

WebSphere IBM WebSphere Partner Gateway Enterprise and Advanced
Editions
Version 6.2.1

Administration Guide

IBM

Note

Before using this information and the product it supports, read the information in "Notices" on page 255.

February 2011

This edition applies to version 6, release 2, modification 1 of IBM WebSphere Partner Gateway Enterprise Edition (product number 5724-L69) and version 6, release 2, modification 1 of Advanced Edition (product number 5724-L68) and to all subsequent releases and modifications until otherwise indicated in new editions.

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.

© Copyright IBM Corporation 2010, 2011.

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

Contents

Chapter 1. About this book 1

Audience	1
Roles, access levels, and responsibilities	1
Typographic conventions	2
Related documents	3
New in release 6.2.1	3

Chapter 2. Managing the WebSphere Partner Gateway component applications 5

Managing WebSphere Partner Gateway components in a simple mode system	5
Managing WebSphere Partner Gateway components in a distributed mode system	6
The Deployment Manager	7
Starting and stopping servers from the command line	8
Starting and stopping FTP Management Server from command line	8
Starting and stopping SFTP Management Server from command line	9
Starting and stopping the components in a simple distributed mode system	9
Starting servers in a simple distributed mode system	9
Stopping servers in a simple distributed mode system	10
Starting and stopping the components in a full distributed mode system	11
Starting servers in a full distributed mode system	12
Stopping servers in a full distributed mode system	13

Chapter 3. Basic Community Console tasks 15

Logging in to the Community Console	15
Navigating through the Community Console	16
Community Console icons	16
Logging off from the Community Console	18

Chapter 4. Hub administration tasks . . 19

Managing password policy	19
Changing database connectivity, database user and password	20
Managing event codes	20
Viewing and editing event codes	21
Exporting event code names	21
Specifying events that can be notified	22
Document Validation Errors	22
Managing receivers	22
Viewing and editing receiver details	22
Enabling or disabling receivers	22
Deleting receivers	23
Localizing HTTP synchronous target time out	23

Managing interactions and document definitions	23
Managing XML formats	24
Large file support	25
Enabling or disabling actions	25
Managing handlers	25
Importing a handler	26
Deleting a handler	26
Configuring the content-type attribute in handlers	26
Managing maps	27
Updating validation maps	27
Viewing validation maps Where used	27
Deleting validation maps	27
Managing transformation maps	27
Managing EDI FA maps	28
Managing EDI	28
Envelope profile	28
Enveloper	29
Connection profiles	30
Control number initialization	30
Current control numbers	31
Managing system configuration data	32
Configuring the alert mail server	33
Viewing system activity	33
Managing event delivery	34
Managing API calls	34
Managing Document Manager information	35
Maximum hold time	35
Maximum files-per-poll-interval	35
Supporting ebMS	36
Uploading a CPA to WebSphere Partner Gateway	36
Non-prepopulated attributes	37
Algorithms supported by the ebMS	38
Configuration details for validating Webservices	38
Using non-repudiation logging	39
Using message store	39
Prerequisite to setup WebSphere Partner Gateway - WebSphere Transformation Extender Integration Environment	40

Chapter 5. Account administration tasks 43

Managing partner profiles	43
Viewing and editing partner profiles	43
Searching for partners	43
Deleting partners	44
Managing destination configurations	44
Required information for destination configuration	44
Viewing and editing destinations	45
Viewing and editing default destination	47
Viewing destination Where used	47
Deleting destination	47
Uploading transports	48
Deleting transports	48

Transport and destination retries	48
Forward proxy support	51
Managing certificates	51
Configuring the certpath related properties	53
Viewing and editing digital certificates	54
Disabling a digital certificate	55
Changing B2B attribute values	55
Managing partner connections	56
Connection components	56
Connection duplication	57
Searching for connections	57
Changing connection configurations	59
Managing exclusion lists	61
Adding partners to the exclusion list	61
Editing the exclusion list	61

Chapter 6. Administering partner migration. 63

Using the migration utility from the command line	63
Invoking from the command line	66
Mapping of XML element with Console	67
Exporting partner migration	70
Considerations when creating your own import data	71
Manual validation of the import file	71
Migration configuration type dependencies	71
Export/Import order	74
BCG and DIS Import	75
Non-migratable configurations	75
Limitations of the migration utilities	75
Forward proxy migration	75

Chapter 7. LDAP support for logon authentication 77

Using LDAP	77
Enabling the container managed authentication mechanism	77
Enabling J2EE security	77
User names and groups	78
Stopping the use of LDAP authentication	78
Sample LDAP configuration	79
Configuring the WebSphere Application Server for the standalone IBM Tivoli Directory Server	79
Specifying LDAP users to use the WebSphere Partner Gateway Console	81

Chapter 8. Support for IPv6 83

Enabling tunneling IPv6 over IPv4	83
RHEL Linux 3	83
Windows 2003/XP	83
HP-UX 11i	84
Enabling IPV6	84
Configuring attributes	85

Chapter 9. Managing the Destination Queue 87

Viewing the Destination Queue	87
Viewing queued documents	88
Stopping the processing of documents from the destination queue	89

Viewing destination details	90
Changing destination status	90

Chapter 10. Analyzing document flows 91

Document Analysis tool	91
Viewing the state of documents in the system	92
Viewing documents in the system	92
Viewing process and event details	93
Document Volume Report	93
Creating a Document Volume Report	93
Exporting the Document Volume Report	94
Printing reports	94
Test Partner Connection	94
Pinging ebMS partners	95
Web Server result codes	95
EDI Reports	98
EDI FA Overdue Search	98
EDI Rejected Transaction Search	99
FTP Reports	100
Statistics	101
Connections	101

