the enumeration value definitions defined by the Entity Instance table.

```
<xsd:simpleType name="_GlobalRegistrationComplexityLevelCode">
  <xsd:restriction base="xsd:string">
    <xsd:enumeration value="Above average"/>
    <xsd:enumeration value="Average"/>
    <xsd:enumeration value="Maximum"/>
    <xsd:enumeration value="Minimum"/>
    <xsd:enumeration value="None"/>
    <xsd:enumeration value="Some"/>
  </xsd:restriction>
</xsd:simpleType>
```

- d. In the new XSD file you are creating for the updated PIP document flow package, create a reference to the XSD file containing the definition you want to reuse. For example, create a reference to `BCG_GlobalRegistrationComplexityLevelCode.xsd` in the `BCG_5C4RegistrationStatusNotification_V01.03.xsd` file as follows:

```
<xsd:include schemaLocation=
  "BCG_GlobalRegistrationComplexityLevelCode_Types.xsd" />
```

- e. In the new XSD file, delete the `ref` attribute of any elements that refer to the element you deleted. Add a `type` attribute that refers to the definition you are reusing. For example, in the `DesignAssemblyInformation` element, delete `ref="GlobalRegistrationComplexityLevelCode"` and add the following:

```
name="GlobalRegistrationComplexityLevelCode"
type="_GlobalRegistrationComplexityLevelCode"
```

If you are creating a PIP document flow package or are upgrading a PIP document flow package but the enumeration value definitions you need do not exist in the other version, do the following for any element with enumerated values in the guidelines:

- a. Delete the definition of the element. For example, delete the `GlobalRegistrationComplexityLevelCode` element.
- b. Create the replacement definition. For example, create the `GlobalRegistrationComplexityLevelCode_localType` definition and include the enumeration value definitions as described by the table.

```

<xsd:simpleType
  name="GlobalRegistrationComplexityLevelCode_localType">
  <xsd:restriction base="xsd:string">
    <xsd:enumeration value="Above average"/>
    <xsd:enumeration value="Average"/>
    <xsd:enumeration value="Maximum"/>
    <xsd:enumeration value="Minimum"/>
    <xsd:enumeration value="None"/>
    <xsd:enumeration value="Some"/>
  </xsd:restriction>
</xsd:simpleType>

```

- c. For any elements that refer to the element you deleted, delete its ref attribute and add a type attribute that refers to the appropriate complex type you defined in the previous step. For example, delete *ref="GlobalRegistrationComplexityLevelCode"* and add the following:

```

name="GlobalRegistrationComplexityLevelCode"
type="GlobalRegistrationComplexityLevelCode_localType"

```

Element DesignAssemblyInformation before modification

```

<xsd:element name="DesignAssemblyInformation">
  <xsd:complexType>
    <xsd:sequence>
      <xsd:element maxOccurs="1" minOccurs="0"
        ref="assemblyComments"/>
      <xsd:element maxOccurs="1" minOccurs="0"
        ref="demandCreatorTrackingIdentifier"/>
      <xsd:element maxOccurs="unbounded" minOccurs="0"
        ref="DesignPartInformation"/>
      <xsd:element ref="DesignRegistrationIdentification"/>
      <xsd:element maxOccurs="1" minOccurs="0"
        ref="GeographicRegion"/>
      <xsd:element maxOccurs="1" minOccurs="0"
        ref="GlobalRegistrationComplexityLevelCode"/>
      <xsd:element maxOccurs="1" minOccurs="0"
        ref="GlobalRegistrationInvolvementLevelCode"/>
      <xsd:element maxOccurs="1" minOccurs="0"
        ref="RegistrationStatus"/>
    </xsd:sequence>
  </xsd:complexType>
</xsd:element>

```

Element DesignAssemblyInformation after modification

```

<xsd:element name="DesignAssemblyInformation">
  <xsd:complexType>
    <xsd:sequence>
      <xsd:element maxOccurs="1" minOccurs="0"
        ref="assemblyComments"/>
      <xsd:element maxOccurs="1" minOccurs="0"
        ref="demandCreatorTrackingIdentifier"/>
      <xsd:element maxOccurs="unbounded" minOccurs="0"
        ref="DesignPartInformation"/>
      <xsd:element ref="DesignRegistrationIdentification"/>
      <xsd:element maxOccurs="1" minOccurs="0"
        ref="GeographicRegion"/>
      <xsd:element maxOccurs="1" minOccurs="0"
        name="GlobalRegistrationComplexityLevelCode"
        type="GlobalRegistrationComplexityLevelCode_localType"/>
      <xsd:element maxOccurs="1" minOccurs="0"
        ref="GlobalRegistrationInvolvementLevelCode"/>
      <xsd:element maxOccurs="1" minOccurs="0"
        ref="RegistrationStatus"/>
    </xsd:sequence>
  </xsd:complexType>
</xsd:element>

```

5. Set the data type, minimum length, maximum length, and representation of the data entities. The RosettaNet XML Message Guidelines provide this information in the Fundamental Business Data Entities table as shown in the following figure:

Fundamental Business Data Entities					
Name	Definition	Data Type	Min	Max	Representation
CommunicationsNumber	The electro-technical communication number, e.g., telephone number, facsimile number, pager number.	String	1	30	X(30)
DateStamp	Specifies a specific date. Date stamp based on the ISO 8601 specification. The "Z" following the day identifier (DD) is used to indicate Coordinated Universal Time. Informal format: YYYYMMDDZ	Date	9	9	9(8)X

If you are updating the PIP document flow package based of another version of the package and want to reuse a data entity definition from the other version, do the following for each set:

- a. Delete the definition for the data entity element. For example, delete the DateStamp element:
- b. Open the PIP document flow package of the version you are replacing. For example, open the BCG_Package_RNIFV02.00_5C4V01.02.zip file.
- c. Find the definition you want to reuse. For example, the `_common_DateStamp_R` definition in the `BCG_common.xsd` file contains the following definition, which complies with the information given in the guidelines.

```

<xsd:simpleType name="_common_DateStamp_R">
  <xsd:restriction base="xsd:string">
    <xsd:pattern value="[0-9]{8}Z" />
  </xsd:restriction>
</xsd:simpleType>

```

- d. In the new XSD file you are creating for the updated PIP document flow package, create a reference to the XSD file containing the definition you want to reuse. For example, create a reference to BCG_common.xsd in the BCG_5C4RegistrationStatusNotification_V01.03.xsd file as follows:

```
<xsd:include schemaLocation="BCG_common.xsd" />
```

- e. In the new XSD file, delete the ref attribute of any elements that refer to the element you deleted. Add a type attribute that refers to the definition you are reusing. For example, in the DesignAssemblyInformation element, delete ref="DateStamp" and add the following:

```
name="DateStamp" type="_common_DateStamp_R"
```

If you are creating a PIP document flow package or are upgrading a PIP document flow package but the data entity definition you need does not exist in the other version, do the following for each data entity element:

- a. Delete the definition of the element. For example, delete the DateStamp element.
- b. Create the replacement definition. For example, use the data type, minimum length, maximum length, and representation information to create the DateStamp_localType definition.

```
<xsd:simpleType name="DateStamp_localType">
  <xsd:restriction base="xsd:string">
    <xsd:pattern value="[0-9]{8}Z" />
  </xsd:restriction>
</xsd:simpleType>
```

- c. For any elements that refer to the element you deleted, delete its ref attribute and add a type attribute that refers to the appropriate complex type you defined in the previous step. For example, delete ref="DateStamp" and add the following:

```
name="DateStamp" type="DateStamp_localType"
```

Element beginDate before modification

```
<xsd:element name="beginDate">
  <xsd:complexType">
    <xsd:sequence>
      <xsd:element ref="DateStamp"/>
    </xsd:sequence>
  </xsd:complexType>
</xsd:element>
```

Element beginDate after modification

```
<xsd:element name="beginDate">
  <xsd:complexType">
    <xsd:sequence>
      <xsd:element name="DateStamp" type="DateStamp_localType"/>
    </xsd:sequence>
  </xsd:complexType>
</xsd:element>
```

Creating the XML file

Once you have created the XSD files for your PIP document flow package, you are ready to create the XML file for the RNIF package and the XML file for the Backend Integration package. For example, these packages are called BCG_RNIFV02.00_5C4V01.03.zip and BCG_RNSC1.0_RNIFV02.00_5C4V01.03.zip respectively. The following procedure describes how to create the XML file for the RNIF package:

1. Extract the XML file from a RNIF PIP document flow package file. If you are upgrading, extract the file from the previous version of the package such as BCG_Package_RNIFV02.00_5C4V01.02.zip. If you are creating a new package, extract the file from a PIP document flow package that is similar to the one you are creating. For example, if you are creating a package to support a two action PIP, copy the XML file from another two action PIP package.
2. Copy the file and rename it appropriately such as RNIFV02.00_5C4V01.03.xml.
3. In the new file, update the elements that contain information about the PIP. For example, the following table lists the information you need to update in the 5C4 PIP example. Note that the information may appear more than once in the file, so make sure that you update all instances.

Table 2-22. 5C4 PIP update information

Information to change	Old value	New value
PIP ID	5C4	5C4
Version of the PIP	V01.02	V01.03
The name of the request message DTD file without the file extension	5C4_MS_V01_02_RegistrationStatusNotification	5C4_MS_V01_03_RegistrationStatusNotification
The name of the confirmation message DTD file without the file extension (for two action PIPs only)	N/A	N/A
The name of the request message XSD file without the file extension	BCG_5C4RegistrationStatusNotification_V01.02	BCG_5C4RegistrationStatusNotification_V01.03
The name of the confirmation message XSD file without the file extension (for two action PIPs only)	N/A	N/A
Root element name in the XSD file for the request message	Pip5C4RegistrationStatusNotification	Pip5C4RegistrationStatusNotification
Root element name in the XSD file for the confirmation message (for two action PIPs only)	N/A	N/A

- Open the PIP Specification document and use it to update the information listed in the following table. If you are doing an update, compare the specifications for the versions because you may not have to update these values.

Table 2-23. 5C4 PIP update information from the PIP specification

Information to update	Description	Value in the 5C4 package
Activity name	Specified in Table 3-2	Distribute Registration Status
Initiator role name	Specified in Table 3-1	Product Provider
Responder role name	Specified in Table 3-1	Demand Creator
Request action name	Specified in Table 4-2	Registration Status Notification
Confirmation action name	Specified in Table 4-2 (for two action PIPs only)	N/A

- Update the package attribute values. If you are doing an update, compare the specifications for the versions because you may not have to update these values.

Table 2-24. 5C4 PIP attribute updates

Information to update	Description	Value in the 5C4 package	Element path in the XML file
NonRepudiationRequired	Specified in Table 3-3	N	ns1:Package ns1:Protocol ns1:Process ns1:Attribute (Its ATTRIBUTEKEY is NonRepudiationRequired) ns1:AttributeValue AttributePickListItem ATTRVALUEKEY
NonRepudiationOfReceipt	Specified in Table 3-3	N	ns1:Package ns1:Protocol ns1:Process ns1:Attribute (Its ATTRIBUTEKEY is NonRepudiationOfReceipt) ns1:AttributeValue AttributePickListItem ATTRVALUEKEY
DigitalSignatureRequired	Specified in Table 5-1	Y	ns1:Package ns1:Protocol ns1:Process ns1:Attribute (Its ATTRIBUTEKEY is DigitalSignatureRequired) ns1:AttributeValue AttributePickListItem ATTRVALUEKEY
TimeToAcknowledge	Specified in Table 3-3	2 (120 min)	ns1:Package ns1:Protocol ns1:Process ns1:Attribute (Its ATTRIBUTEKEY is TimeToAcknowledge) ns1:AttributeValue ATTRVALUE

Table 2-24. 5C4 PIP attribute updates

TimeToPerform	Specified in Table 3-3	2 (120 min)	ns1:Package ns1:Protocol ns1:Process ns1:Attribute (Its ATTRIBUTEKEY is TimeToPerform) ns1:AttributeValue ATTRVALUE
RetryCount	Specified in Table 3-3	3	ns1:Package ns1:Protocol ns1:Process ns1:Attribute (Its ATTRIBUTEKEY is RetryCount) ns1:AttributeValue ATTRVALUE

- Update the ns1:Package/ns1:Protocol/GuidelineMap elements to remove unused XSD files and to add any XSD files you created or referenced as shown in the following example for BCG_common.xsd.

To create the Backend Integration package, repeat the above procedure except for the following differences:

- In step 1, extract the XML file from the Backend Integration package such as BCG_Package_RNSC1.0_RNIFV02.00_5C4V01.02.zip.
- Do not do step 5.

Once you have created the XML and the XSD files, you are ready to create the PIP documentation flow packages.

Creating the package

To create RNIF package, do the following:

- Create a GuidelineMaps directory and copy the package's XSD files into this directory.
- Create a Packages directory and copy the RNIF XML file into this directory.
- Go to the parent directory and create a PIP document flow package (ZIP file) that contains the GuidelineMaps and Packages directory. You must preserve the directory structure in the ZIP file.

To create the Backend Integration package, perform the above procedure but use the Backend Integration XML file instead of the RNIF file.

Once you have created the PIP package, you can upload it using the procedure in [“Uploading RNIF packages” on page 35](#).

About validation

Business Integration Connect validates the service content of a RosettaNet message using validation maps. These validation maps define the structure of a valid message and define the cardinality, format, and valid values (enumeration) of the elements within the message. Within each PIP document flow package, Business Integration Connect supplies the validation maps as XSD files in the GuidelineMaps directory.

Because RosettaNet specifies the format of a PIP message, typically you will not need to customize the validation maps. However, if you do, see [“Creating PIP document flow packages” on page 60](#) for information on the steps needed to upgrade the XSD files used to validate the messages and how to create a custom PIP document flow package.

Cardinality

Cardinality determines the number of times a particular element can or must appear in a message. In the validation maps, the minOccurs and maxOccurs attributes determine the cardinality of the attribute as shown in the following example taken from BCG_5C4RegistrationStatusNotification_V01.02.xsd):

```
<xsd:element name="GeographicRegion" type="GeographicRegionType"
  minOccurs="0"/>
```

If Business Integration Connect does not need to check the cardinality of an element, the values of the element's minOccurs and maxOccurs attributes in the validation map are "0" and "unbounded" respectively as shown in the following example:

```
<xsd:element name="DesignRegistrationIdentification"
  type="DesignRegistrationIdentificationType2"
  minOccurs="0" maxOccurs="unbounded"/>
```

Format

Format determines the arrangement or layout of data for the type of an element. In the validation maps, the type has one of more restrictions as shown in the following examples:

Example 1:

```
<xsd:simpleType name="_common_LineNumber_R">
  <xsd:restriction base="xsd:string">
    <xsd:minLength value="1" />
    <xsd:maxLength value="6" />
  </xsd:restriction>
</xsd:simpleType>
```

All `_common_LineNumber_R` type elements in a message must be Strings and must be 1 to 6 characters in length.

Example 2:

```
<xsd:simpleType name="_GlobalLocationIdentifier">
  <xsd:restriction base="xsd:string">
    <xsd:pattern value="[0-9]{9}.{1,4}" />
  </xsd:restriction>
</xsd:simpleType>
```

All `_GlobalLocationIdentifier` type elements in a message must be Strings and must have nine characters of numeric data followed by one to four characters of alphanumeric data. The minimum length is therefore 10 characters and the maximum is 13.

Example 3:

```
<xsd:element name="DayOfMonth">
  <xsd:simpleType>
    <xsd:restriction base="xsd:positiveInteger">
      <xsd:totalDigits value="2" />
      <xsd:minInclusive value="1" />
      <xsd:maxInclusive value="31" />
    </xsd:restriction>
  </xsd:simpleType>
</xsd:element>
```

All `_GlobalLocationIdentifier` type elements in a message must be `PositiveInteger`, must have one or two characters, and have a value of 1 to 31 inclusive.

Enumeration

Enumeration determines the valid values for an element. In the validation maps, the type of the element has one or more enumeration restrictions as shown in the following example:

```
<xsd:simpleType name="_local_GlobalDesignRegistrationNotificationCode">
  <xsd:restriction base="xsd:string">
    <xsd:enumeration value="Initial" />
    <xsd:enumeration value="Update" />
  </xsd:restriction>
</xsd:simpleType>
```

All `_local_GlobalDesignRegistrationNotificationCode` type elements in a message must have only "Initial" or "Update" for their value.

PIP document flow package contents

The following table shows the PIP document flow packages provided by Business Integration Connect for each PIP. Within each package is an XML file contained in a Packages directory and several XSD files contained in a GuidelineMaps directory, which are common to all PIP document flow packages for the PIP.

Table 2-25. PIP document flow package contents

Package ZIP file name	Packages contents	GuidelineMaps contents
PIP 2A12 Distribute Product Master		
BCG_Package_RNIF1.1_2A12V01.03.zip	BCG_RNIF1.1_2A12V01.03.xml	BCG_2A12ProductMasterNotification_V01.03.xsd
BCG_Package_RNIFV02.00_2A12V01.03.zip	BCG_RNIFV02.00_2A12V01.03.xml	BCG_common.xsd
BCG_Package_RNSC1.0_RNIF1.1_2A12V01.03.zip	BCG_RNSC1.0_RNIF1.1_2A12V01.03.xml	BCG_ContactInformation_Types.xsd
BCG_Package_RNSC1.0_RNIFV02.00_2A12V01.03.zip	BCG_RNSC1.0_RNIFV02.00_2A12V01.03.xml	BCG_PhysicalAddress_Types.xsd
		BCG_PartnerDescription_Types.xsd
		BCG_GlobalAssemblyLevelCode.xsd
		BCG_GlobalIntervalCode.xsd
		BCG_GlobalLeadTimeClassificationCode.xsd
		BCG_GlobalPartnerRoleClassificationCode.xsd
		BCG_GlobalProductUnitOfMeasureCode.xsd
		BCG_GlobalProductLifeCycleStatusCode.xsd
		BCG_GlobalProductProcurementTypeCode.xsd
		BCG_BusinessDescription_Types.xsd
		BCG_BusinessTaxIdentifier_Types.xsd
		BCG_GlobalCountryCode.xsd
		BCG_GlobalPartnerClassificationCode.xsd
		BCG_string_len_0.xsd
		BCG_xml.xsd

Table 2-25. PIP document flow package contents

PIP 3A1 Request Quote		
BCG_Package_RNIF1.1_3A1V02.00.zip	BCG_RNIF1.1_3A1V02.00.xml	BCG_3A1QuoteConfirmation_V02.00.xsd BCG_3A1QuoteRequest_V02.00.xsd
BCG_Package_RNIFV02.00_3A1V02.00.zip	BCG_RNIFV02.00_3A1V02.00.xml	BCG_common.xsd BCG_ContactInformation_Types.xsd BCG_PhysicalAddress_Types.xsd
BCG_Package_RNSC1.0_RNIF1.1_3A1V02.00.zip	BCG_RNSC1.0_RNIF1.1_3A1V02.00.xml	BCG_PartnerDescription_Types.xsd BCG_GlobalCurrencyCode.xsd BCG_GlobalGovernmentPriorityRatingCode.xsd
BCG_Package_RNSC1.0_RNIFV02.00_3A1V02.00.zip	BCG_RNSC1.0_RNIFV02.00_3A1V02.00.xml	BCG_GlobalMonetaryAmountTypeCode.xsd BCG_GlobalPartnerRoleClassificationCode.xsd BCG_GlobalProductUnitOfMeasureCode.xsd BCG_GlobalQuoteTypeCode.xsd BCG_GlobalStockIndicatorCode.xsd BCG_GlobalTaxExemptionCode.xsd BCG_BusinessTaxIdentifier_Types.xsd BCG_GlobalProductSubstitutionReasonCode.xsd BCG_GlobalProductTermsCode.xsd BCG_GlobalQuoteLineItemStatusCode.xsd BCG_BusinessDescription_Types.xsd BCG_GlobalCountryCode.xsd BCG_GlobalPartnerClassificationCode.xsd BCG_string_len_0.xsd BCG_xml.xsd

Table 2-25. PIP document flow package contents

PIP 3A2 Request Price and Availability		
BCG_Package_RNIF1.1_3A2R02.01.zip	BCG_RNIF1.1_3A2R02.01.xml	BCG_3A2PriceAndAvailabilityRequest_R02.01.xsd
BCG_Package_RNIFV02.00_3A2R02.01.zip	BCG_RNIFV02.00_3A2R02.01.xml	BCG_3A2PriceAndAvailabilityResponse_R02.01.xsd BCG_common.xsd
BCG_Package_RNSC1.0_RNIF1.1_3A2R02.01.zip	BCG_RNSC1.0_RNIF1.1_3A2R02.01.xml	BCG_ContactInformation_Types.xsd BCG_PhysicalAddress_Types.xsd BCG_PartnerDescription_Types.xsd
BCG_Package_RNSC1.0_RNIFV02.00_3A2R02.01.zip	BCG_RNSC1.0_RNIFV02.00_3A2R02.01.xml	BCG_BusinessTaxIdentifier_Types.xsd BCG_GlobalPricingTypeCode.xsd BCG_GlobalProductStatusCode.xsd BCG_GlobalCurrencyCode.xsd BCG_GlobalProductUnitOfMeasureCode.xsd BCG_GlobalCustomerAuthorizationCode.xsd BCG_GlobalProductAvailabilityCode.xsd BCG_GlobalProductSubstitutionReasonCode.xsd BCG_BusinessDescription_Types.xsd BCG_GlobalCountryCode.xsd BCG_GlobalPartnerClassificationCode.xsd BCG_string_len_0.xsd BCG_xml.xsd

Table 2-25. PIP document flow package contents

PIP 3A4 Request Purchase Order		
BCG_Package_RNIF1.1_3A4V02.02.zip	BCG_RNIF1.1_3A4V02.02.xml	BCG_3A4PurchaseOrderConfirmation_V02.02.xsd
BCG_Package_RNIFV02.00_3A4V02.02.zip	BCG_RNIFV02.00_3A4V02.02.xml	BCG_3A4PurchaseOrderRequest_V02.02.xsd BCG_common.xsd
BCG_Package_RNSC1.0_RNIF1.1_3A4V02.02.zip	BCG_RNSC1.0_RNIF1.1_3A4V02.02.xml	BCG_ContactInformation_Types.xsd BCG_PhysicalAddress_Types.xsd BCG_PartnerDescription_Types.xsd
BCG_Package_RNSC1.0_RNIFV02.00_3A4V02.02.zip	BCG_RNSC1.0_RNIFV02.00_3A4V02.02.xml	BCG_BusinessTaxIdentifier_Types.xsd BCG_GlobalCountryCode.xsd BCG_GlobalCurrencyCode.xsd BCG_GlobalAccountClassificationCode.xsd BCG_GlobalCreditCardClassificationCode.xsd BCG_GlobalDocumentReferenceTypeCode.xsd BCG_GlobalFinanceTermsCode.xsd BCG_GlobalGovernmentPriorityRatingCode.xsd BCG_GlobalMonetaryAmountTypeCode.xsd BCG_GlobalPartnerRoleClassificationCode.xsd BCG_GlobalPaymentConditionCode.xsd BCG_GlobalProductUnitOfMeasureCode.xsd BCG_GlobalPriceUnitOfMeasureCode.xsd BCG_GlobalPurchaseOrderFillPriorityCode.xsd BCG_GlobalPurchaseOrderTypeCode.xsd BCG_GlobalShipmentTermsCode.xsd BCG_GlobalShippingServiceLevelCode.xsd BCG_GlobalSpecialFulfillmentRequestCode.xsd BCG_GlobalSpecialHandlingCode.xsd BCG_InvoiceChargeTypeCode.xsd BCG_GlobalTaxExemptionCode.xsd BCG_GlobalConfirmationTypeCode.xsd BCG_GlobalProductSubstitutionReasonCode.xsd BCG_GlobalPurchaseOrderAcknowledgmentReasonCode.xsd BCG_GlobalPurchaseOrderStatusCode.xsd BCG_BusinessDescription_Types.xsd BCG_GlobalPartnerClassificationCode.xsd BCG_string_len_0.xsd BCG_xml.xsd

