IBM WebSphere Partner Gateway Enterprise and Advanced Editions

Administrator Guide

Version 6.0

IBM WebSphere Partner Gateway Enterprise and Advanced Editions

Administrator Guide

Version 6.0

Note!
Before using this information and the product it supports, read the information in "Notices" on page 137.

28June2005

This edition applies to Version 6, Release 0, Modification 0, of IBM(TM) WebSphere(TM) Partner Gateway Advanced Edition (5724-L68) and Enterprise Edition (5724-L69), and to all subsequent releases and modifications until otherwise indicated in new editions.

To send us your comments about this document, email doc-comments@us.ibm.com. We look forward to hearing from you.

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

Contents

About this book

This document describes how WebSphere Partner Gateway can be maintained to suit the requirements of the business-to-business (B2B) trading community. This guide assumes that you have already performed the necessary hub configuration tasks provided in the *Hub Configuration Guide*.

New in this release

New in release 6.0

This section highlights the changes to WebSphere Partner Gateway for version 6.0.

- The product name has changed from WebSphere Business Integration Connect to WebSphere Partner Gateway.
- EDI support has been added. See, "Managing EDI" on page 13.
- EDI messages and codes have been added. See, Appendix B, "Failed Events," on page 89.
- Support for resending failed or successful documents has been added. See, "Resending failed and successful documents" on page 59.
- Appendix C has been renamed and updated to reflect the new component-specific property files. See, Appendix C, "Component-specific property files," on page 117.
- File names and directories have been updated to reflect the new naming convention.
- FTP Scripting transport support has been added.
- Multiple certificate support has been added. See, "Managing certificates" on page 27.
- IBM Tivoli License Manager (ITLM) support has been added.

New in release 4.2.2

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

- This guide has been modified to contain only information that is necessary to administer and maintain the WebSphere Partner Gateway environment. All information for configuring the environment has been moved to the new *Hub Configuration Guide*.
- Information for enhancing product performance has been added. See Appendix A, "Performance considerations," on page 87.
- Information for archiving data has been added. See Chapter 8, "Archiving," on page 69.
- The option to delete participants is documented. See, "Deleting participants" on page 22.
- The option to delete transports is documented. See, "Deleting transports" on page 26.
- The new accessibility features that have been added to the Community Console to support screen readers are documented.

Audience

Administrators maintain WebSphere Partner Gateway. This book assumes two types of administrators:

- Hub Admin (also referred to as Community Operator)
- Account Admin

The Hub Admin is the super-administrative user in the community. The Hub Admin is responsible for overall hub community configuration and management, including participant configuration and connection activation. The Account Admin has access to a subset of the Hub Admin features and is the main administrative user for the Community Manager or Community participant.

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 Account Admin personnel.

Related documents

The complete set of documentation available with this product includes comprehensive information about installing, configuring, administering, and using WebSphere Partner Gateway Enterprise and Advanced Editions.

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

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

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

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

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

Getting help

Online Help is available by selecting **Help** on the upper-right side of each window.

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

Customer support

Software support

www.ibm.com/software/support

Passport Advantage(R)

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

Product documentation

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

Typographic conventions

This document uses the following typographic conventions:

Convention	Description
`Monospace font`	Text in this font indicates text that you type, values for arguments or command options, examples and code examples, or information that the system prints on the screen (message text or prompts).
bold	Boldface text indicates graphical user interface controls (for example, online button names, menu names, or menu options) and column headings in tables and text.
Italics	Text in italics indicates emphasis, book titles, new terms and terms that are defined in the text, variable names, or letters of the alphabet used as letters.
`Italic monospace font`	Text in italic monospace font indicates variable names within monospace-font text.
Underlined colored text	Underlined colored text indicates a cross-reference. Click the text to go to the object of the reference.
Text in a blue outline	(In PDF files only) A blue outline around text indicates a cross-reference. Click the outlined text to go to the object of the reference. This convention is the equivalent for PDF files of the "Underlined colored text" convention included in this table.
{INSTALL DIR}	Represents the directory where the product is installed.
UNIX:/Windows:	Paragraphs beginning with either of these indicate notes listing operating system differences.
" "(quotation marks)	(In PDF files only) Quotation marks surround cross-references to other sections of the document.
{ }	In a syntax line, curly braces surround a set of options from which you must choose one and only one.
`[ ]`	In a syntax line, square brackets surround optional parameters.
`...`	In a syntax line, ellipses indicate a repetition of the previous parameter. For example, `option[,...]` means that you can enter multiple, comma-separated options.
`< >`	Angle brackets surround variable elements of a name to distinguish them from one another. For example, *<server_name><connector_name>*tmp.log.
`\, /`	Backslashes (\) are used as component separators in directory paths in Windows installations. For UNIX installations, substitute slashes (/) for backslashes.

New in this release

New in release 6.0

This section highlights the changes to WebSphere Partner Gateway for version 6.0.

- The product name has changed from WebSphere Business Integration Connect to WebSphere Partner Gateway.
- EDI support has been added. See, "Managing EDI" on page 13.
- EDI messages and codes have been added. See, Appendix B, "Failed Events," on page 89.
- Support for resending failed or successful documents has been added. See, "Resending failed and successful documents" on page 59.
- Appendix C has been renamed and updated to reflect the new component-specific property files. See, Appendix C, "Component-specific property files," on page 117.
- File names and directories have been updated to reflect the new naming convention.
- FTP Scripting transport support has been added.
- Multiple certificate support has been added. See, "Managing certificates" on page 27.
- IBM Tivoli License Manager (ITLM) support has been added.

New in release 4.2.2

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

- This guide has been modified to contain only information that is necessary to administer and maintain the WebSphere Partner Gateway environment. All information for configuring the environment has been moved to the new *Hub Configuration Guide*.
- Information for enhancing product performance has been added. See Appendix A, "Performance considerations," on page 87.
- Information for archiving data has been added. See Chapter 8, "Archiving," on page 69.
- The option to delete participants is documented. See, "Deleting participants" on page 22.
- The option to delete transports is documented. See, "Deleting transports" on page 26.
- The new accessibility features that have been added to the Community Console to support screen readers are documented.

Chapter 1. Basic Community Console tasks

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

Topics covered in this chapter include:

Starting the Community Console

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

- UNIX(R) - {INSTALL DIR}/bin/bcgStartServer.sh bcgconsole
- Windows(R) - {INSTALL DIR}\bin\bcgStartServer.bat bcgconsole

Starting the Receiver

To start the Receiver, run one of the following scripts:

- UNIX - {INSTALL DIR}/bin/bcgStartServer.sh bcgreceiver
- Windows - {INSTALL DIR}\bin\bcgStartServer.bat bcgreceiver

Starting the Document Manager

To start the Document Manager, run one of the following scripts:

- UNIX - {INSTALL DIR}/bin/bcgStartServer.sh bcgdocmgr
- Windows - {INSTALL DIR}\bin\bcgStartServer.bat bcgdocmgr

Starting the Help system

For the help system to function, the Help system server must be running. By default, the Help system is installed on the same server as the Console; however, you can specify a different server for the Help system during the Console installation.

You can confirm the help system location by checking the value of the ibm.bcg.help.host property in the bcg_console.properties file, located in {INSTALL DIR}/console/lib/config/bcg_console.properties. If the value for the help server location is localhost, your local machine will be used for the help system.

To start the Help system, run one of the following scripts:

- UNIX - {INSTALL DIR}/bin/bcgStartHelp.sh
- Windows - {INSTALL DIR}\bin\bcgStartHelp.bat

Note: For Windows systems, the window that is used to run the bcgStartHelp script must remain open for the help server to continue running.

Logging in to the Community Console

The Community Console requires one of the following Web browsers:

- Microsoft(R) Internet Explorer versions 6.0 with SP1 or later
- Mozilla version 1.7 or later

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

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

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

To log in to the Community Console, follow these steps:

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

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

   `https://hostname.domain:58443/console (secure)`

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

Navigating through the Community Console

The Community Console consists of various menus used to configure WebSphere Partner Gateway.

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

- **Logout** allows you to log off from the current WebSphere Partner Gateway session. The application continues to run in the background. To log in again, follow the procedure under "Logging in to the Community Console" on page 2.
- **Help** allows you to access the online help for WebSphere Partner Gateway.

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

Community Console icons

Table 1 lists the icons that are used throughout the Community Console windows.

Table 1. Community Console Icons

Icon	Icon name
	A Trade Participant Agreement (TPA) has been entered
	Collapse
	Copy
	Data contained
	Deactivate
	Delete
	Display raw document
	Document in progress
	Document processing failed
	Document processing successful
	Download map
	Edit
	Edit attribute values
	Edit off
	Edit RosettaNet attribute values
	Expand
	Export information
	Export report
	Gateway disabled
	Hide search criteria
	Modify
	No data contained
	Open calendar

Table 1. Community Console Icons (continued)

Icon	Icon name
	Pause
	Print
	Required input
	Role; click to create role
	Start
	Synchronous data flow. No icon is displayed for asynchronous transactions
	Upload map
	View a previously sent original document when there is a duplicate document event
	View details
	View group memberships
	View Help system
	View permissions
	View the Document Flow Definition attribute setup
	View users
	View validation errors
	Where used

Logging off from the Community Console

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

Stopping the Community Console

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

- UNIX - {INSTALL DIR}/bin/bcgStopServer.sh bcgconsole
- Windows - {INSTALL DIR}\bin\bcgStopServer.bat bcgconsole

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

Stopping the Receiver and Document Manager

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

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

UNIX:

- {INSTALL DIR}/bin/bcgStopServer.sh bcgreceiver
- {INSTALL DIR}/bin/bcgStopServer.sh bcgdocmgr

Windows:

- {INSTALL DIR}\bin\bcgStopServer.bat bcgreceiver
- {INSTALL DIR}\bin\bcgStopServer.bat bcgdocmgr

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

Stopping the Help system

To stop the Help system, run one of the following scripts:

- UNIX - {INSTALL DIR}/bin/bcgStopHelp.sh
- Windows - {INSTALL DIR}\bin\bcgStopHelp.bat

Chapter 2. Hub administration tasks

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

Managing password policy

You can set up a password policy for the hub community, if you want to use values other than those set (by the system) as defaults. The password policy applies to all users who log in to the Community Console.

You can change the following elements of the password policy:

- Minimum Length, which represents the minimum number of characters the participant must use for the password. The default is 8 characters.
- Expire Time, which represents the number of days until the password expires. The default is 30 days.
- Uniqueness, which specifies the number of passwords to be held in a history file. A participant cannot use an old password if it exists in the history file. The default is 10 passwords.
- Special Characters, which, when selected, indicates that passwords must contain at least three of the following types of special characters:

  – Uppercase characters

  – Lowercase characters

  – Numeric characters

  – Special characters

  This setting allows for stricter security requirements when passwords are composed of English characters (ASCII). The default setting is off. It is recommended that Special Characters remain off when passwords are composed of international characters. Non-English-language character sets might not contain the required three out of four character types.

  The special characters supported by the system are as follows: '#', '@', '$', '&', '+'.

- Name Variation Checking, which, when selected, prevents the use of passwords that comprise an easily guessed variation of the user's login or full name. This field is selected by default.

To change the default values:

1. Click **Hub Admin** > **Console Configuration** > **Password Policy**. The Password Policy page is displayed.
2. Click the Edit icon.
3. Change any of the default values to the ones you want to use for your password policy.
4. Click **Save**.

Changing the database, database user, and password

After installation, you can change the database that the WebSphere Partner Gateway components use. You can also change the name of the database user and the database user's password.

In the following commands, serverName refers to bcgconsole, bcgreceiver or bcgdocmgr for Console, Receiver, and Document Manager respectively.

- On a Windows platform, change to the {INSTALL DIR}\bin directory and type:

```
bcgwsadmin.bat -f {INSTALL DIR}\scripts\bcgdbup.jacl -conntype NONE
db_type dbNAME dbUserID dbPassword nodeName serverName
```

- For all other platforms, type:

```
./bcgwsadmin.sh -f {INSTALL DIR}/scripts/bcgdbup.jacl -conntype NONE
dbType dbName dbUserID dbPassword nodeName serverName
```

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

```
./bcgwsadmin.sh -f {INSTALL DIR}/scripts/bcgdbup.jacl -conntype NONE
db2 hub_db george ABCD123 DefaultNode bcgdocmgr
```

Managing event codes

When an event occurs within WebSphere Partner Gateway, an event code is generated. Using the Event Codes window, you can see the generated event codes and export them to other applications. Additionally, you can set the alertable status of the event code.

Viewing and editing event codes

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

1. Click **Hub Admin** > **Hub Configuration** > **Event Codes**.
2. On the Event Codes window, click the View details icon next to the event code whose details you want to view.
3. On the Event Code Details window, set the parameters described in Table 2 on page 9:

Table 2. Event code details

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

Saving event code names

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

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

Specifying alertable events

When an event occurs within WebSphere Partner Gateway, an event code is generated. Using the Event Codes page, you can set the alertable status of the event code. When an event is set as alertable, the event appears in the Event Name list of the Alert page. You can then set an alert for the event.

To indicate which events should be alertable:

1. **Click Hub Admin > Hub Configuration > Event Codes**.
   The Event Codes page is displayed.
2. For each event you want made alertable:
   - Click the magnifying glass icon next to the event code.
     The Event Code Details page is displayed.
   - Select **Alertable**.

Managing targets

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

Viewing and editing target details

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

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

Enabling or disabling targets

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

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

Deleting targets

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

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

   Note: The target in the following step is immediately deleted without a warning message. Be sure that you want to delete the target.
2. On the Target List window, click the Delete icon next to the target you want to delete.

Managing Interactions

To enable, disable or edit interactions between two document flow definitions, follow these steps:

1. Click **Hub Admin** > **Hub Configuration** > **Document Flow Definition**.
2. Click **Manage Interactions**.
3. Enter search criteria that WebSphere Partner Gateway 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 Delete icon next to the interaction you want to enable. When a precautionary message asks whether you are sure, click **OK**. WebSphere Partner Gateway replaces the Delete icon with the Deactivate icon to show that you have enabled the interaction.
6. To disable an interaction, click the Deactivate icon next to the interaction you want to disable. When a precautionary message asks whether you are sure, click **OK**. WebSphere Partner Gateway replaces the Deactivate icon with the Delete icon to show that you have disabled the interaction.

7. To edit an interaction, click the Edit icon next to the interaction. In the editing window, edit the interaction, then click **Save**.

Managing XML formats

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

Editing XML format values

To edit XML format values, follow these steps:

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

Deleting an XML format

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

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

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

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

Enabling or disabling actions

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

Click **Hub Admin** > **Hub Configuration** > **Actions** to display the Actions window.

The following parameters are displayed for each action:

- The name of the action
- The status (Enabled or Disabled) of the action
- The provider of the action - either WebSphere Partner Gateway, indicated by **Product**, or a user.

From this page, you can do the following:

- Click the view Details icon to see details about an action. You can modify the information for user-created actions.
- Click the Where used icon to see the transformation maps and connections currently using the action.
- Click the Copy icon to create a new action based on the selected action.
- Click **Create** to create a new action and make it available for use.

Managing Handlers

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

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

Importing a handler

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

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

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

Deleting a handler

To delete a handler, follow these steps:

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

Managing Maps

This section describes how to manage the different types of maps available for use with WebSphere Partner Gateway.

Updating Validation Maps

Use this procedure to update a validation map currently in the system.

1. Click **Hub Admin** > **Hub Configuration** > **Maps** > **Validation Maps**.

   The validation maps currently in the system are displayed.
2. Click the Download map icon to download the validation map to your local computer. Update the map as needed.
3. Click the Upload map icon to load the updated map to the system.

Managing Transformation Maps

Use this page to view a list of transformation maps that are currently in the system or search for a specific map.

From this page, you can perform the following tasks:

- Perform a search (name, description) for a specific map.
- View the transformation maps currently in the system.

Click the Details icon to display details about a map.

Click the Download map icon to download a transformation map to your local computer. This is useful when you need to update a map.

Click the Upload map icon to upload an updated map to the system.

See the *Hub Configuration Guide* for details on creating a new transformation map.

Managing EDI FA Maps

Use this page to view a list of functional acknowledgement (FA) maps that are currently in the system or search for a specific map. A FA map can be associated with routing objects; however, the attribute values cannot be edited.

From this page, you can perform the following tasks:

- Perform a search (name, description) for a specific map.
- View the FA maps that are currently in the system.

Click the View details icon to display details about a map.

Click the Where used icon to see where a FA map is used.

Click the Delete icon to delete a FA map.

Managing EDI

You can modify many attributes that pertain to the exchange of EDI interchanges. For example, you can change the default values that are provided for all envelopes, you can define specific envelopes to be used for certain exchanges, you can set up control numbers that are assigned to the various parts of an interchange, and you can set connection profiles so that the same interchange can be delivered in a different way. These tasks are described in this section.

Envelope Profile

Use the Envelope profiles window to view, edit, create, or delete an envelope profile record. The EDI standard (X12, UCS, EDIFACT) is shown for each listed profile.

Refer to the *Hub Configuration Guide* for descriptions of each Envelope Profile Attribute for the EDI standards.

Editing envelope profile records

1. Click **Hub Admin** > **Hub Configuration** > **EDI** > **Envelope Profile**.
2. Click the View details icon next to the Envelope profile name that you want to edit.

3. Select the envelope profile type that you want to change and click the Edit icon.

   The selected envelope profile attribute values (general, interchange, group, or transaction) are displayed. See the *Hub Configuration Guide* for attribute descriptions.
4. Update the envelope profile attribute values as needed, and click **Save**. See the *Hub Configuration Guide* for attribute descriptions.

Creating envelope profile records

1. Click **Hub Admin** > **Hub Configuration** > **EDI** > **Envelope Profile**.
2. Click **Create** in the Envelope profiles window.
3. Type a value for the following:
   - Envelope profile name: Type a unique name for the new envelope profile. This is a required field.

     Note: If the name is not unique (there is an existing envelope profile with the same name), an error message is returned when you attempt to save the new envelope profile.
   - Description: This is an optional value. Type a brief description of the envelope profile.
4. Select the EDI Standard type (X12, UCS, or EDIFACT) in the drop-down list that is applicable to the new profile. This is a required field.

   After selecting a value in the EDI Standard drop-down list, the envelope profile attributes specific to that standard (General, Interchange, Group, or Transaction) are automatically displayed.
5. Update the envelope profile attribute values as needed, and click **Save**. See *Hub Configuration Guide* for attribute descriptions.

Deleting envelope profile records

1. Click **Hub Admin** > **Hub Configuration** > **EDI** > **Envelope Profile**.
2. Click the delete icon next to the Envelope profile name that you want to delete.

Enveloper

Use the Enveloper page to view and edit the Lock & Queue and Scheduling values for the enveloper.

1. Click **Hub Admin** > **Hub Configuration** > **EDI** > **Enveloper**.
2. Click the Edit icon to edit the Scheduler attributes.
   - For Maximum Lock Time, type the maximum allowed amount of time (in seconds) for the database lock. This value is rendered in seconds. The lock is used to prevent multiple Enveloper instances from accessing the same data.
   - For Maximum Queue Age, type the maximum amount of time (in seconds) allowed for queued requests to obtain the database lock. This value is rendered in seconds.
   - Use Batch Mode is a global setting and is selected by default. When batch mode is turned on, the EDI Enveloper envelopes transactions in batches. Click to clear the Use Batch Mode check box and turn the batch mode off.
   - Click either Interval Based Scheduling (selected by default) or Calendar Based Scheduling. For Interval Based Scheduling, type the amount of time (in seconds) for the interval. For Calendar Based Scheduling, click Daily Schedule, Weekly Schedule, or Custom Schedule, and set the schedule accordingly.

3. Click **Save**.

Connection Profiles

You use connection profiles with de-enveloped transactions and with EDI interchanges created by the Enveloper. For transactions, the connection profile determines how the transaction is processed after it is de-enveloped. For interchanges, the connection profile determines how the interchange is delivered.

Use the Connection Profile window to create a new profile or to edit existing profile information. The name of each currently defined profile and its description, if any, are shown in the Connection Profiles List. Refer to the *Hub Configuration Guide* for more information on Connection Profiles.

Editing connection profiles

1. Click **Hub Admin** > **Hub Configuration** > **EDI** > **Connection Profiles**.
2. Click the View details icon to display the Connection Profile Details page, which provides a listing of all the connection profile's attribute values.
3. Click the Edit icon and edit the attributes as needed.
4. Click **Save**.

Creating connection profiles

1. Click **Hub Admin** > **Hub Configuration** > **EDI** > **Connection Profiles**.
2. Click **Create Connection Profile** to create a new connection profile.
3. Type the applicable information in the following profile attribute fields:
   - Connection Profile Name: A unique name identifier for the new profile. This is the only required field.
   - Description: A brief description of the connection profile.
   - Qualifier1: The value that determines which connection to use for an EDI interchange.
   - EDI Usage Type: Indicates whether this is a test, production, or information interchange.
   - Application Sender ID: The application or company division associated with the sender of the group.
   - Application Receiver ID: The application or company division associated with the recipient of the group.
   - Password: If a password is required between the application sender and application receiver.

   Click **Save**. The Connection Profiles Details page for the newly created connection profile is displayed.