Chapter 11. Viewing events and documents 103

Event Viewer	103
Event types	104
Searching for events	104
Viewing event details	105
Error events	105
AS Viewer	106
Searching for messages	107
Viewing message details	108
RosettaNet Viewer	109
Searching for RosettaNet processes	109
Viewing RosettaNet process details	110
Viewing raw documents	111
Document Viewer	111
Searching for documents	111
Viewing document details, events, and raw documents	113
Mass document resend	114
Viewing EDI documents	115
Document Validation Errors	116
Viewing data validation errors	117
Stopping a document that is in process	118
Re-sending failed and successful documents	118
ebMS Viewer	120
Searching for ebMS processes	120
Viewing ebMS process details	121
Viewing raw documents	121
Requesting and viewing the status of a document	122
Destination Queue	122

Chapter 12. Simulating production traffic 123

Preparing to test	124
Setting up test scenarios	124
Sample scenarios	125

Uploading and viewing your requests and responses	127
Initiating and viewing document type	127
Searching for an open document	128
Responding to an open document	128
Removing an open document	129
Chapter 13. Archiving	131
Archiver configuration	131
View archiver task.	131
Archiver task modification	133
Export and Import of archiver configuration	134
Archiver runtime tasks	134
Archiver reports	135
Archiver Restore	137
Restoring archived data of WebSphere Partner Gateway V6.1 and earlier	138
Searching the restored documents	138
User intervention for archiving	139
Archiver Restrictions	140
Chapter 14. Using logging and tracing features	141
Log and trace files.	141
Log file management	142
Trace file management	143
Configuring tracing in a simple mode system	144
Setting tracing in a distributed mode system	144
Tracing tasks common to both types of systems	145
Setting log detail levels	146
Identifying WebSphere Partner Gateway trace messages	147
EDI, XML, ROD subcomponent tracing.	147
Interpreting WebSphere Application Server log and trace messages	148
WebSphere Application Server event types	148
Integrated FTP Server logging.	148
Integrated SFTP Server logging	149
Chapter 15. FTP and SFTP Server Configuration Management	151
FTP and SFTP user management	151
Chapter 16. Relocation and Redeployment of WebSphere Partner Gateway	153
Prerequisites.	153
Restoring the configuration details	154
Changing host name and IP address of WebSphere Partner Gateway	154
Changing the host name and port number of database	155
Changing the port numbers	155
Relocation and redeployment examples.	156
Chapter 17. Troubleshooting	159
Avoiding long processing time on large encrypted AS documents	160

Avoiding long processing time for large encrypted documents	161
Avoiding out-of-memory errors	161
Document Manager memory configuration	161
Document Manager workload	162
Document structure	162
Increasing the heap size	162
Collating data for multiple languages	162
Ensuring sufficient virtual memory for DB2 agents	163
Fixing DB2 SQL errors	163
SQLCODE -444 error	164
SQLCODE -289 error	164
SQLCODE -1225 error	164
SQL 0964C Transaction log full error on the BCGMAS database	164
IBM service log unreadable.	165
WebSphere Application Server informational messages	165
Increasing the Receiver timeout setting	165
Optimizing database query performance	166
Resolving event 210031	166
Documents routed twice when network is lost or document manager server shutdown abruptly	167
0A1 generated with data validation errors.	167
EDI reports export the first 1000 records only	167
Console does not start after a server restart	167
FTPScripting Receiver receives StringIndexOutOfBoundsException	168
Error scenario	168
Working scenario	168
Receiver Failure to read Configuration File	168
Configuring Users to receiving Alerts Notification	168
Resolving ClassNotFoundException for User Exit classes.	169
Reprocessing events and business documents that fail to log to the database	169
Disabling JIT in a WebSphere Application Server when WebSphere Partner Gateway produces a javacore	170
Defining a custom transport type.	170
Resolving WebSphere Partner Gateway errors BCG210031 and BCG240415	170
Creating File directory destination on a drive other than C:	171
Preventing partner transactions from being processed by WebSphere Partner Gateway.	171
Fixing the browser ERROR: 500	172
Downloading CRL for SSL transactions.	172
Databinding in JMS Exports/Imports within WebSphere Process Server	173
Fixing test partner connection for SSL connections	174
Fixing errors BCGEDIEV0056 and BCG210001	174
Fixing ORA-00988 error	174
Configuring Content-Types attribute for the fixed workflow handlers	174
Fixing BCG210013 error	175
Increasing buffer size to prevent document transmission low performance.	176
WebSphere Partner Gateway hub installer logs error messages	176
DB password required error in bcgHubInstall.log	177

Using revocation check and using CRL DP support	177
Returning document volume report search information about the console	177
Loading the native library	178
Fixing error TCPC0003E and CHF0029E.	178
CA certificate expiration.	179
VBaseException in the SystemOut.log.	180
Reporting file size for documents greater than 2 GB	180
SSL handshake fails because no certificate received	180
Fixing the hanging threads warning.	181
Stopping the Document Manager exception	181
Fixing WebSphere MQ messages	182
MQJMS2007 error	182
MQJMS2013 error	183
java.security.InvalidKeyException: Illegal key size or default parameter	183
The MDN status of 'unknown' for AS transactions	183
Servers fail to start after applying fixes	183
Correcting the shortcut ports for WebSphere Application Server	184
Avoiding duplicate document delivery when there is more than one router	184
Rendering of tab headings on displays with resolution greater than 1024	185
Documents not processed when using Oracle 9i Release 2	185
Document processing when the database goes down	185
java.lang.NoClassDefFoundError with reprocessDbLoggingErrors.bat	186
Recovery process when queue and disk is full or unavailable	186

Workflow Handler Runtime Error	186
Error while invoking WebSphere Transformation Extender Map	187
IBM Support Assistant (ISA) Plugin	187
Partner Migration Utility with LDAP	187
AS signature failure for interop content type	188

Appendix A - performance considerations 189

Managing queue overflow	189
Generating summary data	189

Appendix B - failed events. 191

Appendix C - component-specific system attributes. 225

Configuring attributes as WebSphere Application Server ND environment variables	225
Editing RosettaNet attribute values	225
Editing FTP Administration	226
Editing SFTP Administration	230
Attribute tables.	230

Notices 255

Programming interface information	257
Trademarks and service marks	257

Index 259

Chapter 1. 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 *WebSphere Partner Gateway Hub Configuration Guide*.