Table 2-25. PIP document flow package contents

PIP 3A5 Query Order Status		
BCG_Package_RNIF1.1_3A5R02.00.zip	BCG_RNIF1.1_3A5R02.00.xml	BCG_3A5PurchaseOrderStatusQuery_R02.00.xsd
BCG_Package_RNIFV02.00_3A5R02.00.zip	BCG_RNIFV02.00_3A5R02.00.xml	BCG_3A5PurchaseOrderStatusResponse_R02.00.xsd BCG_common.xsd
BCG_Package_RNSC1.0_RNIF1.1_3A5R02.00.zip	BCG_RNSC1.0_RNIF1.1_3A5R02.00.xml	BCG_ContactInformation_Types.xsd BCG_PhysicalAddress_Types.xsd BCG_PartnerDescription_Types.xsd
BCG_Package_RNSC1.0_RNIFV02.00_3A5R02.00.zip	BCG_RNSC1.0_RNIFV02.00_3A5R02.00.xml	BCG_BusinessTaxIdentifier_Types.xsd BCG_GlobalCreditCardClassificationCode.xsd BCG_GlobalAccountClassificationCode.xsd BCG_GlobalDocumentReferenceTypeCode.xsd BCG_GlobalFinanceTermsCode.xsd BCG_GlobalGovernmentPriorityRatingCode.xsd BCG_GlobalPurchaseOrderAcknowledgmentReasonCode.xsd BCG_GlobalPurchaseOrderStatusCode.xsd BCG_GlobalShippingServiceLevelCode.xsd BCG_GlobalSpecialFulfillmentRequestCode.xsd BCG_GlobalSpecialHandlingCode.xsd BCG_GlobalLineItemStatusCode.xsd BCG_GlobalProductUnitOfMeasureCode.xsd BCG_GlobalOrderQuantityTypeCode.xsd BCG_GlobalPartnerClassificationCode.xsd BCG_GlobalCurrencyCode.xsd BCG_GlobalProductSubstitutionReasonCode.xsd BCG_GlobalTaxExemptionCode.xsd BCG_GlobalPartnerRoleClassificationCode.xsd BCG_GlobalPurchaseOrderFillPriorityCode.xsd BCG_GlobalPurchaseOrderTypeCode.xsd BCG_GlobalShipmentTermsCode.xsd BCG_GlobalFreeOnBoardCode.xsd BCG_GlobalTransportEventCode.xsd BCG_GlobalCustomerTypeCode.xsd BCG_BusinessDescription_Types.xsd BCG_GlobalCountryCode.xsd BCG_string_len_0.xsd BCG_xml.xsd

Table 2-25. PIP document flow package contents

PIP 3A6 Distribute Order Status		
BCG_Package_RNIF1.1_3A6V02.02.zip	BCG_RNIF1.1_3A6V02.02.xml	BCG_3A6PurchaseOrderStatusNotification_V02.02.xsd
BCG_Package_RNIFV02.00_3A6V02.02.zip	BCG_RNIFV02.00_3A6V02.02.xml	BCG_common.xsd BCG_ContactInformation_Types.xsd BCG_PhysicalAddress_Types.xsd
BCG_Package_RNSC1.0_RNIF1.1_3A6V02.02.zip	BCG_RNSC1.0_RNIF1.1_3A6V02.02.xml	BCG_PartnerDescription_Types.xsd BCG_BusinessTaxIdentifier_Types.xsd BCG_GlobalCountryCode.xsd
BCG_Package_RNSC1.0_RNIFV02.00_3A6V02.02.zip	BCG_RNSC1.0_RNIFV02.00_3A6V02.02.xml	BCG_GlobalCurrencyCode.xsd BCG_GlobalAccountClassificationCode.xsd BCG_GlobalCreditCardClassificationCode.xsd BCG_GlobalDocumentReferenceTypeCode.xsd BCG_GlobalFinanceTermsCode.xsd BCG_GlobalGovernmentPriorityRatingCode.xsd BCG_GlobalMonetaryAmountTypeCode.xsd BCG_GlobalLineItemStatusCode.xsd BCG_GlobalNotificationReasonCode.xsd BCG_GlobalOrderQuantityTypeCode.xsd BCG_GlobalPartnerRoleClassificationCode.xsd BCG_GlobalPaymentConditionCode.xsd BCG_GlobalPriceUnitOfMeasureCode.xsd BCG_GlobalProductUnitOfMeasureCode.xsd BCG_GlobalProductSubstitutionReasonCode.xsd BCG_GlobalPurchaseOrderFillPriorityCode.xsd BCG_GlobalPurchaseOrderAcknowledgmentReasonCode.xsd BCG_GlobalPurchaseOrderStatusCode.xsd BCG_GlobalPurchaseOrderTypeCode.xsd BCG_GlobalShipmentTermsCode.xsd BCG_GlobalShippingServiceLevelCode.xsd BCG_GlobalSpecialFulfillmentRequestCode.xsd BCG_GlobalSpecialHandlingCode.xsd BCG_GlobalTrackingReferenceTypeCode.xsd BCG_InvoiceChargeTypeCode.xsd BCG_GlobalTaxExemptionCode.xsd BCG_BusinessDescription_Types.xsd BCG_GlobalPartnerClassificationCode.xsd BCG_string_len_0.xsd BCG_xml.xsd

Table 2-25. PIP document flow package contents

PIP 3A7 Notify of Purchase Order Update		
BCG_Package_RNIF1.1_3A7V02.02.zip	BCG_RNIF1.1_3A7V02.02.xml	BCG_3A7PurchaseOrderUpdateNotification_V02.02.xsd
BCG_Package_RNIFV02.00_3A7V02.02.zip	BCG_RNIFV02.00_3A7V02.02.xml	BCG_common.xsd BCG_string_len_0.xsd BCG_ContactInformation_Types.xsd
BCG_Package_RNSC1.0_RNIF1.1_3A7V02.02.zip	BCG_RNSC1.0_RNIF1.1_3A7V02.02.xml	BCG_PhysicalAddress_Types.xsd BCG_PartnerDescription_Types.xsd BCG_BusinessTaxIdentifier_Types.xsd
BCG_Package_RNSC1.0_RNIFV02.00_3A7V02.02.zip	BCG_RNSC1.0_RNIFV02.00_3A7V02.02.xml	BCG_GlobalActionCode.xsd BCG_GlobalCountryCode.xsd BCG_GlobalCurrencyCode.xsd BCG_GlobalAccountClassificationCode.xsd BCG_GlobalConfirmationTypeCode.xsd BCG_GlobalCreditCardClassificationCode.xsd BCG_GlobalDocumentReferenceTypeCode.xsd BCG_GlobalFinanceTermsCode.xsd BCG_GlobalGovernmentPriorityRatingCode.xsd BCG_GlobalMonetaryAmountTypeCode.xsd BCG_GlobalPartnerRoleClassificationCode.xsd BCG_GlobalPaymentConditionCode.xsd BCG_GlobalProductUnitOfMeasureCode.xsd BCG_GlobalProductSubstitutionReasonCode.xsd BCG_GlobalPriceUnitOfMeasureCode.xsd BCG_GlobalPurchaseOrderFillPriorityCode.xsd BCG_GlobalPurchaseOrderAcknowledgmentReasonCode.xsd BCG_GlobalPurchaseOrderStatusCode.xsd BCG_GlobalPurchaseOrderTypeCode.xsd BCG_GlobalShipmentTermsCode.xsd BCG_GlobalShippingServiceLevelCode.xsd BCG_GlobalSpecialFulfillmentRequestCode.xsd BCG_GlobalSpecialHandlingCode.xsd BCG_InvoiceChargeTypeCode.xsd BCG_GlobalTaxExemptionCode.xsd BCG_BusinessDescription_Types.xsd BCG_GlobalPartnerClassificationCode.xsd BCG_xml.xsd

Table 2-25. PIP document flow package contents

PIP 3A8 Request Purchase Order Change		
BCG_Package_RNIF1.1_3A8V01.02.zip	BCG_RNIF1.1_3A8V01.02.xml	BCG_3A8PurchaseOrderChangeConfirmation_V01.02.xsd
BCG_Package_RNIFV02.00_3A8V01.02.zip	BCG_RNIFV02.00_3A8V01.02.xml	BCG_3A8PurchaseOrderChangeRequest_V01.02.xsd BCG_common.xsd
BCG_Package_RNSC1.0_RNIF1.1_3A8V01.02.zip	BCG_RNSC1.0_RNIF1.1_3A8V01.02.xml	BCG_ContactInformation_Types.xsd BCG_PhysicalAddress_Types.xsd BCG_PartnerDescription_Types.xsd
BCG_Package_RNSC1.0_RNIFV02.00_3A8V01.02.zip	BCG_RNSC1.0_RNIFV02.00_3A8V01.02.xml	BCG_BusinessTaxIdentifier_Types.xsd BCG_GlobalCountryCode.xsd BCG_GlobalCurrencyCode.xsd BCG_GlobalActionCode.xsd BCG_GlobalAccountClassificationCode.xsd BCG_GlobalCreditCardClassificationCode.xsd BCG_GlobalDocumentReferenceTypeCode.xsd BCG_GlobalFinanceTermsCode.xsd BCG_GlobalGovernmentPriorityRatingCode.xsd BCG_GlobalMonetaryAmountTypeCode.xsd BCG_GlobalPartnerRoleClassificationCode.xsd BCG_GlobalPaymentConditionCode.xsd BCG_GlobalProductUnitOfMeasureCode.xsd BCG_GlobalPriceUnitOfMeasureCode.xsd BCG_GlobalPurchaseOrderFillPriorityCode.xsd BCG_GlobalPurchaseOrderTypeCode.xsd BCG_GlobalShipmentTermsCode.xsd BCG_GlobalShippingServiceLevelCode.xsd BCG_GlobalSpecialFulfillmentRequestCode.xsd BCG_GlobalSpecialHandlingCode.xsd BCG_InvoiceChargeTypeCode.xsd BCG_GlobalTaxExemptionCode.xsd BCG_GlobalConfirmationTypeCode.xsd BCG_GlobalProductSubstitutionReasonCode.xsd BCG_GlobalPurchaseOrderAcknowledgmentReasonCode.xsd BCG_GlobalPurchaseOrderStatusCode.xsd BCG_BusinessDescription_Types.xsd BCG_GlobalPartnerClassificationCode.xsd BCG_string_len_0.xsd BCG_xml.xsd

Table 2-25. PIP document flow package contents

PIP 3A9 Request Purchase Order Cancellation		
BCG_Package_RNIF1.1_3A9V01.01.zip	BCG_RNIF1.1_3A9V01.01.xml	BCG_3A9PurchaseOrderCancellationConfirmation_V01.01.xsd
BCG_Package_RNIFV02.00_3A9V01.01.zip	BCG_RNIFV02.00_3A9V01.01.xml	BCG_3A9PurchaseOrderCancellationRequest_V01.01.xsd BCG_common.xsd
BCG_Package_RNSC1.0_RNIF1.1_3A9V01.01.zip	BCG_RNSC1.0_RNIF1.1_3A9V01.01.xml	BCG_ContactInformation_Types.xsd BCG_PhysicalAddress_Types.xsd BCG_PartnerDescription_Types.xsd
BCG_Package_RNSC1.0_RNIFV02.00_3A9V01.01.zip	BCG_RNSC1.0_RNIFV02.00_3A9V01.01.xml	BCG_GlobalPurchaseOrderCancellationCode.xsd BCG_GlobalPurchaseOrderCancellationResponseCode.xsd BCG_BusinessDescription_Types.xsd BCG_BusinessTaxIdentifier_Types.xsd BCG_GlobalCountryCode.xsd BCG_GlobalPartnerClassificationCode.xsd BCG_string_len_0.xsd BCG_xml.xsd
PIP 3B2 Notify of Advance Shipment		
BCG_Package_RNIF1.1_3B2V01.01.zip	BCG_RNIF1.1_3B2V01.01.xml	BCG_3B2AdvanceShipmentNotification_V01.01.xsd BCG_common.xsd
BCG_Package_RNIFV02.00_3B2V01.01.zip	BCG_RNIFV02.00_3B2V01.01.xml	BCG_ContactInformation_Types.xsd BCG_PhysicalAddress_Types.xsd BCG_PartnerDescription_Types.xsd
BCG_Package_RNSC1.0_RNIF1.1_3B2V01.01.zip	BCG_RNSC1.0_RNIF1.1_3B2V01.01.xml	BCG_BusinessTaxIdentifier_Types.xsd BCG_GlobalIncotermsCode.xsd
BCG_Package_RNSC1.0_RNIFV02.00_3B2V01.01.zip	BCG_RNSC1.0_RNIFV02.00_3B2V01.01.xml	BCG_GlobalShipmentChangeDispositionCode.xsd BCG_GlobalShipmentModeCode.xsd BCG_GlobalShippingServiceLevelCode.xsd BCG_GlobalShipDateCode.xsd BCG_GlobalPackageTypeCode.xsd BCG_GlobalPhysicalUnitOfMeasureCode.xsd BCG_GlobalProductUnitOfMeasureCode.xsd BCG_GlobalDocumentReferenceTypeCode.xsd BCG_GlobalLotQuantityClassificationCode.xsd BCG_NationalExportControlClassificationCode.xsd BCG_GlobalCountryCode.xsd BCG_GlobalTrackingReferenceTypeCode.xsd BCG_BusinessDescription_Types.xsd BCG_GlobalPartnerClassificationCode.xsd BCG_string_len_0.xsd BCG_xml.xsd

Table 2-25. PIP document flow package contents

PIP 3C3 Notify of Invoice		
BCG_Package_RNIF1.1_3C3V01.01.zip	BCG_RNIF1.1_3C3V01.01.xml	BCG_3C3InvoiceNotification_V01.01.xsd BCG_common.xsd
BCG_Package_RNIFV02.00_3C3V01.01.zip	BCG_RNIFV02.00_3C3V01.01.xml	BCG_ContactInformation_Types.xsd BCG_PhysicalAddress_Types.xsd BCG_PartnerDescription_Types.xsd
BCG_Package_RNSC1.0_RNIF1.1_3C3V01.01.zip	BCG_RNSC1.0_RNIF1.1_3C3V01.01.xml	BCG_BusinessTaxIdentifier_Types.xsd BCG_GlobalCountryCode.xsd BCG_GlobalCurrencyCode.xsd
BCG_Package_RNSC1.0_RNIFV02.00_3C3V01.01.zip	BCG_RNSC1.0_RNIFV02.00_3C3V01.01.xml	BCG_GlobalDocumentTypeCode.xsd BCG_GlobalMonetaryAmountTypeCode.xsd BCG_GlobalPartnerRoleClassificationCode.xsd BCG_GlobalPaymentTermsCode.xsd BCG_GlobalProductUnitOfMeasureCode.xsd BCG_GlobalSaleTypeCode.xsd BCG_GlobalShipmentTermsCode.xsd BCG_GlobalShippingServiceLevelCode.xsd BCG_GlobalSpecialHandlingCode.xsd BCG_InvoiceChargeTypeCode.xsd BCG_NationalExportControlClassificationCode.xsd BCG_BusinessDescription_Types.xsd BCG_GlobalPartnerClassificationCode.xsd BCG_string_len_0.xsd BCG_xml.xsd
PIP 3C4 Notify of Invoice Reject		
BCG_Package_RNIF1.1_3C4V01.00.zip	BCG_RNIF1.1_3C4V01.00.xml	BCG_3C4InvoiceRejectNotification_V01.00.xsd BCG_common.xsd
BCG_Package_RNIFV02.00_3C4V01.00.zip	BCG_RNIFV02.00_3C4V01.00.xml	BCG_ContactInformation_Types.xsd BCG_PhysicalAddress_Types.xsd BCG_PartnerDescription_Types.xsd
BCG_Package_RNSC1.0_RNIF1.1_3C4V01.00.zip	BCG_RNSC1.0_RNIF1.1_3C4V01.00.xml	BCG_GlobalInvoiceRejectionCode.xsd BCG_GlobalMonetaryAmountTypeCode.xsd
BCG_Package_RNSC1.0_RNIFV02.00_3C4V01.00.zip	BCG_RNSC1.0_RNIFV02.00_3C4V01.00.xml	BCG_BusinessDescription_Types.xsd BCG_BusinessTaxIdentifier_Types.xsd BCG_GlobalCountryCode.xsd BCG_GlobalPartnerClassificationCode.xsd BCG_string_len_0.xsd BCG_xml.xsd

Table 2-25. PIP document flow package contents

PIP 3C6 Notify of Remittance Advice		
BCG_Package_RNIF1.1_3C6V01.00.zip	BCG_RNIF1.1_3C6V01.00.xml	BCG_3C6RemittanceAdviceNotification_V01.00.xsd
BCG_Package_RNIFV02.00_3C6V01.00.zip	BCG_RNIFV02.00_3C6V01.00.xml	BCG_common.xsd BCG_ContactInformation_Types.xsd BCG_PhysicalAddress_Types.xsd
BCG_Package_RNSC1.0_RNIF1.1_3C6V01.00.zip	BCG_RNSC1.0_RNIF1.1_3C6V01.00.xml	BCG_PartnerDescription_Types.xsd BCG_GlobalCurrencyCode.xsd BCG_GlobalFinancialAdjustmentReasonCode.xsd
BCG_Package_RNSC1.0_RNIFV02.00_3C6V01.00.zip	BCG_RNSC1.0_RNIFV02.00_3C6V01.00.xml	BCG_GlobalInvoiceRejectionCode.xsd BCG_GlobalMonetaryAmountTypeCode.xsd BCG_GlobalPaymentMethodCode.xsd BCG_GlobalDocumentTypeCode.xsd BCG_BusinessDescription_Types.xsd BCG_BusinessTaxIdentifier_Types.xsd BCG_GlobalCountryCode.xsd BCG_GlobalPartnerClassificationCode.xsd BCG_string_len_0.xsd BCG_xml.xsd
PIP 3D8 Distribute Work in Process		
BCG_Package_RNIF1.1_3D8V01.00.zip	BCG_RNIF1.1_3D8V01.00.xml	BCG_3D8WorkInProgressNotification_V01.00.xsd
BCG_Package_RNIFV02.00_3D8V01.00.zip	BCG_RNIFV02.00_3D8V01.00.xml	BCG_common.xsd BCG_ContactInformation_Types.xsd BCG_PhysicalAddress_Types.xsd
BCG_Package_RNSC1.0_RNIF1.1_3D8V01.00.zip	BCG_RNSC1.0_RNIF1.1_3D8V01.00.xml	BCG_PartnerDescription_Types.xsd BCG_BusinessTaxIdentifier_Types.xsd BCG_GlobalPriorityCode.xsd
BCG_Package_RNSC1.0_RNIFV02.00_3D8V01.00.zip	BCG_RNSC1.0_RNIFV02.00_3D8V01.00.xml	BCG_GlobalWorkInProgressLocationCode.xsd BCG_GlobalProductUnitOfMeasureCode.xsd BCG_GlobalDocumentReferenceTypeCode.xsd BCG_GlobalWorkInProgressPartTypeCode.xsd BCG_GlobalLotCode.xsd BCG_GlobalLotStatusCode.xsd BCG_GlobalLotQuantityClassificationCode.xsd BCG_GlobalPartnerClassificationCode.xsd BCG_BusinessDescription_Types.xsd BCG_GlobalCountryCode.xsd BCG_string_len_0.xsd BCG_xml.xsd

Table 2-25. PIP document flow package contents

PIP 4A1 Notify of Strategic Forecast		
BCG_Package_RNIF1.1_4A1V02.00.zip	BCG_RNIF1.1_4A1V02.00.xml	BCG_4A1StrategicForecastNotification_V02.00.xsd
BCG_Package_RNIFV02.00_4A1V02.00.zip	BCG_RNIFV02.00_4A1V02.00.xml	BCG_common.xsd BCG_ContactInformation_Types.xsd BCG_PhysicalAddress_Types.xsd
BCG_Package_RNSC1.0_RNIF1.1_4A1V02.00.zip	BCG_RNSC1.0_RNIF1.1_4A1V02.00.xml	BCG_PartnerDescription_Types.xsd BCG_GlobalCurrencyCode.xsd BCG_GlobalForecastEventCode.xsd
BCG_Package_RNSC1.0_RNIFV02.00_4A1V02.00.zip	BCG_RNSC1.0_RNIFV02.00_4A1V02.00.xml	BCG_GlobalForecastTypeCode.xsd BCG_GlobalPartnerReferenceTypeCode.xsd BCG_GlobalProductUnitOfMeasureCode.xsd BCG_StrategicForecastQuantityTypeCode.xsd BCG_GlobalForecastIntervalCode.xsd BCG_BusinessDescription_Types.xsd BCG_BusinessTaxIdentifier_Types.xsd BCG_GlobalCountryCode.xsd BCG_GlobalPartnerClassificationCode.xsd BCG_string_len_0.xsd BCG_xml.xsd
PIP 4A3 Notify of Threshold Release Forecast		
BCG_Package_RNIF1.1_4A3V02.00.zip	BCG_RNIF1.1_4A3V02.00.xml	BCG_4A3ThresholdReleaseForecastNotification_V02.00.xsd
BCG_Package_RNIFV02.00_4A3V02.00.zip	BCG_RNIFV02.00_4A3V02.00.xml	BCG_common.xsd BCG_ContactInformation_Types.xsd BCG_PhysicalAddress_Types.xsd
BCG_Package_RNSC1.0_RNIF1.1_4A3V02.00.zip	BCG_RNSC1.0_RNIF1.1_4A3V02.00.xml	BCG_PartnerDescription_Types.xsd BCG_GlobalCurrencyCode.xsd BCG_GlobalForecastEventCode.xsd
BCG_Package_RNSC1.0_RNIFV02.00_4A3V02.00.zip	BCG_RNSC1.0_RNIFV02.00_4A3V02.00.xml	BCG_GlobalPartnerReferenceTypeCode.xsd BCG_GlobalProductUnitOfMeasureCode.xsd BCG_GlobalForecastIntervalCode.xsd BCG_GlobalForecastReferenceTypeCode.xsd BCG_GlobalForecastInventoryTypeCode.xsd BCG_OrderForecastQuantityTypeCode.xsd BCG_BusinessDescription_Types.xsd BCG_BusinessTaxIdentifier_Types.xsd BCG_GlobalCountryCode.xsd BCG_GlobalPartnerClassificationCode.xsd BCG_string_len_0.xsd BCG_xml.xsd