Deleting connection profiles

1. Click **Hub Admin** > **Hub Configuration** > **EDI** > **Connection Profiles**.
2. Click the Delete icon to delete the connection profile.

Control Number Initialization

Use the Control Number Configuration page to configure control numbers that the Enveloper will use. You can also search for one or more control-number participants by name or by using wildcard search criteria, and optionally, EDI capability. Wildcard searches can contain any combination of letters and asterisks (*) in place of other letters. A search using only an asterisk (*) as the search string

returns a list of all EDI-capable participants. Refer to the *Hub Configuration Guide* for more information on control numbers and control number masks.

1. Click **Hub Admin** > **Hub Configuration** > **EDI** > **Control Number Initialization**.
2. Type the search criteria in the **Participant Name** field. The criteria can be either the name of a participant or wildcard search criteria. If you are not searching for EDI-capable participants, clear the **EDI-capable** check box. By default, the check box is selected. If you are searching for EDI-capable participants, leave the check box selected. Click **Search** to display the information fitting your search criteria in the Control Number Configuration list page.

   Note: If your search does not return any results, the following message is displayed: ″No results were found based on your search criteria.″ Click **Search** to return to the Control Number Configuration search page, and perform another search using new search criteria.
3. Click the View details icon next to the participant.
4. The participant's current control number assignments (if any) are listed on the Control Number Configuration Details page. Click the Edit icon to add or change the values.
5. Type (or change) the value next to **Interchange** to indicate the number you want to use to initialize control number generation for interchanges.
6. Type (or change) the value next to **Group** to indicate the number you want to use to initialize control number generation for groups. Alternatively, you can click **Mask** and type a mask to be used instead of a fixed value.
7. Type (or change) the value next to **Transaction** to indicate the number you want to use to initialize control number generation for transactions. Alternatively, you can click **Mask** and type a mask to be used instead of a fixed value. 8. Click Save.
8. Click **Save**.

Current Control Numbers

Use the Control Number Status Search page to search for the control number status for a participant-pair.

1. Click **Hub Admin** > **Hub Configuration** > **EDI** > **Current Control Numbers**.
2. Use the following options to search for one or more From participants and to search for one or more To participants.
   - **Participant Name**: The name of a specific participant. The search function is case sensitive so you must type the participant name exactly as it appears in the system.

     Note: You must select both a From participant and a To participant.
   - **Find EDI-capable**: By default, this check box is selected. If you are not searching for EDI-capable participants, clear the EDI-capable check box. If you are searching for EDI-capable participants, leave the check box selected.
   - **Search**: Click to initiate a search.
   - **search results**: The search results are displayed in this field. By default, the search results field contains one preselected entry, Any participant. To search for all participants, leave the Participant Name field blank, and click Search. To search for a specific participant, type the name in the Participant Name field, and then click Search.
   - **Display Current Status**: Click to display the control-number status values for the selected participant-pair.

3. Click the Edit icon to make changes if needed.

   CAUTION:
   The Edit and Reset All options should be used for special circumstances only as they can cause the control number to be duplicated.
4. Do one of the following:
   - Click **Save** to save all changes and return to the Control Number Status list.
   - Click **Return** to cancel all changes and return to Control Number Status list.
   - Click **Reset All** to reset the status for the participant-pair so that the status values are reinitialized by the next message exchange that occurs between the participants.

Updating alert mail addresses

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

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

1. Edit the bcg.properties file, located in the {INSTALL DIR}\router\lib\config directory to change the SMTP host e-mail addresses for alert notification. The elements in bcg.properties are:
   - bcg.alertNotifications.mailHost
   - bcg.alertNotifications.mailFrom
   - bcg.alertNotifications.mailReplyTo
   - bcg.alertNotifications.mailEnvelopeFrom
2. Restart the router for the changes to take effect.

Viewing system activity

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

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

To change the time interval, follow these steps:

1. Click **System Administration** > **Event Processing** > **Summary Service**.
2. On the Summary Service Properties window, click the Edit icon next to **Processing Interval (in Minutes)**.
3. Enter a value (from 1 through 60), indicating the number of minutes before data is summarized again. The default value is 15.
4. Click Save.

Managing event delivery

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

Note: On some Windows versions (prior to XP), you may need to change the default values of the JMS Queue Factory Name and the JMS Queue Name if you want to use the default Event Delivery feature. You will need to change the value for JMS Queue Factory Name from WBIC/QCF to WBIC\\QCF as well as the value for JMS Queue Name from WBIC/DeliveryQ to WBIC\\DeliveryQ.

To activate event publishing, follow these steps:

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

   See the *Hub Configuration Guide* for the property descriptions.
3. Click Save.

Note: See "Filtering events" on page 87 for information on excluding specific events from generating.

Managing API calls

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

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

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

Managing DocMgr Information

You can use the Document Manager Administration page to view and modify the Document Manager administration properties. Document Manager obtains files to process by polling three file system folders that are shared by the other components of the WebSphere Partner Gateway system. Since multiple Document Manager processes (each process can have multiple threads) can access the file system folders, WebSphere Partner Gateway locks the documents so only one process (thread) can process the document in the shared folder.

Maximum Hold Time

Set the maximum-lock-hold-time values for each of the three folders (Main, Synchronous, and Signal) to configure the maximum lock time that one of the document acquisition engine (DAE) processes (threads) can keep the lock on the document while processing the document.

- In **Main folder**, type a value (in seconds) representing the maximum lock holding time for the DAE instance that polls the main inbound directory (for example: router_in folder under Common). The default value is **3** seconds.

- In **Synchronous folder**, type a value (in seconds) representing the maximum lock holding time for the DAE instance that polls the synchronous message's directory (for example: sync_in folder under Common). The default value is **3** seconds.
- In **Signal folder**, type a value (in seconds) representing the maximum lock holding time for the DAE instance that polls the signal message's directory (for example: signal_in folder under Common). The default value is **3** seconds.

Maximum Files Per Poll Interval

Set the maximum-files-per-poll-interval values for each of the three folders (Main, Synchronous, and Signal) to configure the maximum number of files that will be handled by each DAE thread to process.

- In **Main folder**, type a value (greater than 0) representing the maximum number of files for the DAE instance that polls the main inbound directory (router_in) to process. The default value is **5**.
- In **Synchronous folder**, type a value (greater than 0) representing the maximum number of files for the DAE instance that polls the synchronous message's directory (sync_in) to process. The default value is **5**.
- In **Signal folder**, type a value (greater than 0) representing the maximum number of files for the DAE instance that polls the signal message's directory (signal_in) to process. The default value is **5**.

To view or modify the administration properties:

1. Click **System Administration** > **DocMgr Administration** > **DocMgr Information**.

   The Document Manager Administration page shows the properties in read-only mode.
2. Click the Edit icon to modify the properties.
3. Click **Save**.

Chapter 3. Account administration tasks

This chapter describes the tasks that can be performed by the Account Admin. These tasks are:

Managing participant profiles

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

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

Viewing and editing participant profiles

Follow these steps to view and edit participant profiles:

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

   Note: If you click **Reset User Passwords**, the Community Console displays a confirmation window. Click **OK** to proceed or click **Cancel** to retain the passwords. Resetting the password forces all users for that participant to enter a new password at the next login.
6. Click **Save**.

Searching for participants

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

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

7. Click **Save**.

Deleting participants

To delete a participant, follow these steps:

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

Managing gateway configurations

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

Required information for gateway configuration

The transport type determines the parameter information needed for gateway setup. In Table 3, the boxes marked with an X require configuration information, boxes marked with the letter O are optional. See Table 4 on page 24 for the gateway parameter descriptions.

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

Table 3. Required transport information

Required transport information	HTTP transport	HTTPS transport	FTP transport	FTPS transport	FTP Scripting transport	File Directory transport	JMS transport	SMTP transport
Authent.. Required							O	O
Auto Queue	O	O	O	O			O	O
Connection Timeout	X	X	X	X	X			
FTPS Mode					O			
JMS Factory Name							X	
JMS JNDI Factory Name							X	
JMS Message Class							X	
JMS Message Type							O	
JMS Queue Name							X	
Lock User					O			
Number of Threads	X	X	X			X	X	X

Table 3. Required transport information (continued)

Required transport information	HTTP transport	HTTPS transport	FTP transport	FTPS transport	FTP Scripting transport	File Directory transport	JMS transport	SMTP transport
Password	O	O	O	O	O	O	O	O
Provider URL Package							O	
Retry Count	X	X	X	X	X	X	X	X
Retry Interval	X	X	X	X	X	X	X	X
Server IP					X			
Target URI	X	X	X	X		X	X	X
User Id					O			
User Name	O	O	O	O		O	O	O
Validate Client IP	O	O	O	O				
Validate Client SSL Cert		O						

Notes:

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

Viewing and editing gateways

To view and edit gateways, follow these steps:

1. Click **Account Admin** > **Profiles** > **Gateways**.
2. Click **Online** or **Offline** in the **Access** column to change the access of a gateway.
3. Click **Enabled** or **Disabled** in the **Status** column to change the status of a gateway.
4. Click the View details icon to view gateway details.
5. Click the Edit icon.
6. On the Gateway Detail window, edit the gateway parameters that are described in Table 4 on page 24.
7. Click **Save**.

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

Table 4. Gateway parameter descriptions

Parameter	Description
Authentication Required	If enabled, user name and password are supplied with JMS or SMTP messages.
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.
Calendar Based Scheduling	When this option is selected, the documents associated with that gateway are processed based on the selected schedule.
Configuration Point Handlers	Used to specify which handlers are used for preprocessing and postprocessing.
Connection Timeout	Number of seconds a socket will remain open with no traffic. Default value is 120 (2 minutes).
Description	Optional description of the gateway.
FTPS Mode	Select Yes or No to control whether a secure connection is used.
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.
Interval Based Scheduling	When this option is selected, the gateway processes the document at the specified interval time.
JMS Factory Name	Name of the Java(TM) class the JMS provider will use to generate connection to the JMS queue.
JMS JNDI Factory Name	Factory name used to connect to the name service.
JMS Message Class	Class of message.
JMS Message Type	Type of JMS message.
JMS Queue Name	Queue name where JMS messages are stored.
Lock Retry Interval (Seconds)	Amount of time that the FTP Script component will wait between lock retry attempts.
Lock Retry Count	Number of times that the FTP Script component will attempt to obtain the lock.
Lock User	Select Yes or No to control whether or not concurrent connections are allowed.
Maximum Lock Time (Seconds)	Maximum amount of time that the FTP Script component will hold the lock. After the maximum time, the lock is returned to the database.
Maximum Queue Age (Seconds	Maximum amount of time that the FTP Script component remains in the lock request queue. It is placed in the lock request queue when it is denied a lock request.
Number of Threads	Number of threads allocated for routing a document. Default value is 3. This parameter is available to Hub Admin users only.
Online / Offline	Indicate whether the gateway is online or offline. If offline, documents are queued until the gateway is placed online.
Password	Password for secure access through the participant firewall.
Provider URL Package	Name of classes or JAR file that Java uses to understand JMS Context URL.
Retry Count	Maximum number of times the system tries to send a document before it fails. Default value is 3.
Retry Interval	Amount of time that the gateway should wait in between retry attempts. Default value is 300 (5 minutes).
Script File	The FTP script that contains the FTP commands.
Server IP	Server IP address.

Table 4. Gateway parameter descriptions (continued)

Parameter	Description
Status	Indicates whether the gateway is enabled or disabled. If disabled, documents passing through the gateway fail processing.
Target URI	Uniform Resource Identifier (URI) of the participant.
Thread Nbr	Number of documents that should be processed simultaneously.
Transport	Protocol for routing documents (see "Required information for gateway configuration" on page 22).
Use Unique File Name	Creates a unique file name when the document is received at the target location. The original file name is stored in the database.
User defined attributes	For FTP script files, users can add their own attributes, which can be defined in the console. These attributes are read at the gateway and replaced in the script file.
User Id	Required to access the FTP server.
User Name	User name for secure access through the participant firewall.
Validate Client IP	Validates the IP address of the sending partner before processing the document. Used with the Gateway that is selected as a source Gateway for a connection.
Validate Client SSL Cert	Validates the sending participant's digital certificate against the business id associated with the document before processing the document. Used with the Gateway that is selected as a source Gateway for a connection.

Viewing and editing default gateways

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

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

Deleting gateway configurations

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

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

Uploading transports

Use the following procedure to upload a transport.

1. Click **Account Admin** > **Profiles** > **Gateways**.
2. Select **Manage Transport Type**.
3. Click **Browse** and select the transport.

4. Select whether or not to commit the new transport to the database.
5. Select whether or not to overwrite the existing data.
6. Click **Upload**.

Deleting transports

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

1. Click **Account Admin** > **Profiles** > **Gateways**.
2. Select **Manage Transport Type**.
3. Click the Delete icon next to the listed transport.

Transport and gateway retries

When delivery of a document to a participant gateway fails, WebSphere Partner Gateway attempts to deliver the document again. Each attempt is called a *retry*. Retry functionality exists at two levels in WebSphere Partner Gateway: transport and gateway.

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.

Gateway retries (also called document retries)

Gateway retry parameters (the number of retries allowed and the interval between retries) are configured by the user in the gateway properties. Usually the gateway retry interval is longer than the built-in transport retries. 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 that the user assign values for each gateway.

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

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

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

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

Gateway retry 3 fails
    Transport retry 0 fails
    Transport retry 1 fails
    Transport retry 2 fails
Document fails delivery

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

Forward proxy support

For the HTTP and HTTPS transports, you can set up forward proxy support so that documents are sent through a configured proxy server. With WebSphere Partner Gateway you can set up the following support types:

- Proxy support over HTTP
- Proxy support over HTTPS
- Proxy support over HTTPS with authentication
- Proxy support over SOCKS

After you set up a forward proxy, you can make it global for the transport by making it the default forward proxy gateway (for example, all HTTP gateways make use of the forward proxy). For each individual gateway you can then choose not to use the default Forward proxy server or you can select to use a different Forward proxy server. See the *Hub Configuration Guide* for more information on Forward proxy support.

Managing certificates

A digital certificate is an online identification credential, similar to a driver's license or passport. A digital certificate can be used to identify an individual or an organization.

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.

WebSphere Partner Gateway 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.

You can specify a primary and a secondary certificate for outbound documents to ensure that the document exchange is not interrupted. The primary is used for all transactions. The secondary is used if the primary is expired or revoked.

Digital certificates are uploaded and identified during the configuration process.

If a certificate is found to be expired or revoked, it is disabled and is reflected as such in the console. If the primary certificate is expired or revoked, it is disabled and the secondary certificate will be set as the primary. An event is generated when a certificate is found to be expired or revoked.

The Certificate Usage option is available based on the certificate type selected. In the Hub Operator profile, Certificate Usage can be set for Digital Signature or SSL

Client certificate. In the participant profile, Certificate Usage can be set for Encryption certificate. If the same certificate is to be used for different purposes, for example, for Digital Signature and Encryption in Hub Operator profile, it needs to be loaded twice, once for the Digital Signature, and again for the Encryption certificate. However, if the certificate is used for Digital Signature and for SSL Client, then the corresponding checkboxes can be set in the same certificate entry.

Such certificates can also be loaded twice, once for Digital Signature and again for SSL Client. If so, the same pattern must be followed for the secondary certificates. For example, if the primary certificates were loaded as different certificates for Digital Signature and for SSL Client, secondary certificates should also be loaded as different certificate entries (even though the certificate may be the same).

For complete certpath building and validation, you are required to upload all of the certificates in the certificate chain. For example, if the certificate chain contains certificates A -> B -> C -> D, where A -> B means A is the issuer of B, then certificates A, B, and C should be uploaded as root certificates. If one of the certificates is not available, the certpath would not be built and the transaction would not succeed. The CA certificates can be obtained from the Certificate Repositories maintained by the Certificate Authorities or from the partner who provided the certificate. Root and intermediate certificates can only be uploaded in the Hub Operator profile.

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

Viewing and editing digital certificates

Use the following procedure to list and edit digital certificates stored under the Hub Operator profile (previously uploaded to system).

Note: To view and edit certificates stored under a trading partner profile, first select the trading partner in the Participant Search page and then select the **Certificates** tab.

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 View details icon next to a certificate. The Console displays the Viewing Certificate Details window.
3. Click the Edit icon to edit the digital certificate.

4. Update the following parameters in the window, then click **Save**.

Table 5. Digital Certificate Parameters

Parameter	Description
Certificate Type	Type of digital certificate: • Digital Signature – 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 and Intermediate — 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.
Certificate Usage	Select usage type: • Primary — used for all transactions. • Secondary — used if the primary is expired or revoked.

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 View details icon next to the certificate you want to disable.
3. Click the Edit icon to edit certificate details.
4. For **Status** select **Disabled**.
5. Click **Save**.

Note: When a primary certificate is disabled, the corresponding secondary certificate is made primary. When a secondary certificate is disabled, a warning is displayed that there is no secondary certificate.

Changing B2B attribute values

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

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

1. Click **Account Admin** > **Profiles** > **B2B Capabilities**. The Console displays the B2B capabilities window.
2. Click to individually expand a node to the appropriate Document Flow Definition level or select a number from 0-4 or All to expand all displayed Document Flow Definition nodes to the selected level.
3. Click the Edit icon to modify the appropriate attribute values in the **Update** column.
4. Click **Save**.

Managing participant connections

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

The system automatically creates connections between the Community Manager and participants based on their B2B capabilities. The data typed in the B2B Capabilities module of 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 6 describes each component.

Table 6. Manage participant components

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

Connection duplication

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

- Source package & version
- Source protocol & version
- Source document flow & version

In the example shown in Figure 1, 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.

Note: EDI documents can have an additional Connection Profile associated with them. The values configured for a Connection Profile will be used to uniquely identify a connection even with the same Source document.

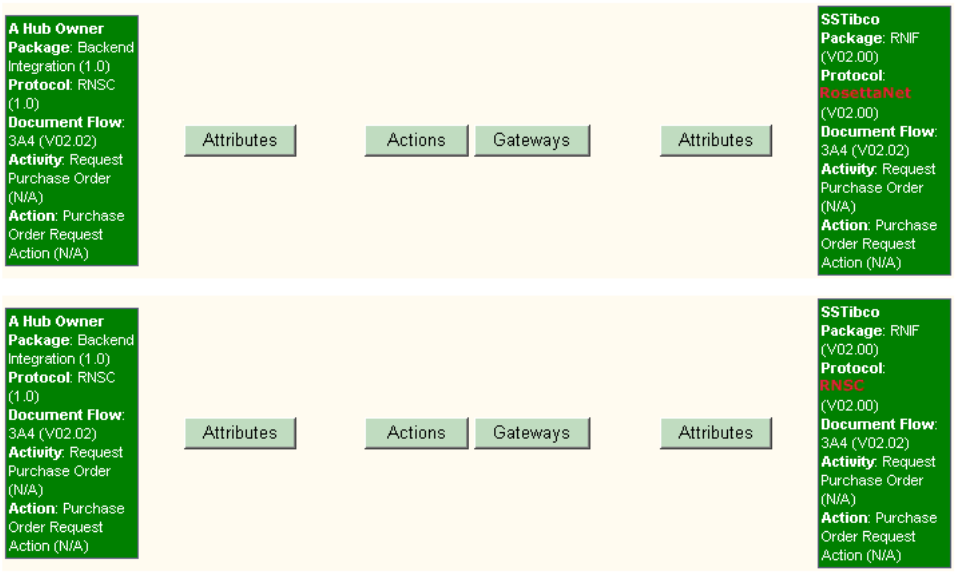


Figure 1. Example connections

Searching for connections

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

- Using the Managing Connections window 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 32.

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 window.
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 window. This window 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 Deactivate icon disables a connection.
   - Clicking the Delete icon enables a connection.
   - Clicking **Attributes** displays the Connection Attributes window, where you can view and change connection attributes. For more information, see "Changing participant attribute values" on page 33.
   - Clicking **Actions** displays the Connection Details window, where you can view and change the Action. For more information, see "Selecting a new action" on page 33.
   - Clicking **Gateways** displays the Connection Management Gateway window, where you can view and change the source or target gateway. For more information, see "Changing the source or target gateway" on page 34.

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 window.
2. Click **Advanced Search** in the upper right corner of the window.

3. Complete the following parameters as shown in Table 7:

Table 7. Advanced Search window

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

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

Changing connection configurations

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

1. Click **Account Admin** > **Participant Connections**. The Console displays the Manage Connections window.
2. Perform a basic search for connections (see "Performing a basic search for connections" on page 31) or advanced search for connections ("Performing an advanced search for connections" on page 32).
3. See the appropriate section:
   - "Changing participant attribute values,"
   - "Selecting a new action,"
   - "Selecting a new transformation map"
   - "Changing the source or target gateway" on page 34.
   - "Disabling or deactivating a connection" on page 34.

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 Expand 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**.

Selecting a new transformation map

To select a new transformation map, use the following procedure.

1. Click **Actions**.

2. Select the new transformation map 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 Deactivate icon 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 Delete icon.

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

For EDI documents, there can be several connections that apply to the same participants. The various connections are differentiated using connection profiles. Deleting a connection with an associated connection profile name will delete the connection from the system. Only a base-level connection without an associated connection profile can be deactivated. For more information about Connection Profiles, see the *Hub Configuration Guide*.