Audience

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

- **Hub administrator:** is the super user in the community. The hub administrator is responsible for overall hub community configuration and management, including partner configuration and connection activation.
- **Account administrator:** has access to a subset of the hub administrator features and is the main administrative user for the internal partner or external partner.
- **Internal Partner:** is the primary company and driving force within the hub community. Internal partner is responsible for the purchase and creation of the hub community. In addition, the internal partner provides the definition of the electronic business process transactions that happen between them and their external partners.
- **External Partner:** is the company that does business with the internal partner through the hub community. External partners have to complete a configuration process to connect to the hub community. Once connected, external partners can exchange electronic business documents with the internal partner.

Refer to *WebSphere Partner Gateway Partner Guide* for more information on hub administrator, internal partner, and external partner.

Roles, access levels, and responsibilities

In WebSphere Partner Gateway, the hub administrator sets up the profiles of the partners. A partner always has at least one administrator user and can have additional users added by the administrator of that profile.

To illustrate the concept of roles, a simple implementation of WebSphere Partner Gateway with a minimum of three profiles is described as follows:

Hub Operator

This is a system defined profile that will be included on the machine during installation. The Hub Operator profile has one defined user name, hubadmin, which is the super-user of the system and can accomplish any configuration task. You can relate this role to the IT group that runs the actual WebSphere Partner Gateway server, but is not actively sending documents back and forth. There can be only one Hub Operator type participant. As hubadmin is a system user, do not modify the User status of the hubadmin.

Internal Partner

This partner is created by the hubadmin user. This user is the company that bought the WebSphere Partner Gateway and is running the system. There can be

many internal partners, but only one default internal partner. Businesses act as both Hub Operator and internal partner if they do not delegate the task of configuring and monitoring the WebSphere Partner Gateway system to some internal IT group or a third-party company.

External Partner

This is the partner with which the internal partner communicates. There can be multiple partners of this type. If the partner has its own implementation of WebSphere Partner Gateway, then it becomes the internal partner on its own system and a external partner on this one.

Each of these profiles has at least one user ID. As mentioned above, Hub Operator profile is the hubadmin super-user of the system. The other two profiles will each have an admin user assigned to them upon initial creation. These users, in turn, can create other users with equal or less abilities. Each of these admin users has certain configuration abilities. For example, the hubadmin user can create any object on the system such as the internal partner or load system-wide security certificates. The internal partner role can create participants or connections. The external partner role is the most limited in scope and can view its own documents and configure the local destinations to which the internal partner has to deliver documents.

Typographic conventions

This document uses the following conventions.

Table 1. 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.
<i>italics</i>	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.
<i>Italic monospace font</i>	Text in italic monospace font indicates variable names within monospace-font text.
<i>ProductDir</i>	<i>ProductDir</i> represents the directory where the product is installed. All IBM WebSphere Partner Gateway product path names are relative to the directory where the IBM WebSphere Partner Gateway product is installed on your system.
<code>%text%</code> and <code>\$text</code>	Text within percent signs (%) indicates the value of the Windows ^(R) text system variable or user variable. The equivalent notation in a UNIX ^(R) environment is <code>\$text</code> , indicating the value of the <code>text</code> UNIX environment variable.
Underlined colored text	Underlined colored text indicates a cross-reference. Click the text to go to the object of the reference.

Table 1. *Typographic conventions (continued)*

Convention	Description
Text in a blue outline	(In PDF files only) An 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.
" " (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.
< >	Angle brackets surround variable elements of a name to distinguish them from one another. For example, <code><server_name><connector_name>tmp.log</code> .
/ or \	Backslashes (\) are used as separators in directory paths in Windows installations. For UNIX installations, substitute slashes (/) for backslashes.

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/>

Note: Refer to Technical Support Technotes and Flashes in WebSphere Partner Gateway Support Web site for the latest information about this product.

Access

<http://www.ibm.com/software/integration/wspartnergateway/support/> and select the component area of interest.

New in release 6.2.1

WebSphere Partner Gateway V6.2.1 supports the following new features:

- Web Mail box is web based support for B2B interaction. Partners, customers, and vendors interact with the WebSphere Partner Gateway hub using only the internet browser.
- SFTP integrated server is supported in addition to FTP integrated server.
- OpenPGP Certificate is supported in WebSphere Partner Gateway.
- Support for WebSphere Application Server ND V7.0.0.13, WebSphere Messaging Queue 7.0, and WTX 8.3.
- Platform support for Windows 2008, Windows 7, and SLES 11.
- Power 7 Support -Toleration Mode (P6/P6+ Compatible Modes).

- Virtualization Support - VMware® ESX with Windows and Linux, Power VM with AIX.

Chapter 2. Managing the WebSphere Partner Gateway component applications

Managing the WebSphere Partner Gateway component applications means starting, stopping, and configuring the application servers that host the WebSphere Partner Gateway components. These administrative tasks generally involve using WebSphere Application Server interfaces that control and configure a set of application servers where the WebSphere Partner Gateway components are deployed by the installation process.

How you manage the WebSphere Partner Gateway component applications depends on whether the product was installed using a simple topology or a distributed topology. In this document, the terms simple mode and distributed mode are used to refer to the topology chosen during product installation.

Note: See the *WebSphere Partner Gateway Installation Guide* for details on simple and distributed topologies.

The administrator managing WebSphere Partner Gateway components is aware of the mode of installation (simple or distributed).