Table 2-25. PIP document flow package contents

PIP 4A5 Notify of Forecast Reply		
BCG_Package_RNIF1.1_4A5V02.00.zip	BCG_RNIF1.1_4A5V02.00.xml	BCG_4A5ForecastReplyNotification_V02.00.xsd
BCG_Package_RNIFV02.00_4A5V02.00.zip	BCG_RNIFV02.00_4A5V02.00.xml	BCG_common.xsd BCG_ContactInformation_Types.xsd BCG_PhysicalAddress_Types.xsd
BCG_Package_RNSC1.0_RNIF1.1_34A5V02.00.zip	BCG_RNSC1.0_RNIF1.1_4A5V02.00.xml	BCG_PartnerDescription_Types.xsd BCG_GlobalCurrencyCode.xsd BCG_GlobalForecastEventCode.xsd
BCG_Package_RNSC1.0_RNIFV02.00_4A5V02.00.zip	BCG_RNSC1.0_RNIFV02.00_4A5V02.00.xml	BCG_GlobalPartnerReferenceTypeCode.xsd BCG_GlobalProductUnitOfMeasureCode.xsd BCG_GlobalForecastIntervalCode.xsd BCG_GlobalForecastReferenceTypeCode.xsd BCG_GlobalForecastResponseCode.xsd BCG_GlobalForecastInventoryTypeCode.xsd BCG_GlobalForecastRevisionReasonCode.xsd BCG_GlobalPartnerClassificationCode.xsd BCG_ForecastReplyQuantityTypeCode.xsd BCG_BusinessDescription_Types.xsd BCG_BusinessTaxIdentifier_Types.xsd BCG_GlobalCountryCode.xsd BCG_string_len_0.xsd BCG_xml.xsd

Table 2-25. PIP document flow package contents

PIP 4B2 Notify of Shipment Receipt		
BCG_Package_RNIF1.1_4B2V01.00.zip	BCG_RNIF1.1_4B2V01.00.xml	BCG_4B2ShipmentReceiptNotification_V01.00.xsd
BCG_Package_RNIFV02.00_4B2V01.00.zip	BCG_RNIFV02.00_4B2V01.00.xml	BCG_common.xsd BCG_ContactInformation_Types.xsd BCG_PhysicalAddress_Types.xsd
BCG_Package_RNSC1.0_RNIF1.1_4B2V01.00.zip	BCG_RNSC1.0_RNIF1.1_4B2V01.00.xml	BCG_PartnerDescription_Types.xsd BCG_BusinessTaxIdentifier_Types.xsd BCG_GlobalCountryCode.xsd
BCG_Package_RNSC1.0_RNIFV02.00_4B2V01.00.zip	BCG_RNSC1.0_RNIFV02.00_4B2V01.00.xml	BCG_GlobalDocumentReferenceTypeCode.xsd BCG_GlobalLotDiscrepancyReasonCode.xsd BCG_GlobalPartnerRoleClassificationCode.xsd BCG_GlobalProductUnitOfMeasureCode.xsd BCG_GlobalReceivingDiscrepancyReasonCode.xsd BCG_GlobalReceivingDiscrepancyCode.xsd BCG_GlobalSpecialFulfillmentRequestCode.xsd BCG_GlobalSpecialHandlingCode.xsd BCG_GlobalTrackingReferenceTypeCode.xsd BCG_BusinessDescription_Types.xsd BCG_GlobalPartnerClassificationCode.xsd BCG_string_len_0.xsd BCG_xml.xsd
PIP 4C1 Distribute Inventory Report		
BCG_Package_RNIF1.1_4C1V02.03.zip	BCG_RNIF1.1_4C1V02.03.xml	BCG_4C1InventoryReportNotification_V02.03.xsd
BCG_Package_RNIFV02.00_4C1V02.03.zip	BCG_RNIFV02.00_4C1V02.03.xml	BCG_common.xsd BCG_ContactInformation_Types.xsd BCG_PhysicalAddress_Types.xsd
BCG_Package_RNSC1.0_RNIF1.1_4C1V02.03.zip	BCG_RNSC1.0_RNIF1.1_4C1V02.03.xml	BCG_BusinessDescription_Types.xsd BCG_BusinessTaxIdentifier_Types.xsd BCG_GlobalCountryCode.xsd
BCG_Package_RNSC1.0_RNIFV02.00_4C1V02.03.zip	BCG_RNSC1.0_RNIFV02.00_4C1V02.03.xml	BCG_GlobalDocumentReferenceTypeCode.xsd BCG_GlobalInventoryCode.xsd BCG_GlobalPartnerRoleClassificationCode.xsd BCG_GlobalProductUnitOfMeasureCode.xsd BCG_GlobalPartnerClassificationCode.xsd BCG_string_len_0.xsd BCG_xml.xsd

Table 2-25. PIP document flow package contents

PIP 5C1 Distribute Product List		
BCG_Package_RNIF1.1_5C1V01.00.zip	BCG_RNIF1.1_5C1V01.00.xml	BCG_5C1ProductListNotification_V01.00.xsd
BCG_Package_RNIFV02.00_5C1V01.00.zip	BCG_RNIFV02.00_5C1V01.00.xml	BCG_common.xsd BCG_ContactInformation_Types.xsd BCG_PartnerDescription_Types.xsd
BCG_Package_RNSC1.0_RNIF1.1_5C1V01.00.zip	BCG_RNSC1.0_RNIF1.1_5C1V01.00.xml	BCG_GlobalPartnerRoleClassificationCode.xsd BCG_GlobalPartnerClassificationCode.xsd
BCG_Package_RNSC1.0_RNIFV02.00_5C1V01.00.zip	BCG_RNSC1.0_RNIFV02.00_5C1V01.00.xml	BCG_GlobalCountryCode.xsd BCG_GlobalPriceTypeCode.xsd BCG_GlobalCurrencyCode.xsd BCG_BusinessDescription_Types.xsd BCG_BusinessTaxIdentifier_Types.xsd BCG_PhysicalAddress_Types.xsd BCG_string_len_0.xsd BCG_xml.xsd
PIP 5C4 Distribute Registration Status		
BCG_Package_RNIF1.1_5C4V01.02.zip	BCG_RNIF1.1_5C4V01.02.xml	BCG_5C4RegistrationStatusNotification_V01.02.xsd
BCG_Package_RNIFV02.00_5C4V01.02.zip	BCG_RNIFV02.00_5C4V01.02.xml	BCG_common.xsd BCG_ContactInformation_Types.xsd BCG_PhysicalAddress_Types.xsd
BCG_Package_RNSC1.0_RNIF1.1_5C4V01.023.zip	BCG_RNSC1.0_RNIF1.1_5C4V01.02.xml	BCG_PartnerDescription_Types.xsd BCG_GlobalCountryCode.xsd BCG_GlobalRegistrationComplexityLevelCode.xsd
BCG_Package_RNSC1.0_RNIFV02.00_5C4V01.02.zip	BCG_RNSC1.0_RNIFV02.00_5C4V01.02.xml	BCG_GlobalRegistrationInvolvementLevelCode.xsd BCG_GlobalPartnerRoleClassificationCode.xsd BCG_GlobalPartnerClassificationCode.xsd BCG_BusinessDescription_Types.xsd BCG_BusinessTaxIdentifier_Types.xsd BCG_string_len_0.xsd BCG_xml.xsd

Table 2-25. PIP document flow package contents

PIP 5D1 Request Ship From Stock And Debit Authorization Status		
BCG_Package_RNIF1.1_5D1V01.00.zip	BCG_RNIF1.1_5D1V01.00.xml	BCG_5D1ShipFromStockAndDebitAuthorizationConfirmation_V01.00.xsd
BCG_Package_RNIFV02.00_5D1V01.00.zip	BCG_RNIFV02.00_5D1V01.00.xml	BCG_5D1ShipFromStockAndDebitAuthorizationRequest_V01.00.xsd BCG_common.xsd
BCG_Package_RNSC1.0_RNIF1.1_5D1V01.00.zip	BCG_RNSC1.0_RNIF1.1_5D1V01.00.xml	BCG_BusinessDescription_Types.xsd BCG_ContactInformation_Types.xsd BCG_PhysicalAddress_Types.xsd
BCG_Package_RNSC1.0_RNIFV02.00_5D1V01.00.zip	BCG_RNSC1.0_RNIFV02.00_5D1V01.00.xml	BCG_PartnerDescription_Types.xsd BCG_GlobalCurrencyCode.xsd BCG_GlobalCountryCode.xsd BCG_GlobalPartnerRoleClassificationCode.xsd BCG_GlobalProductUnitOfMeasureCode.xsd BCG_GlobalDocumentReferenceTypeCode.xsd BCG_GlobalPartnerClassificationCode.xsd BCG_GlobalPriceTypeCode.xsd BCG_GlobalShipFromStockAndDebitAuthorizationRejectionCode.xsd BCG_BusinessTaxIdentifier_Types.xsd BCG_string_len_0.xsd BCG_xml.xsd

Table 2-25. PIP document flow package contents

PIP 7B1 Distribute Work in Process		
BCG_Package_RNIF1.1_7B1V01.00.zip	BCG_RNIF1.1_7B1V01.00.xml	BCG_7B1WorkInProgressNotification_V01.00.xsd
BCG_Package_RNIFV02.00_37B1V01.00.zip	BCG_RNIFV02.00_7B1V01.00.xml	BCG_common.xsd BCG_ContactInformation_Types.xsd BCG_PhysicalAddress_Types.xsd
BCG_Package_RNSC1.0_RNIF1.1_7B1V01.00.zip	BCG_RNSC1.0_RNIF1.1_7B1V01.00.xml	BCG_PartnerDescription_Types.xsd BCG_GlobalChangeReasonCode.xsd BCG_GlobalDocumentReferenceTypeCode.xsd
BCG_Package_RNSC1.0_RNIFV02.00_7B1V01.00.zip	BCG_RNSC1.0_RNIFV02.00_7B1V01.00.xml	BCG_GlobalEquipmentTypeCode.xsd BCG_GlobalLotCode.xsd BCG_GlobalLotStatusCode.xsd BCG_GlobalLotQuantityClassificationCode.xsd BCG_GlobalPartnerRoleClassificationCode.xsd BCG_GlobalPriorityCode.xsd BCG_GlobalProductUnitOfMeasureCode.xsd BCG_GlobalWorkInProgressTypeCode.xsd BCG_GlobalWorkInProgressQuantityChangeCode.xsd BCG_GlobalWorkInProgressLocationCode.xsd BCG_GlobalWorkInProgressPartTypeCode.xsd BCG_BusinessDescription_Types.xsd BCG_BusinessTaxIdentifier_Types.xsd BCG_GlobalCountryCode.xsd BCG_GlobalPartnerClassificationCode.xsd BCG_string_len_0.xsd BCG_xml.xsd
PIP 0A1 Notification of Failure v1.0		
BCG_Package_RNIF1.1_0A11.0.zip	BCG_RNIF1.1_0A11.0.xml	0A1FailureNotification_1.0.xml BCG_0A1FailureNotification_1.0.xsd BCG_GlobalPartnerClassificationCode.xsd
BCG_Package_RNSC1.0_RNIF1.1_0A11.0.zip	BCG_RNSC1.0_RNIF1.1_0A11.0.xml	BCG_GlobalPartnerRoleClassificationCode.xsd BCG_common.xsd BCG_string_len_0.xsd BCG_xml.xsd

Table 2-25. PIP document flow package contents

PIP 0A1 Notification of Failure V02.00.00		
BCG_Package_RNIF1.1_0A1V02.00.zip	BCG_RNIF1.1_0A1V02.00.xml	0A1FailureNotification_V02.00.xml BCG_0A1FailureNotification_V02.00.xsd BCG_common.xsd
BCG_Package_RNIFV02.00_0A1V02.00.zip	BCG_RNIFV02.00_0A1V02.00.xml	BCG_GlobalPartnerClassificationCode.xsd
BCG_Package_RNSC1.0_RNIF1.1_0A1V02.00.zip	BCG_RNSC1.0_RNIF1.1_0A1V02.00.xml	BCG_GlobalPartnerRoleClassificationCode.xsd
BCG_Package_RNSC1.0_RNIFV02.00_0A1V02.00.zip	BCG_RNSC1.0_RNIFV02.00_0A1V02.00.xml	BCG_string_len_0.xsd BCG_xml.xsd

Updating alert mail addresses

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 within BCG.Properties are:
 - bcg.alertNotifications.mailHost
 - bcg.alertNotifications.mailFrom
 - bcg.alertNotifications.mailReplyTo
 - bcg.alertNotifications.mailEnvelopeFrom
2. Restart the router in order for the changes to take affect.

Managing XML formats

XML, or Extensible Markup Language, is the universal format for structured documents and data on the World Wide Web. XML is increasingly becoming the general standard document format of structured data. Using the Manage XML Protocols screen, you can create and manage custom XML formats that can be added to Document Flow Definitions.

An XML format defines the paths within a set of XML documents. Using this information, you can create and manage custom XML formats that can be added to the system as a Document Flow Definition. An XML format defines the paths within a set of XML documents. This enables the Document Manager to retrieve the values that uniquely identify an incoming document and access information within the document necessary for proper routing and processing.

NOTE: When using a custom XML format within the Backend Integration package, the Document Manager will override the protocol and use the x-aux values contained in the document HTTP/S header to determine the protocol, protocol version, document flow, and document flow version (see example below). However, if using a custom XML format combined with a non Backend Integration package such as AS1, AS2, None, or RNIF, the system will normally determine the protocol, protocol version, document flow, and document flow version from the element path defined in the XML format guideline.

Example HTTP/S header:

```
From HTTP/S Post set headers=%headers% x-aux-protocol: XML x-aux-protocol-version:
1.0 x-aux-sender-id: 987654321 x-aux-receiver-id: 102420488 x-aux-process-type:
XML_DTD x-aux-process-version: 1.0 x-aux-production: true x-aux-system-msg-id:
GWYN_OBID_H2_DTD_00000004
```

Creating an XML format

To create an XML format, use the following procedure.

1. Click **Hub Admin > Hub Configuration > XML Formats**. The Console displays the Manage XML Formats screen.
2. Click **Create XML Format** in the upper right corner of the screen. The Console displays the View XML Format screen.
3. Complete the following parameters in the screen:

Table 2-26. View XML Format

Parameter	Description
Routing Format	The Document Flow Definition with which this protocol will be associated. This definition must be created before creating the XML format (see “Implementing Document Flow Definitions” on page 30).
File Type	XML is the only option.
Identifier Type	The element used to identify the incoming document type: DTD, Name Space, or Root Tag.
Source / Target BusinessId	Path of the Business ID. For Type, select: <ul style="list-style-type: none">• Element Path – path to Business ID in document.• Constant – actual Business ID value in document.


Table 2-26. View XML Format (continued)

Parameter	Description
Source Document Flow	An expression that defines the path to the document flow within the XML document. For Type, select: <ul style="list-style-type: none">• Element Path – path to value in document.• Constant – actual value in document.
Source Document Flow Version	An expression that defines the path to the version value within the XML document. For Type, select: <ul style="list-style-type: none">• Element Path – path to value in document.• Constant – actual value in document.
Document Identifier	Path for the document ID number.
Document Timestamp	Path for the document creation timestamp.
Duplicate Check Key 1 – 5	Paths for identifying the routing of a duplicate document. For Type, select: <ul style="list-style-type: none">• Element Path – path to check key value in document.• Constant – actual check key value in document.

4. Click **Save**.

Editing XML format values

There may be times when you need to edit XML format values. To edit these values, use the following procedure.


1. Click **Hub Admin > Hub Configuration > XML Formats**. The Console displays the Manage XML Formats screen.
2. Click the  icon next to the XML format you want to edit. The Console displays the View XML Protocol screen, with the values that have already been defined for the selected XML protocol.
3. Change the appropriate values. If you need assistance, see [Table 2-26](#).
4. Click **Save**.

Deleting an XML format

If you no longer need an XML format, use the following procedure to delete it.

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.

IMPORTANT: Deleting an XML format disables any pre-existing connection 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**. The Console displays the Manage XML Formats screen.
2. Click the  icon next to the XML format you want to delete. The XML format is deleted.

Enabling or disabling Actions

The Actions screen is a read-only screen that shows the steps the system uses when processing documents. Click **Hub Admin > Hub Configuration > Actions** to display the Actions screen.

Figure 2-4 shows an example of an Actions screen. The following parameters are displayed for each action:

- Action Name — name used to identify action based on activities the action will perform.
- Status — when enabled, the action is available to the hub-community for creating or updating a connection.

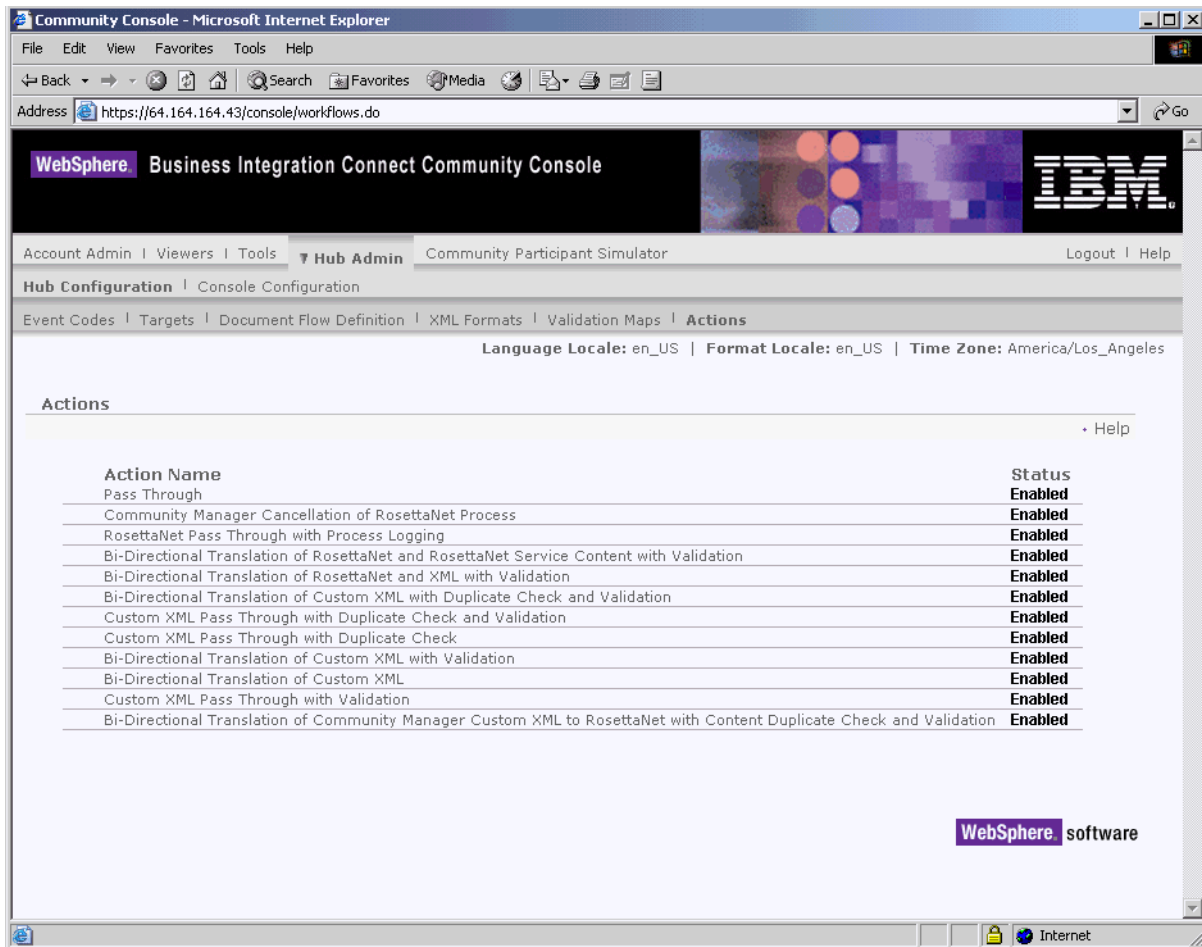


Figure 2-4. Actions Screen

Managing event codes

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

Viewing and editing permission details

The following procedure describes how to view details for an event code. As part of this procedure, you can edit the visibility and alertable status of the event code and view the severity of the code.


1. Click **Hub Admin > Hub Configuration > Event Codes**. The Console displays the Event Codes screen.
2. Click the  icon next to the event code whose details you want to view. The Console displays the Event Code Details screen.
3. Complete the following parameters in the screen:

Table 2-27. Event Code Details

Parameter	Description
Event Code	Read-only field that shows the unique number for this event code.
Event Name	Read-only field that shows the name used to identify event in relation to action that triggered the event.
Internal Description	Read-only field that describes the circumstances that triggered the event.
Visibility	Check the users that will be able to view the event code: Community Operator, Manager, or Participant.
Severity	Read-only field that shows the seriousness associated with this event code, from Debug (least serious) to Critical (most serious): <ul style="list-style-type: none">• Debug – used for low-level system operations and support. Visibility and use are subject to the permission level of the user.• Info – generated when a system operation ends successfully. These events are also used to provide the status of documents being processed. Informational events require no user action.• Warning – occurs due to non-critical anomalies in document processing or system functions that allow the operation to continue.• Error – occurs due to anomalies in document processing that cause the process to end.• Critical – generated when services end due to system failure. Critical events require intervention by support personnel.
Alertable	When checked, the event appears in the Event Name drop-down list on the Define tab of the Alert screen. This allows an alert to be set for this event. The procedure for associating an alert with an event is described in the WebSphere Business Integration Connect Community Console User Guide.

Saving event code names

The Event Codes screen provides two ways to save event codes:

- Click **Export Names** to save only the event names in the event list.

- Click **Export Text** to save the internal descriptions in the event list in text format.

To save event names or internal descriptions, use the following procedure:

1. Click **Hub Admin > Hub Configuration > Event Codes**. The Console displays the Event Codes screen.
2. Click **Export Names** or **Export Text**, depending on what you want to export. The Console displays the File Download screen.
3. Click **OK**.
4. When prompted, save the exported file. Click **Save**.

Sending and receiving large files

If you are going to send or receive large files (those larger than 50 megabytes), you must make some changes to your configuration, as described in the following steps:

1. Open the following file for editing:
<wbic-root>\router\scripts\bcgSetJVMHeapAttrs.jacl.
2. Change the value of the following property so that it is set to the maximum Java VM heap size needed to process your largest file:

```
MAX_HEAP_SIZE="512"
```

A value of "1024" should be sufficient to process a 100-megabyte file sent through AS2.

3. Save the change to the bcgSetJVMHeapAttrs.jacl file.
4. Open a command prompt to <wbic-root>\router\was\bin. Then run the script with the following command:

```
[Windows]  
wsadmin -conntype NONE -f <wbic-root>  
\router\scripts\bcgSetJVMHeapAttrs.jacl
```

```
[Unix]  
./wsadmin.sh -conntype NONE -f <wbic-root>  
\router\scripts\bcgSetJVMHeapAttrs.jacl
```

Be sure to substitute the actual path for <wbic-root>. After the script runs the values for min and max heap have been changed.