Managing Exclusion Lists

An Exclusion List lets the Community Operator configure the Document Manager to restrict RosettaNet 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 window.
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 window.
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 Edit icon next to the notification you want to edit.
4. Check the check box below the notification to restrict the notification from being routed to the Community Manager. Select **Send All Notifications** to remove all routing restrictions.

Chapter 4. Managing 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.

  Note: If you are implementing an FTP Scripting Gateway with an interval or calender schedule, documents may stay in this queue for an extended period until that interval or date and time is reached. This is expected operation, and the documents should not be removed 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 queue

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 window.
2. Input the parameters shown in Table 8.

Table 8. Gateway Queue window

Criteria	Description
Queued at least	Minimum number of minutes a document has been waiting in the gateway queue. For example, if 6 minutes is selected, all gateways containing documents that have been waiting for delivery for 6 minutes or more will be displayed. The default is 0.
Minimum Queued	Minimum number of documents in a gateway queue. The 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 the beginning of the alphabet.
Refresh	Turn refresh on or off (default).
Refresh Rate	Number of seconds the Console waits before updating displayed data.

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

Table 9. Results after gateway queue search

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

Viewing queued documents

To search for queued documents that meet specific search criteria, use the following procedure:

1. Click **Viewers** > **Gateway Queue**.
2. From the Gateway Queue window, click **Search**.
3. Complete the following parameters in the window:

Table 10. Search criteria for the Gateway Queue

Parameter	Description
Participant	Name of the trading partner receiving the document
Gateway	Name of the gateway
Reference ID	Unique identification number assigned to the document by the system
Document ID	Unique identification number assigned to the document by the source participant
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 descriptions of the in-depth information displayed when viewing document details, see the topic "About document viewer" in the online help.

Removing documents from the delivery queue

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

1. Click **Viewers** > **Gateway Queue**.
2. From the Gateway Queue window, click **Search**.
3. Complete the parameters in the window (see Table 10 on page 38).
4. Click the delete icon to delete the document.

Viewing gateway details

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

1. Click **Viewers** > **Gateway Queue**.
2. From the Gateway Queue window, type the search criteria (see Table 8 on page 37).
3. Click **Search**.
4. From the list of gateways, 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**.
2. From the Gateway Queue window, type the search criteria (see Table 8 on page 37).
3. Click **Search**.
4. From the list of gateways, click the document count link in the **Queued** column. Gateway details and a list of queued documents appear.
5. Click **Online** in **Gateway Info** to place a gateway offline, or click **Offline** to place gateway online. (You must be logged in as Hub Admin to change gateway status.)

Chapter 5. Analyzing document flows

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

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

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

Features covered in this chapter include:

Document Analysis

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

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

Viewing the state of documents in the system

The following table describes the different document states.

Table 11. Document states

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

Viewing documents in the system

The following procedure describes how to view documents in the system:

1. Click **Tools** > **Document Analysis**.
2. From the Document Analysis Search window, select the search criteria from the drop-down lists.

   Table 12 describes the values that you can specify to determine which documents are displayed.

Table 12. Document search criteria

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

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

Viewing process and event details

The following procedure describes how to view process and event details:

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

Document Volume Report

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

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

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

Table 13. Document States

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

Use this report to perform the following tasks:

- Determine if key business processes have completed
- Track trends in process volume for cost control
- Manage process quality, success and failure
- Track process efficiency

Creating a Document Volume Report

The following procedure describes how to create a document volume report:

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

Table 14. Document Volume Report Search Criteria

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

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

Exporting the Document Volume Report

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

Note: Reports are saved as comma-separated value (csv) files.

Printing reports

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

Test Participant Connection

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

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

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

To test a participant connection:

1. Click **Tools > Test Participant Connection**.
2. From the Test Participant Connection window, select the test criteria from the drop-down lists.

Table 15. Test Participant Connection values

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

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

Web Server result codes

The following sections describe the server result codes:

200 Series:

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

300 Series:

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

400 Series:

- 400 - Bad Request - The request could not be understood by the server because it has a malformed syntax. Bad request was made by the client.
- 401 - Unauthorized - The request requires user authentication. The response must include a WWW-Authenticate header field containing a challenge applicable to the requested source. The user asked for a document but did not provide a valid username or password.
- 402 - Payment Required - This code is not currently supported, but is reserved for future use.
- 403 - Forbidden - The server understood the request but is refusing to perform the request because of an unspecified reason. Access is explicitly denied to this document. (This might happen because the web server doesn't have read permission for the file you're requesting.) The server refuses to send you this file. Maybe permission has been explicitly turned off.
- 404 - Not Found - The server has not found anything matching the requested URL. This file doesn't exist. This is the message you get if you type bad URL into your browser. This can also be sent if the server has been told to protect the document by telling unauthorized people that it does not exist. 404 errors are the result of requests for pages which do not exist, and can come from a URL typed incorrectly, a bookmark which points to a file that is no longer there, search engines looking for a robots.txt file (which is used to mark pages that are not to be indexed by search engines), people guessing filenames, bad links from your site or other sites, etc.
- 405 - Method Not Allowed - The method specified in the request line is not allowed for the resource identified by the request URL.
- 406 - None Acceptable - The server has found a resource matching the request URL, but not one that satisfies the conditions identified by the Accept and Accept-Encoding request headers.

- 407 - Proxy Authentication Required - This code is reserved for future use. It is similar to 401 (Unauthorized) but indicates that the client must first authenticate itself with a proxy. HTTP 1.0 does not provide a means for proxy authentication.
- 408 - Request Time Out - The client did not produce a request within the time the server was prepared to wait.
- 409 - Conflict - The request could not be completed due to a conflict with the current state of the resource.
- 410 - Gone - The requested resource is no longer available at the server and no forwarding address is known.
- 411 - Authorization Refused - The request credentials provided by the client were rejected by the server or were insufficient to grant authorization to access the resource.
- 412 - Precondition Failed
- 413 - Request Entity Too Large
- 414 - Request URI Too Large
- 415 - Unsupported Media Type

500 Series:

- 500 - Internal Server Error - The server encountered an unexpected condition that prevented it from filling the request. Something went wrong with the Web server and it could not give you a meaningful response. There is usually nothing that can be done from the browser end to fix this error; the server administrator will probably need to check the server's error log to see what happened. This is often the error message for a CGI script which has not been properly coded.
- 501 - Method Not Implemented - The server does not support the functionality required to fulfill the request. Application method (either GET or POST) is not implemented.
- 502 - Bad Gateway - The server received an invalid response from the gateway or upstream server it accessed in attempting to fulfill the request.
- 503 - Service Temporarily Unavailable - The server is currently unable to handle the request due to a temporary overloading or maintenance of the server. The server is out of resources.
- 504 - Gateway Time Out - The server did not receive a timely response from the gateway or upstream server it accessed in attempting to complete the request.
- 505 - HTTP Version Not Supported

Chapter 6. Viewing events and documents

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

- "Event Viewer"
- "AS1/AS2 Viewer" on page 49
- "RosettaNet Viewer" on page 51
- "Document Viewer" on page 53
- "Gateway Queue" on page 60

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

Event Viewer

Use the Event Viewer to view and research events.

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

WebSphere Partner Gateway includes predefined events. Through the product's Alerts feature, the Account Admin module, you can create event-based alerts. You can identify the events that are of concern to you. Then use the Contacts feature, also in the Account Admin module, to identify the staff members that the system will notify if those events occur.

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

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

Event types

WebSphere Partner Gateway includes the event types listed in Table 16.

Table 16. Event types

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

Searching for events

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

   Events are organized by severity from left to right in the Event Viewer Search window. Information on the left is the least severe event type; Critical information located on the right side of the window is the most severe. For any selected event, that event and all events with greater severity are displayed in the Event Viewer. For example, if the Warning event type is selected in the search criteria, Warning, Error, and Critical events are displayed. If Informational events are selected, all event types are displayed.

   Note: Debug events cannot be viewed by all users.

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

Table 17. Event search criteria

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

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

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

Viewing event details

1. Click **Viewers** > **Event Viewer**.
2. Select the search criteria from the drop-down lists.
3. Click **Search**.
4. From the displayed list of events, click the View details icon next to the event you want to view.
5. From the displayed event details, click the View details icon next to the document that you want to view, if one exists.
6. Click the Display raw document icon to view the raw document, if one exists.
7. Click the View validation errors icon to view validation errors.

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

AS1/AS2 Viewer

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

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

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

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

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

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

Searching for messages

1. Click **Viewers** > **AS1/AS2 Viewer**. The system displays the AS1/AS2 Viewer window.
2. Select the search criteria from the drop-down lists, described in Table 18.

Table 18. AS1/AS2 Viewer search criteria

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

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

Viewing message details

1. Click **Viewers** > **AS1/AS2 Viewer**. The system displays the AS1/AS2 Viewer Search window.
2. Select the search criteria from the drop-down lists.
3. Click **Search**. The system displays a list of messages.
4. Click the View details icon next to the message that you want to view. The system displays the message and the associated document details, described in Table 19 on page 51.

Table 19. Message details

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

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

RosettaNet Viewer

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

The RosettaNet Viewer displays the required order of sub-transactions needed to successfully complete a document flow. Values that can be viewed using the RosettaNet Viewer include process state, details, raw documents, and associated process events.

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

The RosettaNet Viewer displays processes based on specific search criteria.

Searching for RosettaNet processes

1. Click **Viewers** > **RosettaNet Viewer**.
2. From the RosettaNet Viewer Search window, select the search criteria from the drop-down lists, described in Table 20 on page 52.

Table 20. RosettaNet search criteria

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

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

Viewing RosettaNet process details

1. Click **Viewers** > **RosettaNet Viewer**. The system displays the RosettaNet Viewer Search window.
2. Select the search criteria from the drop-down lists.
3. Click **Search**. The system displays the results of your search, described in Table 21.

Table 21. Document processing details

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

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

Viewing raw documents

Use this procedure to view a raw document associated with a document flow.

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

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

Tips:

- To troubleshoot documents that have failed processing, see "Viewing data validation errors" on page 57.
- The raw document viewer displays the HTTP header with the raw document.

Document Viewer

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

Searching for documents

1. Click **Viewers** > **Document Viewer**. The system displays the Document Viewer Search window.
2. Select the search criteria from the drop-down lists, described in Table 22 on page 54.

Table 22. Document Viewer search criteria

Value	Description
Start Date	Date the document flow process was initiated.
Start Time	Time the document flow process was initiated.
End Date	Date the document flow process was completed.
End Time	Time the document flow process was completed.
Source Participant	Represents the participant that initiated the document flow. The default is All.
Target Participant	Represents the participant that received the document flow. The default is All.
Search on	Indicates whether to search on source document flow or target document flow. The default is Source Document Flow.
Gateway Type	Identifies the nature of the document being exchanged (for example, whether it is used for production or test purposes). The default is All.
Document Status	Current document status in system: In Progress, Successful, or Failed. The default is All.
Package	Describes the document format, packaging, encryption, and content-type identification. Limits the search to the package listed. The default is All.
Protocol	Type of process protocol available to the participants.
Document Flow	The specific business process.
Original File Name	The original file name.
Document ID	Created by the source participant. Criteria can include asterisk (*) wildcard.
Reference ID	The ID number created by the system for tracking document status.
Source IP Address	The IP address of the source participant.
Filter	Search for documents received in synchronous mode. This means that the connection between the initiator and the Document Manager stays open until the transaction is complete, including request and acknowledgment or request and response.
Sort By	Indicates whether the documents will be sorted by Target Timestamp, Source Document Flow, or Target Document Flow. The default is Target Timestamp. You can also indicate whether the documents should be sorted in ascending or descending order. The default is Descend.
Results Per Page	Number of records displayed per page.
Descend	Sort results in either descending or ascending order.

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

3. Click **Search**. The system displays the results of your search, described in Table 23.

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

Table 23. Document details

Value	Description
Participants	Source (From) and target (To) participants involved in the business process.
Time Stamps	Date and time the document begins and ends processing.

Table 23. Document details (continued)

Value	Description
Document Flow	Business process that is being transacted.
Gateway Type	Test or production. Test is only available on systems that support the test gateway type.
Synchronous	Identifies that the document was received in synchronous mode. This means that the connection between the initiator and the Document Manager stays open until the transaction is complete, including request and acknowledgment or request and response.

Viewing document details, events, and raw documents

1. Click **Viewers** > **Document Viewer**. The system displays the Document Viewer Search window.
2. Select the search criteria from the drop-down lists.
3. Click **Search**. The system displays a list of documents.
   - To view a document's details and events, click the open folder icon next to the document displayed under the Associated Documents header. The system displays process details and events for the selected document. For EDI Interchange documents, if there are child EDI transactions from either de-enveloping or enveloping, they can be shown by selecting the **Document children** source or target radio button. See "Viewing EDI documents" on page 56 for details.
   - To view the raw document along with any transport headers, click the Display raw document icon next to the document. The system displays the raw document's content.

The document processing information is displayed when you view document details, described in Table 24.

Table 24. Document processing values available through Document Viewer

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

Restrictions: Raw documents greater than 100K are truncated. For example, when the signature is located at the bottom of the raw document (.rno file),

and the size of the raw document exceeds 100K, or the signature is present after the first 100K of the .rno file, the signature will not be shown in Document Viewer.

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

Tip: For information on how to troubleshoot documents that have failed processing, see "Viewing data validation errors" on page 57 in the following section.

Viewing EDI documents

In addition to pass through support for EDI Interchanges, WebSphere Partner Gateway supports the de-enveloping and enveloping of EDI Interchanges. The EDI interchange documents are de-enveloped when received from either a Community participant or a Community manager. Transaction documents that are de-enveloped from the incoming interchange can then be processed by WebSphere Partner Gateway like any other business document.

WebSphere Partner Gateway envelopes EDI transactions and generates EDI Interchanges. EDI transaction documents are generated by transforming XML, EDI, and ROD documents into EDI transactions. EDI transaction documents that were de-enveloped from the EDI interchanges received by WebSphere Partner Gateway can be transformed into another EDI transaction document type. WebSphere Partner Gateway envelopes EDI transaction documents into an EDI Interchange document and then sends the EDI interchange document to its intended recipient.

The following scenarios will assist you in locating this information:

- "Viewing EDI document source transactions"
- "Viewing EDI document target transactions"
- "Locating the source interchange" on page 57
- "Locating the target interchange" on page 57

Refer to the *Hub Configuration Guide* for more information on de-enveloping and enveloping EDI Interchanges.

Viewing EDI document source transactions

WebSphere Partner Gateway de-envelopes incoming EDI transactions from EDI interchanges.

To view the resulting EDI transaction children:

1. Click **Viewers** > **Document Viewer**. The system displays the Document Viewer Search window.
2. Select the search criteria from the drop-down lists.
3. Click **Search**. The system displays a list of documents.
4. Click the View details icon next to the Document ID.
5. Click the **Source** radio button in the Document Children section to view the document children details.

Viewing EDI document target transactions

WebSphere Partner Gateway routes outgoing EDI transactions to the interchange to be enveloped.

To view the EDI transaction children that are contained in the resulting interchange:.

1. Click **Viewers** > **Document Viewer**. The system displays the Document Viewer Search window.
2. Specify the search criteria to locate the EDI interchanges received by WebSphere Partner Gateway.
3. Click **Search**. The system displays a list of all the documents that meet your search criteria.
4. Click the View details icon next to the Document ID for the document that you want to view.
5. Click the **Target** radio button in the Document Children section to view the document children details.

Locating the source interchange

You can use the Document Viewer to obtain the source interchange for an EDI transaction:

1. Click **Viewers** > **Document Viewer**. The system displays the Document Viewer Search window.
2. Select the search criteria from the drop-down lists.
3. Click **Search**. The system displays a list of documents.

   The source interchange Document ID is listed for each EDI transaction.

Locating the target interchange

You can use the Document Viewer to obtain the target interchange for an EDI child transaction:

1. Click **Viewers** > **Document Viewer**. The system displays the Document Viewer Search window.
2. Select the search criteria from the drop-down lists.
3. Click **Search**. The system displays a list of documents.
4. Click the View details icon next to the Document ID.
5. Click the **Information** radio button in the Document Events section.
6. Click the Expand icon next to EDI Transaction Enveloped in the Event Name column.
7. Locate and copy the Envelope activity id from the Event Details list.
8. Click **Viewers** > **Document Viewer**. The system displays the Document Viewer Search window.
9. Paste the Envelope activity id into the Reference ID field and click **Search**.

   The Document Viewer displays the target interchange information.

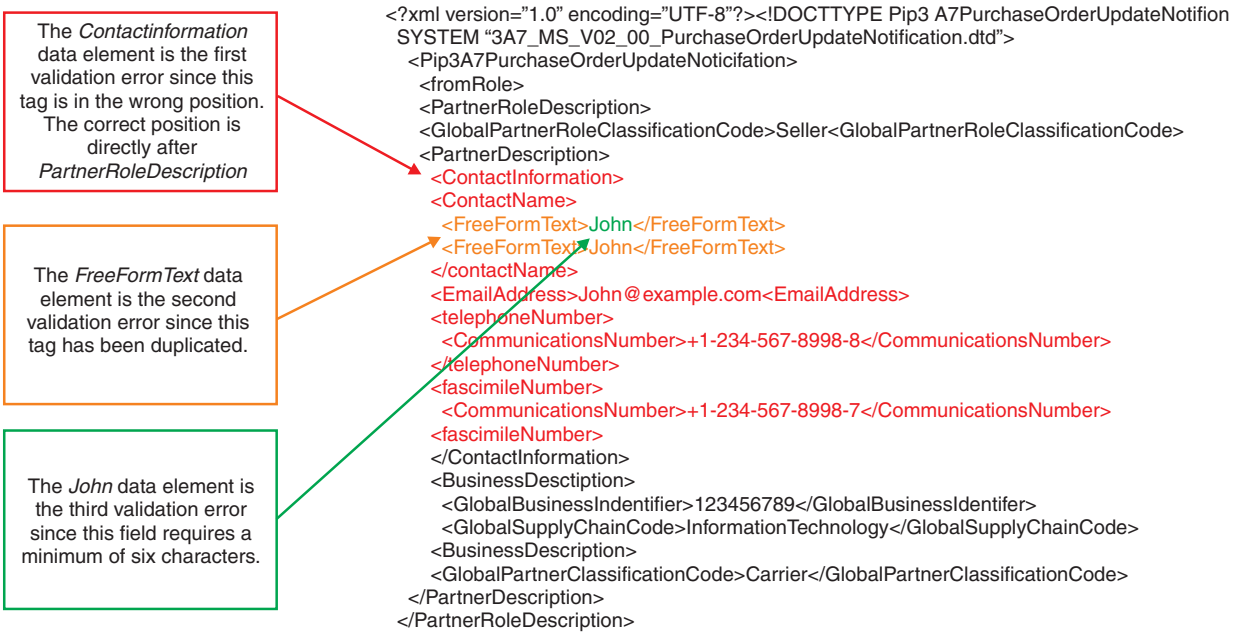
Viewing data validation errors

You can quickly search for documents that have failed processing using the color-coded text in the XML fields that contain validation errors. Fields that contain validation errors are displayed in red. If up to three separate validation errors occur within nested XML fields, the colors are used to distinguish between the error fields, as outlined in Table 25 on page 58.

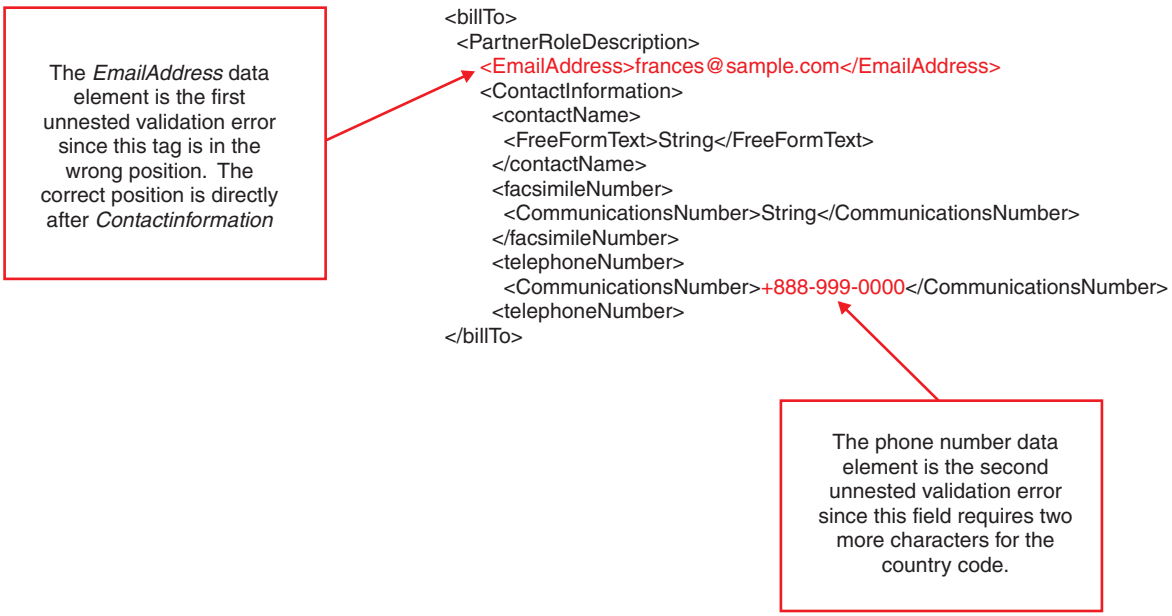
Table 25. Color-coded document validation errors

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

The following is an example of nested XML validation errors:



Example of non-nested XML validation errors:



For details on viewing validation errors in a raw document, see "Viewing raw documents" on page 53.