In a simple mode installation, the WebSphere Partner Gateway components are all installed on the same computer using one application server called server1. As simple mode system does not use Deployment Manager, the mechanics of starting and stopping the WebSphere Partner Gateway components are similar to usage of WebSphere Application Server base (rather than network deployment).

All the computers can have WebSphere Application Server installed, but only the Deployment Manager requires the installation of WebSphere Application Server Network Deployment.

The application servers hosting the WebSphere Partner Gateway components are all logically contained in a Deployment Manager cell that is administered using the Deployment Manager application. However, the distinction is hidden when you use the Deployment Manager for administration tasks. The Deployment Manager console provides a view of the distributed WebSphere Partner Gateway component applications that hides the details about where they are installed.

Managing WebSphere Partner Gateway components in a simple mode system

For a simple mode system, it is necessary to know how to start and stop the application server that hosts all of the WebSphere Partner Gateway components.

To start the WebSphere Partner Gateway components, run one of the following scripts:

- UNIX^(R)
`<install dir>/bin/bcgStartServer.sh`
- Windows^(R)
`<install dir>\bin\bcgStartServer.bat`

To stop the WebSphere Partner Gateway components, run one of the following scripts:

Note: You do not have to specify a server name. The server name is always `server1` when simple mode is used.

- UNIX^(R)
`<install dir>/bin/bcgStopServer.sh`
- Windows^(R)
`<install dir>\bin\bcgStopServer.bat`

Managing WebSphere Partner Gateway components in a distributed mode system

For a distributed mode system, the WebSphere Deployment Manager application is used to control all of the WebSphere Partner Gateway applications. One of the computers in the distributed mode system is chosen during installation to host the Deployment Manager. When the WebSphere Partner Gateway applications are installed, the application server or servers that they are installed on are placed under control of the Deployment Manager. As the system administrator, you manage the WebSphere Partner Gateway components by using the Deployment Manager. This provides a single point of access to all the components, even if they are on different computers.

See the WebSphere Application Server Network Deployment product documentation for a detailed description of the way that a Deployment Manager is used to administer application servers. For purposes of this document, there are some terms and concepts regarding the way that the Deployment Manager operates.

Distributed topology terms and concepts

- The system consists of one or more nodes.
- The WebSphere Deployment Manager is an application that runs on one of the nodes in the system.
- The WebSphere Partner Gateway components (console, receiver, and router) are installed on application servers on the nodes in the system.
- The default messaging support of WebSphere Application Server is used, so `bcgmas` server contains the message queues required by WebSphere Partner Gateway for its internal messaging support.
- Each node that hosts WebSphere Partner Gateway components has a special application called the node agent. The node agent provides a connection between the application servers on the node and the Deployment Manager application.
- The nodes are combined into a logical grouping called a cell. The Deployment Manager provides you with a view of the cell from which you can manage the applications in the system.
- The application servers on the nodes within the cell are organized into clusters. All the application servers in a cluster have the same WebSphere Partner Gateway components.
- The cell is administered by the central WebSphere Deployment Manager. This means that:
 - All the servers within the cell can be started, stopped, and modified from the Deployment Manager.

- The internal messaging can be managed from the Deployment Manager.
- There are two variations on distributed mode called simple distributed mode and full distributed mode.
 - In simple distributed mode all three WebSphere Partner Gateway components are part of the same cluster. This also includes a cluster of bcgmas server.
 - In full distributed mode each component is typically in its own cluster, for example the console is in a bcgconsole cluster, receiver in a bcgreceiver cluster, and the document manager in a bcgdocmgr cluster. In addition there is a messaging bcgmas cluster used for internal communication between the WebSphere Partner Gateway components.

The Deployment Manager

The role of the Deployment Manager is to give you a single view of all of the application servers in the cell from which you can administer the servers. To achieve this, a node agent has to be running on each node that hosts WebSphere Partner Gateway components. The Deployment Manager uses the node agents to interact with the application servers in the system. During a distributed mode installation, for each node in the system a node agent is installed and configured to communicate with the Deployment Manager.

You use the Deployment Manager's web interface to manage the applications that are in the cell. If for some reason the Deployment Manager is not available then the WebSphere Partner Gateway components can be manually started or stopped from the command line, but other administration tasks cannot be performed until the Deployment Manager is available again.

The most common administration task that is performed is starting and stopping the WebSphere Partner Gateway components. Other administration tasks like configuring a server for logging and tracing or changing the startup parameters for the Java Virtual Machine used by a server can also be performed with the Deployment Manager.

To use the Deployment Manager:

1. Start the node agent on each node that hosts WebSphere Partner Gateway applications and the node where the bcgmas server is installed. To start the node agent on a computer use the WebSphere `startNode` script with no arguments. This script is located in the *<WebSphere Partner Gateway install dir>/wasND/Profiles/bcgprofile/bin* directory.
2. Start the Deployment Manager. To start the Deployment Manager use the WebSphere Partner Gateway `bcgStartServer` script with no arguments. This script is located in the *<Deployment Manager install dir>\bin* directory.
3. Open an appropriate Internet browser.
4. Navigate to `http://<computer name or IP address of the Deployment Manager>:55090/ibm/console` to open the WebSphere Integrated Solutions Console Welcome login screen, and log in.

Note: A user id is not required for logging in. On the left side of the Welcome screen you will see a list of tasks that can be done from this console.

5. To start or to stop all servers in a cluster:
 - In the left pane click **Clusters**
 - In the right pane, select the cluster to start or stop.
 - Click **start** or **stop**

Note: This operation may take a few minutes. You can refresh the view periodically to see the status.

6. To start or to stop individual servers:
 - a. In the left pane click Application Servers
 - b. In the right pane, select the server for the node to start or stop.

Note: Remember that a node represents an instance of WebSphere Application Server deployed on a computer in your system.

- c. Click **start** or **stop**.