5. Restart the Document Manager so that the changes take effect.

Note: To set the maximum size for inbound and outbound files, edit the bcg.bpe_max_file_size=0 property in the router\was\wbic\config\bcg.properties file. See [“BCG.Properties” on page 175](#).

Changing the database, database user, and password

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

- Windows platform

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 Admin Activities

This chapter describes how to perform the following Account Admin activities:

- [“Managing Participant profiles” on page 101](#)
- [“Managing gateway configurations” on page 105](#)
- [“Creating an FTP account” on page 113](#)
- [“Managing certificates” on page 114](#)
- [“Managing B2B capabilities” on page 117](#)
- [“Managing Participant connections” on page 120](#)
- [“Managing Exclusion Lists” on page 126](#)

These Account Admin activities can be performed by the Hub Admin, Manager Admin, and Participant Admin users, with the following limitations:

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

Managing Participant profiles

The Account Admin Participants feature allows Hub Admin users to create, view, and edit Participant profile. A Participant profile identifies companies to the system.

NOTE: Participant Admin and Manager Admin users can only edit their own Participant Profile.

Creating Participants

Hub Admin users can create new Participants using the following procedure.

1. Click **Account Admin > Profiles > Community Participant**.
2. Click **Create** in the upper right corner. The Console displays the New Participant screen.
3. Complete the parameters as shown in [Table 3-1 on page 102](#).

Table 3-1. Participant Detail Screen Parameters

Parameter	Description
Participant Login Name / Participant Name	Name that identifies the trading entity to the system. Both the company name and a modified version used for login are used.
Participant Type	<p>Community Operator, Participant, or Community Manager.</p> <ul style="list-style-type: none"> The Community Operator is responsible for managing day-to-day operation of the hub-community. This can include maintaining the hardware and software infrastructure, ensuring the hub-community is properly configured for use, and assisting with the adding of new Participants. The Community Participant is the individual company conducting business with the Community Manager via the hub-community. The Community Manager is responsible for purchasing and building the hub-community. This can include defining the electronic business processes exchanged between them and their Participants. <p>The system supports one Community Operator and one Community Manager. Trying to create a second Community Operator or Community Manager displays the error message "An error occurred while saving this record."</p>
Participant Status	Enabled or Disabled. If disabled, the Participant will be absent from all search criteria and drop-down menus in the Tools and Viewers modules.
Vendor Type	Business function. Vendor Type is used during provisioning.
Web Site	Participant Web site. Web site is used during Provisioning.
Business ID	<p>DUNS, DUNS+4, or Freeform number that the system uses to route documents.</p> <ul style="list-style-type: none"> DUNS numbers must equal nine digits. DUNS+4 numbers must equal 13 digits. Freeform ID numbers accept up to 60 alpha, numeric, and special characters.
IP Address	Gateway type and corresponding IP address for receiving incoming documents.

4. Click **New** under **Business ID**.

5. Specify a business ID type and input the appropriate identifier.

NOTE: To remove an identifier from the system, type the identifier and check **Remove**. The identifier will be removed when you click **Save**.

Observe the following guidelines when typing the identifier:



- DUNS numbers must equal nine digits.
- DUNS+4 must equal 13 digits.
- Freeform ID numbers accept up to 60 alphanumeric and special characters.

6. Under **IP Address**, click **New**.
7. Specify the gateway type and input the Participant's IP address(es).
8. Click **Save**.

NOTE: The system supports one Community Operator and one Community Manager. Trying to create a second Community Operator or Community Manager displays the error message "An error occurred while saving this record."

Viewing and editing Participant profiles

There might be times when you need to modify a Participant profile. Use the following procedure 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. The Console displays the Participant Details screen.
4. Click the  icon to edit the profile details.
5. Modify the Participant profile as necessary (see [Table 3-1](#)).

NOTE: If you click **Reset User Passwords**, the Console displays the message in [Figure 3-1](#). Click **OK** to proceed (the Console displays the message in [Figure 3-2 on page 103](#)) or click **Cancel** to retain the passwords. If you clicked **OK**, click it again to reset the passwords or click **Cancel** to not reset them.

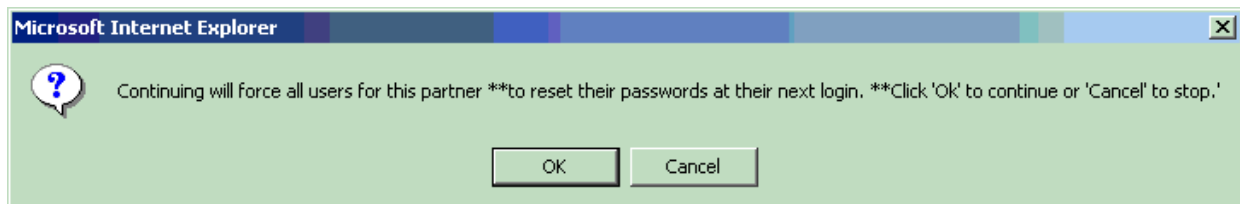


Figure 3-1. Reset User Password Message

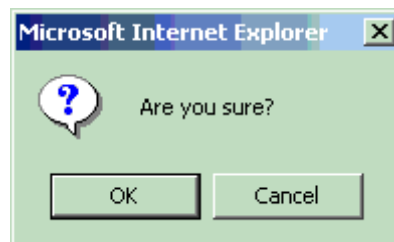




Figure 3-2. Are You Sure Message

6. When you finish, click **Save**.


Searching for Participants

The Participants screen allows the system to find Participants that meet your search criteria.

1. Click **Account Admin > Profiles > Community Participant**.
2. Type the Participant name or business ID in the appropriate text boxes.
3. Click **Search**. The system finds that Participants that match your criteria.
4. To change the Participant's 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 and see [Table 3-1 on page 102](#).
7. When you finish, click **Save**.

Viewing your profile

To view your profile, use the following procedure.


1. Click **Account Admin > Profiles > Community Participant**.
2. Click **My Profile** in the upper right corner of the screen.
3. Click the  icon to edit your profile.
4. Edit your profile (see [Table 3-1 on page 102](#)).
5. When you finish, click **Save**.

Managing gateway configurations

Use gateways to 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.

Viewing and editing gateways

Use the following procedure to view the gateways configured for the system and edit them.

1. Click **Account Admin > Profiles > Gateways**.
2. To change the access of a gateway, click **Online** or **Offline** under the **Access** column.
3. To change the status of a gateway, click **Enabled** or **Disabled** under the **Status** column.
4. Click the  icon to view gateway details.
5. To edit the gateway details, click the  icon. The Console displays the Gateway Detail screen. Edit the parameters in the screen (see [Table 3-2 on page 105](#)), then click **Save**.

Alternatively, you can delete this gateway by clicking **Delete**.

Table 3-2. 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	Indicate 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 107).
Target URI	Uniform Resource Identifier (URL) 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).

Table 3-2. Gateway Detail Screen (continued)

Parameter	Description
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 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 default gateways

Use the following procedure 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**.
5. Alternatively, you can delete this default gateway by clicking **Delete**.

Creating gateways



To create gateways, use the following procedure.

1. Click **Account Admin > Profiles > Gateways**.
2. Click **Create** in the upper right corner of the screen. The Console displays the Gateway Detail screen.

3. Complete the parameters in the screen (see [Table 3-2 on page 105](#)).
4. 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**.

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

NOTE: 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.

Managing FTP

If you do not plan to use Business Integration Connect's FTP functionality, you can disregard this section. The Community Operator may disable this feature if your company is not using FTP.

FTP is a file transfer protocol used to copy files to and from remote computer systems on the Internet. Business Integration Connect can receive inbound documents through FTP.

All XML sent by a Participant to Business Integration Connect must be XML documents that have all of the required routing information in the content of the document. All other documents are treated as binary documents for pass-through routing.

NOTE: Consult your security and system administrators before integrating FTP functionality into WebSphere Business Integration Connect. Certain FTP implementations can result in security concerns. Pay close attention to file permissions and directory owners. The bcguser (or whatever account the WebSphere Business Integration Connect application is running under) requires read and write access to all files sent in via FTP.

Community Console FTP configuration

The Hub Admin uses the Community Console to perform the following tasks:

- Enable or disable FTP for Participants.
- Set the password for the FTP login.

If you are a Participant, you can enable your own FTP account through the console. However, documents cannot be received by the Community Manager until the Hub Admin creates a target to receive documents through FTP.

When your FTP account is enabled, Business Integration Connect performs the following tasks:

- Creates a user account in the FTP server. The FTP login name is the Participant's login name and the initial password is auto-generated.
- Creates a home FTP login for the Participant. The home directory is the login name of the Participant.
- Creates binary and document sub-directories under the Participant's home directory, and a sub-directory below both the binary and document sub-directories for each gateway type configured in the product. For more information about the FTP directory structure, see ["Creating a valid FTP directory structure" on page 109](#).

The Community Console allows Participants to view the information they need to transfer files using FTP. This includes the following information:

- The user name to log in to the FTP server (not editable).
- Account status (Enabled or Disabled). Participants can view and change their FTP account status.
- Password for FTP account (editable).
- The hostname of the Community Manager's FTP server. For example: ftp.myHub.com <ftp://ftp.myHub.com> (not editable).

Participants can update the password used to log in to the FTP server. Note that this password is different from the password the Participant uses to log in to the console. When updating the password, Business Integration Connect's password policy is enforced.

Creating a valid FTP directory structure

When FTP is enabled for a Participant, the user must create the following three-level directory structure under the default FTP directory at /<common shared directory>/receiver/ftp. These directories must have the same read/write permission given to the Business Integration Connect receiver application:

<Participant FTP Login1> (The FTP login must match the Community Console login user name.)

- binary
 - <destination type 1>
 - <destination type 2>
- documents
 - <destination type 1>
 - <destination type 2>

<Participant FTP Login2>

- binary
 - <destination type 1>
 - <destination type 2>
- documents
 - <destination type 1>
 - <destination type 2>

<Participant FTP LoginN>

The receiver will only scan a maximum of three FTP sub-directory levels. All directories deeper than three levels will be ignored. Second level directories must also be named *binary* and *documents*. The receiver will ignore any second-level directory with a name other than *binary* or *documents*. There is no naming restriction on third-level directories, therefore, the receiver will scan all third-level directories for FTP documents. The user must ensure that third-level directories contain FTP documents suitable for routing.

The Participant transfers files to IBM WebSphere Business Integration Connect by putting the file in the directory corresponding to the correct document type (binary or documents) and correct destination type.

It is assumed that all documents placed in a destination type directory under the documents directory are documents that include all routing information within the document. These are limited to custom XML formats defined in the product. It is the responsibility of the Participant to ensure that the files they transfer using FTP do not clash with any existing files within the FTP directory. All documents placed in a destination type directory under the binary directory must follow specific file naming conventions.

Binary file naming convention

Files sent by FTP and placed in a destination type sub-directory under the Participant's Binary sub-directory must conform to the following naming convention that identifies the file's destination:

<To Business Identifier>.<unique name>

The following is a description of each part of the file name:

- *<To Business Identifier>* represents one of the business identifiers associated with the destination Participant.
- *.* is the period character.
- *<unique name>* is any set of valid file name characters, and can contain the '.' (period) character. The unique name ensures that the full file name does not conflict with the names of any other transferred files.

The complete list of valid file name characters is dependent on the FTP server and operating system where the product is installed.

The system does not process Binary files other than ensure that the sending community member has permission (that is, a connection) to send to the destination community member. The system passes the binary file exactly as received to the destination community member.

Setting up FTP

Most FTP servers use system accounts as FTP user accounts. You are responsible for user account management and can modify the scripts, shown in [Table 3-3](#) to support your FTP server.

Using the same user for FTP and Business Integration Connect eliminates permission issues.

Your FTP server can be installed in any directory, as long as the directory allows Business Integration Connect read-write permissions, and the configuration points to the shared directory.

FTP script functions

The scripts shown in [Table 3-3](#) must exist in 4.2.1 for the Console to function properly. They only contain comments, but can be modified according to your FTP server environment. Their descriptions provide an example of how they can be used.

FTP values are stored in your FTP server's configuration file.

Business Integration Connect FTP scripts are located in the *../<common shared directory>/ftp/bin/* directory.

The following table describes the purpose of each script. You can modify the scripts (recommended) or manually edit the FTP password file. Your FTP password file is identified in your FTP configuration file.

Table 3-3. FTP scripts and their functions

Script	Function
con_createFtpAcct.sh	<p>This script creates a FTP account on the FTP server. This script will need to provide the correct formatting for your FTP server's password file, or call an appropriate external program to add an account.</p> <p>Number of input parameters: 1.</p> <p>Description of input parameters: By default, the login and password delimited by a double-colon '::'. This delimiter can be changed in the <i>bcg_console.properties</i> file.</p> <p>Output: Error messages.</p> <p>Error messages are dependent on the operating system and actions being taken. If the FTP server uses a UNIX style file based password file, an error you may see is "Unable to open file". Another possible error is "Account already exists" an account is added that already exists.</p> <p>See the text that follows this table for an example of an FTP password file.</p>
con_createFtpDirectories.sh	<p>This script creates a directory. The full absolute path of the directory must be specified. WebSphere Business Integration Connect will call this script for each directory that needs to be created.</p> <p>Number of input parameters: 1.</p> <p>Description of input parameters: The directory to be created.</p> <p>Output: Error Messages.</p> <p>Error messages are dependent on the operating system and actions being taken. A possible error messages is "Directory already exists".</p>
con_disableFtpAcct.sh	<p>This script disables a FTP account on the FTP server.</p> <p>Number of input parameters: 1.</p> <p>Description of input parameters: Login to be disabled.</p> <p>Output: Error Messages</p> <p>Error messages are dependent on the operating system and actions being taken. A possible error messages is "Login does not exist".</p>

Table 3-3. FTP scripts and their functions

Script	Function
con_enableFtpAcct.sh	<p>This script enables a FTP account on the FTP server that was previously disabled.</p> <p>Number of input parameters: 1.</p> <p>Description of input parameters: Login to be enabled.</p> <p>Output: Error Messages</p> <p>Error messages are dependent on the operating system and actions being taken. A possible error messages is "Login does not exist".</p>
con_modifyFtpAcct.sh	<p>This script changes the password of a FTP account on the FTP server.</p> <p>Number of input parameters: 1.</p> <p>Description of input parameters: By default, the login and password delimited by a double-colon ':'. This delimiter can be changed in the bcg_console.properties file.</p> <p>Output: Error Messages</p> <p>Error messages are dependent on the operating system and actions being taken. A possible error messages is "Login does not exist".</p>

The following are sample entries in an FTP password file.

```
Username1:2ES.ehig1fRHqvc:2002:100::/opt/IBM/WBIC/shared/vms/receiver/ftp/username1:/bin/bash
```

```
Username2:979HSRGpv1WI6:2003:100::/opt/IBM/WBIC/shared/vms/receiver/ftp/username2:/bin/bash
```

The following is a description of the fields in these entries:

Table 3-4. Description of fields in FTP password file

Field	Description
Field 1	The account login
Field 2	Encrypted password
Field 3	User ID
Field 4	Group ID
Field 5	Not Used
Field 6	Account home directory
Field 7	shell - not used

Creating an FTP account

The File Transfer Protocol (FTP) is a protocol used on the internet for sending files. Documents sent by participants to the WebSphere Business Integration Connect system are routed through an FTP server. You can create an FTP account for routing documents using the FTP module.

NOTE: FTP documents routed to the system with a disabled status or incorrect password are rejected.

Consult your security and system administrators before integrating FTP functionality into WebSphere Business Integration Connect. Certain FTP implementations can result in security concerns. Pay close attention to file permissions and directory owners. The bcguser (or whatever account the WebSphere Business Integration Connect application is running under) requires read and write access to all files sent in via FTP.

Specifying an FTP server

To define an FTP server for Business Integration Connect, use the following procedure.

1. Click **Account Admin > Profiles > FTP**.

NOTE: The FTP module's default status is disabled. If FTP is not visible, contact your hub administrator to enable the FTP module.


2. Click **Create New FTP Account**. The system creates the account with a system-supplied password.
3. To change the password or status, click the  icon. The Console displays the FTP screen.
4. Complete the following parameters in the screen:

Table 3-5. FTP Configuration Screen

Value	Description
Account Status	Allows you to enable or disable your FTP account.
Password	Password for access to the FTP directory. For security, each password character is displayed as an asterisk (*).
Re-enter Password	Same entry as Password. For security, each password character is displayed as an asterisk (*).

5. Click **Save**.

Editing FTP details

To change the FTP password or status, use the following procedure.


1. Click **Account Admin > Profiles > FTP**.
2. Click the  icon.
3. Complete the following parameters in the screen:

Table 3-6. FTP Configuration Screen

Value	Description
Account Status	Allows you to enable or disable your FTP account.
Password	Password for access to the FTP directory. For security, each password character is displayed as an asterisk (*).
Re-enter Password	Same entry as Password. For security, each password character is displayed as an asterisk (*).

4. Click **Save**.

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, refer to [“Administering Certificates” on page 157](#).

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 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. Complete the following parameters in the screen, then click **Save**. Alternatively, you can delete the certificate by clicking **Delete**.

Table 3-7. Digital Certificate Parameters

Parameter	Description
Certificate Type	Type of digital certificate: <ul style="list-style-type: none">• 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.

Creating digital certificates

To create digital certificates, use the following procedure.

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 **Create**. The Console displays the Create New Certificate screen.
3. Complete the parameters as shown in [Table 3-8 on page 116](#).

Table 3-8. Digital Certificate Parameters



Parameter	Description
Certificate Type	Type of digital certificate: <ul style="list-style-type: none">• 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.
Certificate	Type the path and name of the certificate you want to use or browse and select the certificate.
private Key	Type the path and name of the private key you want to use for this certificate or browse and select the private key.
Password	Type the password you want to use.
Gateway Type	If you are creating an SSL certificate, select the type of gateway associated with the certificate.

NOTE: If a connection requires a digital certificate, and all certificates for that connection are disabled, the document fails processing.

4. Click **Upload**.

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**.

Managing B2B capabilities

The B2B industry consists of various business processes, protocols, and delivery standards. Business Integration Connect supports these different business-collaboration types using the concepts of Document Flow Definitions and nodes. With Document Flow Definitions and nodes, the Participant types his or her B2B capabilities into the system, so connections can be created for document routing and processing.

The core of Business Integration Connect is B2B connectivity between disparate business processes, protocols, and delivery standards. The system handles these requirements using Document Flow Definitions and nodes. Participants use the B2B Capabilities feature to define their B2B capabilities using Document Flow Definitions and nodes.

A Document Flow Definition is a collection of metadata that defines how Business Integration Connect processes a specific set of documents. This information includes the name, version, type, attributes, and context to which the Document Flow Definition belongs. See [“Implementing Document Flow Definitions” on page 30](#) for more information.

Because of the different types of business processes, protocols, and delivery standards available in the B2B industry, the system contains different node configurations to meet the various business-processing requirements of the Community Manager and Participants. To ensure that the system meets these requirements, you can use the B2B Capabilities feature to associate a Participant's B2B capabilities to a Document Flow Definition. The system then uses values added to each Document Setting B2B capabilities

Use the following procedure to set the B2B capabilities of your system.

1. Click **Account Admin > Profiles > B2B Capabilities**. The Console displays the B2B capabilities screen (see [Figure 3-3 on page 118](#)). The right side of the screen shows the packages, protocols, and business processes supported by the system as Document Flow Definitions (for more information, see [“About Document Flow Definition types” on page 30](#)).

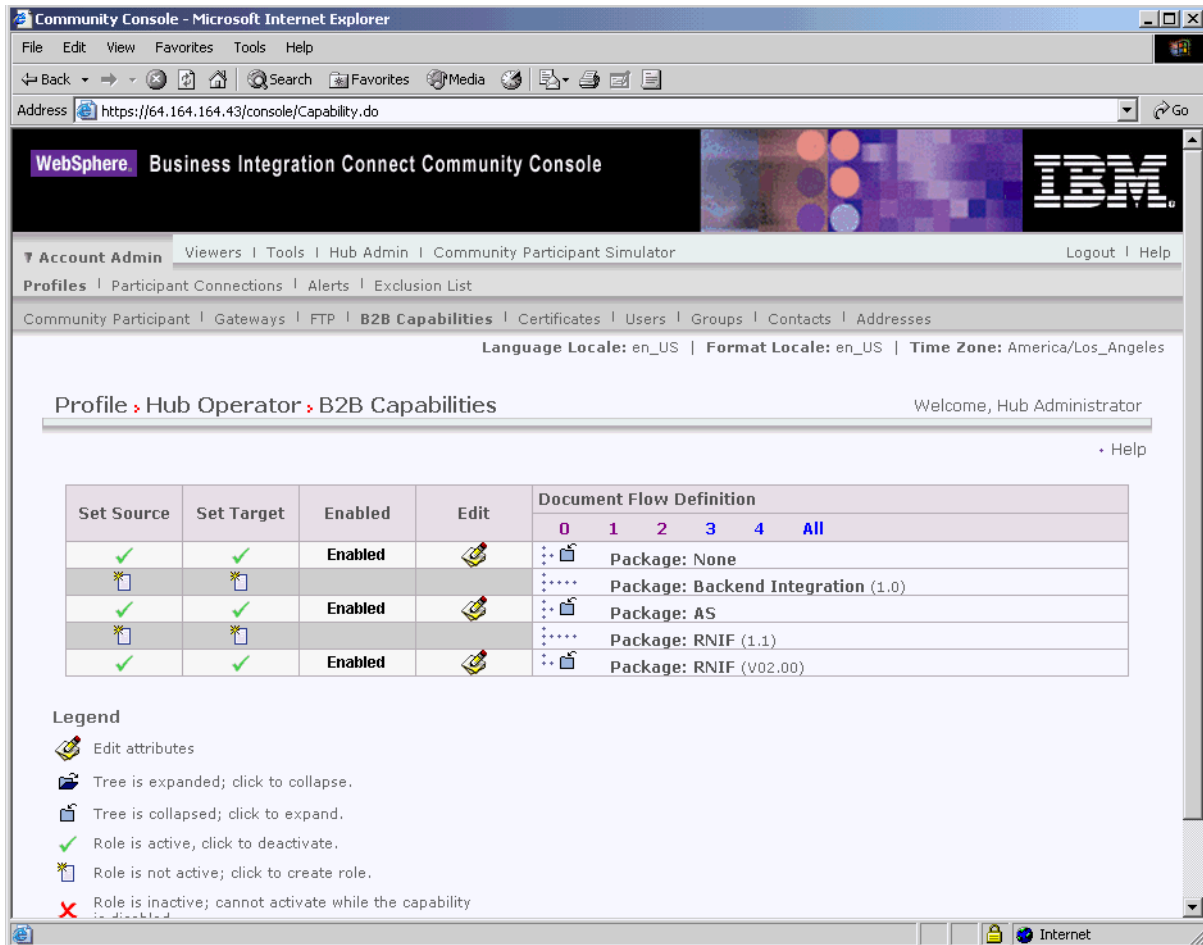






Figure 3-3. B2B Capabilities Screen

2. Click the  icon under the **Set Source** column for the Packages on the right that contain business processes you will send to the Community Manager.
Click the  icon under **Set Target** for the Packages that contain business processes you will receive from the Community Manager.
Select both if you will send and receive those same processes. The Console displays a  icon if the Document Flow Definition is enabled.
NOTE: The selection of **Set Source** will be the same for all actions in 2-way PIP regardless that the request will originate from one Participant and the corresponding confirmation from another. This also applies to **Set Target**.
3. Click the  icon at the Package level to expand an individual 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.