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

Stopping a document that is in process

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

Note: It can take up to one hour for the system to stop the document. During this time, the Document Viewer continues to display the document status as in progress.

Resending failed and successful documents

You can resend failed documents after correcting the cause of the failure. Additionally, you can resend successfully processed documents if requested. For example, a partner may request that a document be resent if the original document was lost on the client server before it interfaced with the back-end system. This feature is only available to hub admin users.

There are two basic types of documents that Administrators can resend:

- **In** documents are those that come into WebSphere Partner Gateway, either from the Backend or the participant. These documents can fail in the Receiver, Document Acquisition Engine (DAE), or Business Process Engine (BPE).
- **Out** documents are those that leave WebSphere Partner Gateway, either to the Backend or to the participant. These documents can fail either in the BPE or Delivery Manager.

To resend a failed **In** document, the Administrator selects the **In** document and clicks the **Resend** button. The document is resubmitted either from DAE or BPE based on the failure location. For example, **In** document failures can occur in DAE in the following cases:

- Received document size is more than the maximum size limit.
- Non-repudiation of the received document failed.
- Failed sending the document to BPE.

In document failures can occur in BPE in the following cases:

- Fixed inbound workflow failures
  - While unpackaging, the message failures can occur while decrypting the message or verifying the signature. This can be caused by incorrect configuration of certificates at the partner or hub.
  - B2B capabilities are not configured for the partner.
- Variable workflow failures
  - Validation maps are not configured.
  - Invalid Translation maps are configured.

Note: Documents that fail in the Receiver are resubmitted when the Administrator resolves the problem.

To resend failed **Out** documents, the Administrator selects the **Out** document and clicks the **Resend** button. The document is resubmitted either from BPE or Delivery Manager.

Out document failures can occur in the following cases:

- For a BPE failure resubmitting the **Out** document itself does not make sense, so in a BPE failure the **In** document should be resubmitted. This will insure that anything that was incorrect in the BPE flow that was corrected will get picked up. An example of a correction may be in the transformation. **Out** document failures in BPE can be Fixed outbound workflow failures. Packaging of the message can fail while encrypting or signing the message due to incorrect certificate configurations for partner or hub.
- For a Delivery Manager failure:
  - If the problem was due to an error in the BPE flow, the **In** document should be resubmitted. This insures that anything that any corrections in the BPE flow will get picked up. For example, if the Gateway target information was incorrect.
  - If the failure was caused by something else, for example, the Gateway target transport was down, then a re-submit of the **Out** document can be done, although the **In** document can also be resubmitted.

There is an underlying assumption that nothing has changed that would break a resend, especially from the DAE or BPE. For example, if the **In** document is encrypted, the certificates required to decrypt the document should not have been changed from the certificates that were used to encrypt the document. The administrator has to be aware of any potential consequences of the resend.

To resend a document:

1. Click **Viewers** > **Document Viewer**. The system displays the Document Viewer Search window.
2. Select the search criteria from the drop-down lists.
3. Click **Search**. The system displays a list of documents.
4. Place a checkmark in the box next to the document or documents that you want to resend.
5. Click **Resend**.

   You will receive a confirmation message after the resend is processed.

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. Refer to Chapter 4, “Managing the gateway queue,” on page 37 for more information.

Chapter 7. Simulating production traffic

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

The purpose of the CPS is:

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

The Community Manager uses the cps to verify that documents are formatted correctly and contain valid business content.

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

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

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

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

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

or

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

This chapter contains the following sections:

Preparing to test

Before you start the test, you must perform the following tasks, which may vary by the role that you are simulating, either a request or response from the Community Manager, or a request or response from a participant:

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

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

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

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

   WebSphere Partner Gateway automatically loads the VTP digital certificate for every participant in the database, allowing you to post to any participant. These certificates are not visible on the console.
2. Verify that your gateways and connections are configured and that they are working properly.
3. Verify that your targets are enabled and configured with the appropriate URL for incoming messages. Different traffic occurs on different targets. If the target's URLs are not correct, documents will not be processed.

   This requirement only applies when you are testing a document that requires a response. For more information about targets, see the *Hub Configuration Guide*.
4. Verify the Business IDs that appear in the header of your test document. The Business IDs drive the routing process and control where the document is sent.

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

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

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

Setting up test scenarios

You can use the CPS to test the scenarios shown in Table 26 between you and your participants.

Table 26. Test scenarios

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

Sample scenarios

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

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

Community Manager:

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

The sink gateway should be specified as the default CPS participant and CPS Manager gateway for the Community Manager.

Community participant:

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

RosettaNet PIP XML files:

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

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

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

Configuring the Console and Router Servers:

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

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

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

Configuring 3A4 Connectivity:

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

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

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

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

   - `Package_RNIF_V02.00.zip`
   - `BCG_Package_RNIFV02.00_3A4V02.02.zip`
   - `Package_RNSC_1.0_RNIF_V02.00.zip`
   - `BCG_Package_RNSC1.0_RNIFV02.00_3A4V02.02.zip`
2. Define the capabilities (called interactions) for 3A4 purchase order requests and confirmations to be routed through the hub.
3. Configure the Community Manager and Community participant to be the source and target of participant 3A4 requests and confirmations that use RNSC content.
4. Establish the participant connections between the Manager and the participant to support the scenario you want to simulate.
5. Set the attributes of the connection to optionally specify signing and encryption using the security artifacts that you have placed on your system.

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

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

Uploading and viewing your requests and responses

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

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

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

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

After the upload completes, the CPS view changes to the routing results window, which contains links to the RosettaNet Viewer and the Document Viewer. These two links are for your convenience. They take you to the two viewers that you will check for routing results. You should wait a few seconds to allow the Document Manager time to handle the message before attempting to view the results.

Initiating and viewing document flow

This feature provides a convenient method for testing internal applications by simulating the initiation and receipt of one-way and two-way RosettaNet PIPs.

To initiate a document flow:

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

Searching for an open document

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

Responding to an open document

1. Use a text editor to edit the to and destination sections of the process requiring a response document (change VTP_OWNER to VTP_TP, or change VTP_TP to VTP_OWNER), and make the appropriate changes to the target's URL. See Table 27 for test scenario information.

Table 27. Test scenarios

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

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

Removing an open document

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

Chapter 8. Archiving

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

This chapter contains the following sections:

Archiving data

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

Caution: Purging certain database tables will remove information about files stored in the system. Before purging database tables, review "Removing old files" on page 75.

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

   Oracle

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

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

   Before you begin using Export, confirm the following:

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

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

   UNIX: /opt/{INSTALL DIR}/DBLoader/scripts/Oracle/export.sh

   Windows: \{INSTALL DIR}\DBLoader\scripts\Oracle\export.bat The export script takes the following parameters for Oracle:

   - system password
   - connect string

- destination directory
- schema name
- cut off date, in the following format: YYYYMMDD

Syntax of export script:

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

Example of export script:

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

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

DB2

The export script needs to be run from the DB2 command window after establishing a connection with the database. The script is located in one of the following, based on your platform:

UNIX: /opt/{INSTALL DIR}/DBLoader/scripts/DB2/export.sh

Windows: \{INSTALL DIR}\DBLoader\scripts\DB2\export.bat The `export` script takes the following parameters for DB2:

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

Syntax of export script:

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

Example of export script:

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

Note: The `export` script gives an SQL3100W warning which can be safely ignored.

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

2. Run the archive script to copy the payload data files from the non-repudiation store on the file system to the archive. This script needs to be run on the machines that have the non-repudiation file storage system. The script can be found in one of the following paths, depending on your platform:

   UNIX: /opt/{INSTALL DIR}/bin

   Windows: \{INSTALL DIR}\bin

   a. Execute the setenv script to ensure that the PATH and CLASSPATH variables are set properly.
   b. The DBArchiveParams.properties file is used by the archive script to get all of the required information. Edit the DBArchiveParams.properties file to ensure that the correct parameters are being passed. Refer to the sample entries for more details. Make sure that the entries correspond to the correct database type. The cut-off date should be the same as in step 1. The DB_ARCHIVE_TASK parameter should be kept as 1.
   c. Run the archive script. The results of the copy operation will be kept in the destination directory, as specified in the DBOutput.txt file.

CAUTION:
Steps 1 and 2 above copy the data from the data stores to the archive location. Do not execute steps 3 and 4, which remove the data from the data stores, until the copy operations have completed successfully.

3. Set the DB_ARCHIVE_TASK parameter in the DBArchiveParams.properties to 0.
4. Run the archive script again to purge the payload data files from the non-repudiation store on the file system.

   This script needs to be run on the machines which have the non-repudiation file storage system. Also, this script must be run with administrator or root privileges.
5. Run the AR_NONREP_MAINTENANCE database stored procedure to purge the archived data from the LG_MSG_ARCHIVE and LG_CERT_ARCHIVE tables. It takes the cut-off date as the input parameter. This stored procedure is available in the database and is added during installation.

   Syntax of the AR_NONREP_MAINTENANCE stored procedure:

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

Archiving and purging file system and database logs

To maintain the operating efficiency of WebSphere Partner Gateway, use the following procedures to archive or purge the file system and database log files.

Purging application log files

Application log files are located in three areas: receiver, console, and router.

For example:

{INSTALL DIR}/logs/*<bcgreceiver, bcgconsole, and bcgdocmgr>*

To purge the application log files, follow these steps:

1. Stop the appropriate component, See "Stopping the Community Console" on page 4 or "Stopping the Receiver and Document Manager" on page 4.
2. Remove the unwanted log files as needed.

Purging non-repudiation directories

Non-repudiation files and directories are located in the following directory: {INSTALL DIR}/common/non_rep/. Start by archiving the oldest files located in directories starting at 0, and increasing in number for newer files.

1. Stop the Document Manager. See, "Stopping the Receiver and Document Manager" on page 4.
2. Compress the files using the UNIX tar command or WinZip.
3. Move the files to an external media source for offsite storage if necessary.

Purging database tables

Certain database tables may be purged when necessary, but other tables must not be modified in order to maintain proper system functionality. Tables starting with BP_ and LG_ may be purged with two exceptions: BP_ tables ending with _QUE and _HIST are continuously maintained by the RosettaNet engine and must not be changed. The BP_ tables ending with _QUE are queue tables, and the BP_ tables

ending with _HIST are history tables which are used for archiving. For example, the BP_RNSTATEHDR_QUE table is archived in the BP_RNSTATEHDR_HIST table.

Tables starting with CG_ and PR_ contain configuration or profile data and must also remain unchanged for the system to function properly.

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

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

The purge criterion contains only one input parameter, p_days, which is the number of days that data should be kept online.

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

Data retention time

The procedure purges data based upon the combination of the record creation date in the header and the p_days input parameter. The Time to perform TPA stored in the header is not considered. It is the responsibility of the DBA to make sure that the p_days parameter 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, except DB_ProcAuditLog, are metadata tables. If DB_ProcAuditLog is on, it should be either purged or truncated daily, or done based on the needs of the user. This log is normally turned off for production because it is primarily used in development and QA environments.

Log and summary tables

With the exception of: LG_EventCd, LG_Media, and LG_media_Cfg, tables with names starting with LG_ are log and summary tables. These are metadata tables and must remain unchanged in order to maintain proper system functionality. Tables starting with LG_Access_ are no longer used by WebSphere Partner Gateway.

The following log tables can be archived and purged based upon Activity ID, and the driving table should be LG_Activity. The createdate or RcvDocTS can be used

to determine the number of days that data should be retained online. RcvDocTS may be a better option because it is an indexed column. Data can remain online for seven days or ((*TimeToPerform*/1440) +1 day), whichever is greater.

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

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

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

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

Table	Notes
Event Summary Tables	

LG_EVENTSUMMARY

LG_EVENTSUMMARY_XREF

Process Summary Tables

LG_PROCESSSUMMARY_AS

LG_PROCESSSUMMARY_AS_MI

LG_PROCESSSUMMARY_AS_XREF

LG_PROCESSSUMMARY_RN

LG_PROCESSSUMMARY_RN_MI

LG_PROCESSSUMMARY_XREF

Document Summary Tables

LG_DOCPROCESSING_SUMLG_MSGLENGTH_SUMMARY

LG_SUMMARY

LG_SUMMARY_MI

LG_SUMMARY_PROCESSSUMMARY
Links LG_Sum_Xref_Lnk to LG_ProcessSummary_Xref

LG_SUMMARY_RN

LG_SUMMARY_RN_MI

LG_SUM_XREF_LNK
Links LG_SUM_XREF_PART and LG_SUM_XREF_PRCS to LG_Summary

LG_SUM_XREF_PART

LG_SUM_XREF_PRCS

Message Length Summary

LG_MSGLENGTH_SUMMARY

Restoring data

To restore data to the database, follow these steps:

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

   Oracle

   The import script needs to be run from a machine running Oracle client. The script can be found in the following directories:

   UNIX: {INSTALL DIR}/DBLoader/scripts/Oracle/import.sh

   Windows: {INSTALL DIR}\DBLoader\scripts\Oracle\import.bat The import script takes the following parameters for Oracle:

   - Oracle user system password
   - Connect string
   - Archive location

   DB2

   The import script needs to be run from the DB2 command prompt after you connect to the database. The script can be found in the following directories:

   UNIX: {INSTALL DIR}/DBLoader/scripts/DB2/import.sh

Windows: {INSTALL DIR}\DBLoader\scripts\DB2\import.bat The import script takes the following parameters for DB2:

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

Syntax of import script:

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

Example using import script:

./import.sh /tmp/2003-01-01 db2inst1 bcgapps
db2inst1 pa55word

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

   UNIX: {INSTALL DIR}/bin

   Windows: {INSTALL DIR}\bin The Restore script takes the following parameters:

   - The location of the archives. For example: C:\tmp
   - The location of the log file DBOutput.txt from "Archiving data" on page 69, step 2. For example: \Installers\DBOutput.txt

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

Removing old files

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

CAUTION:
If the LG_MSG_ARCHIVE has already been purged, the file locations will be lost from the database. Purge the message store before archiving.

Removing data from State Engine tables

To remove data from State Engine tables, use the AR_STATEENGINE_MAINTENANCE stored procedure. It takes the number of days for which you want to retain the data as the input parameter. All records before that number of days are removed from the database. The default is 7 days.

Syntax:

DB2:

```
call AR_STATEENGINE_MAINTENANCE(<number of days data will be retained>)
```

For example: `call AR_STATEENGINE_MAINTENANCE(15)`

Oracle:

```
execute AR_STATEENGINE_MAINTENANCE(<number of days data will be retained>)
```

For example: `execute AR_STATEENGINE_MAINTENANCE(15)`

Removing data from Summary tables

To remove data from Summary tables, use the AR_SUMMARY_MAINTENANCE stored procedure. It takes the cut-off date as the input parameter.

Syntax:

DB2:

```
call AR_SUMMARY_MAINTENANCE(<cut-off date, format:'YYYY-MM-DD'>)
```

For example: `call AR_SUMMARY_MAINTENANCE('2005-10-21')`

Oracle:

```
execute AR_SUMMARY_MAINTENANCE(<cut-off date, format:'DD-MON-YY'>)
```

For example: `execute AR_SUMMARY_MAINTENANCE('21-OCT-2005')`

Removing data from Logging tables

To remove data from Logging tables, use the AR_PURGE_HEADERS stored procedure. It takes the cut-off date as the input parameter.

Syntax:

DB2:

```
call AR_PURGE_HEADERS(<cut-off date, format:'YYYY-MM-DD'>)
```

For example: `call AR_PURGE_HEADERS('2005-10-21')`

Oracle:

```
execute AR_PURGE_HEADERS(<cut-off date, format:'DD-MON-YY'>)
```

For example: `execute AR_PURGE_HEADERS('21-OCT-2005')`

Chapter 9. Troubleshooting

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

Topics in this chapter include:

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, take the following actions:

1. Set the AS Compressed attribute to **Yes** to decrease the size of the document being sent.
2. Follow the steps in the "Avoiding out-of-memory errors" section above to increase memory size and speed processing of encrypted documents.

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 sizes:

Enter the following command to query the current heap size:

```
{INSTALL DIR}/bin/bcgwsadmin.sh -conntype
NONE -f {INSTALL DIR}/scripts/bcgQueryJVMHeapAttrs.jacl
```

Enter the following command to set the min/max heap size:

```
{INSTALL DIR}/bin/bcgwsadmin.sh -conntype
NONE -f {INSTALL DIR}/scripts/bcgSetJVMHeapAttrs.jacl
```

Change the heap size to the recommended values by editing the bcgSetJVMHeapAttrs.jacl file as shown.

Default:

- Xms=50
- Xmx=256

First recommendation:

- Xms=256
- Xmx=512

Second recommendation:

- Xms=256
- Xmx=1024

Collating data for multiple languages

WebSphere Partner Gateway depends on the underlying databases for collating data. If your installation supports multiple languages and your unicode data is not sorted correctly please review this section.

DB2

WebSphere Partner Gateway 6.0 on DB2 uses the UCA400_NO collating setting. DB2 version 8.2 does not support all special cases (as described in Unicode Standard version 4.00 Technical Standard #10) for all languages. In these instances please contact DB2 directly.

Oracle

Oracle databases allow dynamic changing for collation sequences. In order to utilize this functionality, WebSphere Partner Gateway changes the value of the NLS_SORT session variable depending on the locale of the current user. Table 28 contains possible user locales, supported WebSphere Partner Gateway languages, and their corresponding NLS_SORT values. This information is stored in the PR_LOCALE database table.

Table 28. Locale information

Browser Locale	Language	NLS_SORT Value
pt_BR	Brazil/Portuguese	BINARY
zh	Chinese	SCHINESE_RADICAL_M
en_US	English	BINARY
fr	French	FRENCH_M
de	German	XGERMAN
it	Italian	BINARY
ja	Japanese	JAPANESE_M
ko	Korean	KOREAN_M
es	Spanish	SPANISH_M
zh_TW	Traditional Chinese	TCHINESE_RADICAL_M
Other	Other	BINARY

Ensuring sufficient virtual memory for DB2 agents

The following error, located in the WebSphere Partner Gateway logs, indicates that there is insufficient virtual memory available to the database agent for sort processing. To correct this situation, decrease the value of the SORTHEAP parameter for the database that you created for WebSphere Partner Gateway. Contact your database administrator for specifics on how to set that parameter in your environment.

The following is an example of an insufficient virtual memory error:

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

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

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

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

Exporting your current configuration for support

IBM support personnel may request that you export your configuration information to them for review. This can be done using the BCGConfigurationExport and BCG_DBConfigurationExport tools, located in the {INSTALL DIR}\bin directory.

- BCGConfigurationExport

  This utility copies the logs and properties files. The output will be a file called BCGConfigurationExport.output.<hostname>.jar, where <hostname> is the hostname of the machine running WebSphere Partner Gateway. It will be created in a directory that you specify. The utility expects 3 parameters:

  – WAS log root directory ({INSTALL DIR}\was)
  – WebSphere Partner Gateway root directory ({INSTALL DIR}\
  – destination location

- BCG_DBConfigurationExport

  This utility copies configuration data from the WebSphere Partner Gateway database. The output will be a file called BCGDB_ConfigurationExport.DB.output.<dbname>.jar, where <dbname> is the name of the database. It will be created in a directory that you specify. The utility expects 5 parameters:

  – destination directory
  – database flag - DB2 or ORA
  – database name
  – database login id
  – database password

Before running either utility, ensure that your path includes the JAVA (i.e. {INSTALL DIR}\was\java\bin\) jre directory. When running BCG_DBConfigurationExport with DB2, use a DB2 command line. For Oracle, ensure that you have your environment set up to run Oracle tools.

Note: If WebSphere Partner Gateway is installed on multiple machines, you will need to run these utilities on each machine. Once the export files have been created, IBM support personnel will instruct you on how to deliver them.

Fixing DB2 SQLCODE -444 error when starting servers

If you encounter SQLCODE -444 error messages when starting any of the WebSphere Partner Gateway components (bcgconsole, bcgreceiver, bcgdocmgr), you should increase the value of the DB2 Database Manager SHEAPTHRES parameter. This parameter should be at least two times larger than the highest sortheap value defined for any database within the DB2 instance. Please consult your database administrator or refer to your DB2 administrator's guide before changing this setting. A sample command is given below:

```
db2 UPDATE DBM CFG USING SHEAPTHRES xxxxx IMMEDIATE
```

If the SQLCODE -444 persists after changing the value of SHEAPTHRES, you may also need to decrease the values of STMTHEAP and APPLHEAPSZ for your WPG database. A sample command is given below:

db2 UPDATE DB CFG FOR <dbname> USING STMTHEAP xxxxx

db2 UPDATE DB CFG FOR <dbname> USING APPLHEAPSZ xxxxx

Please consult your DBA or refer to your DB2 Administrator's Guide before changing any settings.