Starting and stopping servers from the command line

When the Deployment Manager is not available, the WebSphere Partner Gateway components in a distributed mode system can be manually started and stopped on the individual computers. General administration tasks, for example changing log/trace settings, cannot be performed unless the Deployment Manager is available.

About this task

To use the command line scripts:

1. Start the node agent on each node that hosts WebSphere Partner Gateway applications and the node where the bcgmas server is installed. To start the node agent on a computer, use the WebSphere `startNode` script with no arguments. This script is located in the *WebSphere Partner Gateway Install Dir/wasND/Profiles/bcgprofile/bin* directory.
2. Start each WebSphere Partner Gateway server by running the `startServer` script located in the *<WebSphere Partner Gateway Install Dir>/wasND/Profiles/bcgprofile/bin* directory on the computer where the server was installed. The syntax is:

```
startServer <server_name>
```

Where the *server_name* is `bcgconsole`, `bcgreceiver`, `bcgdocmgr` or `bcgmas`.

3. Stop each WebSphere Partner Gateway server by running the `stopServer` script located in the *WebSphere Partner Gateway Install Dir/wasND/Profiles/bcgprofile/bin* directory on the computer where the server was installed.

The syntax is:

```
stopServer <server_name>
```

Where the *server_name* is `bcgconsole`, `bcgreceiver`, `bcgdocmgr` or `bcgmas`.

Starting and stopping FTP Management Server from command line

The FTP Management server must be running to manage the FTP server from WebSphere Partner Gateway console. To start the FTP Management server on a computer, use the **startftpmgmtserver** script. This script is located at WebSphere Partner Gateway Install Dir/ftpserver/bin. This script does not require any command line arguments. The Integrated FTP Server is started implicitly when the FTP Management server starts.

To Stop the FTP Management server on a computer, use **stopftpmgmtserver** script. This script is located in the WPG Install Dir/ftpserver/bin. This script does not

require any command line arguments. The Integrated FTP Server is stopped implicitly when the FTP Management server stops.

Note: This is applicable for all deployment modes.

Starting and stopping SFTP Management Server from command line

The SFTP runs within the SFTP management server. As a result, whenever the SFTP management server is started, the SFTP server also gets started automatically. The default port of SFTP management server is 2050. To start the server on a different port, add

```
bcg.config.ftpmanagement.sftpmgmt.port=<port>
```

to the
ftpserver.ini

properties file. This will replace the default port value with the value you provide in <port>. If you start the server without configuring the Host key, a warning message is displayed – “Warning: No host key defined for the server.”

To start and stop the SFTP Server from command prompt, execute
./startsftpmgmtserver.sh

and
./startsftpmgmtserver.bat

for Linux and Windows respectively.

Starting and stopping the components in a simple distributed mode system

There are two clusters in a simple distributed mode system:

bcgmasCluster

The messaging cluster that has messaging servers. There has to be at least one messaging server running for the WebSphere Partner Gateway components to operate.

bcgserverCluster

The WebSphere Partner Gateway component cluster that has servers named bcgserver. All three components (console, receiver and router) are installed on the bcgserver.

The names shown here are default names used by the installer. Be aware that the installer might have chosen different names and that you must use these names if the default names were not used.

Starting servers in a simple distributed mode system

Before starting your server in a simple distributed mode system, start the messaging servers prior to starting the WebSphere Partner Gateway component servers.

Starting all the servers using the Deployment Manager

About this task

1. Confirm that the node agent is running for each node with the bcgmas server and the bcgserver installed.
2. Using the Deployment Manager console, select the messaging cluster bcgmasCluster and click **Start**.
3. Wait for the bcgmasCluster to start before performing the next step.
4. Select the bcgserverCluster and click **Start**.

Starting individual servers on each computer

About this task

1. Confirm that the node agent(s) are running for each node with the bcgmas server and the bcgserver installed.
2. Select the messaging bcgmas server and click **Start**.
3. Repeat the previous step starting all of the other bcgmas servers.

Note: Wait until at least one of the messaging servers has started before starting the WebSphere Partner Gateway component servers.

4. Select the bcgserver server and click **Start**.
5. Repeat step 4 to start all of the required component servers. A cluster can contain more than one server. You can select any of the servers in the cluster, and start them.

Starting the servers when the Deployment Manager is unavailable

About this task

If the Deployment Manager is unavailable for use, you can Start the messaging bcgmas and the bcgserver servers manually with the following steps:

1. Confirm that the node agents are running for each node with the bcgmas server and the bcgserver installed.
2. Start each WebSphere Partner Gateway server by running the startServer script located in the `<WebSphere Install Dir>/wasND/Profiles/bcgprofile/bin` directory on the computer where the server is installed.

The syntax for starting the messaging server, console, receiver, or Document Manager for the component servers is:

```
startServer <server_name>
```

Where *server_name* is bcgmas for starting the messaging server, and bcgserver for the component servers.

Stopping servers in a simple distributed mode system

When stopping servers in a simple distributed mode system stop the WebSphere Partner Gateway component servers before stopping the messaging servers.

Stopping all the servers using the Deployment Manager

About this task

1. Select the bcgserverCluster and click **Stop**. Wait for the cluster to stop before performing the next step.
2. Select the messaging cluster bcgmasCluster and click **Stop**.

Stopping the individual servers on each computer

About this task

If you do not want to stop all servers in each cluster, you can stop the servers on each computer where they are installed. To stop the servers on each computer, perform the following steps:

1. Select the bcgserver server to stop and click **Stop**.
2. Repeat the previous step until you have stopped all of the servers you want to stop. Wait for the servers to stop before performing the next step.
3. Select the bcgmas server messaging you want to stop and click **Stop**.
4. Repeat the previous step until you have stopped all of the servers. If any of the bcgserver servers are still running then leave at least one bcgmas server running.

Stopping the servers when the Deployment Manager is unavailable

About this task

First, stop the bcgserver servers before the messaging bcgmas servers.