Again, select the **Set Source**, **Set Target**, or both roles for the lower Protocol, Document Flow, Action, and Activity levels for each Document Flow Definition your system supports.


TIP: If a definition is activated at the Document Flow level, both the Action and Activity definitions will be activated automatically.

4. (Optional) Click **Enabled** under the **Enabled** column to place a Document Flow Definition offline. Click **Disabled** to place online.

NOTE: If a package Document Flow Definition is disabled, all lower-level Document Flow Definitions in that same node are also disabled, regardless of whether their individual status was enabled.

If a lower-level Document Flow Definition is disabled, all higher-level definitions within the same node remain enabled.

When a Document Flow Definition is disabled, all preexisting connections and attributes continue to function. The disabled Document Flow Definition only restricts the creation of new connections.


5. (Optional) Click the  icon to display the screen in [Figure 3-4 on page 120](#). Then edit the attribute values for each Document Flow Definition.
6. Click **Save**.

Changing B2B attribute values

Attributes values give a Document Flow Definition its functionality. The system uses the attribute values for various document processing and routing functions such as validation, checking for encryption, retry count, synchronous or asynchronous communication, etc. Changes to the attribute values for a higher-level Document Flow Definition will be inherited by the lower-level definitions within the same node.

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

1. Click **Account Admin > Profiles > B2B Capabilities**. The Console displays the B2B capabilities screen (see [Figure 3-3 on page 118](#)).
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.

- Click the  icon to display the screen in [Figure 3-4 on page 120](#). Then modify the appropriate attribute values in the **Update** column.

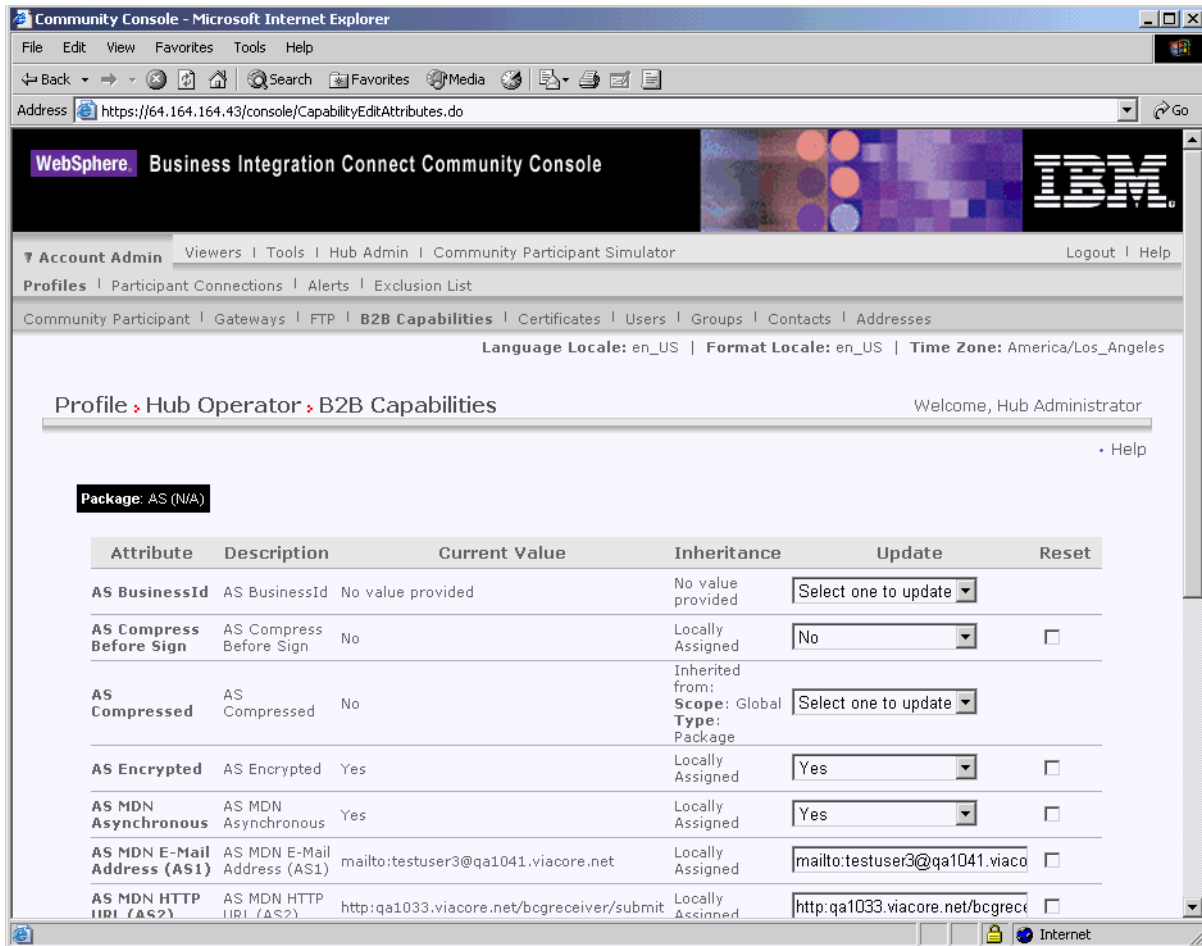


Figure 3-4. Screen for Changing B2B Attribute Values

- 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 the 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 3-9](#) describes each component.

Table 3-9. Manage Participant Components

Component	Description
Attributes	<p>Attributes are the information the connection uses for various document processing and routing functions such as validation, checking for encryption, and retry count.</p> <p>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.</p>
Action	<p>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.</p>
Gateway	<p>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.</p> <p>The target gateway contains the URI and transport information of the Participant receiving a document flow.</p>
Gateway Type	<p>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 than 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.</p>

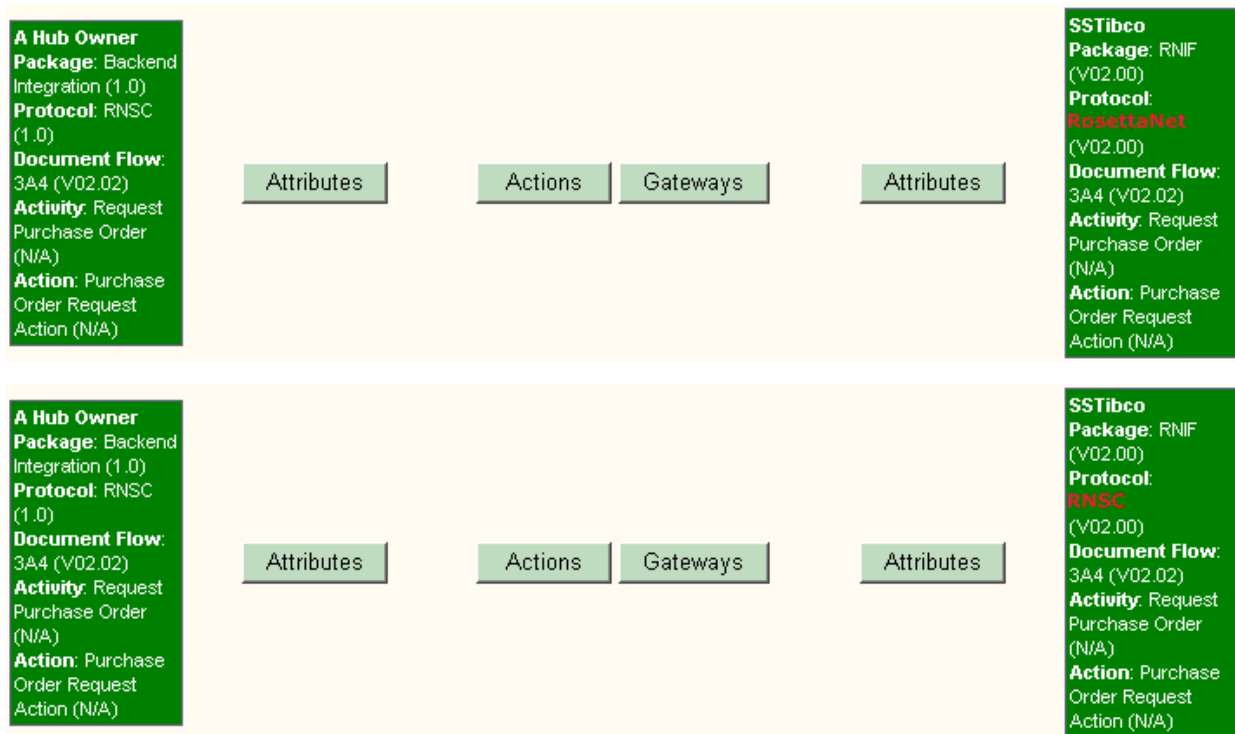
Connection duplication

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 124.](#)

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 125.](#)
- 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 125.](#)
- 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 126.](#)

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 3-10](#):

Table 3-10. 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, disabled, or 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 123](#)) or advanced search for connections ([“Performing an advanced search for connections” on page 124](#)).
3. See the appropriate section:
 - To change Participant attribute values, see [“Changing Participant attribute values,”](#) below.
 - To select a new action, see [“Selecting a new action,”](#) below.
 - To change the source or target gateway, see [“Changing the source or target gateway” on page 126](#).
 - To disable or activate a configuration, see [“Disabling or deactivating a connection” on page 126](#).

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. Web Services Support

WebSphere Business Integration Connect can be invoked by a Community Participant of a Web Service provided by the Community Manager, or by the Community Manager of a Web Service provided by a Community Participant. WebSphere Business Integration Connect acts as a proxy, passing the Web Service request to the Web Service provider and returning the response synchronously from the provider to the requestor.

This chapter contains the following information for setting up a Web Service for use by a Community Participant or a Community Manager:

- [“Identifying the participants for a Web Service” on page 129](#)
- [“Setting up Document Flow Definitions for a Web Service” on page 130](#)
- [“Adding Document Flows to Participants B2B Capabilities” on page 133](#)
- [“Activating the Participant Connection” on page 134](#)
- [“Restrictions and Limitations of Web Service support” on page 134](#)

Identifying the participants for a Web Service

When Web Service is provided by the Community Manager for use by Community Participants, WebSphere Business Integration Connect requires that a Community Participant identify itself to WebSphere Business Integration Connect. When posting the web service request to the WebSphere Business Integration Connect's Web Service public URL, set the identity in one of the following two ways:

- Use HTTP Basic Authentication with User ID of the form:
 - a. <participant's business ID e.g. DUNS>/<console user name> e.g. 123456789/joesmith
 - b. password equal to the console user name's password.
- Present an SSL client certificate which has been previously loaded into WebSphere Business Integration Connect for the Community Participant

When the WS is provided by a Community Participant, for use by the Community Manager, the public URL used by the CM to invoke the WS should contain the query string '?to=<CP WS Provider's business ID>', e.g. `http://WBICHost/bcgreceiver/Receiver?to=123456789`. This tells WebSphere Business Integration Connect that the provider of the WS is the participant with business ID '123456789'.

Setting up Document Flow Definitions for a Web Service

This is accomplished by uploading the WSDL (Web Service Definition Language) files that define the web service, through the Community Console. Alternatively, the user may enter the equivalent Document Flow Definitions manually through the Console. To enter the equivalent Document Flow Definitions manually, follow the procedures in [“Creating Document Flow Definitions” on page 32](#). You must also create the Document Flow, Activity and Action entries individually under the Protocol Web Service, as described below, paying particular attention to the requirements for the Action and its relationship to the received SOAP messages.

In terms of the Package/Protocol/Document Flow/Activity/Action hierarchy of Document Flow Definitions, a supported web service is represented as:

Package: 'None' (name and code), version 'N/A'

Protocol: 'Web Service' (name and code), version '1.0'

Document Flow: '{<web service namespace>}:<web service name>' (name and code), required to be unique among document flows for Web Service protocol, this is normally the WSDL's namespace and name

Activities: One activity for each web service operation, with name and code:

'{<operation namespace>}:<operation name>'

Actions: One action for the input message of each operation, with name and code:

'{<namespace of identifying xml element = first child of soap:body>}:<name of identifying xml element = first child of soap:body>'

The critical definitions are the Actions because WebSphere Business Integration Connect will use an Action's namespace and name to recognize an incoming web service request SOAP message and route it appropriately based on a defined Participant Connection. The requirement is that the namespace and name of the first child xml element of the received SOAP message's soap:body element must match a known Action's namespace and name in WebSphere Business Integration Connect's Document Flow Definitions.

For example, if a WS request SOAP message is as follows (for a Document-Literal SOAP binding):

```
<?xml version="1.0" encoding="UTF-8"?>
<soapenv:Envelope xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/"
xmlns:xsd="http://www.w3.org/2001/XMLSchema"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
  <soapenv:Body>
    <nameAndAddressElt xmlns="http://www.helloworld.com/xsd/helloDocLitSchema">
      <titleElt xmlns="">Mr</titleElt>
      <nameElt xmlns="">Joe Smith</nameElt>
      <addressElt xmlns="">
        <numberElt>123</numberElt>
        <streetElt>Elm St</streetElt>
        <cityElt>Peoria</cityElt>
      </addressElt>
    </nameAndAddressElt>
  </soapenv:Body>
</soapenv:Envelope>
```

```
</nameAndAddressElt>
</soapenv:Body>
</soapenv:Envelope>
```

Then WebSphere Business Integration Connect would look for a defined Web Service Action with this code:

```
{http://www.helloworld.com/xsd/helloDocLitSchema}:nameAndAddressElt
```

For an RPC binding style SOAP request message for example:

```
<?xml version="1.0" encoding="UTF-8"?>
<soapenv:Envelope xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/"
xmlns:xsd="http://www.w3.org/2001/XMLSchema"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
  <soapenv:Body>
    <ns1:helloWorldRPC soapenv:encodingStyle="http://schemas.xmlsoap.org/soap/encoding/"
xmlns:ns1="http://www.helloworld.com/helloRPC">
      <name xsi:type="xsd:string">Joe Smith</name>
    </ns1:helloWorldRPC>
  </soapenv:Body>
</soapenv:Envelope>
```

WebSphere Business Integration Connect would look for a defined Web Service action with this code: {http://www.helloworld.com/helloRPC}:helloWorldRPC

For an RPC binding, the namespace and name of the first child element of the soap:body of a SOAP request message should be the namespace and name of the applicable WS operation.

For Document-Literal binding, the namespace and name of the first child element of the soap:body of a SOAP request message should be the namespace and name of the xml 'element' attribute in the 'part' element of the input 'message' definition for the Web Service.

Uploading the WSDL files for a Web Service

The definition for a Web Service should be contained in a primary WSDL file, with extension ".wsdl", which may import additional WSDL files through the "import" element. If there are imported files, these may be uploaded with the primary file using one of the following methods:

- If the file path or (http) URL in each import element's "location" attribute is reachable from the Community Console's server (not the user's machine) the primary file may be uploaded directly and the imported files will be uploaded automatically.
- If all the imported files and primary file are zipped into one zip file, each with a zip path corresponding to the path (if any) in the import "location" attribute, uploading the zip file will upload all the contained primary and imported WSDL files.

Example:

Primary WSDL file 'helloworldRPC.wsdl' contains

```
'<import namespace="http://www.helloworld.com/wsdl/helloRPC.wsdl"
location="bindingRPC.wsdl"/>'
```

Imported WSDL file 'bindingRPC.wsdl' contains

```
'<import namespace="http://www.helloworld.com/wsdl/helloRPC.wsdl"
location="port/porttypeRPC.wsdl"/>'
```

Zip file should contain the following:

Name	Path
helloworldRPC.wsdl	
bindingRPC.wsdl	
porttypeRPC.wsdl	port\

When a WSDL file definition of a web service is uploaded, the original WSDL is saved as a "Validation Map" (however, web service messages are not actually validated by WebSphere Business Integration Connect, they are passed through directly), with the original service end point URL. This is called the 'private' WSDL. In addition a 'public' WSDL is saved with the private URL replaced by a target URL, as provided by the user in the Document Flow Upload input. The intent is that the public WSDL will be provided to the users of the web service, who will invoke the web service at the target's URL (the 'public' URL). WebSphere Business Integration Connect will then route the WS request to a Gateway that is the original web service provider's private URL. WebSphere Business Integration Connect acts as a proxy, forwarding the WS request to a private provider URL which is hidden from the WS user. Both the private and public WSDLs (including any imported files) may be downloaded from the Community Console after the WSDL has been uploaded.

Uploading WSDL files using the Community Console

Business Integration Connect provides a way to import WSDL files. If a web service is defined in a single WSDL file, you can upload the WSDL file directly. If the web service is defined using multiple WSDL files (this happens when you have imported WSDL files, within a primary WSDL file), they would be uploaded in a ZIP archive.

IMPORTANT: The WSDL files within the ZIP archive must be within a directory specified in the WSDL import element. For example, with the following import element: `<import namespace="http://www.helloworld.com/wsdl/helloRPC.wsdl" location="path1/bindingRPC.wsdl"/>`, the directory structure within the ZIP archive would be `path1/bindingRPC.wsdl`. In the next example: `<import namespace="http://www.helloworld.com/wsdl/helloRPC.wsdl" location="bindingRPC.wsdl"/>`, the `bindingRPC.wsdl` file would be at the root level within the ZIP archive.

To upload a single WSDL file or ZIP archive, use the following procedure.

1. Click **Hub Admin > Hub Configuration > Document Flow Definition**.
2. Click **Upload/Download Packages**.

3. Select **Yes** for WSDL Package to upload a WSDL file. For **Web Service Public URL**, enter the public URL of the Web service provided by the Community Manager (which will be invoked by a Community Participant). For example, `http(s)://<target host:port>/bcgreceiver/Receiver`. The URL is typically the same as the production HTTP target defined in Targets.

For a Web service provided by a Community Participant (which will be invoked by the Community Manager), enter the public URL of the participant with a query string. For example, `http(s)://<target host:port>/bcgreceiver/Receiver?to=<participant business ID>`.

4. Click **Browse** and select the WSDL file or ZIP archive.
5. For Commit to Database, select **No** to upload the file in test mode, the file will not be installed into the system. Use the system generated messages displayed in the Messages box to troubleshoot upload errors. Select **Yes** to upload the file into the system database.
6. For Overwrite Data, select **Yes** to replace a file currently in the database. Select **No** to add the file to the database.
7. Click **Upload**. The WSDL file is installed into the system.

Validating packages using schema files

A set of XML schemas that describe the XML files that can be uploaded through the console is provided on the Business Integration Connect installation medium. Uploaded files are validated against these schemas. The schema files are a useful reference for determining the cause of an error when a file cannot be uploaded because of non-conforming XML. The files are: `wSDL.xsd`, `wSDLhttp.xsd`, and `wSDLsoap.xsd`, which contain the schema describing valid Web Service Definition Language (WSDL) files.

The files are located in: `B2BIntegrate\packagingSchemas`

Setting up a Valid Interaction for a new Web Service

The final step in creating the necessary Document Flow Definitions for a new Web Service is to set up a Valid Interaction with the same Web Service Document Flow Action as both the Source and the Target.

To create interactions, use the following procedure.

1. Click **Hub Admin > Hub Configuration > Document Flow Definition**.
2. Click **Manage Interactions**.
3. Click **Create a Valid Interaction**.
4. Select **Pass Through** from the **Action** dropdown at the bottom of the screen (**Pass Through** is the only valid option supported in WebSphere Business Integration Connect for a Web Service).

Adding Document Flows to Participants B2B Capabilities

Add the Web Service Document flows to the source and target participants B2B capabilities to set up a Participant Connection between the source and target participants for the new Web Service's Document Flow created in [“Setting up Document Flow Definitions for a Web Service” on page 130](#).

Setting up Source and Target Gateways for the Web Service participants

Prior to setting up a Participant Connection between the Web Service user and the Web Service provider, you need to set up the Gateways that will be used in the Participant Connection. See [“Managing gateway configurations” on page 105](#).

The Source Gateway's URL is not used by the Web Service it can be a dummy URL. The Source Gateway can be used to set the 'Validate Client IP' and/or 'Validate Client SSL Cert' options on the sender side.

For the Target gateway, specify the private URL supplied by the Web Service provider. This is where WebSphere Business Integration Connect will invoke the web service when it acts as a proxy for the Web Service provider.

Activating the Participant Connection

The new document flow should appear as an available choice for participant connections between the two selected participants. Activate the Participant Connection to make the Web Service available to the Source participant. See [“Managing Participant connections” on page 120](#).

Restrictions and Limitations of Web Service support

The following restrictions and limitations apply to Web Service support for WebSphere Business Integration Connect:

- WSDL 1.1
- SOAP 1.1
- WS-I Basic Profile v. 1.0 (important restrictions on form of SOAP messages for document-literal binding).
- SOAP/HTTP binding are supported.
- Rebinding is not supported.
- RPC-encoded/RPC-literal and Document-literal binding styles are supported (subject to the restrictions in the WS-I Basic Profile).
- Soap With Attachments is not supported.

Chapter 5. cXML Support

This chapter contains the following information for configuring cXML support in WebSphere Business Integration Connect:

- [“cXML support overview” on page 135](#)
- [“Creating a cXML document flow definition” on page 139](#)

cXML support overview

The WebSphere Business Integration Connect Document Manager identifies a cXML document by the root element name of the XML document, which is "cXML", and the version identified by the cXML DOCTYPE (DTD). For example, the following DOCTYPE is for cXML version 1.2.009:

```
<!DOCTYPE cXML SYSTEM "http://xml.cXML.org/schemas/cXML/1.2.009/cXML.dtd">
```

The Document Manager performs the DTD validation on cXML documents, however, Business Integration Connect does not provide cXML DTDs. They can be downloaded from www.cxml.org; and then uploaded into Business Integration Connect through the Validation Map module in the Community Console. Once the DTD is uploaded, it must be associated to the cXML document flow. Refer to Validation Maps in chapter two for more information on associating the DTD to the cXML document flow.

The Document Manager uses two attributes of the cXML root element for document management: the payloadID and timestamp. The cXML payloadID and timestamp are used by Business Integration Connect as the document ID number and document timestamp. Both are viewable in the Community Console for document management.

The From and To elements within the cXML header contain the Credential element that is used for document routing and authentication. The example below shows the From and To elements as the source and destination of the cXML document:

```
<Header>
  <From>
    <Credential domain="AcmeUserId">
      <Identity>admin@acme.com</Identity>
    </Credential>
    <Credential domain="DUNS">
      <Identity>130313038</Identity>
    </Credential>
  </From>
  <To>
```

```

    <Credential domain="DUNS">
      <Identity>987654321</Identity>
    </Credential>

    <Credential domain="ViacoreUserId">
      <Identity>test@viacore.net</Identity>
    </Credential>

  </To>

```

If more than one credential element is used, the document manager will use the DUNS number as the Business Identifier for routing and authentication. In the case where there is no DUNS number given, the first Credential will be used.