The error messages are located in one the following log files, depending on the component:

```
{INSTALL DIR}\was\profiles\bcgconsole\logs\bcgconsole\bcg_console.log
{INSTALL DIR}\was\profiles\bcgreceiver\logs\bcgreceiver\bcg_receiver.log
{INSTALL DIR}\was\profiles\bcgdocmgr\logs\bcgdocmgr\bcg_docmgr.log
```

It can also be found in the <DB2Home>\SQLLIB\bin\db2diag.log file.

Fixing DB2 SQLCODE -444 error when routing polymorphic documents

Depending on your DB2 UDB configuration you may see SQLCODE -444 error messages when routing polymorphic (map chain) documents. These error messages would be located in the file {INSTALL DIR}\was\profiles\bcgdocmgr\logs \bcgdocmgr\bcg_router.log as well as <DB2Home>\SQLLIB\bin\db2diag.log. If you see this message you should increase the value of the DB2 Database Manager parameter SHEAPTHRES. This parameter should be at least two times the largest sortheap value defined for any database within the DB2 instance. A sample command is given below:

```
db2 UPDATE DBM CFG USING SHEAPTHRES xxxxx IMMEDIATE
```

If the SQLCODE -444 persists after changing the value of SHEAPTHRES, you may also need to decrease the values of STMTHEAP and APPLHEAPSZ for your WPG database. A sample command is given below:

db2 UPDATE DB CFG FOR <dbname> USING STMTHEAP xxxxx

db2 UPDATE DB CFG FOR <dbname> USING APPLHEAPSZ xxxxx

Please consult your DBA or refer to your DB2 Administrator's Guide before changing any settings.

Fixing JMS Exception message in log files

If the bcg_receiver.log and bcg_router.log files contain the following Exception message, the MQSeries Queue Manager may be down:

```
javax.jms.JMSException: MQJMS2002: failed to get message from MQ queue
```

Confirm that the MQSeries components are started. Refer to "Starting the system after a machine shutdown" on page 83. The log files will probably be very large with the error messages so you may want to delete the log files. To do so, you must stop the Receiver or DocMgr component to free up the appropriate log file before you can delete it.

Fixing poor system performance and events that are not processing

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

Note: this only applies to UNIX systems.

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

   ```
   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 WebSphere Partner Gateway (see Stopping the Community Console and "Stopping the Receiver and Document Manager" on page 4).
4. Stop WebSphere MQ using the following steps:
   a. Stop the publish/subscribe broker, by entering the following:

      ```
      endmqbrk -m <hostname>.queue.manager
      ```

   b. Stop the listener, by entering the following:

      ```
      endmqlsr -m <hostname>.queue.manager
      ```

   c. Stop the queue manager, by entering the following:

      ```
      endmqm <hostname>.queue.manager
      ```

5. Create and start WebSphere MQ, using the instructions in the *WebSphere Partner Gateway Installation Guide*. However, do not perform steps 2 through 4 in the procedure.
6. Restart WebSphere Partner Gateway, using the instructions in the *WebSphere Partner Gateway Installation Guide*.

Console Help not appearing when selected

If you click the **Help** button in the Console and browser page appears telling you that the Help Server is not running then there are two possible problems:

- You need to start the Help Server on the machine the Console is running on. See, "Starting the Help system" on page 1.
- If you are running the Console in a browser from a machine that the Help Server is not installed on, and the value for the Help Server location is set to localhost, your local machine will be used for the Help system. To change the location to the correct IP address, edit the value of the ibm.bcg.help.host key in the bcg_console.properties file, which is located in the {INSTALL DIR}/console/lib/config directory.

Note: Users must log out of the Console and then log back in to access the Help System after starting it.

Increasing the Receiver timeout setting

If a participant opens a connection to WebSphere Partner Gateway and receives the error message "Connection aborted by peer: socket write error", the WebSphere Partner Gateway Receiver is initiating a timeout due to the slow transmission rate from the participant.

To correct this problem run the bcgHttp.jacl script, located in the {INSTALL DIR}\scripts directory, and update the following information:

- Set the PORT_NUMBER parameter.
- Modify the PROPERTY_VALUE attribute. Default is 30.

To execute the bcgHttp.jacl script, enter the following command:

```
{INSTALL DIR}/bin/bcgwsadmin.sh -conntype NONE -f {INSTALL DIR}/scripts/bcgHttp.jacl
```

Verify the changes by reviewing the server.xml file, located in the {INSTALL DIR}\receiver\was\config\cells\DefaultNode\node\servers\server1 directory. You should see the following parameter: <address xmi:id="EndPoint_1" host="" port="port_number"/> <properties xmi:id="Property_1096557327403" name="ConnectionIOTimeout" value="30"/>

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 Partner Gateway application and database activity is at a minimum. As database traffic increases, run RUNSTATS more frequently, up to once a day.

Notes:

1. Since RUNSTATS updates database system information, lock timeouts potentially can occur under specific circumstances. The WebSphere Partner Gateway application be quiesced and database access be limited to running RUNSTATS.
2. A lock timeout may occur when RUNSTATS and db2rbind are run simultaneously. It is recommended that these commands be run daily at different times.

Processing transaction rollback errors

If a critical error like Process transaction rolled back is displayed for a document, ensure that the WebSphere MQ logging configuration parameters, located in <MQInstallDir>/qmgrs/<qmgr>/qm.ini, are set to the following:

- LogPrimaryFiles=62
- LogSecondaryFiles=2
- LogFilePages=2048
- LogBufferPages=128

Note: For Windows, use the Log tab of the queue manager's Properties window in MQ Services to view the log settings.

Refer to the WebSphere MQ documentation for specific information on these attributes.

Restarting the router after a crash

If the router crashes, 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 files with the extension vmd_locked.
2. If there are files with the extension vmd_locked that are more than two minutes old, rename them to a file with the extension vmd_restart.

   Note: If multiple instances of the router are 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 a document's processing state, 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 vmd_locked extension to a file with the extension vmd_restart. Then move the files for the document to the directory router_in dir for processing.

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 WebSphere Partner Gateway components.

Starting DB2

To start DB2, use the following procedure:

UNIX:

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

Windows:

Start the database instance, by entering the following:

```
db2start
```

Starting WebSphere MQ

To start WebSphere MQ, use the following procedure:

UNIX:

1. Change to the WebSphere MQ user, by entering the following:
   ```
   su - mqm
   ```
2. Start the queue manager, by entering the following:
   ```
   strmqm <hostname>.queue.manager
   ```
3. Start the listener, by entering the following:
   ```
   runmqlsr -t tcp -p <port number> -m <hostname>.queue.manager &
   ```
4. Wait about 10 seconds and press **Enter** to return to the command prompt.
5. Start the JMS Broker (the publish/subscribe broker), by entering the following:
   ```
   strmqbrk -m <hostname>.queue.manager
   ```

Windows:

1. Start the queue manager with the following command:
   ```
   strmqm bcg.queue.manager
   ```
2. Start the listener with the following command:
   ```
   runmqlsr -t tcp -p 9999 -m bcg.queue.manager
   ```
3. The listener runs in this window, so leave it open.
4. Open a new window and start the JMS Broker (the publish and subscribe broker) with the following command:
   ```
   strmqbrk -m bcg.queue.manager
   ```

Starting the Community Console, Receiver, and Document Manager

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

Note: Modify the following steps to use the .bat extension and backslashes for Windows.

1. Change to the general WebSphere Partner Gateway user:
   ```
   su - bcguser
   ```
2. Navigate to the following directory:
   ```
   cd {INSTALL DIR}/bin
   ```
3. Start the Community Console, by entering the following:
   ```
   ./bcgStartServer.sh bcgconsole
   ```
4. Start the Receiver, by entering the following:
   ```
   ./bcgStartServer.sh bcgreceiver
   ```
5. Start the Document Manager, by entering the following:
   ```
   ./bcgStartServer.sh bcgdocmgr
   ```

0A1 generated with data validation errors

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

To add the attribute:

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

Appendix A. Performance considerations

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

Filtering events

The bcg.event_log_exclude property allows you to exclude the recording of selected events within the event log (DataLogQ). By default, normal and successful processing of documents will produce several events that are recorded in the event log. It may be useful to decrease the number of events that are recorded for successful document processing. Reducing this number may increase the performance or transaction capacity of the system. Some messages may not be excluded with this parameter.

By default the bcg.event_log_exclude property is not included in the bcg_receiver.properties (Receiver) and bcg.properties (Router) files. The property must be added as needed.

The format of the bcg.event_log_exclude property is a comma delimited list of message numbers to exclude. For example:

```
bcg.event_log_exclude=210060,210062,230011,240018,240019,250004
```

Messages that may be useful to exclude include the following:

```
210060 Passed destination parse
210062 Destination process successful
210100 Timing start event
210101 Timing end event
230011 Sequence validation successful
240018 Digital Signature Key Not Loaded for Operator
240019 Encryption Key Not Loaded for Operator
250004 Document delivery successful
```

Generating summary data

WebSphere Partner Gateway periodically summarizes data about system activity. This Summary Service data is the information you see when you use the Document Analysis or Document Volume Report functions.

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

To change the time interval that summary data is generated:

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

Appendix B. Failed Events

When a document fails processing, the WebSphere Partner Gateway system generates an event. Refer to Table 29 for a list of WebSphere Partner Gateway failed events and their corresponding descriptions. Refer to Table 30 on page 97 for a list of events that can be generated by the EDI components.

Note: The HTTP Receiver component will return an HTTP error code if it is unable to persist the document. For all other Receiver component types, the document content will be persisted at its current location at the time of failure.

Table 29. Failed events

Event code	Event name	Internal description	Severity	Extended description
BCG103001	Database Failure	Database Error: {0} failed in {1} with exception {3}	Critical	
BCG103101	Cache Engine Error	Cache Engine instanceId {0} on host {1} failed to initialized, please correct the problem and restart the service, error reason:{2}	Critical	
BCG103201	Hub Owner State Engine Error	Error Reason:{0}	Error	This event is generated when a fatal system occurs causing a document to fail processing. An example can be a database write error.
BCG103203	Receiver Processing Error	Receiver '{0},{1}' failed to processing document, error: {2}.	Error	This event is generated when the receiver is unable to process a document due to document or system errors.
BCG103205	Target Error	Target '{0},{1}' failed to process target: {2}.	Error	
BCG106004	No Default Gateway Pair	Connection create failed. A pair of default gateways does not exist between participants: {0} and {1}	Error	
BCG106005	No Action Found	A connection could not be created for the B2B capability because no actions are associated with the interaction.	Error	
BCG106600	Document Flow Definition Create Error	Child level = {0} greater than or equal to parent level = {1}	Error	
BCG111001	FTP Account Create Error	FTP account create failed for participant {0}. Error message: {1}	Error	
BCG112002	Failed to Create Directory	Failed to create directory: {0}	Error	
BCG112002	Document Root Directory Exists	Document root directory {0} already exists	Error	

Table 29. Failed events (continued)

Event code	Event name	Internal description	Severity	Extended description
BCG200000	No Default Gateway Pair	Connection create failed. A pair of default gateways does not exist between participants: {0} and {1}.	Error	
BCG200001	Get Protocol Transformer Business Process Failed	Factory failed to get an instance of the protocol transformer business process because {0}	Critical	This event is generated due to system failure when attempting to locate an instance of the protocol transformer business process.
BCG200005	Document Transformation Failure	Document failed transformation due to {0}	Error	This event is generated due to a failure during document transformation.
BCG200006	Protocol Transformer Input File Failure	Protocol transformer input file error: {0}	Critical	This event is generated due to a failure with the input file during action processing, for example, when the file is corrupted.
BCG200007	Protocol Transformer Output File Failure	Protocol transformer output file error: {0}	Critical	This event is generated due to a failure when attempting to write to the output file directory.
BCG200009	Failed to Parse Document	Failed to parse: {0}	Error	This event is generated due to failure when attempting to parse the document.
BCG200013	Community Manager Provided RN Process-Instance-ID Error	{0}	Error	This event is generated when an invalid Process Instance ID is received and the configuration property indicates that the system will not generate a new Process Instance ID.
BCG200015	Community Manager Provided RosettaNet GlobalUsageCode Error	{0}	Error	This event is generated when the x-aux-production header value is invalid and the configuration property indicates that the system will not use the default value on error.
BCG210000	Check Channel Error	Check Channel Error	Error	This event is generated when there is a check channel related error.
BCG210001	Check Channel Error	Check Channel Error	Error	This event is generated when data required to lookup a connection is available but the matching connection is not found.
BCG210002	Connection Lookup Failed	Connection lookup failed {0}	Error	This event is generated when data required to lookup a connection is not available.
BCG210007	Outbound Document Cannot be Packaged	Error in Outbound Processor	Critical	This event is generated when a packager is not available for an outbound document.
BCG210008	IP Address Validation Failure	From IP address is not in the participant profile {0}	Error	This event is generated when a document is posted from an unapproved IP Address for that participant.

Table 29. Failed events (continued)

Event code	Event name	Internal description	Severity	Extended description
BCG210009	SSL Certificate Validation Failure	Client SSL certificate name is not in the participant profile {0}	Error	This event is generated when the SSL Certificate used to post the document is not in the approved certificate list for that participant.
BCG210010	Document Too Large	Document too large: {0} bytes	Error	This event is generated when the document received is too large to be processed.
BCG210011	Community Manager Transport Unpackage Failure	Insufficient Community Manager transport information provided: {0}	Error	This event is generated when insufficient transport information is provided.
BCG210012	B2B Capability Not Found	B2B capability not found {0}	Error	This event is generated when the B2B capability required to route the document is not enabled.
BCG210013	Connection Not Fully Configured	Connection not fully configured {0}	Error	This event is generated when the connection for the document is not fully configured. Most likely the destination for the document does not have a configured gateway.
BCG210014	MIME Multipart Unpackaging Failure	Failed to unpackage a MIME multipart document: {0}	Error	This event is generated when the system failed to unpackage a MIME multipart document.
BCG210015	cXML Packaging Failure	Failed to packaing a cXML document: {0}	Error	
BCG210016	cXML Channel Parse Failure	Failed to parse cXML routing information: {0}	Error	
BCG210017	EDI Connection Parse Failure	Failed to parse EDI routing information: {0}	Error	This event is generated when the system failed to parse EDI routing information.
BCG210019	Synchronous Operation not Supported on this Connection	Synchronous Operation not Supported on this Connection	Error	This event is generated when the document requests synchronous operation but the connection does not support synchronous operations.
BCG210031	Unable to Non-Rep document	Unable to Non-Rep document {0}	Critical	This event is generated when the system is unable to non-repudiate the document. Insure that the system has sufficient disk space, and that the following directories contain system-only files: • /*<common information directory>*/non_rep/ • /*<common information directory>*/msg_store/ If these two directories contain user generated files, document processing will fail.

Table 29. Failed events (continued)

Event code	Event name	Internal description	Severity	Extended description
BCG210032	System Error in the Inbound Processor	System error in the Inbound Processor for document: {0}	Critical	This event is generated when the system encounters an error in the inbound processor.
BCG210033	Message Store Failed	Unable to store document plain text	Error	This event is generated when the system is unable to store the document in plain text. Insure that the system has sufficient disk space, and that the following directories contain system-only files: • /<*common information directory*>/non_rep/ • /<*common information directory*>/msg_store/ If these two directories contain user generated files, document processing will fail.
BCG210034	System Error in the document manager	System error in the document manager for document: {0}	Critical	This event is generated when the system encounters an error in the document manager.
BCG210051	Duplicate Processing Failure	System error - failure in duplicate process	Critical	This event is generated when the system is unable to contact the database server during duplicate processing.
BCG210052	Duplicate Document Received	This document appears to be a duplication of a document sent on {2}	Error	This event is generated when a document received is a duplicate and rejected.
BCG210061	Destination Parse Failure	Error in destination Parse	Critical	This event is generated when destination parse fails. Usually due to a database problem.
BCG210063	Destination Process Failure	Destination Process failed	Critical	This event is generated when destination processing fails. Usually due to a database problem.
BCG210065	Destination Determination Failure	{0}	Error	This event is generated when there are conflicting inputs when processing the destination.
BCG210066	Package and Content Business Id's map to different partners	From Partner ID = {0}, To Partner ID = {1}, From Package Partner ID = {2}, To Package Partner ID = {3}	Error	This event is generated when there is a mismatch between the content and package routing information
BCG210201	PIP Load During Doctype Processing Failure	Unable to load PIP for a document during Doctype processing	Critical	This event is generated when a spec for the PIP cannot be found. Should not occur unless there is a configuration problem.
BCG210202	Exception in Doctype Processing	Exception during Doctype Processing: {0}	Critical	This event is generated when the system fails when attempting to insert the DocType tag.

Table 29. Failed events (continued)

Event code	Event name	Internal description	Severity	Extended description
BCG210203	DoctypeProcess Error - No Action Found	DoctypeProcess Error - No action found	Critical	This event is generated when a spec for the PIP DocType cannot be found.
BCG210205	Document Processing Cancelled	Document Processing Cancelled. Reason: Associated document processing for {0} failed.	Critical	This event is generated when the document processing is cancelled due to the Discard envelope on Error attribute set to Yes.
BCG230004	Validation Internal Error	{0}	Critical	This event is generated due to internal system failure during validation processing.
BCG230006	Validation Database Error	{0}	Critical	This event is generated due to a database error during validation processing.
BCG230007	Validation Business Process Factory Error	{0}	Critical	This event is generated when the system is unable to determine the process to send to the validation engine.
BCG230009	RosettaNet Validation Error	{0}	Error	This event is generated when a document fails to complete RosettaNet process validation.
BCG230010	Data Validation Error	Document failed data validation: {0}	Error	This event is generated when a document fails data validation and is rejected.
BCG230012	AS Sequence Validation Error	{0}	Error	This event is generated when a document fails to complete EDIINT process validation.
BCG240003	RosettaNet Unpackaging Error	RosettaNet Unpackaging Error	Error	This event is generated when the system is unable to parse the RosettaNet preamble during unpackaging.
BCG240005	RNPackager Delivery Header Parser Failure	Delivery Header Parser Error: {0}	Error	This event is generated when the system is unable to parse the RosettaNet delivery header during unpackaging.
BCG240007	RNPackager Service Header Failure	Service Header parser error: {0}	Error	This event is generated when the system is unable to parse the RosettaNet service header during unpackaging.
BCG240009	RNPackager Mime Parsing Failure	Mime parsing error: {0}	Error	This event is generated when an error occurs in Mime parsing of the RosettaNet message during unpackaging.
BCG240011	RNPackager Signature Failed	Digital Signature validation failed: {0}	Error	This event is generated when digital signature validation fails during unpackaging.
BCG240012	RN Unpackaging State Update Error	Database access failure: Could not update the RosettaNet state	Critical	This event is generated when the unpackager encounters database communication errors when updating the RosettaNet state.

Table 29. Failed events (continued)

Event code	Event name	Internal description	Severity	Extended description
BCG240013	Participant Certificate Did Not Match Signer	Name/serial on signer certificate did not match database entry	Error	This event is generated when Certificate to DUNS check fails for digital signature.
BCG240014	Missing Signature in Document	Signature not found in document	Error	This event is generated when a signature is required by the TPA, but not found in the document.
BCG240015	RosettaNet Document Creation Failure	{0}	Critical	This event is generated when an attempt to construct a RosettaNet document fails.
BCG240016	RosettaNet Non-Repudiation Error	{0}	Error	This event is generated when the Receipt Ack does not contain correct digest of previous message, or the digest is missing.
BCG240017	Synchronous Acknowledgement Not Received	Synchronous acknowledgement is required but was not received in the synchronous response	Error	
BCG240025	WBIC Security Manager Initialization Exception	WBICSecurityManager initialization failed Exception: {1}	Critical	
BCG240026	Certificate Is Not Yet Valid	Certificate is not yet valid: Serial number: {0} Subject DN: {1} Issuer DN: {2}	Critical	
BCG240027	Certificate Is Expired	Certificate is expired: Serial number: {0} Subject DN: {1} Issuer DN: {2}	Critical	
BCG240028	Certificate Is Revoked	Certificate is revoked: Serial number: {0} Subject DN: {1} Issuer DN: {2}	Critical	
BCG240029	Certificate Not Found	Certificate not found	Critical	
BCG240030	No Valid Signing Certificate was found	No valid signing certificate found	Critical	
BCG240031	Packaging Instance Error	Error: {0}	Critical	This event is generated when the system is unable to find a packager for the supplied document type.
BCG240032	No valid encryption certificate found	No valid encryption certificate found	Critical	This event is generated when a valid certificate is not found. When this event is displayed, neither the primary nor the secondary certificate is valid. The certificates might be expired or they might have been revoked. If the certificates were expired or revoked, you see the corresponding event (Certificate revoked or expired) in the Event Viewer along with the event.
BCG240033	No valid SSL client certificate found	No valid SSL client certificate found	Critical	

Table 29. Failed events (continued)

Event code	Event name	Internal description	Severity	Extended description
BCG240036	Unpackaging Instance Error	Error: {0}	Error	This event is generated when the system cannot find an unpackager for a document.
BCG240065	Connection Parse XML Failure	XML connection parsing failed: {0}	Error	This event is generated when connection info for an XML message could not be found.
BCG240068	Connection Parser RosettaNet Failure	Connection Parse RosettaNet Failure	Error	This event is generated when connection info could not be found in a RosettaNet document.
BCG240070	XML Connection Parse Failure	XML connection parse failed	Error	This event is generated when the system is unable to find connection information for an XML file.
BCG240071	Flat File Connection Parse Failure	Flat File connection parse failed: {0}	Error	This event is generated when the system is unable to find connection information for a Flat File.
BCG240078	Web Service Connection Parse Failed	Web Service connection parse failed	Error	This event is generated when the system is unable to find connection information for a SOAP message.
BCG240409	AS Unpackager Failure	AS Unpackager Error: {0}	Error	This event is generated when the AS unpackager fails.
BCG240411	AS Signature Failure	AS Signature Validation Error: {0}	Error	This event is generated when AS signature validation fails.
BCG240412	AS State Engine DB Failure	AS State Engine DB error: {0}	Critical	This event is generated when the AS state engine database fails.
BCG240415	AS Packager Failure	AS Packager Error: {0}	Critical	This event is generated when the AS packager fails.
BCG240416	AS Non-Repudiation Error	{0}	Error	This event is generated when AS Non-Repudiation fails.
BCG240417	Decryption Failed	{0}	Error	This event is generated when decryption fails.
BCG240418	Unable to Generate Message Digest	{0}	Error	This event is generated when the system is unable to generate a message digest.
BCG240419	Unsupported Signature Format	{0}	Error	This event is generated when the system receives an unsupported signature format.
BCG240420	Unsupported Signature Algorithm	{0}	Error	This event is generated when the system receives unsupported signature algorithm.
BCG240421	Unexpected Error	{0}	Critical	This event is generated when the system encounters an unexpected error.
BCG240422	AS document not found for this MDN	{0}	Error	This event is generated when a MDN is received and the system is unable to locate the corresponding document.

Table 29. Failed events (continued)

Event code	Event name	Internal description	Severity	Extended description
BCG240423	Input File Failure	Invalid input file passed in the document	Error	This event is generated when the system encounters an invalid input file.
BCG240424	Insufficient Message Security	{0}	Error	This event is generated when the system encounters insufficient message security.
BCG240500	RosettaNet State Engine Error	RosettaNet State Engine Error	Critical	This event is generated when the RosettaNet State Engine encounters a system error.
BCG240550	POP3 Poll Error	Error polling POP3 server: {0}; rejected message VUID: {1}	Error	
BCG240600	AS State Engine Error	AS State Engine Error: {0}	Critical	This event is generated when the RosettaNet State Engine encounters a system error.
BCG240601	AS Retry Failure	AS Attribute max retry limit reached	Error	This event is generated when the system fails AS retries. The maximum retry limit may have been reached.
BCG240606	Packaging Error	Packaging error {0}	Error	
BCG240610	Unpackaging Error	Unpackaging error {0}	Error	
BCG240615	Protocol Parse Error	Protocol parse error {0}	Error	
BCG240701	Activity Logging Error	Error occured while logging activity details: {0}	Error	This event is generated when a search for an activity Id for a document Id for a partner is not found.
BCG250001	Document Delivery Failed	Document delivery to participant gateway failed: {0}	Error	This event is generated when document delivery to a participant's gateway fails and the document is set to a failed state.
BCG250002	Delivery Scheduler Failed	An internal error occurred in the Delivery Scheduler: {0}	Critical	This event is generated when an uncategorized internal error occurred within the Delivery Manager, due to bad gateway or document data, rather than failure to deliver.
BCG250005	FTP Delivery Failed	FTP delivery to participant gateway failed with exception: {0}	Error	This event is generated when the FTP protocol document delivery failed but more retries may be possible. Final failure will generate event 250001.
BCG260002	RosettaNet Pass Through Logging Failed	RosettaNet pass through process view logging failed: {0}	Error	This event is generated when a document fails RN pass through logging.
BCG280006	Document Processing Error	Unable to find content, meta-data and header files in {0} reject and oversize folders for document: {1}	Error	

Table 29. Failed events (continued)

Event code	Event name	Internal description	Severity	Extended description
BCG281001	Console Resend Placed Document In Queue	Console resend placed document in queue: {0}	Critical	
BCG281002	Console Resend Document Already In Queue	Console resend document already in queue :{0}	Critical	
BCG310002	EDI Transaction Enveloped	EDI Transaction Enveloped. Envelope activity id: {0}	Error	This event is generated when the EDI transaction document is enveloped. The envelope activity id is that of the new envelope document.
BCG310003	EDI Transaction Enveloping failed	EDI Transaction Enveloping failed	Error	This event is generated when the EDI transaction document is not enveloped. This event should be preceded by an event with details of the failure.
BCG800000	Get Community Manager Business Process Failed	Failed to get an instance of the Community Manager business process because {0}	Critical	This event is generated when the system fails to locate the Community Manager action for business processing.
BCG800004	Community Manager Business Process Encounters Database Error	{0}	Critical	This event is generated due to database error while processing the Community Manager's action.
BCG800005	Community Manager Process Encounters Internal Error	{0}	Critical	This event is generated due to internal system error while processing the Community Manager's action.

Table 30. EDI event codes and messages

EDI Event code	Event name	Internal description	Severity	Extended description
BCGEDICM0001	Unexpected Exception Occurred	An unexpected exception occurred in component: {0}. Exception text: {1}	Error	
BCGEDICM0003	Missing Required Property	Invalid input for component {0}. Missing required property {1}	Error	
BCGEDICM0004	Invalid Property Value	Invalid input for component {0}. Value {1} is invalid for property {2}	Error	
BCGEDICM0005	Unsupported Character Set	Invalid input for component {0}. Character set {1} specified in property {2} is not supported	Error	
BCGEDICM0006	Invalid Document Syntax for Component	Invalid input for component {0}. The document syntax {1} is not valid for this component	Error	
BCGEDICM0010	I/O Error Occurred	An I/O error occurred in component {0}. The exception text is: {1}	Error	

Table 30. EDI event codes and messages (continued)

EDI Event code	Event name	Internal description	Severity	Extended description
BCGEDICM0011	File Open Failed	Component {0} could not open file: {1}	Error	
BCGEDICM0012	Failure Accessing Memory Buffer	Component {0} could not access the memory buffer	Error	
BCGEDICM0013	Missing Input Data Source	No input data source was specified for component {0}	Error	
BCGEDICM0014	Missing Output Data Source	No output data source was specified for component {0}	Error	
BCGEDICM0020	Parsing Error in Component	Component {0} failed due to errors parsing the input data	Error	
BCGEDICM0021	Database Error	An error occurred while trying to access the database. Class name: {0}, Method: {1}, Exception: {2}	Error	
BCGEDICM0022	Unexpected Database Exception	An unexpected exception occurred while trying to access the database. Class name: {0}, Method: {1}, Exception: {2}	Error	
BCGEDICM0023	No Database Connection	The database connection manager class {0} did not return a valid connection	Critical	
BCGEDICM0101	Missing or Invalid Object for Component	An internal error occurred. The object passed to component {0} was missing or invalid	Error	
BCGEDICM0102	Class Load Failure	A dynamically configured class could not be loaded. Configuration key: {0}, Class name: {1}	Critical	
BCGEDICM0103	Invalid Function Parameter	An internal error occurred in component {0}. An invalid value '{1}' was passed to function {2}	Error	
BCGEDICM0104	Invalid Source Document	The source document is not applicable to component {0}	Error	
BCGEDIEM0100	Transcript File Contents	Transcript File Contents. {0}	Error	
BCGEDIEM0101	An exception occurred while retrieving certificates	An exception occurred while retrieving certificates. Details: {0}	Error	
BCGEDIEM0102	Exception when reading the transcript file	Exception when reading the transcript file. Details: {0}	Error	
BCGEDIEM0103	Required attribute is null	Required attribute {0} is null.	Error	

Table 30. EDI event codes and messages (continued)

EDI Event code	Event name	Internal description	Severity	Extended description
BCGEDIEM0104	Exception occurred when trying to write the file to be sent to a temporary location	Exception occurred when trying to write the file to be sent to a temporary location. Details: {0}	Error	
BCGEDIEM0105	Certificates need to be uploaded to the certificate repository	Certificates need to be uploaded to the certificate repository.	Error	
BCGEDIEM0106	Could not load private key file. Alias not found	Could not load private key file. Alias not found.	Error	
BCGEDIEM0107	Client Certificate (local certificate) validation has failed, certificate could be invalid or revoked	Client Certificate (local certificate) validation has failed, certificate could be invalid or revoked.	Error	
BCGEDIEM0108	Security Exception	Security Exception. Details: {0}	Error	
BCGEDIEM0109	The temporary directory value provided for the receiver is null	The temporary directory value provided for the receiver is null.	Error	
BCGEDIEM0110	The BusinessDoucument Array passed is null	The BusinessDoucument Array passed is null.	Error	
BCGEDIEM0111	Input file is null	The input file is null.	Error	
BCGEDIEM0112	A splitter exception was received.	Splitter Exception was received. Details : {0}	Error	
BCGEDIEM0113	A splitter exception was received.	Splitter Exception was received. Details : {0}	Error	
BCGEDIEM0114	Cannot find reader	Cannot find reader	Error	
BCGEDIEM0118	Character Encoding Error	Error encoding ″{0}″ into character set {1}.	Error	
BCGEDIEM0120	Error initializing RODScanner	Error initializing RODScanner. Details : {0}	Error	
BCGEDIEM0128	Network error message received from IBM VAN.	Network error message received from IBM VAN. Details are Message Id = {0}, Message Description = {1}, Severity Code = {2}	Error	
BCGEDIEM0150	The document passed does not apply to EDIAckHandler	The document passed does not apply to EDIAckHandler	Error	
BCGEDIEM0151	Error processing edi ack	Error processing edi ack. Message got in Error terminal.	Error	
BCGEDIEM0152	Cannot get database Connection from context	Cannot get database Connection from context	Error	

Table 30. EDI event codes and messages (continued)

EDI Event code	Event name	Internal description	Severity	Extended description
BCGEDIEM0200	Database Connection Error.	Invalid or missing database connection object in the context.	Error	