1. Confirm that the node agents are running for each node with the bcgmas server and the bcgserver installed.
2. Stop each WebSphere Partner Gateway server by running the stopServer script located in the `<WebSphere Parnter Gateway Install Dir>/wasND/Profiles/bcgprofile/bin` directory on the computer where the server is installed.

The syntax is for stopping the messaging server or bcgserver for the component servers is:

```
stopServer <server_name>
```

Where *server_name* is bcgmas for stopping the messaging server, and bcgserver for the component servers.

Starting and stopping the components in a full distributed mode system

Before you begin, you must know that there are four clusters in full distributed mode system. They are as follows:

- bcgmasCluster

The messaging cluster that has messaging servers named bcgmas. There must be at least one messaging server running for the WebSphere Partner Gateway components to operate.

- bcgconsoleCluster

The WebSphere Partner Gateway Console component cluster that has servers named bcgconsole.

- bcgreceiverCluster

The WebSphere Partner Gateway Receiver component cluster that has servers named bcgreceiver.

- bcgdocmgrCluster

The WebSphere Partner Gateway Document Manager component cluster that has servers named bcgdocmgr.

The names shown here are the installation default names. Be aware that during installation, the installer might have chosen different names and you must use these names instead of the default names.

Starting servers in a full distributed mode system

To start your servers in a full distributed mode system, the startup sequence is as follows:

1. Messaging servers
2. WebSphere Partner Gateway document manager servers
3. WebSphere Partner Gateway receiver servers (or console servers)
4. WebSphere Partner Gateway console servers (or receiver servers)

Note: The receiver and console servers can be started in either order.

Starting all the servers using the Deployment Manager About this task

1. Select the messaging cluster `bcgmasCluster` and click **Start**.

Note: Wait until the cluster has started before starting the WebSphere Partner Gateway component clusters.

2. Select the `bcgdocmgrCluster` and click **Start**.
3. Select the `bcgreceiverCluster` (or the `bcgconsoleCluster`) and click **Start**.
4. Select the `bcgconsoleCluster` (or the `bcgreceiverCluster`) and click **Start**.

Starting individual servers on each computer About this task

1. Select the messaging `bcgmas` server to start and click **Start**.

Note: Wait until at least one of the servers has started before starting the WebSphere Partner Gateway component servers.

2. Repeat the previous step until you have started all of the servers.
3. Select the `bcgdocmgr` server to start and click **Start**.
4. Repeat the previous step until you have started all of the servers.
5. Select the `bcgreceiver` (or `bcgconsole`) server to start and click **Start**.
6. Repeat the previous step until you have started all of the servers.
7. Select the `bcgconsole` (or `bcgreceiver`) server to start and click **Start**.
8. Repeat the previous step until you have started all of the servers.

Note: If more than one servers have to be started, then select those servers, and click **Start**.

Starting the servers when the Deployment Manager is unavailable About this task

Note: Start the servers in the order shown in the previous section.

1. For each node with the `bcgmas` server and any of the WebSphere Partner Gateway component servers installed make sure that the node agent(s) are running.

2. Start each WebSphere Partner Gateway server by running the startServer script located in the `<WebSphere Partner Gateway Install Dir>/wasND/Profiles/bcgprofile/bin` directory on the computer where the server was installed. The syntax is:

```
startServer <server name>
```

Where *server name* is bcgmas for starting the messaging server, bcgconsole, bcgreceiver and bcgdocmgr for the component servers.

Note: Start bcgmas server first and then start the rest of the servers.

Note: Ensure that the user you use to start and stop the server is WPG user and is not the root user.

Stopping servers in a full distributed mode system

It is important to note that the shutdown sequence is the opposite of the startup sequence. It is as follows:

1. WebSphere Partner Gateway console (or receiver) servers.
2. WebSphere Partner Gateway receiver (or console) servers.

Note: The receiver and console servers can be stopped in either order.

3. WebSphere Partner Gateway document manager servers.
4. Messaging servers.

Stopping all the servers using the Deployment Manager About this task

1. Select the bcgconsoleCluster (or bcgreceiverCluster) and click **Stop**.
2. Select the bcgreceiverCluster (or bcgconsoleCluster) and click **Stop**.
3. Select the bcgdocmgrCluster and click **Stop**.

Note: Wait until the cluster has stopped before stopping the messaging cluster.

4. Select the messaging cluster bcgmasCluster and click **Stop**.

Stopping individual servers on each computer at a time About this task

If you do not want to stop all servers in each cluster, you can stop the servers on each computer where they are installed. To stop a server where it is installed, perform the following steps:

1. Select the bcgconsole (or bcgreceiver) server to stop and click **Stop**.
2. Repeat the previous step until you have stopped all of the servers you want to stop.
3. Select the bcgreceiver (or bcgconsole) server to stop and click **Stop**.
4. Repeat the previous step until you have stopped all of the servers you want to stop.
5. Select the bcgdocmgr server to stop and click **Stop**.
6. Repeat the previous step until you have stopped all the servers you want to stop.
7. Wait until the servers have stopped before stopping the messaging servers.
8. Select the bcgmas server messaging you want to stop and click **Stop**.
9. Repeat the previous step until you have stopped all of the servers.

Note: If some of the WebSphere Partner Gateway component servers are still running then keep at least one bcgmas server running.

Stopping the servers when the Deployment Manager is unavailable

About this task

It is important to note that you must stop the WebSphere Partner Gateway servers before the messaging bcgmas servers.

1. Confirm that for each node with the bcgmas server and any of the WebSphere Partner Gateway component servers installed make sure that the node agent(s) are running.
2. Stop each WebSphere Partner Gateway server by running the stopServer script located in the *<WebSphere Partner Gateway Install Dir>/wasND/Profiles/bcgprofile/bin* directory on the computer where the server was installed. The syntax is:

```
stopServer <server_name>
```

Where *server_name* is bcgmas for stopping the messaging server, bcgconsole, bcgreceiver and bcgdocmgr for the component servers.