Business Integration Connect does not use the information in the Sender element.

In a synchronous transaction, the From and To header is not used in a cXML response document. The response document is sent through the same HTTP connection that is established by the request document.

cXML document types

A cXML document can be one of three types: Request, Response, or Message.

Request

There are many types of cXML requests. The request element within the cXML document corresponds to the document flow definition in Business Integration Connect. Typical request elements are:

- OrderRequest
- ProfileRequest
- PunchOutSetupRequest
- StatusUpdateRequest
- GetPendingRequest
- ConfirmationRequest
- ShipNoticeRequest

The following table shows the relationship between the elements in a cXML request document and document flow definitions within Business Integration Connect:

cXML element	Document flow definition
cXML DOCTYPE	Protocol
DTD version	Protocol version
Request (type) For example, OrderRequest	Document flow

Response

The target Participant will send a cXML response to inform the source Participant the results of the cXML request. Because the result of some requests might not have any data, the Response element can optionally contain nothing but a Status element. A Response element can also contain any application-level data. During PunchOut, for example, the application-level data is contained in a PunchOutSetupResponse element. The typical Response elements are:

- ProfileResponse
- PunchOutSetupResponse
- GetPendingResponse

The following table shows the relationship between the elements in a cXML request document and document flow definitions within Business Integration Connect:

cXML element	Document flow definition
cXML DOCTYPE	Protocol
DTD version	Protocol version
Response (type) For example, ProfileResponse	Document flow

Message

A cXML message contains the Business Integration Connect document flow information in the cXML message element. It can contain an optional status element identical to that found in a Response element. It would be used in messages that are responses to request messages.

The content of the message is custom defined by the business needs of the user. The element directly below the <Message> element corresponds to the document flow created in Business Integration Connect. In the example below, SubscriptionChangeMessage would be the document flow:

```
<Message>
  <SubscriptionChangeMessage type="new">
    <Subscription>
      <InternalID>1234</InternalID>
      <Name xml:lang="en-US">Q2 Prices</Name>
      <Changetime>1999-03-12T18:39:09-08:00</Changetime>
      <SupplierID domain="DUNS">942888711</SupplierID>
      <Format version="2.1">CIF</Format>
    </Subscription>
  </SubscriptionChangeMessage>
</Message>
```

The following table shows the relationship between the elements in a cXML message and the document flow definitions within Business Integration Connect:

cXML element	Document flow definition
cXML DOCTYPE	Protocol
DTD version	Protocol version
Message	Document flow

The easiest way to tell the difference between a one-way message and a Request-Response document is the presence of a message element instead of a request or response element.

A message can have the following attributes:

- deploymentMode - Indicates whether the message is a test document or a production document. Allowed values are production (default) or test.
- inReplyTo - Specifies to which message this message responds. The contents of the inReplyTo attribute would be the payloadID of a message that was received earlier. This would be used to construct a two-way transaction with many messages.

Content-type headers and attached documents

All cXML documents must contain a Content-type header. For cXML documents without attachments, the following Content-type headers are used:

- Content-Type: text/xml
- Content-Type: application/xml

The cXML protocol supports attachment of external files through MIME. For example, buyers often need to clarify purchase orders with supporting memos, drawings, or faxes. One of the Content-type headers listed below must be used in cXML documents that contain attachments:

- Content-Type: multipart/related; boundary="something unique"
- Content-Type: multipart/mixed; boundary="something unique"

The boundary element is any unique text that is used to separate the body from the payload portion of the MIME message. Please refer to the cXML User Guide at www.cxml.org for more information.

Valid cXML interactions

Business Integration Connect supports the following cXML document flow definition interactions:

Source	Target	Source Package	Target Package	Source Protocol	Target Protocol	Pass Through	Validation	Translation
Participant	Manager	None	None	cXML	cXML	x	x	
Manager	Participant	None	None	cXML	cXML	x	x	
Manager	Participant		None	XML	cXML	x	x	x

Creating a cXML document flow definition

Use the following process to create a new document flow definition for a cXML document.

NOTE: You must ensure that the correct version of cXML is defined prior to creating a cXML document flow definition. The default is version 1.2.009. To define a different version, see [“Creating Document Flow Definitions” on page 32](#).

1. Click **Hub Admin > Hub Configuration > Document Flow Definition**.
2. Click **Create Document Flow Definition**. The Console displays the Create Document Flow Definitions screen. See [Figure 5-1 on page 141](#).
3. Select **Document Flow** for Document flow type.
4. Enter either the request type, such as *OrderRequest*, in the **Code** and **Name** boxes. For Response document, if the Response does not have any other child tags other than <Status>, enter *Response*, otherwise enter the next tag name following <Status>. For example:

```
<cXML>
  <Response>
    <Status code="200" text="OK"/> --> The DocumentFlow code
  </Response>
</cXML>
```

```
<cXML>
  <Response>
    <Status code="200" text="OK"/>
    <ProfileResponse --> The DocumentFlow code
  </Response>
</cXML>
```

5. Enter **1.0** for **Version**.
The version number is for reference only. The actual protocol version is derived from the DTD version within the cXML document.
6. Enter a **Description**.
7. Select **Yes** for **Document level**.
8. Select **Enabled** for **Status**.
9. Select **Yes** for all **Visibility** attributes.
10. Click on the **Package: None** folder to expand the package selection options. See [Figure 5-1 on page 141](#) to view the expanded folder selection in the bottom of the figure.
11. Select the Protocol: cXML (1.2.009): cXML.
12. Click Save.

Once the document flow definition is created, enable the Participant connections as needed. See [“Managing Participant connections” on page 120](#) for more information. See the screenshots below for examples of creating a cXML document flow definition and Participant connection.

Figure 5-1.

Account Admin | Viewers | Tools | **Hub Admin** | Community Participant Simulator | Logout | Help

Hub Configuration | Console Configuration

Event Codes | Targets | **Document Flow Definition** | XML Formats | Validation Maps | Actions

Language Locale: en_US | Format Locale: en_US | Time Zone: UTC

Create Document Flow Definitions

Welcome, Hub Administrator

[Manage Document Flow Definitions](#) | [Help](#)

Document flow type *

Code *

Name *

Version *

Description

Document level Yes No

Status Enabled Disabled

Visibility

Community Operator	<input checked="" type="radio"/> Yes	<input type="radio"/> No
Community Manager	<input checked="" type="radio"/> Yes	<input type="radio"/> No
Community Participant	<input checked="" type="radio"/> Yes	<input type="radio"/> No

Validation maps No maps found

Top level

- Package: None (N/A): None**
- Protocol: Binary (1.0): Binary**
- Protocol: EDI-X12 (ALL): EDI-X12**
- Protocol: EDI-EDIFACT (ALL): EDI-EDIFACT**
- Protocol: EDI-Consent (ALL): EDI-Consent**
- Protocol: cXML (1.2.009): cXML**
- Protocol: Web Service (1.0): Web Service**
- Protocol: jimXML (1.0): jimXML**
- Protocol: mjI XML (1.0): mjI XML**
- Protocol: DSXML (1.0): DSXML**
- Protocol: CAXmlTest (2.0): CAXmlTest**
- Protocol: NameSpace (1.0): NameSpace**
- Protocol: 3A7_Diane (2.0): 3A7_Diane**
- Package: Backend Integration (1.0): Backend Integration**

Chapter 6. Using the Gateway Queue

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 6-1](#).

Table 6-1. 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.

Table 6-1. Gateway Queue Screen (continued)

Criteria	Description
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 6-2](#) shows the information returned from the search.

Table 6-2. 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 6-3. 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.


Table 6-3. Search Criteria for the Gateway Queue

Parameter	Description
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 6-3 on page 144](#)).
4. Click the  icon.

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 6-1 on page 143](#)).
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 6-1 on page 143](#)).
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 7. 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” on page 147](#)
- [“Increasing the Receiver timeout setting” on page 147](#)
- [“Avoiding out-of-memory errors” on page 148](#)
- [“Reprocessing events and business documents that fail to log to the database” on page 148](#)
- [“Archiving and purging filesystem and database logs” on page 149](#)
- [“Shutting down” on page 154](#)
- [“Starting the system after a machine shutdown” on page 154](#)
- [“Restarting the router after a crash” on page 155](#)

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
```

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:

- `/opt/IBM/WBICConnect/console/was/bin/wsadmin.sh -conntype NONE -f $LOCATION_OF_SCRIPTS$/queryJVMAattrs.jacl`

Set min/max heap size:

- `/opt/IBM/WBICConnect/console/was/bin/wsadmin.sh -conntype NONE -f $LOCATION_OF_SCRIPTS$/setJVMAattrs.jacl`

Change the heap size to the recommended values by editing `setJVMAattrs.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`

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 in WebSphere Business Integration Connect 4.2.0 and 4.2.1.

Purging application log files

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

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

Purging non-repudiation directories

Non-repudiation files and directories are located in: `$INSTALLATION_DIRECTORY/vcrouter/vms/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/bin/stopServer.ksh 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

Database tables starting with BP_ and LG_ are the only tables that can be purged using this procedure. However, there are two exceptions-BP tables ending with _QUE and _HIST. BP tables ending with _QUE are queue tables and purged by the RN engine on an ongoing basis. BP tables ending with _HIST are history tables, and are used for archiving. For example, BP_RNSTATEHDR table is archived as BP_RNSTATEHDR_HIST. These two table groups must remain unchanged in order to maintain proper system functionality.

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. A daily cron job is run to archive the data in a _Hist table, and then the data is purged. However, the log, if any, is truncated every day.

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 (not in 4.2.1)
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.

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 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 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.

Table	Notes
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_MS GLENGTH_SUMMARY	
LG_SUMMARY	
LG_SUMMARY_MI	
LG_SUMMARY_PROCESSSUMMAR Y	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	

Table	Notes
LG_SUM_XREF_PRCs	
Message Length Summary	
LG_MSGLLENGTH_SUMMARY	

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:

```
runmqldr -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 the Community Console, Receiver, and Document Manager

To start the 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 the 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. Administering Certificates

With Business Integration Connect, you can install and use the following types of certificates for inbound and outbound transactions:

- SSL (server side)
- SSL (client)
- Digital signature
- Encryption

As the Hub Admin or Operator Admin, you use Business Integration Connect's Community Console to install all of the required client, signature, and encryption certificates for Business Integration Connect storage. You can use the ikeyman tool for WebSphere Application Server (WAS) storage.

NOTE: When a Participant's certificate expires, it is the Participant's responsibility to obtain a new certificate. The Console's Alert feature includes certificate expiration alerts for certificates stored in Business Integration Connect. For more information, see the IBM WebSphere Business Integration Connect Community Console User Guide.

You can use one certificate for multiple purposes. For inbound SSL, however, the private key and associated certificate must be in formats suitable for WAS storage.

Certificate Overview

Table 8-1 summarizes the way certificates are used in Business Integration Connect.

NOTE: Certificate locations are shown in parenthesis “()”.

Table 8-1. Certificate Summary Information

Message Delivery Method (Note 1)	Hub Owner Certificate	Obtain Certificate & CA from Partner	CA (Note 2)	Give Certificate to Partner (Note 3)	Comments
Inbound SSL	Install on WAS for Server side SSL (Place in WAS Keystore)	N/A	Only needed if client authentication is used (Place CA or self-signed certificate in WAS Truststore)	Hub owner certificate if self-signed or the CA root certificate if it is CA authenticated	
Outbound SSL	If Client authentication is being used. (Business Integration Connect)	Partner server side certificate CA root certificate if it is CA authenticated.	WebSphere Business Integration Connect	Hub owner certificate if self-signed or public key if signed by a third party	
Inbound Encrypt	Private key (Business Integration Connect)	N/A	N/A	Hub owner certificate	For decrypting the message
Inbound Signature	N/A	Certificate for validating the certificate used for the digital signature (Business Integration Connect)	WebSphere Business Integration Connect	N/A	For verification and non-repudiation
Outbound Encrypt	N/A	Use certificate obtained from trading partner (certificate is installed in partner's profile)	CA for client certificate if not self-signed	N/A	For encryption of outgoing messages
Outbound Signature	Private key (Business Integration Connect)	N/A	N/A	Optional, depending on partner; give WBIC public key	
Cert to DUNS validation	N/A	Load in Console Trading Partner Profile	Load same certificate (as one in column to left) in hub operator as the CA certificate		Validates that this cert is for this DUNS when the SSL check is done

Note 1: Inbound - message coming into Business Integration Connect from a partner. Outbound - message going out of Business Integration Connect to a partner.

Note 2: If the certificate is CA issued then issuing CA certificate must be obtained and stored. This applies to either the Hub owner certificate or the Partners certificate.

Note 3: If a private key is involved then this certificate corresponds to the private key.

Understanding terms and concepts

The following terms are specific to the creation and use of certificates in the Business Integration Connect environment:

- **ikeyman** — a key management utility used to create key databases, public and private key pairs, and certificate requests (CSR). You can also use ikeyman to create self-signed certificates.
- **keystore** — a file that contains your public and private keys.
- **truststore** — a key database file that contains the public keys for your partner's self-signed and the CA certificates. The public key is stored as a signer certificate. For commercial CA, the CA root certificate is added. The truststore file can be a more publicly accessible key database file that contains all the trusted certificates.

Creating and installing certificates

The following sections describe how to create and install certificates that you want to use with WebSphere Business Integration Connect.

Inbound SSL certificates

If your community is not using SSL, neither you nor your Participants need an inbound or outbound SSL certificate.

This server certificate is used by WAS when it receives connection requests from Participants through SSL. It is the certificate that the Document Receiver presents to identify the hub to the Participant. This server certificate can be self-signed, or it can be signed by a CA. In most cases you will use a CA certificate to increase security. You might use a self-signed certificate in a test environment. Use ikeyman to generate a certificate and key pair. Refer to documentation available from IBM for more information about using ikeyman.

IBM WebSphere Application Server (WAS) is embedded in WebSphere Business Integration Connect. WAS handles all inbound SSL connections. The installation provides a keystore and truststore for the Document Receiver and for the Console. By default, all four keystores are created in the `WBIC_install_root/common/security/keystore/` directory. The names are:

- receiver.jks
- receiverTrust.jks
- console.jks
- consoleTrust.jks

The default password for accessing all four stores is WebAS. The embedded WAS is configured to use these four stores.

NOTE: The following Unix command can be used to change the password of the keystore file:
`/opt/IBM/WBICConnect/console/was/java/bin/keytool -storepasswd
-new $NEW_PASSWORD$ -keystore $KEYSTORE_LOCATION$ -storepass
$CURRENT_PASSWORD$ -storetype JKS`

If the keystore passwords are changed, each WAS instance configuration must also be changed. This can be done using the `bcgChgPassword.jacl` script:

```
./wsadmin.sh -f <jacl-path>/bcgChgPassword.jacl -conntype NONE.
```

You will be prompted for the new password.

After you generate the certificate and key pair, use the certificate for inbound SSL traffic for all Participants. If you have multiple Document Receivers or Consoles, copy the resultant keystore to each instance. If the certificate is self-signed, provide this certificate to the Participants. To obtain the certificate, use `ikeyman` to extract the certificate to a file.

NOTE: Use `ikeyman` to delete the WebSphere "dummy" server certificate from the keystores that you have installed or created the new certificates in. If this certificate is not removed, it will be presented to the partner during SSL session establishment..

If you also use SSL Client Authentication, obtain either the participant's self-signed certificate or the certificate provided by a CA and install it in the appropriate truststore. After installing the certificate, configure WAS to use client authentication by running the utility script `bcgClientAuth.jacl`.

There is an additional feature that can be used with SSL Client Authentication. This feature is enabled via the Community Console. For HTTPS, WebSphere Business Integration Connect checks certificates against the Business IDs in the inbound documents. To use this feature, create the Participant's profile, import client certificate and flag as SSL. Select the Validate Client SSL Certificate option on the Participant's Gateway screen. For more information, see ["Managing gateway configurations" on page 105](#).

If you use self-signed server certificates, use one of the following procedures.

1. **ikeyman:**

- a. Use `ikeyman` to generate a self-signed certificate and a key pair for the Document Receiver or Console keystore. The `ikeyman` utility is located in the `was/bin` directory. It is included with WAS, which is embedded in Business Integration Connect. Instructions for running `ikeyman` can be found in documentation available from IBM.
- b. Use `ikeyman` to extract to a file the certificate that will contain your public key.
- c. Distribute the certificate to your Participants. The preferred method for distribution is to send the certificate in a zip file that is password protected, by e-mail. Your Participants must call you and request the password for the zip file.

2. **createCert.sh:**

- a. Use the `createCert.sh` script, located in the `was/bin` directory, to generate a self-signed certificate in X.509 format, a private key in PKCS 8 format, and a PKCS12 file which contains both the private key and certificate.
- b. Install the `pkcs12` file into the Document Receiver or Console keystore that it was created for.
- c. Distribute the certificate to your Participants. The preferred method for distribution is to send the certificate in a zip file that is password protected, by e-mail. Your Participants must call you and request the password for the zip file.

If the certificate is signed by a CA, use the following procedure.

1. Use `ikeyman` to generate a certificate request and a key pair for the Document Receiver. The `ikeyman` utility is located in the `was/bin` directory. It is included with WAS, which is embedded in Business Integration Connect. Instructions for running `ikeyman` can be found in documentation available from IBM.
2. Submit a Certificate Signing Request (CSR) to a CA.
3. When you receive the signed certificate from the CA, use `ikeyman` to place the signed certificate into the keystore.
4. Distribute the signing CA certificate to all Participants.

For client authentication, use the following procedure:

1. Obtain your Participants' certificates.
2. Install the certificate into the truststore using `ikeyman`.
3. Place related CA in CA directory or related keystore.

NOTE: When you add more Participants to your hub-community, you can use `ikeyman` to add their certificates to the truststore. If a Participant leaves the community, you can use `ikeyman` to remove the Participant's certificates from the truststore

Outbound SSL certificate

If your community is not using SSL, you do not need an inbound or outbound SSL certificate.

When SSL is being used to send outbound documents to your Participants, WebSphere Business Integration Connect will request a server side certificate from the Participants. If a Participant's certificate is self-signed, use the Console to import it into the hub operator in Business Integration Connect and flag it as a SSL certificate. If the certificate is CA signed, you need only import the CAs certificate into the Console.

NOTE: The same CA certificate can be used for multiple participants. The certificate must be in X.509 DER format.

If SSL client authentication is required, the Participant will, in turn, request a certificate from Business Integration Connect. For Business Integration Connect to present the certificate to the Participant, use the Console to import your certificate into Business Integration Connect. You can generate the certificate using `ikeyman` or the `createCert.sh` script in the `was/bin` directory. If the certificate is a self-signed certificate, it must be provided to the Participant. If a CA signed certificate, the CA must be given to the Participant.

To set up for server authentication from the Participant, install the Partner's self-signed or CA signed certificate through the console's certificate feature. The certificate must be in binary format using DER encoding. You perform this task logged in to the console as the Hub Operator, and install the certificate in your own profile. All CA certificates are loaded under the hub operator profile.

If client authentication is required by the Participant, use one of the following procedures.

1. **ikeyman:**

- a. Use `ikeyman` to generate a self-signed certificate and a key pair for the Document Receiver or keystore (this is not the same Document Receiver keystore used for Inbound SSL by WAS). The `ikeyman` utility is located in the `was/bin` directory. It is included with WAS, which is embedded in Business Integration Connect. Instructions for running `ikeyman` can be found in documentation available from IBM.
- b. Use `ikeyman` to extract to a file the certificate that will contain your public key.
- c. Distribute the certificate to your Participants. The preferred method for distribution is to send the certificate in a zip file that is password protected, by e-mail. Your Participants must call you and request the password for the zip file.
- d. Use `ikeyman` to export the self-signed certificate and private key pair in the form of a PKCS12 file.
- e. Install the self-signed certificate and key through the Console's certificate feature. You perform this task logged in to the Console as the Hub Operator, and install the certificate in your own profile.

2. **createCert.sh:**

- a. Use the `createCert.sh` script, located in the `was/bin` directory, to generate a self-signed certificate in X.509 format, a private key in PKCS 8 format, and a PKCS12 file which contains both the private key and certificate.
- b. Install the self-signed certificate and key through the Console's certificate feature. You perform this task logged in to the Console as the Hub Operator, and install the certificate in your own profile.
- c. Send your self-signed certificate or CA to all Participants.

If the certificate is signed by a CA, use the following procedure.

1. Use `ikeyman` to generate a certificate request and a key pair for the Document Receiver. The `ikeyman` utility is located in the `was/bin` directory. It is included with WAS, which is embedded in Business Integration Connect. Instructions for running `ikeyman` can be found in documentation available from IBM.
2. Submit a Certificate Signing Request (CSR) to a CA.
3. When you receive the signed certificate from the CA, use `ikeyman` to place the signed certificate into the keystore.
4. Distribute the signing CA certificate to all Participants.

Adding a Certificate Revocation List (CRL)

Business Integration Connect includes a Certificate Revocation List (CRL) feature. The CRL, issued by a Certificate Authority (CA), identifies Community Participants who have revoked certificates prior to their scheduled expiration date. Participants with revoked certificates will be denied access to Business Integration Connect.

Each revoked certificate is identified in a CRL by its certificate serial number. Business Integration Connect's Document Manager scans the CRL every 60 seconds and refuses the certificate if it is contained within the CRL list.

CRLs are stored in the following location: `/<shared data directory>/security/crl`. Business Integration Connect uses the setting `bcg.http.CRLDir` in the `bcg.properties` file to identify the location of the CRL directory.

Create `.crl` file containing the revoked certificates and place it in the CRL directory.

For example, in the `bcg.properties` file, you would use the following setting:

```
bcg.http.CRLDir=/<shared data directory>/security/crl.
```

Inbound signature certificate

The Document Manager uses the participants signed certificate to verify the sender's signature when you receive documents. The Participants send their self-signed signature certificates in X.509 DER format to you. You, in turn, install the Participants' certificates through the Console under the respective trading partner profile.

To install the certificate, use the following procedure.

1. Receive the Participant's signature certificate in X.509 DER format.
2. Install the certificates through the Console's certificate feature. You perform this task logged in to the console as the Hub Operator, and install the certificate in the Participant's profile, denoting the certificate as a signature certificate.
3. If the certificate was signed by a CA and the CA root certificate is not installed in the Hub Admin account, install the CA certificate through the Console's certificate feature. You perform this task logged in to the console as the Hub Operator, and install the certificate in your own profile. If the certificate is self-signed, add it as a CA in the Hub Operator profile.
NOTE: You do not have to perform the previous step if the CA certificate is already installed.
4. Enable at the package (highest level), Partner, or connection level (lowest level). Your setting can override other settings at the connection level. The connection summary will inform you if any required attribute is missing.

Outbound signature certificate

The Document Router uses this certificate when it sends outbound, signed documents to Participants. The same certificate and key are used for all ports and protocols.