BCGEDIEM0201	I/O Error While Writting to File.	Unable to Create a File in PROCESS DIR {0}	Error	
BCGEDIEM0202	Unable to Serialize AbsDocument.	Parser Exception Occured while trying to serialize the AbsDocument.	Error	
BCGEDIEM0203	Exception occurred while serializing AbsDocument.	Exception Occured while trying to serialize the AbsDocument.	Error	
BCGEDIEM0204	Unable To Introduce Business Document	Unable to Introduce Business Document with ID {0} back into workflow.	Error	
BCGEDIEM0205	Unable to find state information.	Unable to find state information in the state management service.	Error	
BCGEDIEV0003	Interchange Begin Not Found	An attempt to deenvelope a message failed because a valid interchange begin could not be found	Error	
BCGEDIEV0009	Trading Partner Nickname Lookup Failed	Unable to find trading partner nickname: {0}	Error	
BCGEDIEV0010	Internal Error for Function	Internal error occurred. Function: {0}, Return code: {1}	Error	
BCGEDIEV0011	Database transaction failed	Database transaction failed. SQL Error: {0}	Error	
BCGEDIEV0018	Envelope Segment Not Found	The {0} enveloper or de-enveloper detected an error: The {1} segment was not found	Error	
BCGEDIEV0050	Translation Table Lookup Failed	A translation table lookup failed while enveloping or deenveloping a message. Translation table: {0}, value: {1}	Error	
BCGEDIEV0051	Envelope Segment Not Found	The {0} deenveloper detected an error: {1} found with no {2}	Error	
BCGEDIEV0052	Empty Message to Envelope	The {0} enveloper detected an error: Received an empty message to envelope	Error	
BCGEDIEV0053	Maximum Groups Exceeded for Control Number Mask	The {0} enveloper detected an error: Total groups greater than number allowed by control number mask	Error	

Table 30. EDI event codes and messages (continued)

EDI Event code	Event name	Internal description	Severity	Extended description
BCGEDIEV0054	Multiple Interchanges Error	The {0} deenveloper detected an error: Multiple interchanges were detected but not allowed.	Error	
BCGEDIEV0055	Translation Table Lookup Warning	A translation table lookup returned no entry while enveloping a message. Translation table: {0}, value: {1}.	Error	
BCGEDIEV0056	Translation Table Lookup Warning	A translation table lookup returned no entry while deenveloping a message. Translation table: {0}, value: {1}, group/transaction control number {2}.	Error	
BCGEDIEV0057	Envelope Failed	An attempt to envelope a message failed. The envelope type was {0}	Error	
BCGEDIEV0058	Deenvelope Failed	An attempt to deenvelope a message failed	Error	
BCGEDIFT0100	Expected Argument Missing	Syntax error on command: {0}. An expected argument was missing	Error	
BCGEDIFT0110	FTP script Processing Stopped	Error caused FTP script processing to stop	Error	
BCGEDIFT0111	Missing File Base Name	No base name provided for retrieved files	Error	
BCGEDIFT0112	Missing or Invalid Object for Component	Unknown object on input terminal	Error	
BCGEDIFT0113	Unexpected Error Executing Command	Unexpected error executing command: {0}	Error	
BCGEDIFT0114	Unexpected Error Downloading File	Unexpected error downloading file: {0}	Error	
BCGEDIFT0115	FTP Script File Not Found	FTP script file not found	Error	
BCGEDIFT0116	IO Exception Reading Script	IO Exception caught when reading script	Error	
BCGEDIFT0117	Unexpected Exception Parsing FTP Script	Unexpected exception caught while parsing FTP Script. Contact your system administrator. Further details about the exception and a stacktrace can be found in the trace file	Error	
BCGEDIFT0118	File Upload Failed	Unable to upload file. File name was: {0}	Error	
BCGEDIFT0119	No File for MPUT	MPUT issued but no file was found to be sent. Filename was: {0}. Directory was: {1}	Error	

Table 30. EDI event codes and messages (continued)

EDI Event code	Event name	Internal description	Severity	Extended description
BCGEDIFT0120	FTP Command Timed Out	FTP Command timed out. The command being sent was: {0}	Error	
BCGEDIFT0200	IO Exception	An IO Exception has occured.Exception Text {0}	Error	
BCGEDIFT0201	Data Socket Create Failed	Data Socket could not be created. Connection or ControlSocket is null	Error	
BCGEDIFT0202	Reply Codes Are Null	Null Pointer Exception: StringBuffer that has replycodes for processing is null	Error	
BCGEDIFT0203	Invalid Argument Values	Invalid values for the arguments, any or all may be null	Error	
BCGEDIFT0204	Control Socket Not Created	Control Socket not created	Error	
BCGEDIFT0205	Required File Not Found	Required File Not Found	Error	
BCGEDIFT0206	Exception occured	Exception occured	Error	
BCGEDIFT0207	Active Data Socket Is Null	Active Data Socket is null	Error	
BCGEDIFT0208	SocketException Has Occurred	SocketException has occurred	Error	
BCGEDIFT0209	Passive Data Socket Is Null	Passive Data Socket is null	Error	
BCGEDIFT0210	Data Socket Is Null	Data Socket is null	Error	
BCGEDIFT0211	Load Private Key Failed	Could not load private key file from filename - {0} Alias not found	Error	
BCGEDIFT0212	Client Certificate Validation Failed	Client Certificate (local certificate) validation has failed,certificate could be invalid or revoked	Error	
BCGEDIFT0220	OPEN Command Failed	OPEN command failed. Reason: {0}	Error	
BCGEDIFT0221	CWD Command Failed	CWD command failed. Reason: {0}	Error	
BCGEDIFT0222	DELE Command Failed	DELE command failed. Reason: {0}	Error	
BCGEDIFT0223	PUT Command Failed	PUT command failed. Reason: {0}	Error	
BCGEDIFT0224	GET Command Failed	GET command failed. Reason: {0}	Error	
BCGEDIFT0225	LIST Command Failed	LIST command failed. Reason: {0}	Error	
BCGEDIFT0226	QUIT Command Failed	QUIT command failed. Reason: {0}	Error	

Table 30. EDI event codes and messages (continued)

EDI Event code	Event name	Internal description	Severity	Extended description
BCGEDIFT0227	RMD Command Failed	RMD command failed. Reason: {0}	Error	
BCGEDIFT0228	MKD Command Failed	MKD command failed. Reason: {0}	Error	
BCGEDIFT0229	PASV Command Failed	PASV command failed. Reason: {0}	Error	
BCGEDIFT0230	GETDEL Command Failed	GETDEL command failed. Reason: {0}	Error	
BCGEDIFT0231	FTP Command Failed	FTP command {0} failed. Reason: {1}	Error	
BCGEDIFT0232	Null Reply From FTP Server	The reply from the FTP Server is null	Error	
BCGEDIMD0001	Unexpected Exception Reading Metadata	An unexpected exception occurred while reading the metadata. Syntax: {0}, Dictionary: {1}, Document: {2}, Exception text: {3}	Error	
BCGEDIMD0002	Metadata Control String Invalid	The metadata control string is invalid, or is compiled for a different version. Syntax: {0}, Dictionary: {1}, Document: {2}	Error	
BCGEDIMD0003	Metadata Control String Read Failed	The metadata control string could not be read from the database. Syntax: {0}, Dictionary: {1}, Document: {2}	Error	
BCGEDINK0001	Invalid Network Acknowledgement	The document passed to the IBM VAN network acknowledgement component is not a valid network acknowledgement	Error	
BCGEDINK0002	Invalid Attribute Value	The attribute {0} has an invalid value {1}	Error	
BCGEDISP0002	Unable to Determine Encoding	The XML splitter could not determine the encoding of the XML input data	Error	
BCGEDISP0003	Invalid XML Data	The data passed to the XML splitter is not valid XML data	Error	
BCGEDISP0005	Interchange Iterator is Null	An internal error occurred. The interchange iterator was not set during a previous call	Error	
BCGEDISP0006	End of Input Data	The splitter has reached the end of the input data	Error	
BCGEDIUP0001	Fatal XML Parsing Error	A fatal error occured during parsing of XML document {0} at line {1}, column {2}. Message text from parser is: {3}	Error	

Table 30. EDI event codes and messages (continued)

EDI Event code	Event name	Internal description	Severity	Extended description
BCGEDIUP0002	Severe XML Parsing Error	A severe error occured during parsing of XML document {0} at line {1}, column {2}. Message text from parser is: {3}	Error	
BCGEDIUP0015	Metadata Read Failed	An attempt to get the metadata for the message failed	Error	
BCGEDIUP0118	Character Encoding Error	Error encoding ″{0}″ into character set {1}.	Error	
BCGEDIUP0021	Unable to Identify Input Data Record	Unable to identify the input data record. Record number was {0}. Data Image {1}	Error	
BCGEDIUP0023	Record Exceeded Maximum Repetitions specified	The data received has exceeded the maximum repetitions specified. Record number was {0}. Data Identification was {1} and maximum reptitions was {2}	Error	
BCGEDIUP0033	Missing Dictionary or Document values	The Dictionary or Document values used for parsing were not specified or are blank	Error	
BCGEDIUP0034	Invalid Structure Usage	Character separated data is not a supported option for data formats that contain structures	Error	
BCGEDIUP0038	Missing Record Delimiter	End of record reached without record delimiter detected. Record delimiter expected was {0}. Record number was {1}. Record name was {2}. Byte offset was {3}	Error	
BCGEDIUP0039	Character Conversion Failed	An attempt to convert data to unicode characters failed. The input data was {0}, and the data length was {1}. Error received: {2}	Error	
BCGEDIUP0040	Invalid Data for Data Type	Invalid data found attempting to convert {0} type data. Invalid data was {1}	Error	
BCGEDIUP0041	Unsupported Character Set	The character set used for the ROD data is not supported. The character set was {0}	Error	

Table 30. EDI event codes and messages (continued)

EDI Event code	Event name	Internal description	Severity	Extended description
BCGEDIUP0042	Unsupported Record Found	An unsupported record was found processing C and D records. The character C, D, or Z was expected in the first position. {0} was received. Byte offset was {1}	Error	
BCGEDIUP0052	Unexpected Serialization Exception	An unexpected exception occurred while serializing the document. Exception text is: {0}	Error	
BCGEDIUP0053	Parser or Serializer Creation Failed	No parser or serializer could be created for syntax {0}	Error	
BCGEDIUP0055	Empty Document for Serialization	The document could not be serialized because it is empty	Error	
BCGEDIUP0057	Invalid Document for Serialization	The document could not be serialized because its internal structure is invalid	Error	
BCGEDIUP0099	No Recognized Input Data	Parser found no recognizable input data. Parser component {0}	Error	
BCGEDIUP0100	MetaData Details Not Found	MetaData details not found in document. Dictionary{0}, Document{1}, Syntax{2}	Error	
BCGEDIUP0101	MetaData Control String Not Found	MetaData Control String not Found. Dictionary{0}, Document{1}, Syntax{2}	Error	
BCGEDIUP0106	Invalid ROD Data Format	Invalid ROD DataFormat. No Child Nodes (STRUCTURES or FIELDS) found in Record node. Record Name: {0}	Error	
BCGEDIUP0107	Missing Record Name in Record	NULL RecordName found in document for D Record	Error	
BCGEDIUP0108	Unexpected Nodes Under Root Node	Invalid ROD DataFormat. ROD ROOT node: {0} has child nodes other than RECORD & LOOP	Error	
BCGEDIUP0109	Missing Record Name in Node	NULL or empty RecordName found in RECORD node	Error	
BCGEDIUP0110	Error Getting Metadata Information	Unable to get RODMetaDataElement from MetaData for the record: {0}	Error	
BCGEDIUP0111	Empty Record Found	Child Elements not found in MetaDataElement: {0}, Element Type RECORD	Error	

Table 30. EDI event codes and messages (continued)

EDI Event code	Event name	Internal description	Severity	Extended description
BCGEDIUP0112	Unexpected Nodes Under Record Node	Invalid ROD DataFormat. ROD RECORD node: {0} has child nodes other than STRUCTURE & FIELD	Error	
BCGEDIUP0113	Unexpected Nodes Under Loop Node	Invalid ROD DataFormat. ROD LOOP node: {0} has child nodes other than LOOP & RECORD	Error	
BCGEDIUP0114	Unexpected Nodes Under Structure Node	Invalid ROD DataFormat. ROD STRUCTURE node: {0} has child nodes other than STRUCTURE & FIELD	Error	
BCGEDIUP0115	Empty Structure Found	Child Elements not found in MetaDataElement: {0}, Element Type STRUCTURE	Error	
BCGEDIUP0116	Invalid Character in Data Format	Invalid Character found with {0} data format. Character is: {1}	Error	
BCGEDIUP0117	Character Decoding Error	Character decoding error at offset {0}	Error	
BCGEDIUP0118	Character Encoding Error	Error encoding {2} into character set {3}	Error	
BCGEDIUT0008	Current Map Name	Map name being processed: {0}	Error	
BCGEDIUT0011	Control String Instruction Failed	The transformation node (DTC) was unable to process a control string instruction. The control string instruction was {0}, the instruction stream offset was {1}, and the map name was {2}	Error	
BCGEDIUT0023	Output Document Creation Failed	An attempt to create an output document failed. The root node name was {0}, the syntax was {1}	Error	
BCGEDIUT0033	User Specified Message Text	User specified message text: {0}. This message was logged with severity code {1} and user code {2}	Error	
BCGEDIUT0034	HexDecode String Length Invalid	The transformation component attempted to HexDecode a string, but the string length was not valid. The number of characters in a string to be decoded must be an even number	Error	

Table 30. EDI event codes and messages (continued)

EDI Event code	Event name	Internal description	Severity	Extended description
BCGEDIUT0035	HexDecode Character Invalid	The transformation component was executing a HexDecode command, and a character value was encountered that could not be decoded. The character value was {0}	Error	
BCGEDIUT0041	Translation Table Lookup Failed	Translation table lookup entry {0} not found in {1}. The default value returned was {2}.	Error	
BCGEDIUT0061	Invalid Value for Imbedded Map	Imbedded map requires a byte array element. the instruction stream offset was {1}, and the map name was {2}	Error	
BCGEDIUT0100	User Exit Not Found	User exit {0} was not found	Error	
BCGEDIUT0101	Unexpected Exception in User Exit	User exit {0} had an unexpected exception: {1}	Error	
BCGEDIUT0401	Map Control String Not Found	The control string for map {0} was not found in the database	Error	
BCGEDIUT0402	Map Control String Invalid	The control string for map {0} is invalid, or was compiled for a different version	Error	
BCGEDIUT0403	Global Variable Not Found	The global variable {0} was not found. The map control string {1} could not be loaded	Error	
BCGEDIUT0404	Global Variable has Invalid Initial Value	The global variable {0} has an invalid initial value. The map control string {1} could not be loaded	Error	
BCGEDIUT0405	Unexpected Exception Reading Map Control String	An unexpected exception occurred while reading the map control string from the database. Map name: {0}, Exception text: {1}	Error	
BCGEDIUT0406	Unexpected Exception Reading Global Variable	An unexpected exception occurred while reading the global variable from the database. Variable name: {0}, Map name: {1}, Exception text: {2}	Error	
BCGEDIUT0407	Database Error Reading Map Control String	The control string for map {0} could not be loaded because of a database error	Error	
BCGEDIUT0501	Input Document for Transformation is Empty	The input document for the transformation is empty	Error	

Table 30. EDI event codes and messages (continued)

EDI Event code	Event name	Internal description	Severity	Extended description
BCGEDIVA0001	Mandatory Data Element Missing	Mandatory data element is missing, element name = {0}, segment name = {1}, segment position = {2}, sending trading partner id/qualfier = {3}/{4}, receiving trading partner id/qualifier = {5}/{6}, control numbers = {7}	Error	
BCGEDIVA0002	Data Element Too Long	Data element is too long, element name = {0}, segment name = {1}, segment position = {2}, sending trading partner id/qualfier = {3}/{4}, receiving trading partner id/qualifier = {5}/{6}, control numbers = {7}. Element type = {8}, value = {9}, effective length = {10}, defined maximum length = {11}	Error	
BCGEDIVA0003	Data Element Too Short	Data element is too short, element name = {0}, segment name = {1}, segment position = {2}, sending trading partner id/qualfier = {3}/{4}, receiving trading partner id/qualifier = {5}/{6}, control numbers = {7}. Element type = {8}, value = {9}, effective length = {10}, defined minimum length = {11}	Error	
BCGEDIVA0004	Coded Value Not Found in Validation Table	Coded value not found in validation table, element name = {0}, segment name = {1}, segment position = {2}, sending trading partner id/qualfier = {3}/{4}, receiving trading partner id/qualifier = {5}/{6}, control numbers = {7}. Element type = {8}, value = {9}, validation table = {10}	Error	

Table 30. EDI event codes and messages (continued)

EDI Event code	Event name	Internal description	Severity	Extended description
BCGEDIVA0010	Failed 'Paired' (P) Condition	Failed 'paired' (P) condition, the standard defines items {0} as paired, but only item {1} was present. Segment name = {2}, segment position = {3}, sending trading partner id/qualfier = {4}/{5}, receiving trading partner id/qualifier = {6}/{7}, control numbers = {8}	Error	
BCGEDIVA0011	Failed 'Required' (R) Condition	Failed 'required' (R) condition, the standard defines items {0} as required, but all are missing. Segment name = {2}, segment position = {3}, sending trading partner id/qualfier = {4}/{5}, receiving trading partner id/qualifier = {6}/{7}, control numbers = {8}	Error	
BCGEDIVA0012	Failed 'Exclusive' (E) Condition	Failed 'exclusive' (E) condition, the standard defines items {0} as mutually exclusive, but {1} are present. Segment name = {2}, segment position = {3}, sending trading partner id/qualfier = {4}/{5}, receiving trading partner id/qualifier = {6}/{7}, control numbers = {8}	Error	
BCGEDIVA0013	Failed 'Conditional' (C) Condition	Failed 'conditional' (C) condition, the standard defines items {0} as conditionally required, but only {1} is present. If the first item is present, all the other must be present. Segment name = {2}, segment position = {3}, sending trading partner id/qualfier = {4}/{5}, receiving trading partner id/qualifier = {6}/{7}, control numbers = {8}	Error	

Table 30. EDI event codes and messages (continued)

EDI Event code	Event name	Internal description	Severity	Extended description
BCGEDIVA0014	Failed 'List Conditional' (L) Condition	Failed 'list conditional' (L) condition, the standard defines items {0} as conditionally paired, but only {1} is present. If the first item is present, at least on of the others must be present. Segment name = {2}, segment position = {3}, sending trading partner id/qualfier = {4}/{5}, receiving trading partner id/qualifier = {6}/{7}, control numbers = {8}	Error	
BCGEDIVA0015	Mandatory Composite Element Missing	Mandatory composite element is missing, element name = {0}, segment name = {1}, segment position = {2}, sending trading partner id/qualfier = {3}/{4}, receiving trading partner id/qualifier = {5}/{6}, control numbers = {7}	Error	
BCGEDIVA0016	Composite Data Element Maximum Repetitions Exceeded	Composite element repeats more times than defined by standard, element name = {0}, segment name = {1}, segment position = {2}, sending trading partner id/qualfier = {3}/{4}, receiving trading partner id/qualifier = {5}/{6}, control numbers = {7}. Repetition number = {8}, maximum defined repetitions = {9}	Error	
BCGEDIVA0025	Duplicate Transaction or Message in Interchange or Group	Duplicate transction set or message within current interchange or functional group, transaction set or message control number = {0}, sending trading partner id/qualfier = {1}/{2}, receiving trading partner id/qualifier = {3}/{4}, control numbers = {5}	Error	

Table 30. EDI event codes and messages (continued)

EDI Event code	Event name	Internal description	Severity	Extended description
BCGEDIVA0030	Data Element Failed Character Set Validation	Data element failed character set validation, element name = {0}, segment name = {1}, segment position = {2}, sending trading partner id/qualfier = {3}/{4}, receiving trading partner id/qualifier = {5}/{6}, control numbers = {7}. Element type = {8}, value = {9}, validation table = {10}	Error	
BCGEDIVA0031	Invalid Numeric Element	Invalid numeric element, element name = {0}, segment name = {1}, segment position = {2}, sending trading partner id/qualfier = {3}/{4}, receiving trading partner id/qualifier = {5}/{6}, control numbers = {7}. Element type = {8}, value = {9}	Error	
BCGEDIVA0032	Invalid Real Numeric Element	Invalid real numeric element, element name = {0}, segment name = {1}, segment position = {2}, sending trading partner id/qualfier = {3}/{4}, receiving trading partner id/qualifier = {5}/{6}, control numbers = {7}. Element type = {8}, value = {9}	Error	
BCGEDIVA0033	Invalid Date Element	Invalid date element, element name = {0}, segment name = {1}, segment position = {2}, sending trading partner id/qualfier = {3}/{4}, receiving trading partner id/qualifier = {5}/{6}, control numbers = {7}. Element type = {8}, value = {9}	Error	
BCGEDIVA0034	Invalid Time Element	Invalid time element, element name = {0}, segment name = {1}, segment position = {2}, sending trading partner id/qualfier = {3}/{4}, receiving trading partner id/qualifier = {5}/{6}, control numbers = {7}. Element type = {8}, value = {9}	Error	

Table 30. EDI event codes and messages (continued)

EDI Event code	Event name	Internal description	Severity	Extended description
BCGEDIVA0035	Data Element Maximum Repetitions Exceeded	Element repeats more times than defined by standard, element name = {0}, segment name = {1}, segment position = {2}, sending trading partner id/qualfier = {3}/{4}, receiving trading partner id/qualifier = {5}/{6}, control numbers = {7}. Repetition number = {8}, maximum defined repetitions = {9}	Error	
BCGEDIVA0050	Too Many Elements or Unexpected Element in Segment	Too many elements or unexpected element in segment, element name = {0}, segment name = {1}, segment position = {2}, sending trading partner id/qualfier = {3}/{4}, receiving trading partner id/qualifier = {5}/{6}, control numbers = {7}	Error	
BCGEDIVA0051	Unrecognized Segment Id	Unrecognized segment id, segment name = {0}, segment position = {1}, sending trading partner id/qualfier = {2}/{3}, receiving trading partner id/qualifier = {4}/{5}, control numbers = {6}	Error	
BCGEDIVA0052	Mandatory Segment Missing	Mandatory segment missing, segment name = {0}, segment position = {1}, sending trading partner id/qualfier = {2}/{3}, receiving trading partner id/qualifier = {4}/{5}, control numbers = {6}	Error	
BCGEDIVA0054	Loop Repeats More Times than Defined by Standard	Loop repeats more times than defined by standard, loop name = {0}, segment position = {1}, sending trading partner id/qualfier = {2}/{3}, receiving trading partner id/qualifier = {4}/{5}, control numbers = {6}. Repetition number = {7}, maximum defined repetitions = {8}	Error	

Table 30. EDI event codes and messages (continued)

EDI Event code	Event name	Internal description	Severity	Extended description
BCGEDIVA0055	Segment Repeats More Times than Defined by Standard	Segment repeats more times than defined by standard, segment name = {0}, segment position = {1}, sending trading partner id/qualfier = {2}/{3}, receiving trading partner id/qualifier = {4}/{5}, control numbers = {6}. Repetition number = {7}, maximum defined repetitions = {8}	Error	
BCGEDIVA0101	Transaction Set or Message Control Numbers Mismatch	Transaction set or message control numbers do not match in header and trailer, group header control number = {0}, group trailer control number = {1}, sending trading partner id/qualfier = {2}/{3}, receiving trading partner id/qualifier = {4}/{5}, control numbers = {6}	Error	
BCGEDIVA0102	Transaction Set or Message Trailer Missing or Invalid	Transaction set or message trailer missing or invalid, control number = {0}, sending trading partner id/qualfier = {1}/{2}, receiving trading partner id/qualifier = {3}/{4}, control numbers = {5}	Error	
BCGEDIVA0103	Transaction Set or Message Trailer Count Invalid	Transaction set or message trailer contains an invalid segment count, transaction set or message control number = {0}, sending trading partner id/qualfier = {1}/{2}, receiving trading partner id/qualifier = {3}/{4}. Value from trailer = {5}, actual number received = {6}	Error	
BCGEDIVA0151	Functional Group Control Numbers Mismatch	Functional group control numbers do not match in header and trailer, header control number = {0}, trailer control number = {1}, sending trading partner id/qualfier = {2}/{3}, receiving trading partner id/qualifier = {4}/{5}, control numbers = {6}	Error	

Table 30. EDI event codes and messages (continued)

EDI Event code	Event name	Internal description	Severity	Extended description
BCGEDIVA0152	Functional Group Trailer Missing or Invalid	Functional group trailer missing or invalid, functional control number = {0}, sending trading partner id/qualfier = {1}/{2}, receiving trading partner id/qualifier = {3}/{4}, control numbers = {5}	Error	
BCGEDIVA0153	Functional Group Trailer Count Invalid	Functional group trailer contains invalid transaction set or message count, functional control number = {0}, sending trading partner id/qualfier = {1}/{2}, receiving trading partner id/qualifier = {3}/{4}, control numbers = {5}. Value from trailer = {6}, actual number received = {7}	Error	
BCGEDIVA0158	Duplicate Group in Interchange	Duplicate group detected within current interchange, group control number = {0}, sending trading partner id/qualfier = {1}/{2}, receiving trading partner id/qualifier = {3}/{4}, control numbers = {5}	Error	
BCGEDIVA0202	Interchange Trailer Missing or Invalid	Interchange trailer missing or invalid, interchange header control number = {0}, sending trading partner id/qualfier = {1}/{2}, receiving trading partner id/qualifier = {3}/{4}	Error	
BCGEDIVA0203	Interchange Control Numbers Mismatch	Interchange control numbers do not match in header and trailer, interchange header control number = {0}, interchange trailer control number = {1}, sending trading partner id/qualfier = {2}/{3}, receiving trading partner id/qualifier = {4}/{5}	Error	

Table 30. EDI event codes and messages (continued)

EDI Event code	Event name	Internal description	Severity	Extended description
BCGEDIVA0205	Interchange Trailer Count Invalid	Interchange trailer contains an invalid group or message count, interchange header control number = {0}, sending trading partner id/qualfier = {1}/{2}, receiving trading partner id/qualifier = {3}/{4}. Value from trailer = {5}, actual number received = {6}	Error	
BCGEDIVA0211	Duplicate Interchange	Duplicate interchange detected, interchange header control number = {0}, sending trading partner id/qualfier = {1}/{2}, receiving trading partner id/qualifier = {3}/{4}	Error	