Chapter 3. Basic Community Console tasks

The tasks described in this guide are performed using the WebSphere Partner Gateway Community Console. The Community Console is a Web application providing a secure access point accessible through a web browser.

Topics covered in this chapter include:

- “ Logging in to the Community Console”
- “ Navigating through the Community Console” on page 16
- “Community Console icons” on page 16
- “ Logging off from the Community Console” on page 18

Logging in to the Community Console

The Community Console requires supported Web browsers. For more information on the supported browser versions of WebSphere Partner Gateway 6.2.1, refer to <http://www-01.ibm.com/support/docview.wss?rs=2311&uid=swg27020525>.

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 minimum screen resolution of 1024 x 768.

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, type the appropriate name:
 - For the hub administrator, the default user name is `hubadmin`.
 - For the operator administrator, the default user name is `Admin`.
3. In the **Password** field, type the password for your site. The default password is `Pa55word`.
4. In the **Company Login Name** field, type the Admin login name. The default login name for both the hub administrator and operator administrator user is `Operator`

Note: If user IDs and passwords are going to be centrally managed from Lightweight Directory Access Protocol (LDAP) then a **Company Login Name** field will not display. For further information about LDAP see the section, Chapter 7, “LDAP support for logon authentication,” on page 77.

5. Click **Login**.
6. The first time you log in, the system prompts you to create a new password. Type a new password, then type it again in the **verify** field.

7. Click **Save**.

Note: In Firefox browser, if you save the user name and password in the login page, the saved user name and password values are filled automatically in the user screens that have user name and password fields. This is observed regardless of whether it is a login page or not. For example, in the User create page, the Fax field is pre-filled with password and user name values.

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**

Logs off the current WebSphere Partner Gateway session. The application continues to run on the server. To log in again, follow the procedure under “Logging in to the Community Console” on page 15.

- **Help**

Opens 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 2 lists the icons that are used throughout the Community Console windows.

Table 2. Community Console Icons













Icon	Icon name
	Collapse
	Copy
	Data contained
	Activate
	Delete
	Destination disabled
	Display raw document
	Document in progress
	Document processing failed
	Document processing successful
	Download map
	Edit

Table 2. Community Console Icons (continued)





























Icon	Icon name
	Edit attribute values
	Edit off
	Edit RosettaNet attribute values
	Expand
	Export information
	Export report
	Hide search criteria
	Modify
	No data contained
	Open calendar
	Out of sequence
	Pause
	Print
	Required input
	Role; click to create role
	Start
	Stop Submitted
	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 Note: The Help icon is translated when using the console with one of the IBM supported language locales.
	View permissions
	View the Document Definition attribute setup

Table 2. Community Console Icons (continued)

Icon	Icon name
	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.

Chapter 4. Hub administration tasks

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

- “Managing password policy”
- “Changing database connectivity, database user and password” on page 20
- “Managing event codes” on page 20
- “Managing receivers” on page 22
- “Managing interactions and document definitions” on page 23
- “Managing XML formats” on page 24
- “Enabling or disabling actions” on page 25
- “Managing handlers” on page 25
- “Managing maps” on page 27
- “Managing EDI” on page 28
- “Configuring the alert mail server” on page 33
- “Viewing system activity” on page 33
- “Managing event delivery” on page 34
- “Managing API calls” on page 34
- “Supporting ebMS” on page 36
- “Configuration details for validating Webservices” on page 38
- “Using non-repudiation logging” on page 39
- “Using message store” on page 39
- “Prerequisite to setup WebSphere Partner Gateway - WebSphere Transformation Extender Integration Environment” on page 40

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 partner has to 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 partner cannot use an old password if it exists in the history file. The default is 10 passwords.
- **Special Characters**, when selected, indicates that passwords has to contain at least three of the following types of special characters:
 - Uppercase characters
 - Lowercase characters
 - Numeric characters
 - Special characters

This setting enables 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, 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 **Edit**.
3. Change any of the default values to the ones you want to use for your password policy.
4. Click **Save**.

Changing database connectivity, database user and password

About this task

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

You can change the connectivity properties for the database by modifying the data sources. The data sources are configured in the WebSphere Application Server for use by the component applications. You can use the WebSphere Application Server admin console to modify the data sources.

To configure the database connections used by the components, perform the following steps:

1. Use a browser to view the administrative console.
2. Click **Resources** > **JDBC** > **Data sources** in the left pane of the console.
3. Locate the data source that you want to change. Look at the JNDI names for the sources that are available and choose the one you want to change based on the node and server name.
4. Click the data source name to view and change the database name, host, and port number.
5. Click **JAAS-J2C authentication data** and then choose an alias to view and change the user ID and password used for the connection to the database.
6. Click **OK** to make the changes, and then click **Save** to save them.

Managing event codes

An event is logged for important activities or information within WebSphere Partner Gateway. There are some pre-defined events with specific event codes. To view the event codes, navigate to **Hub Admin** > **Hub Configuration** > **Event Codes**. You can export them to other applications and can set the alert status of the event code as well and you can even define whether an event code is alertable or not.

Viewing and editing event codes

About this task

The following procedure describes how to view the details of an event code. You can edit the visibility and alert 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 3:

Table 3. Event code details

Parameter	Description
Event Code	A read-only field that shows the unique number for this event code.
Event Name	A read-only field that shows the name used to identify the event in relation to the action that triggered the event.
Internal Description	A read-only field that describes the circumstances that triggered it.
Visibility	Select the users who can view the event code: Community Operator, Manager, partner, 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 Low-level system operations and support. Visibility and use of the debug information are subject to the permission level of the user. Info Successful system operations. These events also provide the status of documents being processed. Informational events require no user action. Warning Non-critical anomalies in document processing or system functions that enable the operation to continue. Error Anomalies in document processing that cause the process to end. Critical Services that end because of a system failure. Critical events require intervention by support personnel.
Alertable	You can create an event alert by selecting "Alertable" to display the Event Name in the list on the Define tab of the Alert window.