Use one of the following procedures to generate a self-signed certificate:

1. **ikeyman:**
 - a. Use `ikeyman` to generate a self-signed certificate and a key pair for the Document Receiver or keystore (this is not the same Document Receiver keystore used for Inbound SSL by WAS). The `ikeyman` utility is located in the `was/bin` directory. It is included with WAS, which is embedded in Business Integration Connect. Instructions for running `ikeyman` can be found in documentation available from IBM.
 - b. Use `ikeyman` to extract to a file the certificate that will contain your public key.
 - c. Distribute the certificate to your Participants. The preferred method for distribution is to send the certificate in a zip file that is password protected, by e-mail. Your Participants must call you and request the password for the zip file.

- d. Use `ikeyman` to export the self-signed certificate and private key pair in the form of a PKCS12 file.
- e. Install the self-signed certificate and private key pair in the form of a PKCS12 file through the Console's certificate feature. You perform this task logged in to the Console as the Hub Operator, and install the certificate in your own profile.

2. **createCert.sh:**

- a. Use the `createCert.sh` script, located in the `was/bin` directory, to generate a self-signed certificate in X.509 format, a private key in PKCS 8 format, and a PKCS12 file which contains both the private key and certificate.
- b. Install the self-signed certificate and key through the Console's certificate feature. You perform this task logged in to the Console as the Hub Operator, and install the certificate in your own profile.
- c. Distribute the certificate to your Participants. The preferred method for distribution is to send the certificate in a zip file that is password protected, by e-mail. Your Participants must call you and request the password for the zip file.
- d. Enable at package (highest level), Partner, or connection level (lowest level). Your setting can override other settings at the connection level. The connection summary will inform you if any required attribute is missing.

If the certificate is signed by a CA, use the following procedure.

- 1. Use `ikeyman` to generate a certificate request and a key pair for the Document Receiver. The `ikeyman` utility is located in the `was/bin` directory. It is included with WAS, which is embedded in Business Integration Connect. Instructions for running `ikeyman` can be found in documentation available from IBM.
- 2. Submit a Certificate Signing Request (CSR) to a CA.
- 3. When you receive the signed certificate from the CA, use `ikeyman` to place the signed certificate into the keystore.
- 4. Distribute the signing CA certificate to all Participants.

Inbound encryption certificate

This certificate is used by the Document Receiver to decrypt encrypted files received from Participants. The Document Receiver uses our private key to decrypt the documents. Encryption is used to keep anyone other than the sender and intended recipient from viewing documents in transit.

Use one of the following procedures to generate a self-signed certificate:

1. **ikeyman:**

- a. Use `ikeyman` to generate a self-signed certificate and a key pair for the Document Receiver or keystore (this is not the same Document Receiver keystore used for Inbound SSL by WAS). The `ikeyman` utility is located in the `was/bin` directory. It is included with WAS, which is embedded in Business Integration Connect. Instructions for running `ikeyman` can be found in documentation available from IBM.
- b. Use `ikeyman` to extract to a file the certificate that will contain your public key.

- c. Distribute the certificate to your Participants. They are required to import the file into their B2B product for use as an encryption certificate. Advise them to use it when they want to send encrypted files to the Community Manager. If your certificate is CA signed, provide the CA certificate as well.
- d. Use `ikeyman` to export the self-signed certificate and private key pair in the form of a PKCS12 file.
- e. Install the self-signed certificate and private key pair in the form of a PKCS12 file through the Console's certificate feature. You perform this task logged in to the Console as the Hub Operator, and install the certificate in your own profile.
- f. Enable at package (highest level), Partner, or connection level (lowest level). Your setting can override other settings at the connection level. The connection summary will inform you if any required attribute is missing.

2. **createCert.sh:**

- a. Use the `createCert.sh` script, located in the `was/bin` directory, to generate a self-signed certificate in X.509 format, a private key in PKCS 8 format, and a PKCS12 file which contains both the private key and certificate.
- b. Install the self-signed certificate and key through the Console's certificate feature. You perform this task logged in to the Console as the Hub Operator, and install the certificate in your own profile.
- c. Distribute the certificate to your Participants. They are required to import the file into their B2B product for use as an encryption certificate. Advise them to use it when they want to send encrypted files to the Community Manager.
- d. Enable at package (highest level), Partner, or connection level (lowest level). Your setting can override other settings at the connection level. The connection summary will inform you if any required attribute is missing.

If the certificate is signed by a CA, use the following procedure.

1. Use `ikeyman` to generate a certificate request and a key pair for the Document Receiver. The `ikeyman` utility is located in the `was/bin` directory. It is included with WAS, which is embedded in Business Integration Connect. Instructions for running `ikeyman` can be found in documentation available from IBM.
2. Submit a Certificate Signing Request (CSR) to a CA.
3. When you receive the signed certificate from the CA, use `ikeyman` to place the signed certificate into the keystore.
4. Distribute the signing CA certificate to all Participants.

Outbound encryption certificate

The outbound encryption certificate is used when the hub sends an encrypted document to a Participant. Business Integration Connect encrypts the document with the Participant's public key, and the Participant decrypts the document with their private key.

1. Obtain the Participant's encryption certificate. The certificate must be in X.509 DER format.

2. Install the certificate through the console's certificate feature. You perform this task logged in to the console as the Hub Operator, and install the certificate in the Participant's profile, denoting the certificate as an encryption certificate.
3. If the certificate is signed by a CA, and you do not have the CA's certificate installed in the system, log in to the console as Hub Operator and install this certificate in your own profile. You need only load a CA's certificate once. If this is a self-signed certificate, also load this as the CA in the hub operator profile.
4. Enable at package (highest level), Partner, or connection level (lowest level). Your setting can override other settings at the connection level. The connection summary will inform you if any required attribute is missing.

Configuring Inbound SSL for the Console and Receiver

The WebSphere Business Integration Connect keystores are preconfigured in WAS. This section only applies if you are using different keystores.

To configure SSL for the Console and Receiver in Business Integration Connect, use the following procedure.

1. Obtain the following information:
 - The full path names of the key file and the trust file; for example:


```
/opt/IBM/WBICConnect/common/security/keystore/receiver.jks
and
/opt/IBM/WBICConnect/common/security/keystore/receiverTrust.jks
```

You must enter these names correctly. In the Unix environment, these names are case-sensitive.
 - The new passwords for each file.
 - The format of each file. This must be chosen from one of the values JKS, JCEK, or PKCS12. Enter this value in upper-case exactly as shown.
 - The path to the script file named `bcgssl.jacl`.
2. Open a Console window and change to `<server-root>/bin`. The server does not need to be running to change the passwords.
3. Enter the following command, substituting the values that are enclosed in `<>`. All values must be entered.


```
./wsadmin.sh -f <jacl-path>/bcgssl.jacl -conntype NONE install
<keyFile pathname> <keyFile password> <keyFile format> <trustFile
pathname> <trustFile password> <trustFile format>
```
4. Start the server. If the server fails to start, it may be due to an error when running `bcgssl.jacl`. If you make a mistake, you can rerun the script to correct it.
5. If you used `bcgClientAuth.jacl` to set the `clientAuthentication SSL` property, reset it after using `bcgssl.jacl`. This is because `bcgssl.jacl` overwrites any values that may have been set for `clientAuthentication` with the value `false`.

Appendix B. Failed Events

When a document fails processing, the WebSphere Business Integration Connect system generates an event. [Table B-1](#) 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 B-1. Failed Events

Event	Event Name	Internal Description	Severity	Extended Description
103201	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.
103203	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.
200001	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.
200005	Document Transformation Failure	Document failed transformation due to {0}	Error	This event is generated due to a failure during document transformation.
200006	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.
200007	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.
200009	Failed to Parse Document	Failed to parse: {0}	Error	This event is generated due to failure when attempting to parse the document.
200013	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.

Table B-1. Failed Events

Event	Event Name	Internal Description	Severity	Extended Description
200015	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.
210000	Check Channel Error	Check Channel Error	Error	This event is generated when there is a check channel related error.
210001	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.
210002	Connection Lookup Failed	Connection lookup failed {0}	Error	This event is generated when data required to lookup a connection is not available.
210007	Outbound Document Cannot be Packaged	Error in Outbound Processor	Critical	This event is generated when a packager is not available for an outbound document.
210008	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.
210009	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.
210010	Document Too Large	Document too large: {0} bytes	Error	This event is generated when the document received is too large to be processed.
210011	Community Manager Transport Unpackage Failure	Insufficient Community Manager transport information provided: {0}	Error	This event is generated when insufficient transport information is provided.
210012	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.

Table B-1. Failed Events

Event	Event Name	Internal Description	Severity	Extended Description
210013	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.
210014	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.
210017	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.
210019	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.
210031	Unable to Non-Rep document	Unable to Non-Rep document {0}	Critical	<p>This event is generated when the system is unable to non-repudiate the document.</p> <p>Insure that the system has sufficient disk space, and that the following directories contain system-only files:</p> <p><i>./<common information directory>/non_rep/</i></p> <p><i>./<common information directory>/msg_store/</i></p> <p>If these two directories contain user generated files, document processing will fail.</p>
210032	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.

Table B-1. Failed Events

Event	Event Name	Internal Description	Severity	Extended Description
210033	Message Store Failed	Unable to store document plain text	Error	<p>This event is generated when the system is unable to store the document in plain text.</p> <p>Insure that the system has sufficient disk space, and that the following directories contain system-only files:</p> <p><i>./<common information directory>/non_rep/</i></p> <p><i>./<common information directory>/msg_store/</i></p> <p>If these two directories contain user generated files, document processing will fail.</p>
210034	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.
210051	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.
210052	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.
210061	Destination Parse Failure	Error in destination Parse	Critical	This event is generated when destination parse fails. Usually due to a database problem.
210063	Destination Process Failure	Destination Process failed	Critical	This event is generated when destination processing fails. Usually due to a database problem.
210065	Destination Determination Failure	{0}	Error	This event is generated when there are conflicting inputs when processing the destination.
210066	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
210201	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.

Table B-1. Failed Events

Event	Event Name	Internal Description	Severity	Extended Description
210202	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.
210203	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.
230004	Validation Internal Error	{0}	Critical	This event is generated due to internal system failure during validation processing.
230006	Validation Database Error	{0}	Critical	This event is generated due to a database error during validation processing.
230007	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.
230009	RosettaNet Validation Error	{0}	Error	This event is generated when a document fails to complete RosettaNet process validation.
230010	Data Validation Error	Document failed data validation: {0}	Error	This event is generated when a document fails data validation and is rejected.
230012	AS Sequence Validation Error	{0}	Error	This event is generated when a document fails to complete EDIINT process validation.
240003	RosettaNet Unpackaging Error	RosettaNet Unpackaging Error	Error	This event is generated when the system is unable to parse the RosettaNet preamble during unpackaging.
240005	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.
240007	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.
240009	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.
240011	RNPackager Signature Failed	Digital Signature validation failed: {0}	Error	This event is generated when digital signature validation fails during unpackaging.

Table B-1. Failed Events

Event	Event Name	Internal Description	Severity	Extended Description
240012	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.
240013	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.
240014	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.
240015	RosettaNet Document Creation Failure	{0}	Critical	This event is generated when an attempt to construct a RosettaNet document fails.
240016	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.
240031	Packaging Instance Error	Error: {0}	Critical	This event is generated when the system is unable to find a packager for the supplied document type.
240036	Unpackaging Instance Error	Error: {0}	Error	This event is generated when the system cannot find an unpackager for a document.
240065	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.
240068	Connection Parser RosettaNet Failure	Connection Parse RosettaNet Failure	Error	This event is generated when connection info could not be found in a RosettaNet document.
240070	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.
240071	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.
240078	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.

Table B-1. Failed Events

Event	Event Name	Internal Description	Severity	Extended Description
240409	AS Unpackager Failure	AS Unpackager Error: {0}	Error	This event is generated when the AS unpackager fails.
240411	AS Signature Failure	AS Signature Validation Error: {0}	Error	This event is generated when AS signature validation fails.
240412	AS State Engine DB Failure	AS State Engine DB error: {0}	Critical	This event is generated when the AS state engine database fails.
240415	AS Packager Failure	AS Packager Error: {0}	Critical	This event is generated when the AS packager fails.
240416	AS Non-Repudiation Error	{0}	Error	This event is generated when AS Non-Repudiation fails.
240417	Decryption Failed	{0}	Error	This event is generated when decryption fails.
240418	Unable to Generate Message Digest	{0}	Error	This event is generated when the system is unable to generate a message digest.
240419	Unsupported Signature Format	{0}	Error	This event is generated when the system receives an unsupported signature format.
240420	Unsupported Signature Algorithm	{0}	Error	This event is generated when the system receives unsupported signature algorithm.
240421	Unexpected Error	{0}	Critical	This event is generated when the system encounters an unexpected error.
240422	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.
240423	Input File Failure	Invalid input file passed in the document	Error	This event is generated when the system encounters an invalid input file.
240424	Insufficient Message Security	{0}	Error	This event is generated when the system encounters insufficient message security.
240500	RosettaNet State Engine Error	RosettaNet State Engine Error	Critical	This event is generated when the RosettaNet State Engine encounters a system error.
240600	AS State Engine Error	AS State Engine Error: {0}	Critical	This event is generated when the RosettaNet State Engine encounters a system error.

Table B-1. Failed Events

Event	Event Name	Internal Description	Severity	Extended Description
240601	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.
250001	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.
250002	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.
250005	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.
260002	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.
800000	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.
800004	Community Manager Business Process Encounters Database Error	{0}	Critical	This event is generated due to database error while processing the Community Manager's action.
800005	Community Manager Process Encounters Internal Error	{0}	Critical	This event is generated due to internal system error while processing the Community Manager's action.

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 C-1. 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 debuggin 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

Table C-1. Console-specific properties

Entry	Default value	Possible setting	Description
log4j.appender.stdout.layout.ConversionPattern	%d{ABSOLUTE} %c{1} [%t] - %m%n		Logging pattern for log file
log4j.appender.RollingFile	org.apache.log4j.RollingFileAppender		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.
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

Table C-1. Console-specific properties

Entry	Default value	Possible setting	Description
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
ibm.bcg.jms_jndi_factor_y	com.sun.jndi.fscontext.ReffSContextFactory		
## 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
ibm.bcg.jms.topic.name	WBIC/ reloadCacheT		JMS Topic Name

Table C-1. Console-specific properties

Entry	Default value	Possible setting	Description
## FTP Configuration Parameters for FTP Client config on the console			
## Scripts are as follows:			
## con_createFtpAcct.pl [username]::[password]			
## con_modifyFtpAcct.pl [username]::[password]			
## con_disableFtpAcct.pl username			
## con_enableFtpAcct.pl username			
## con_createFtpDirectories.pl directory_to_create			
## FTP Host Address			
ibm.bcg.ftp.host			FTP Hostname for environment
## Argument delimiter			
ibm.bcg.ftp.script.argDelimitter	::		Delimiter to be used w/ FTP scripts
## doc directory names			
ibm.bcg.ftp.docDir	documents		Subdirectory for xml documents
ibm.bcg.ftp.binDir	binary		Subdirectory for binary documents
## Scripts			
ibm.bcg.ftp.script.ftpAcct.create	\$SHARED_DATA_DIR\$/ftp/bin/ con_createFtpAcct.\$SCRIPT_SUFFIX\$		Create FTP Account
ibm.bcg.ftp.script.ftpAcct.update	\$SHARED_DATA_DIR\$/ftp/bin/ con_modifyFtpAcct.\$SCRIPT_SUFFIX\$		Change FTP Account password
ibm.bcg.ftp.script.ftpAcct.disable	\$SHARED_DATA_DIR\$/ftp/bin/ con_disableFtpAcct.\$SCRIPT_SUFFIX\$		Disable FTP Account

Table C-1. Console-specific properties

Entry	Default value	Possible setting	Description
ibm.bcg.ftp.script.ftpAccount.enable	\$\$SHARED_DATA_DIR\$/ftp/bin/con_enableFtpAcct.\$SCRIPT_SUFFIX\$		Enable FTP Account
ibm.bcg.ftp.script.createDirs	\$\$SHARED_DATA_DIR\$/ftp/bin/con_createFtpDirectories.\$SCRIPT_SUFFIX\$		Create directories for FTP Account
## 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.Password			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

Table C-1. Console-specific properties

Entry	Default value	Possible setting	Description
## 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 C-2. 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.D B.TYPE\$	db2,oracle	Database type
bcg.co.db.DBPoolName	\$RECEIVER.J NDI\$	datasources/ DB2DS,datasour ces/OraclePool	Datasource JNDI Prefix
bcg.co.jndiContextURL	corbaloc:iiop:lo calhost:57809		JNDI Provider URL
bcg.co.jndiFactory	com.ibm.webs phere.naming. WsnInitialCont extFactory		JNDI Context Factory
bcg.co.db.schema	\$RECEIVER.D B.SID\$		schema information (DB2 - Database Owner, Oracle - Schema Owner)
##### MQ PROPS			
bcg.use_oaq	FALSE	true, false	

Table C-2. Receiver-specific properties

Entry	Default value	Possible settings	Description
<code>bcg.jms.queue.factory</code>	WBIC/QCF		JMS Queue Connection Factory Name
<code>bcg.jms.topic.factory</code>	WBIC/TCF		JMS Topic Connection Factory Name
<code>bcg.jms.jndi_factory</code>	<code>com.sun.jndi.fscontext.RefsContextFactory</code>		Class used to connect to the JNDI server
<code>bcg.jms.context_url</code>	<code>file:\$RECEIVER_INSTALL_DIR\$/jndi</code>		Location of .binding file, used for JMS information
##### BPE			
<code>bcg.oaq_log_q</code>	WBIC/ datalogQ		JMS Queue Name
##### RECEIVER MBEAN			
<code>bcg.vms_receiver_reject_dir</code>	<code>\$\$SHARED_DATA_DIR\$/receiver/reject</code>		File system path where the Receiver puts rejected messages
<code>bcg.vms_receiver_tmp_dir</code>	<code>\$\$SHARED_DATA_DIR\$/receiver/tmp</code>		File system path where the Receiver puts temporary messages
##### END RECEIVER MBEAN			
<code>bcg.receiver.persistpath</code>	<code>\$\$SHARED_DATA_DIR\$/router_in/</code>		File system path where the "Receiver" persists inbound RosettaNet signals.
<code>bcg.receiver.sync.persistpath</code>	<code>\$\$SHARED_DATA_DIR\$/sync_in</code>		File system path where the "Receiver" persists Synchronous RosettaNet signals.

Table C-2. Receiver-specific properties

Entry	Default value	Possible settings	Description
<code>bcg.receiver.sync.syncC heckClasses</code>	<code>com.ibm.bcg.s erver.sync.Syn cRosettaNetR equest com.ib m.bcg.server.s ync.SyncAS2R equest com.ib m.bcg.server.s ync.SyncSOA PRequest com .ibm.bcg.serve r.sync.SyncCX MLRequest</code>		
<code>bcg.receiver.sync.respo nseURL</code>	<code>/bcgreceiver/ SyncResponse</code>		URI to post Synchronous Responses
<code>bcg.receiver.sync.respo nseURL.port</code>	<code>\$RECEIVER_ HTTP_PORT\$</code>		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.			
<code>bcg.http.hdrdef.fromID</code>	<code>x-aux-sender- id</code>		HTTP header persisted in metadata file for the BPE to process
<code>bcg.http.hdrdef.toID</code>	<code>x-aux-receiver- id</code>		HTTP header persisted in metadata file for the BPE to process
<code>bcg.http.hdrdef.protoco l</code>	<code>x-aux-protocol</code>		HTTP header persisted in metadata file for the BPE to process
<code>bcg.http.hdrdef.protoco lVersion</code>	<code>x-aux-protocol- version</code>		HTTP header persisted in metadata file for the BPE to process
<code>bcg.http.hdrdef.process</code>	<code>x-aux-process- type</code>		HTTP header persisted in metadata file for the BPE to process

Table C-2. Receiver-specific properties

Entry	Default value	Possible settings	Description
<code>bcg.http.hdrdef.processVersion</code>	x-aux-process-version		HTTP header persisted in metadata file for the BPE to process
<code>bcg.http.hdrdef.msgid</code>	x-aux-msg-id		HTTP header persisted in metadata file for the BPE to process
<code>bcg.http.hdrdef.contentType</code>	content-type		HTTP header persisted in metadata file for the BPE to process
<code>bcg.http.hdrdef.systemMsgId</code>	x-aux-system-msg-id		HTTP header persisted in metadata file for the BPE to process
<code>bcg.http.hdrdef.RNResponseType</code>	x-rn-response-type		HTTP header persisted in metadata file for the BPE to process
<code>bcg.http.hdrdef.RNVersion</code>	x-rn-version		HTTP header persisted in metadata file for the BPE to process
<code>bcg.http.hdrdef.productionFlag</code>	x-aux-production		HTTP header persisted in metadata file for the BPE to process
<code>bcg.http.hdrdef.provSessionId</code>	x-aux-prov-session-id		HTTP header persisted in metadata file for the BPE to process
<code>bcg.http.hdrdef.processInstanceId</code>	x-aux-process-instance-id		HTTP header persisted in metadata file for the BPE to process
<code>bcg.http.hdrdef.contentLength</code>	Content-Length		HTTP header persisted in metadata file for the BPE to process
<code>bcg.http.hdrdef.as2From</code>	AS2-From		HTTP header persisted in metadata file for the BPE to process
<code>bcg.http.hdrdef.as2To</code>	AS2-To		HTTP header persisted in metadata file for the BPE to process
<code>bcg.http.hdrdef.as2Version</code>	AS2-Version		HTTP header persisted in metadata file for the BPE to process
<code>bcg.http.hdrdef.mimeVersion</code>	Mime-Version		HTTP header persisted in metadata file for the BPE to process

Table C-2. Receiver-specific properties

Entry	Default value	Possible settings	Description
<code>bcg.http.hdrdef.messageId</code>	Message-ID		HTTP header persisted in metadata file for the BPE to process
<code>bcg.http.hdrdef.date</code>	Date		HTTP header persisted in metadata file for the BPE to process
<code>bcg.http.hdrdef.from</code>	From		HTTP header persisted in metadata file for the BPE to process
<code>bcg.http.hdrdef.subject</code>	Subject		HTTP header persisted in metadata file for the BPE to process
<code>bcg.http.hdrdef.contentTransferEncoding</code>	Content-Transfer-Encoding		HTTP header persisted in metadata file for the BPE to process
<code>bcg.http.hdrdef.contentDisposition</code>	Content-Disposition		HTTP header persisted in metadata file for the BPE to process
<code>bcg.http.hdrdef.dispositionNotificationTo</code>	Disposition-Notification-To		HTTP header persisted in metadata file for the BPE to process
<code>bcg.http.hdrdef.dispositionNotificationOptions</code>	Disposition-Notification-Options		HTTP header persisted in metadata file for the BPE to process
<code>bcg.http.hdrdef.receiptDeliveryOption</code>	Receipt-Delivery-Option		HTTP header persisted in metadata file for the BPE to process
<code>bcg.http.hdrdef.toPackagingName</code>	ToPackagingName		HTTP header persisted in metadata file for the BPE to process
<code>bcg.http.hdrdef.asDocType</code>	ASDocType		HTTP header persisted in metadata file for the BPE to process
<code>bcg.http.hdrdef.recipientAddress</code>	Recipient-Address		HTTP header persisted in metadata file for the BPE to process
<code>bcg.http.hdrdef.authorization</code>	Authorization		HTTP header persisted in metadata file for the BPE to process
<code>bcg.http.hdrdef.soapAction</code>	SOAPAction		HTTP header persisted in metadata file for the BPE to process