BCGEDIVA0981	User-specified validation map not found.	User-specified validation map {0} not found	Error	
BCGEDIVA0982	Service segment validation map not found.	Service segment validation map {0} not found	Error	
BCGEDIVA0983	Service segment validation not supported for document syntax.	Service segment validation not supported for document syntax	Error	
BCGEDIVA0991	Required Property or Content Element Not Found	Required property or content element {0} not found	Error	
BCGEDIVA0992	No Message Properties Found	No message properties found	Error	
BCGEDIVA0993	Metadata Not Found	Metadata not found, dictionary = {0}, document type = {1}, syntax = {2}	Error	
BCGEDIVA0994	Empty Transaction Set or Message	EDI transaction set or message is empty	Error	
BCGEDIVA0995	Fatal Parser Error	Fatal parser error encountered	Error	
BCGEDIVA0997	Unknown Flow Direction	Unknown flow direction {0} specified	Error	
BCGEDIVA0998	Unsupported Syntax Type	Unsupported syntax type {0} specified	Error	
BCGEDIVA0999	Unknown Object Received	Unknown object of type {0} received	Error	

Appendix C. Component-specific property files

The Console, Receiver, and Document Manager components each contain component-specific property files. The following tables list all of the basic runtime properties for each component:

- Console-specific properties - Table 31
- Receiver-specific properties - Table 32 on page 120
- Receiver-was logging properties - Table 33 on page 124
- Router-specific properties - Table 34 on page 125
- Router-was logging properties - Table 35 on page 134

Table 31. bcg_console.properties file contents (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	6..0.0	Version #	Text string used for informational purposes
## DB Proc Audit Debug level ## 0 = off, 1 = on			
ibm.bcg.db.debugLevel	0	0,1	Turns database debugging on and off
########## Start log4j Debug Properties ################## # Log4J Debug Properties # Possible Categories - debug/info/warn/error/fatal # Default Category "error", Output to: stdout and RollingFile			
log4j.rootCategory	error, stdout, RollingFile	All, Off, debug, info, warn, error, fatal	Root logging setting for all containers. Logging can be switched off completely by setting log4j.rootCategory=OFF.
log4j.appender.stdout	org.apache.log4j. FileAppender		Logging java class using for Log4J libraries
log4j.appender.stdout.File	System.out		
log4j.appender.stdout.layout	org.apache.log4j. PatternLayout		Logging java class using for Log4J libraries
`log4j.appender.stdout.layout. ConversionPattern`	%d{ABSOLUTE} %c{1} [%t] - %m%n		Logging pattern for log file
`log4j.appender.RollingFile`	org.apache.log4j. RollingFile Appender		Logging java class using for Log4J libraries

Table 31. bcg_console.properties file contents (Console-specific properties) (continued)

Entry	Default value	Possible setting	Description
log4j.appender.RollingFile.File	{INSTALL DIR}/ was/profiles/ bcgconsole/logs/ bcgconsole/ bcg_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.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.Wsn InitialContext Factory		JNDI Context Factory
ibm.bcg.appserver. jndiContextProviderURL	corbaloc:iiop: localhost:52809		JNDI Provider URL
ibm.bcg.appserver.jdbcJndiPool	$CONSOLE .JNDI$	datasources/DB2 DS,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			

Table 31. bcg_console.properties file contents (Console-specific properties) (continued)

Entry	Default value	Possible setting	Description
ibm.bcg.jmsPosterInstance	com.ibm.bcg.shared.event.MQSeriesPoster		
## JMS Properties for Event Posting ## JNDI Provider URL			
ibm.bcg.jms_cntxt_url	{INSTALL DIR}/console/lib/config/jndi		Location of .binding file, used for JMS information
ibm.bcg.jms_jndi_factory	com.sun.jndi.fscontext.RefFSContext Factory		
## Connection Factory Names			
ibm.bcg.jms.qconnFactory.name	WBIC/QCF		JMS Queue Connection Factory Name
ibm.bcg.jms.topicconnFactory.name	WBIC/TCF		JMS Topic Connection Factory Name
ibm.bcg.jms.queue.name	WBIC/datalogQ		JMS Queue Name
## Gateway Queue			
ibm.bcg.outbound.gatewayDirectory	$SHARED_DATA_DIR$/gateways		Gateway Directory
## VTP			
ibm.bcg.certs.vtp.CertificateDir	$SHARED_DATA_DIR$/security/certs		Location of Client Certificates for use w/ VTP If the value is not provided correctly, it will throw an error in the Console_SystemErr.log. This error will not affect the flow and can be treated as warning.
ibm.bcg.certs.vtp.Certificate			VTP Public Key (DER, binary format)
ibm.bcg.certs.vtp.PrivateKey			VTP Private Key (pkcs8, binary format)
ibm.bcg.certs.vtp.Passwd			VTP Private Key Password
ibm.bcg.certs.vtp.VerifySig	FALSE	true, false	Determine whether the VTP should verify signer or not (true, false)
ibm.bcg.vtp.RouterIn	$SHARED_DATA_DIR$/router_in		Router In directory
## EAI Directory Management			
ibm.bcg.EAIDocDir	Documents		This provides the console with the name of the EAI directory used by the router

Table 31. bcg_console.properties file contents (Console-specific properties) (continued)

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 32. bcg_receiver.properties file contents (Receiver-specific properties)

Entry	Default value	Possible settings	Description
###### Set this so bcg.prperties logging settings are ignored!!			
bcg.use_container_logging	TRUE	true, false	
############ BCG DB ##			
bcg.co.db.DBType	$RECEIVER.DB.TYPE$	db2,oracle	Database type
bcg.co.db.DBPoolName	$RECEIVER.JNDI$	datasources/DB2DS, datasources/Oracle Pool	Datasource JNDI Prefix
bcg.co.jndiContextURL	corbaloc:iiop:localhost:57809		JNDI Provider URL
bcg.co.jndiFactory	com.ibm.websphere.naming.WsnInitialContextFactory		JNDI Context Factory
bcg.co.db.schema	$RECEIVER.DB.SID$		schema information (DB2 - Database Owner, Oracle - Schema Owner)
############ MQ PROPS			
bcg.use_oaq	FALSE	true, false	
bcg.jms.queue.factory	WBIC/QCF		JMS Queue Connection Factory Name
bcg.jms.topic.factory	WBIC/TCF		JMS Topic Connection Factory Name
bcg.jms.jndi_factory	com.sun.jndi.fscontext.RefFSContextFactory		Class used to connect to the JNDI server
bcg.jms.context_url	{INSTALL DIR}/receiver/lib/config/jndi		Location of .binding file, used for JMS information

Table 32. bcg_receiver.properties file contents (Receiver-specific properties) (continued)

Entry	Default value	Possible settings	Description
########## BPE			
bcg.oaq_log_q	WBIC/datalogQ		JMS Queue Name
########## RECEIVER MBEAN			
bcg.vms_receiver_reject_dir	$SHARED_DATA _DIR$/receiver /reject		File system path where the Receiver puts rejected messages
bcg.vms_receiver_tmp_dir	$SHARED_DATA _DIR$/receiver /tmp		File system path where the Receiver puts temporary messages
########## END RECEIVER MBEAN			
bcg.receiver.persistpath	$SHARED_DATA _DIR$/router_in/		File system path where the Receiver persists inbound RosettaNet signals.
bcg.receiver.sync.persistpath	$SHARED_DATA _DIR$/sync_in		File system path where the Receiver persists Synchronous RosettaNet signals.
bcg.receiver.sync.sync CheckClasses	com.ibm.bcg. server.sync. SyncRosettaNet Request|com.ibm .bcg.server.sync. SyncAS2Request| com.ibm.bcg. server.sync.Sync SOAPRequest| com.ibm.bcg. server.sync.Sync cXMLRequest		
bcg.receiver.sync.responseURL	/bcgreceiver/ SyncResponse		URI to post Synchronous Responses
bcg.receiver.sync. responseURL.port	$RECEIVER _HTTP_PORT$		HTTP Port for Receiver
## Servlet properties ## HTTP headers to be persisted as meta-data by the receiver servlet. ## All properties beginning with "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

Table 32. bcg_receiver.properties file contents (Receiver-specific properties) (continued)

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

Table 32. bcg_receiver.properties file contents (Receiver-specific properties) (continued)

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

Table 33. receiver-was.logging.properties file contents

Entry	Default value	Possible setting	Description
########## Start log4j Debug Properties ################## # Possible Categories - debug/info/warn/error/fatal # Default Category "error", Output to: stdout and RollingFile			
log4j.rootCategory	error, stdout, RollingFile	All, Off, debug, info, warn, error, fatal	Root logging setting for all containers. Logging can be switched off completely by setting log4j.rootCategory=OFF.
log4j.appender.stdout	org.apache.log4j.ConsoleAppender		Logging java class using for Log4J libraries
log4j.appender.stdout.layout	org.apache.log4j.PatternLayout		Logging java class using for Log4J libraries
# Pattern to output the caller's file name and line number.			
`log4j.appender.stdout.layout.ConversionPattern`	%d{DATE} %-5p [%c{1}] [%t] - %m%n		Logging pattern for log file
`log4j.appender.RollingFile`	org.apache.log4j.RollingFile Appender		Logging java class using for Log4J libraries
# Log File Name			
`log4j.appender.RollingFile.File`	{INSTALL DIR}/was/profiles/bcgreceiver/logs bcgreceiver/bcg_receiver.log		Rolling log file name and path
`log4j.appender.RollingFile.MaxFileSize`	1000KB		Maximum size of log file before being rolled.
# number of backup files to keep			
`log4j.appender.RollingFile.MaxBackupIndex`	10		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} %-5p [%c{1}] [%t] - %m%n		Logging pattern for log file
log4j.category.com.ibm.bcg.util.threadPool	error		
#log4j.category.com.ibm.bcg.server.util	debug		
#log4j.category.com.ibm.bcg.server	debug		
log4j.category.com.ibm.bcg.co.db	error		

Table 34. bcg.properties (Router-specific properties)

Entry	Default value	Possible settings	Description
###### Set this so properties logging settings are ignored!!			
bcg.use_container_ logging	TRUE	true, false	
############ Third party duns #####	105217165		
bcg.duns			
############ BCG DB ##			
bcg.co.db.DBType	$ROUTER.DB. TYPE$	db2,oracle	Database type
bcg.co.db.DBPoolName	$ROUTER.JNDI$	datasources/DB2 DS,datasources /OraclePool	Datasource JNDI Prefix
bcg.co.jndiContextURL	corbaloc:iiop: localhost:56809		JNDI Provider URL
bcg.co.jndiFactory	com.ibm. websphere. naming. WsnInitialContext Factory		JNDI Context Factory
bcg.co.db.schema	$ROUTER.DB. SID$		schema information (DB2 - Database Owner, Oracle - Schema Owner)
############ MQ PROPS			
bcg.use_oaq	FALSE	true, false	
bcg.jms.queue.factory	WBIC/QCF		JMS Queue Connection Factory Name
bcg.jms.topic.factory	WBIC/TCF		JMS Topic Connection Factory Name
bcg.jms.jndi_factory	com.sun.jndi. fscontext.RefFS ContextFactory		Class used to connect to the JNDI server
bcg.jms.context_url	{INSTALL DIR}/ router/lib/ config/jndi		Location of .binding file, used for JMS information
########## BPE ##########			
bcg.oaq_log_q	WBIC/datalogQ		JMS Log Receiver Queue Name
# Maximum File Size Supported by Document Manager # in bytes. ex. 52000000 = 52MB. 0 = no limit.			
bcg.bpe_max_file_size	0		Max filesize (in bytes)
## MAIN RTR ##			
bcg.oaq_bpe_in.main	WBIC/main_ InboundQ		JMS Main In Queue Name
bcg.oaq_bpe_out.main	WBIC/delivery ManagerQ		JMS Delivery Manager Queue Name

Table 34. bcg.properties (Router-specific properties) (continued)

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/delivery ManagerQ		JMS Delivery Manager Queue Name
bcg.inbound_poll_interval.signal	1000		Time in milliseconds for each directory scan
bcg.inbound_files_per_pass.signal	5		Max files to pick up per scan
bcg.in_thread_count.signal	2		Number of Inbound threads for Signal Router
bcg.bpe_thread_count.signal	2		Number of BPE threads for Signal Router
bcg.vms_inbound_directory.signal	$SHARED_DATA _DIR$/signal_in		Signal Router inbound directory
bcg.bpe_temp_directory.signal	$SHARED_DATA _DIR$/data		Signal Router data directory
## SYNCHRONOUS RTR ##			
bcg.oaq_bpe_in.synchronous	WBIC/sync _InboundQ		JMS Synchronous In Queue Name
bcg.oaq_bpe_out.synchronous	WBIC/delivery ManagerQ		JMS Delivery Manager Queue Name
bcg.inbound_poll_interval. synchronous	1000		Time in milliseconds for each directory scan
bcg.inbound_files_per_pass. synchronous	5		Max files to pick up per scan
bcg.in_thread_count.synchronous	2		Number of Inbound threads for Synchronous Router
bcg.bpe_thread_count.synchronous	2		Number of BPE threads for Synchronous Router
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 ##			

Table 34. bcg.properties (Router-specific properties) (continued)

Entry	Default value	Possible settings	Description
bcg.destination.destination_class	com.ibm.bcg.destination.H2 Destination Process		Destination Class
### RECEIVER MBEAN ###			
bcg.vms_receiver_reject_dir	$SHARED_DATA_DIR$/receiver/reject		File system path where the Receiver puts rejected messages
bcg.vms_receiver_tmp_dir	$SHARED_DATA_DIR$/receiver/tmp		File system path where the Receiver puts temporary messages
### DUPLICATE ###			
bcg.duplicate.DupField1	x-aux-system -msg-id		
bcg.duplicate.DupField2	none		
bcg.duplicate.DupField3	none		
bcg.duplicate.DupField4	none		
bcg.duplicate.DupField5	none		
bcg.duplicate.DupField6	none		
bcg.duplicate.DupField7	none		
bcg.duplicate.DupField8	none		
bcg.duplicate.DupField9	none		
bcg.duplicate.DupField10	none		
### LogReceiver ###			
bcg.logReceiver.queue	WBIC/datalogQ		JMS Log Receiver Queue Name
bcg.logReceiver.initial NumberOfReceivers	4		Number of Log Receivers
bcg.dberrors.queue	WBIC/datalog ErrorQ		JMS Log Receiver Errors Queue Name
### Alert Engine ###			
bcg.alertQueue.queue	WBIC/alertQ		JMS Alert Queue Name
bcg.alertQReceiver.initial NumberOfReceivers	1		Number of Alert Receivers
bcg.alertQReceiver.maxRetries	100		Max Alert Retries
bcg.alertQReceiver.retryInterval	60000		Alert retry interval in milliseconds
bcg.eventAlertQReceiver.queue	WBIC/alert EventQ		JMS Alert Event Queue Name
bcg.eventAlertQReceiver. initialNumberOfReceivers\	1		Number of Alert Event Receivers
# Allow this much time after the volume alert end time to record that the doc # was received in our system, before evaluating the alert:			

Table 34. bcg.properties (Router-specific properties) (continued)

Entry	Default value	Possible settings	Description
bcg.volumeAlertScheduler.allowance ForProcessingReceivedDocInMins	10		
# These parameters avoid excessive email notifications. If there are more than 'maxNotificationsInInterval' # in the time interval 'maxNotificationIntervalInMins' for the same alert, alerts are held and batched every # 'heldAlertsBatchTimeInMins' until no alerts of that type are received for 'minNotificationQuietInterval InMins':			
bcg.alertNotifications. maxNotificationsInInterval	10		
bcg.alertNotifications. maxNotificationIntervalInMins	30		
bcg.alertNotifications. minNotificationQuietInterval InMins	30		
bcg.alertNotifications. heldAlertsBatchTimeInMin	30		
# Notifications that are returned because of e.g. invalid partner email addresses will go # to bcg.alertNotifications. mailEnvelopeFrom.			
bcg.alertNotifications. mailHost	$ROUTER.ALERT S.SMTP_RELAY$		SMTP Relay Host
bcg.alertNotifications. mailFrom	$ROUTER.ALERT S.MAIL_FROM$		Alerts ″from″ mail address
bcg.alertNotifications. mailReplyTo	$ROUTER.ALERT S.MAIL_FROM$		Alerts ″from″ mail address
bcg.alertNotifications. mailEnvelopeFrom	$ROUTER.ALERT S.MAIL_FROM$		Alerts ″from″ mail address
# time for running cert expiration event generator # <minutes> <hour> <class name> # this runs at 1:13 am:			
alert.eventGenerator.schedule	13 1 Certificate Expiration		
### Delivery Manager ###			
bcg.delivery.gatewayDirectory	$SHARED_DATA _DIR$/gateways		Location of Gateways directory
bcg.delivery.smtpHost	$ROUTER.DM. SMTP_RELAY$		SMTP Mail host

Table 34. bcg.properties (Router-specific properties) (continued)

Entry	Default value	Possible settings	Description
bcg.delivery.smtpHostPort	$ROUTER.DM. SMTP_RELAY. PORT$		SMTP Mail port
bcg.delivery.responseDir	$SHARED_DATA _DIR$/sync_in		Location of Synchronous directory
bcg.delivery.msMaxFileLockLife	180000		Max time for a file to be locked in milliseconds
bcg.delivery.threadPoolMaxThreads	50		
bcg.delivery.gatewayMaxThreads	20		Max Gateway threads
bcg.delivery.gwTransportMaxRetries	3		Number of Retries per gateway
# in millisecs, applies to all gateways			
bcg.delivery.gwTransport RetryInterval	3000		Gateway retry interval in milliseconds
bcg.delivery.queue	WBIC/delivery ManagerQ		JMS Delivery Manager Queue Name
bcg.deliveryQReceiver. initialNumberOfReceivers	10		Number of Gateway receivers
bcg.delivery.numberOfLoggers	10		
# sync response delivery to Response Servlet			
bcg.syncdelivery.queue	WBIC/sync DeliveryManagerQ		JMS Synchronous Delivery Manager Queue Name
bcg.syncdeliveryQReceiver. initialNumberOfReceivers	3		Number of Synchronous Delivery Manager receivers
#bcg.deliveryQReceiver.jmsLog	jms.log		
bcg.delivery.jmstimeout	60000		
# socket timeout for posting in ms			
bcg.http.socketTimeout	120000		HTTP Socket Timeout
bcg.http.version	1.1	1.0,1.1	HTTP Version
### RosettaNet ###			
bcg.rosettanet.retryWaitTmMS	5000		
bcg.rosettanet.strictBoundaryParse	FALSE	true,false	
bcg.rosettanet.mimeBoundaryValidate	FALSE	true,false	
## If property exists and = ″Literal″, we expect the x-aux-production to ## literally be ″Production″, ″Test″. If property doesn’t exist or not ## equal to ″Literal″, we expect the x-aux-production to be ″True″ or ″False″. ## All values are case insensitive.			
bcg.rosettanet.globalUsageCode	Literal	Literal, Production,Test	

Table 34. bcg.properties (Router-specific properties) (continued)

Entry	Default value	Possible settings	Description
## 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 rosettanet.defaultGlbUsageCd.			
bcg.rosettanet.default UsageCdOnErr	1		
bcg.rosettanet.defaultGlbUsageCd	Production	Production,Test	
## If property exist and equals '1', we expect the builder to provide ## x-aux-process-instance-id to be used as the process instance id an ## outbound request.			
bcg.rosettanet.useBuilder ProcessInstanceId	1		
## If builder provided process-instance-id is invalid (for whatever reason), we ## can generate a new process-instance-id.			
bcg.rosettanet.genProcess InstanceIdOnError	1		
################			
bcg.receiver.persistpath	$SHARED_DATA _DIR$/router_in/		
### RNE ###			
bcg.rne.inbound_poll_interval	1000		RosettaNet Engine poll interval in milliseconds
bcg.rne.in_thread_count	2		RosettaNet Engine Threadcount
bcg.rne.work_size	50		
bcg.0A1.fromContactName	$ROUTER. CONTACT_ NAME$		0A1 Contact Name
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.SSLDebug	FALSE	true,false	

Table 34. bcg.properties (Router-specific properties) (continued)

Entry	Default value	Possible settings	Description
## Digital signature related properties			
# Possible values: SHA1,MD5			
bcg.rosettanet.signature. DigestAlgorithm	SHA1	sha1,md5	This algorithm is used to generate Message Digest. **Note:** This Property is applicable to all protocols.
# Possible values: true, false			
bcg.rosettanet.signature. RejectIfFailVal	TRUE	true, false	
# Possible values: true, false			
bcg.rosettanet.signature. VerifySigner	TRUE	true, false	This property is used to verify Signer. **Note:** This Property is applicable to all protocols.
## Encryption properties			
bcg.CRLDir	$SHARED_DATA _DIR$/security /crl/		Path to CRL directory
bcg.rosettanet.encrypt. CertDbRefreshInterval	600000		The CRLs and the VTP certificates will be reloaded after the specified mili seconds. **Note:** This Property is applicable to all protocols.
# valid values: 3des, rc2-40			
bcg.rosettanet.encrypt.Algorithm	3des	3des, des, aes, rc2-40	Specifies the algorithm used to encrypt Messages. **Note:** This Property is applicable to all protocols.
# 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 ″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

Table 34. bcg.properties (Router-specific properties) (continued)

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

Table 34. bcg.properties (Router-specific properties) (continued)

Entry	Default value	Possible settings	Description
bcg.http.hdrdef.mimeVersion	Mime-Version		HTTP header persisted in metadata file for the BPE to process
bcg.http.hdrdef.messageId	Message-ID		HTTP header persisted in metadata file for the BPE to process
bcg.http.hdrdef.date	Date		HTTP header persisted in metadata file for the BPE to process
bcg.http.hdrdef.from	From		HTTP header persisted in metadata file for the BPE to process
bcg.http.hdrdef.subject	Subject		HTTP header persisted in metadata file for the BPE to process
bcg.http.hdrdef.content TransferEncoding	Content-Transfer-Encoding		HTTP header persisted in metadata file for the BPE to process
bcg.http.hdrdef.contentDisposition	Content-Disposition		HTTP header persisted in metadata file for the BPE to process
bcg.http.hdrdef.disposition NotificationTo	Disposition-Notification-To		HTTP header persisted in metadata file for the BPE to process
bcg.http.hdrdef.disposition NotificationOptions	Disposition-Notification-Options		HTTP header persisted in metadata file for the BPE to process
bcg.http.hdrdef.receipt DeliveryOption	Receipt-Delivery-Option		HTTP header persisted in metadata file for the BPE to process
bcg.http.hdrdef.toPackagingName	ToPackaging Name		HTTP header persisted in metadata file for the BPE to process
bcg.http.hdrdef.asDocType	ASDocType		HTTP header persisted in metadata file for the BPE to process
# Packaging related properties # Attachments with one of the following content types will not be base64 encoded			
bcg.pkg.sponsor.contenttypes	bcg.pkg.sponsor. contenttypes		
### START of SPONSOR ENGINE ###			
bcg.sponsor.inbound_poll_interval	10000		
bcg.sponsor.in_thread_count	2		Number of Inbound threads for Sponsor Engine
bcg.sponsor.work_size	10		

Table 34. bcg.properties (Router-specific properties) (continued)

Entry	Default value	Possible settings	Description
bcg.delivery.sponsor.eventMsgClass	com.ibm.bcg.delivery.sponsor.SponsorEventMessage		
### DB proc debug properties###			
DBProcDebug	1		Database debugging flag
# Global State engines instance ID			
GlobalStateEngInstanceId	bcg		
# Possible non rep values#			
bcg.nonrep.inbound-doc	true	true,false	To enable non-repudiation for incoming documents
bcg.nonrep.outbound-doc	true	true,false	To enable non-repudiation for outgoing documents
# Possible Values 1.0 or 1.1#			
wbipackaging_version = 1.0	1.0	1.0,1.1	For Backend Integration XML packaging transport envelope. Version 1.0 is for version 4.2.2 FP1 and earlier. Version 1.1 is for 4.2.2 FP2 and later. Version 1.1 contains the content ID associated with attachments.
#ITLM Required Jar Files#			
bcg.ITLMJar={INSTALLDIR}/router/lib/support/ITLMToolkit.jar			Required for licensing support.
bcg.logJar={INSTALLDIR}/router/lib/support/jlog.jar			Required for licensing support.

Table 35. router-was.logging.properties file contents

Entry	Default value	Possible setting	Description
########## Start log4j Debug Properties ################## # Possible Categories - debug/info/warn/error/fatal # Default Category "error", Output to: stdout and RollingFile		debug/info/warn error/fatal	
log4j.rootCategory	error, stdout, RollingFile	All, Off, debug, info, warn, error, fatal	Root logging setting for all containers. Logging can be switched off completely by setting log4j.rootCategory=OFF.
log4j.appender.stdout	org.apache.log4j.ConsoleAppender		Logging java class using for Log4J libraries
log4j.appender.stdout.layout	org.apache.log4j.PatternLayout		Logging java class using for Log4J libraries
# Pattern to output the caller's file name and line number.			

Table 35. router-was.logging.properties file contents (continued)

Entry	Default value	Possible setting	Description
`log4j.appender.stdout.layout.ConversionPattern`	%d{DATE} %-5p [%c{1}] [%t] - %m%n		Logging pattern for log file
`log4j.appender.RollingFile`	org.apache.log4j.RollingFile Appender		Logging java class using for Log4J libraries
# Log File Name			
`log4j.appender.RollingFile.File`	{INSTALL DIR}/was/profiles/bcgdocmgr/logs/bcgdocmgr/bcg_router.log		Rolling log file name and path
`log4j.appender.RollingFile.MaxFileSize`	50000KB		Maximum size of log file before being rolled.
# number of backup files to keep			
`log4j.appender.RollingFile.MaxBackupIndex`	10		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} %-5p [%c{1}] [%t] - %m%n		Logging pattern for log file
log4j.category.com.ibm.bcg.co.db	error		
#### Added to suppress the generation of unnecessary timing events			
#log4j.category.com.ibm.bcg.timing	error		

Notices

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

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

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

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

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

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

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

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

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

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

Burlingame, CA 94010
U.S.A

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

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

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

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

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

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

COPYRIGHT LICENSE

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

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

COPYRIGHT AND PERMISSION NOTICE

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

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

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

Programming interface information

Programming interface information, if provided, is intended to help you create application software using this program. General-use programming interfaces allow you to write application software that obtain the services of this program's tools. However, this information may also contain diagnosis, modification, and tuning information. Diagnosis, modification and tuning information is provided to help you debug your application software.

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

Trademarks and service marks

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

i5/OS
IBM
the IBM logo
AIX
CICS
CrossWorlds
DB2
DB2 Universal Database
Domino
IMS
Informix
iSeries
Lotus
Lotus Notes
MQIntegrator

MQSeries
MVS
OS/400
Passport Advantage
SupportPac
WebSphere
z/OS

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

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

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

Linux is a trademark of Linus Torvalds in the United States, other countries, or both.

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

WebSphere Partner Gateway Enterprise and Advanced Editions Version 6.0.

Index

E

G

H

I

L

M

N

W

X

Printed in USA