Table C-3. 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 #####			
bcg.duns	105217165		
##### BCG DB ##			
bcg.co.db.DBType	\$ROUTER.DB.TYPE\$	db2,oracle	Database type
bcg.co.db.DBPoolName	\$ROUTER.JNDI\$	datasources/DB2DS,datasources/OraclePool	Datasource JNDI Prefix
bcg.co.jndiContextURL	corbaloc:iiop:localhost:56809		JNDI Provider URL
bcg.co.jndiFactory	com.ibm.websphere.naming.WsnInitialContextFactory		JNDI Context Factory
bcg.co.db.schema	\$ROUTER.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.RefFSContextFactory		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

Table C-3. Router-specific properties

Entry	Default value	Possible settings	Description
# 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		
## MAIN RTR ##			
bcg.oaq_bpe_in.main	WBIC/main_InboundQ		JMS Main In Queue Name
bcg.oaq_bpe_out.main	WBIC/deliveryManagerQ		JMS Delivery Manager Queue Name

Table C-3. Router-specific properties

Entry	Default value	Possible settings	Description
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/deliveryManagerQ		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

Table C-3. Router-specific properties

Entry	Default value	Possible settings	Description
bcg.oaq_bpe_out.synchronous	WBIC/deliveryManagerQ		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
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.H2DestinationProcess		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		

Table C-3. Router-specific properties

Entry	Default value	Possible settings	Description
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.initialNumberOfReceivers	4		Number of Log Receivers
bcg.dberrors.queue	WBIC/ datalogErrorQ		JMS Log Receiver Errors Queue Name
### Alert Engine ###			
bcg.alertQueue.queue	WBIC/alertQ		JMS Alert Queue Name
bcg.alertQReceiver.initialNumberOfReceivers	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/ alertEventQ		JMS Alert Event Queue Name
bcg.eventAlertQReceiver.initialNumberOfReceivers	1		Number of Alert Event Receivers
<p># Allow this much time after the volume alert end time to record that the doc</p> <p># was received in our system, before evaluating the alert:</p>			
bcg.volumeAlertScheduler.allowanceForProcessingReceivedDocInMins	10		

Table C-3. Router-specific properties

Entry	Default value	Possible settings	Description
<pre># 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 'minNotificationQuietIntervalInMins':</pre>			
bcg.alertNotifications.maxNotificationsInInterval	10		
bcg.alertNotifications.maxNotificationIntervalInMins	30		
bcg.alertNotifications.minNotificationQuietIntervalInMins	30		
bcg.alertNotifications.heldAlertsBatchTimeInMins	30		
<pre># Notifications that are returned because of e.g. invalid partner email addresses will go # to bcg.alertNotifications.mailEnvelopeFrom.</pre>			
bcg.alertNotifications.mailHost	\$ROUTER.ALERTS.SMTP_RELAY\$		SMTP Relay Host
bcg.alertNotifications.mailFrom	\$ROUTER.ALERTS.MAIL_FROM\$		Alerts "from" mail address

Table C-3. Router-specific properties

Entry	Default value	Possible settings	Description
bcg.alertNotifications.mailReplyTo	\$ROUTER.ALERTS.MAIL_FOLDER\$		Alerts "from" mail address
bcg.alertNotifications.mailEnvelopeFrom	\$ROUTER.ALERTS.MAIL_FOLDER\$		Alerts "from" mail address
<pre> # time for running cert expiration event generator # <minutes> <hour> <class name> # this runs at 1:13 am: </pre>			
alert.eventGenerator.schedule	13 1	CertificateExpiration	
### 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
<pre> # in millisecs, applies to all gateways </pre>			
bcg.delivery.gwTransportRetryInterval	3000		Gateway retry interval in milliseconds

Table C-3. Router-specific properties

Entry	Default value	Possible settings	Description
bcg.delivery.queue	WBIC/ deliveryManagerQ		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/ syncDeliveryManagerQ		JMS Synchronous Delivery Manager Queue Name
bcg.syncdeliveryQReceiver.initialNumberOfReceivers	3		Number of Synchronous Delivery Manager receivers
# 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	
## 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.			

Table C-3. Router-specific properties

Entry	Default value	Possible settings	Description
<pre>bcg.rosettanet.globalUsageCode ## 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.</pre>	Literal	Literal, Production, Test	
<pre>bcg.rosettanet.defaultUsageCdOnError</pre>	1		
<pre>bcg.rosettanet.defaultGlbUsageCd ## 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.</pre>	Production	Production, Test	
<pre>bcg.rosettanet.useBuilderProcessInstanceId ## If builder provided process-instance-id is invalid (for whatever reason), we ## can generate a new process-instance-id.</pre>	1		
<pre>bcg.rosettanet.generateProcessInstanceIdOnError #####</pre>	1		
<pre>bcg.receiver.persistpath ### RNE ###</pre>	<pre>\$\$SHARED_DATA_DIR\$/ router_in/</pre>		

Table C-3. Router-specific properties

Entry	Default value	Possible settings	Description
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
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			

Table C-3. Router-specific properties

Entry	Default value	Possible settings	Description
bcg.rosettnet.signature.VerifySigner	TRUE	true, false	
## Encryption properties			
bcg.rosettnet.encrypt.CRLDir	\$SHARED_DATA_DIR\$/security/crl/		Path to CRL directory
bcg.rosettnet.encrypt.CertDbRefreshInterval	600000		
# valid values: 3des, rc5, rc2-40			
bcg.rosettnet.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		
## 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

Table C-3. Router-specific properties

Entry	Default value	Possible settings	Description
<code>bcg.http.hdrdef.process</code>	<code>x-aux-process-type</code>		HTTP header persisted in metadata file for the BPE to process
<code>bcg.http.hdrdef.processVersion</code>	<code>x-aux-process-version</code>		HTTP header persisted in metadata file for the BPE to process
<code>bcg.http.hdrdef.msgid</code>	<code>x-aux-msg-id</code>		HTTP header persisted in metadata file for the BPE to process
<code>bcg.http.hdrdef.contentType</code>	<code>content-type</code>		HTTP header persisted in metadata file for the BPE to process
<code>bcg.http.hdrdef.systemMsgId</code>	<code>x-aux-system-msg-id</code>		HTTP header persisted in metadata file for the BPE to process
<code>bcg.http.hdrdef.RNResponseType</code>	<code>x-rn-response-type</code>		HTTP header persisted in metadata file for the BPE to process
<code>bcg.http.hdrdef.RNVersion</code>	<code>x-rn-version</code>		HTTP header persisted in metadata file for the BPE to process
<code>bcg.http.hdrdef.productionFlag</code>	<code>x-aux-production</code>		HTTP header persisted in metadata file for the BPE to process
<code>bcg.http.hdrdef.provSessionId</code>	<code>x-aux-prov-session-id</code>		HTTP header persisted in metadata file for the BPE to process
<code>bcg.http.hdrdef.processInstanceId</code>	<code>x-aux-process-instance-id</code>		HTTP header persisted in metadata file for the BPE to process
<code>bcg.http.hdrdef.contentLength</code>	<code>Content-Length</code>		HTTP header persisted in metadata file for the BPE to process
<code>bcg.http.hdrdef.as2From</code>	<code>AS2-From</code>		HTTP header persisted in metadata file for the BPE to process
<code>bcg.http.hdrdef.as2To</code>	<code>AS2-To</code>		HTTP header persisted in metadata file for the BPE to process
<code>bcg.http.hdrdef.as2Version</code>	<code>AS2-Version</code>		HTTP header persisted in metadata file for the BPE to process

Table C-3. Router-specific properties

Entry	Default value	Possible settings	Description
<code>bcg.http.hdrdef.mimeVersion</code>	Mime-Version		HTTP header persisted in metadata file for the BPE to process
<code>bcg.http.hdrdef.messageId</code>	Message-ID		HTTP header persisted in metadata file for the BPE to process
<code>bcg.http.hdrdef.date</code>	Date		HTTP header persisted in metadata file for the BPE to process
<code>bcg.http.hdrdef.from</code>	From		HTTP header persisted in metadata file for the BPE to process
<code>bcg.http.hdrdef.subject</code>	Subject		HTTP header persisted in metadata file for the BPE to process
<code>bcg.http.hdrdef.contentType</code>	Content-Transfer-Encoding		HTTP header persisted in metadata file for the BPE to process
<code>bcg.http.hdrdef.contentDisposition</code>	Content-Disposition		HTTP header persisted in metadata file for the BPE to process
<code>bcg.http.hdrdef.dispositionNotificationTo</code>	Disposition-Notification-To		HTTP header persisted in metadata file for the BPE to process
<code>bcg.http.hdrdef.dispositionNotificationOptions</code>	Disposition-Notification-Options		HTTP header persisted in metadata file for the BPE to process
<code>bcg.http.hdrdef.receiptDeliveryOption</code>	Receipt-Delivery-Option		HTTP header persisted in metadata file for the BPE to process
<code>bcg.http.hdrdef.toPackagingName</code>	ToPackagingName		HTTP header persisted in metadata file for the BPE to process
<code>bcg.http.hdrdef.asDocType</code>	ASDocType		HTTP header persisted in metadata file for the BPE to process
# Packaging related properties			
# Attachments with one of the following content types will not be base64 encoded			

Table C-3. Router-specific properties

Entry	Default value	Possible settings	Description
<code>bcg.pkg.sponsor.contenttypes</code>	<code>bcg.pkg.sponsor.contenttypes</code>		
### START of SPONSOR ENGINE ###			
<code>bcg.sponsor.inbound_poll_interval</code>	10000		
<code>bcg.sponsor.in_thread_count</code>	2		Number of Inbound threads for Sponsor Engine
<code>bcg.sponsor.work_size</code>	10		
<code>bcg.delivery.sponsor.eventMsgClass</code>	<code>com.ibm.bcg.delivery.sponsor.SponsorEventMessage</code>		
### DB proc debug properties###			
<code>DBProcDebug</code>	1		Database debugging flag
# Global State engines instance ID			
<code>GlobalStateEngInstanceId</code>	<code>bcg</code>		
# EDIINT defaults			
<code>bcg.ediint.reportingUA</code>	<code>WBI_Connect</code>		
<code>bcg.ediint.retryWaitTmMS</code>	5000		

Appendix D. 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 1 fails
Transport retry 2 fails
Transport retry 3 fails

Gateway retry 1 fails

Transport retry 1 fails
Transport retry 2 fails
Transport retry 3 fails

Gateway retry 2 fails

Transport retry 1 fails
Transport retry 2 fails
Transport retry 3 fails

Gateway retry 3 fails

Transport retry 1 fails
Transport retry 2 fails
Transport retry 3 fails

Document fails delivery

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

Index

A

- Account Admin activities 101
 - adding Participants to the Exclusion List 126
 - changing B2B attribute values 119
 - changing connection configurations 125
 - changing Participant attribute values 125
 - changing the source or target gateway 126
 - connection components 121
 - connection duplication 121
 - creating an FTP account 108
 - creating digital certificates 115
 - creating gateways 106
 - creating Participants 101
 - deleting gateway configurations 107
 - disabling a digital certificate 116
 - disabling or deactivating a connection 126
 - editing FTP details 114
 - editing the Exclusion List 126
 - information for gateway configuration 107
 - managing certificates 114
 - managing exclusion lists 126
 - managing gateway configurations 105
 - managing Participant connections 120
 - managing Participant profiles 101
 - performing a basic search for connections 123
 - performing an advanced search 124
 - searching for connections 123
 - searching for Participants 104
 - selecting a new Action 125
 - specifying an FTP server 108
 - viewing and editing digital certificates 115
 - viewing and editing gateways 105
 - viewing and editing Participant profiles 103
 - viewing default gateways 106
 - viewing your profile 104
- Account, creating an FTP 108
- Actions
 - enabling or disabling 96
 - selecting a new 125

Activities

- Account Admin 101
- Hub Admin 19

Adding

- a validation map to a Document Flow Definition 43
- Participants to the Exclusion List 126

Advanced search

- for connections 124

Are You Sure Message 103

Associating a map to Document Flow Definition 44

Attributes

- changing B2B 119
- changing Participant values 125
- selecting Document Flow Definition 38
- setting Document Flow Definition 36

Avoiding out-of-memory errors 148

B

B2B attributes, changing 119

B2B capabilities

- screen 118

Basic search, for connections 123

Branding the Community Console 19

C

Certificates

- creating 115
- disabling 116
- managing 114
- viewing and editing 115

Changing

- B2B attribute values 119
- connection configurations 125
- gateway status 145
- Participant attribute values 125
- the source or target gateway 126

Cloning from an existing object in the current context 38

- Community Console
 - branding [19](#)
 - icons [16](#)
 - logging in [13](#)
 - logging out [18](#)
 - navigating through [15](#)
 - stopping [18](#)
- Company
 - logo uploading [22](#)
 - Website [10](#)
- Components
 - connections [121](#)
 - Document Flow Definition [31](#)
- Configurations
 - changing connection [125](#)
 - deleting gateway [107](#)
 - gateway required information [107](#)
 - managing gateway [105](#)
- Configuring
 - Document Flow Definitions [30](#)
 - download packages [30](#)
 - permissions [23](#)
 - targets [25](#)
- Connections
 - changing configurations [125](#)
 - components [121](#)
 - disabling or deactivating [126](#)
 - duplication [121](#)
 - managing Participant [120](#)
 - performing a basic search [123](#)
 - searching for [123](#)
- Console Branding screen [20](#)
- Crash, restarting after [155](#)
- Creating
 - a new target [25](#)
 - an FTP account [108](#)
 - an XML format [93](#)
 - digital certificates [115](#)
 - Document Flow Definitions [32](#)
 - document flow interactions [39](#)

- gateways [106](#)
- Participants [101](#)
- Customer Service [10](#)

D

- Database query performance, optimizing [147](#)
- Database, reprocessing events and business documents [148](#)
- Deactivating a connection [126](#)
- Default
 - gateways [106](#)
- Deleting
 - an XML format [95](#)
 - gateway configurations [107](#)
 - targets [30](#)
- Details, viewing gateway [145](#)
- Digital certificates
 - creating [115](#)
 - disabling [116](#)
 - managing [114](#)
 - viewing and editing [115](#)
- Disabling
 - a connection [126](#)
 - a digital certificate [116](#)
 - actions [96](#)
 - permissions quickly [24](#)
 - targets [30](#)
- Document Flow Definition
 - adding a validation map [43](#)
 - associating a validation map [44](#)
 - attributes [36](#)
 - cloning from existing object [38](#)
 - components [31](#)
 - configuring [30](#)
 - creating [32](#)
 - creating interactions [39](#)
 - downloading a package to a local computer [36](#)
 - selecting attributes [38](#)
 - understanding [30](#)
 - uploading and downloading a package [35](#)
- Document processing terms [9](#)

Documents
 removing from the queue [145](#)
 reprocessing [148](#)
 viewing queued [144](#)
Download packages, configuring [30](#)
Downloading
 a Document Flow Definition package [35](#)
 a package to a local computer [36](#)
 sample images [21](#)
DUNS numbers [102](#)
DUNS+4 [102](#)

E

Editing
 digital certificates [115](#)
 FTP details [114](#)
 gateways [105](#)
 Participant profiles [103](#)
 password policy details [22](#)
 permission details [23, 97](#)
 target details [29](#)
 the Exclusion List [126](#)
 XML format values [94](#)

Enabling
 actions [96](#)
 permissions quickly [24](#)
 targets [30](#)

Event codes
 managing [96](#)
 saving names [97](#)

Events, reprocessing [148](#)

Exclusion List
 adding Participants [126](#)
 editing [126](#)
 managing [126](#)

Existing object, cloning from current context [38](#)

F

Fail to log, reprocessing events and business documents [148](#)

File directory [28](#)
File Transfer Protocol, creating an account [108](#)
Format, creating an XML format [93](#)
Freeform ID numbers [102](#)
FTP
 configuration [108](#)
 creating an account [108](#)
 description [108](#)
 directory [26](#)
 editing details [114](#)
 password file, description [111](#)
 scripts [111](#)

G

Gateway
 changing source or target [126](#)
 changing status [145](#)
 creating [106](#)
 deleting configurations [107](#)
 managing configurations [105](#)
 removing documents from the queue [145](#)
 required configuration information [107](#)
 using Queue [143](#)
 viewing and editing [105](#)
 viewing default [106](#)
 viewing details [145](#)
 viewing queued documents [144](#)
 viewing the list [143](#)

Getting Help [10](#)

H

Header background, uploading [22](#)
Help [10](#)
HTTP/S [28](#)
Hub Admin activities [19](#)
 adding a validation map to a Document Flow Definition [43](#)
 associating a map to Document Flow Definition [44](#)
 branding the Community Console [19](#)
 cloning from an existing object in the current context [38](#)

- configuring Document Flow Definitions and download packages [30](#)
- configuring permissions [23](#)
- configuring targets [25](#)
- creating a new target [25](#)
- creating an XML format [93](#)
- creating Document Flow Definitions [32](#)
- creating document flow interactions [39](#)
- deleting an XML format [95](#)
- deleting targets [30](#)
- Document Flow Definition
 - components [31](#)
- downloading a package to a local computer [36](#)
- downloading sample images [21](#)
- editing XML format values [94](#)
- enabling or disabling actions [96](#)
- enabling or disabling permissions quickly [24](#)
- enabling or disabling targets [30](#)
- file directory [28](#)
- FTP directory [26](#)
- HTTP/S [28](#)
- JMS [27](#)
- managing event codes [96](#)
- managing password policy [22](#)
- managing XML formats [93](#)
- POP3 [27](#)
- saving event code names [97](#)
- selecting attributes from a list [38](#)
- setting Document Flow Definition attributes [36](#)
- understanding Document Flow Definitions [30](#)
- updating a validation map [43](#)
- uploading a header background and company logo [22](#)
- uploading and downloading a package [35](#)
- viewing and editing password policy details [22](#)
- viewing and editing permission details [23, 97](#)
- viewing and editing target details [29](#)

I

Icons in the Community Console [16](#)

Image

- downloading sample [21](#)
- specifications [21](#)

Information required for gateway configuration [107](#)

Interaction

- creating document flow [39](#)

J

JMS [27](#)

L

Logging in [13](#)

Logging out [18](#)

M

Machine shutdown, starting the system after [154](#)

Managing

- certificates [114](#)

- event codes [96](#)

- exclusion lists [126](#)

- gateway configurations [105](#)

- Participant connections [120](#)

- Participant profiles [101](#)

- password policy [22](#)

- XML formats [93](#)

N

Navigating through Community Console [15](#)

New action, selecting [125](#)

New target, creating [25](#)

O

Online Help [10](#)

Optimizing database query performance [147](#)

Out-of-memory errors, avoiding [148](#)

P

Package

- downloading to a local computer [36](#)

- uploading and downloading [35](#)

Participant

- adding to Exclusion Lists [126](#)

- advanced search for connections [124](#)
- basic search for connections [123](#)
- changing attribute values [125](#)
- connection components [121](#)
- connection duplication [121](#)
- creating [101](#)
- managing connections [120](#)
- managing profiles [101](#)
- searching [104](#)
- searching for connections [123](#)
- viewing and editing profiles [103](#)
- viewing profile [104](#)

Password

- viewing and editing policy details [22](#)

Performing

- advanced search for connections [124](#)
- basic search for connections [123](#)

Permission

- configuring [23](#)
- enabling or disabling quickly [24](#)
- viewing and editing details [23, 97](#)

Poor performance and system events are not working [153](#)

POP3 [27](#)

Profile

- managing Participant [101](#)
- viewing [104](#)

Q

Queue, removing documents from [145](#)

Queued documents, viewing [144](#)

R

Removing documents from the queue [145](#)

Reprocessing events and business documents [148](#)

Reprocessing events and business documents that fail to log to the database [148](#)

Required information, gateway configuration [107](#)

Reset user password message [103](#)

Restarting the router [155](#)

Restarting the router after a crash [155](#)

Router and receiver, stopping [18](#)

Router, restarting [155](#)

Router, restarting after a crash [155](#)

S

Sample images, downloading [21](#)

Saving event code names [97](#)

Screens

- Are You Sure Message [103](#)

- B2B Capabilities [118](#)

- Console Branding [20](#)

- Reset User Password Message [103](#)

- Target Details [25](#)

Search

- advanced for connections [124](#)

- basic for connections [123](#)

Searching

- for connections [123](#)

- for Participants [104](#)

Selecting

- a new action [125](#)

- attributes from a list [38](#)

Setting

- Document Flow Definition attributes [36](#)

Shutting down [154](#)

Source gateway, changing [126](#)

Starting WebSphere Business Integration Connect [13](#)

Status, change gateway [145](#)

Stopping

- Community Console [18](#)

- router and receiver [18](#)

System events not working [153](#)

T

Target

- changing gateway [126](#)

- configuring [25](#)

- creating new [25](#)

- deleting [30](#)

- Details screen [25](#)

- enabling or disabling [30](#)

viewing and editing details [29](#)

Terms [9](#)

Transport

file directory [28](#)

FTP [26](#)

HTTP/S [28](#)

JMS [27](#)

POP3 [27](#)

Troubleshooting [147](#)

avoiding out-of-memory errors [148](#)

optimizing database query performance [147](#)

poor performance and system events are not working [153](#)

reprocessing [148](#)

reprocessing events and business documents that fail to log to the database [148](#)

restarting the router [155](#)

restarting the router after a crash [155](#)

shutting down [154](#)

starting the system after a machine shutdown [154](#)

U

Understanding Document Flow Definitions [30](#)

Updating a validation map [43](#)

Uploading

company logo [22](#)

Document Flow Definition package [35](#)

header background [22](#)

Using the Gateway Queue [143](#)

V

Validation maps

adding to a Document Flow Definition [43](#)

associating a map to Document Flow Definition [44](#)

updating [43](#)

Viewing

default gateways [106](#)

digital certificates [115](#)

gateway details [145](#)

gateway list [143](#)

gateways [105](#)

Participant profile [103](#), [104](#)

password policy details [22](#)

permission details [23](#), [97](#)

queued documents [144](#)

target details [29](#)

W

WBIC terms [9](#)

WebSphere Business Integration Connect

starting [13](#)

starting after machine shutdown [154](#)

X

XML

creating a format [93](#)

deleting a format [95](#)

editing format values [94](#)

managing formats [93](#)

Notices and Trademarks

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 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 contains 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 contains 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. 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 IBM's application programming interfaces.

Programming interface information

Programming interface information 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 of International Business Machines Corporation in the United States, other countries, or both:

IBM
the IBM logo
CrossWorlds
DB2
DB2 Universal Database
MQSeries
Tivoli
WebSphere

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

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

Solaris, 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.