Exporting event code names

About this task

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 events that can be notified

About this task

An event is logged for important activities or information within WebSphere Partner Gateway. There are some pre-defined events with specific event codes. To view the event codes, navigate to **Hub Admin > Hub Configuration > Event Codes**. 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 make events alertable:

1. Click **Hub Admin > Hub Configuration > Event Codes**.
The Event Codes page is displayed.
2. To enable the alerts for the event, perform the following:
 - Click the **View details** icon next to the event code.
The Event Code Details page is displayed.
 - Select **Alertable**.

Document Validation Errors

To view document validation errors, click the **View document** icon on the Document details page under the Document Viewer tab. For more information about document validation errors, see “Document Validation Errors” on page 116.

Managing receivers

The **Receiver List** window is used to view and edit existing receivers details, and enable, disable, or delete receivers.

Viewing and editing receiver details

About this task

The following procedure describes how to view details for a receiver. As part of this procedure, you can edit the parameters of the receivers:

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

Enabling or disabling receivers

About this task

You can enable or disable receivers from the **Receiver List** window by clicking **Enabled** or **Disabled** in the **Status** column. You can also enable or disable the receiver by following these steps:

1. Click **Hub Admin > Hub Configuration > Receivers**.
2. On the **Receiver List** window, click the **View Details** icon to view the receiver details.

3. Click **Edit** icon to edit the receiver parameters.
4. In the Status field, select either **Enabled** or **Disabled** option to change the receiver status.
5. Click **Save** to save the modification.

Deleting receivers

About this task

You can delete receivers that you are not going to use.

1. Click **Hub Admin > Hub Configuration > Receivers**.
2. On the **Receiver List** window, click the **Delete** icon next to the receiver you want to delete.

Note: A delete confirmation window opens. After you confirm, the selected receiver is deleted.

Localizing HTTP synchronous target time out

About this task

WebSphere Partner Gateway allows you to have a localized synchronous time out and synchronous connection values for every HTTP Receiver. The synchronous connection value cannot exceed the container allowed TCP connection limit. The maximum synchronous connection per receiver alone is controlled in the super set of container limit. Web container (WebSphere Application Server) is configured separately through managed application to allow or limit the number of HTTP connections. To modify the values of **Max sync time out** and **Max sync connection**:

1. Navigate to **Receiver creation page > Hubadmin > Receivers**.
2. Click **Edit** icon corresponding to the HTTP receiver.
3. Modify the values of **Max sync time out** and **Max sync connection**.

Note: **Max sync time out** does not accept negative values. Entering the value zero for **Max synchronous connection** removes the restriction of **Max sync connection** over any receiver.

Managing interactions and document definitions

About this task

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

1. Click **Hub Admin > Hub Configuration > Document Definition**.
2. Click **Manage Interactions**.
3. Enter the search criteria that WebSphere Partner Gateway will use 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 **Activate** icon next to the interaction you want to enable. Click **OK** to confirm. WebSphere Partner Gateway replaces the **Activate** icon with the **Deactivate** icon. This indicates that the interaction is enabled.

6. To disable an interaction, click the **Disabled Default Definition** icon next to the interaction. Click **OK** to confirm. WebSphere Partner Gateway replaces the **Delete** icon with the **Enabled Default Definition** icon. This indicates that the interaction is disabled.
7. To edit an interaction, click the **Edit** icon next to the interaction. In the **Editing** window, edit the interaction, then click **Save**.

To view where an interaction is being used, follow these steps:

1. Click **Hub Admin > Hub Configuration > Document Definition**.
2. Click **Manage Interactions**.
3. Enter the search criteria that will be used by WebSphere Partner Gateway to find the interaction you want to view.
4. Click **Search**. The system finds all interactions that meet your search criteria.
5. Click **Where used** icon. This lists all the connections where this interaction is used. Every page will have a maximum of 10 connection information for that particular interaction.

To delete an interaction, follow these steps:

1. Click **Hub Admin > Hub Configuration > Document Definition**.
2. Click **Manage Interactions**.
3. Type the search criteria that WebSphere Partner Gateway uses to find the interaction you want to delete.
4. Click **Search**. The system finds all interactions that meet your search criteria.
5. Click **Delete** icon. A warning message is displayed when the interaction is used by any of the channels.
6. Click **OK** to delete the interaction along with its corresponding channels.

To find out where document definitions are being used, follow these steps:

WHERE USED icon displays information on where all the selected Document definition is being used.

1. Click **Hub Admin > Hub Configuration > Document Definition**.
2. Click **Where used** icon of the document definition you want to view. This lists all the interactions and B2B capabilities where this document definition is used.

To delete a document definition, follow these steps:

1. Click **Hub Admin > Hub Configuration > Document Definition**.
2. Click **Delete** icon against the document definition you want to delete. The warning message is displayed only if the Document definition is used by any of interaction or B2B capabilities.
3. Click **OK** in the warning message window. This will delete the corresponding channels, interactions, B2B capabilities of all the partners, and all the related attributes of the Document definition.
4. Click **Cancel** in the warning message window to abort deletion.

Managing XML formats

You can use the Manage XML Formats windows to access the XML formats in the system. XML formats are organized using XML document families. Using the console, you can add, delete, and modify XML document families. For each family you can add, delete, and modify the XML formats in the family. You can also copy formats in a family, and move formats from one family to another.

For complete information about creating XML document families and formats, see the *WebSphere Partner Gateway Hub Configuration Guide*.

Large file support

WebSphere Partner Gateway can use XPath version 1.0 expressions in formats. The processing power of XPath support limits the size of files that can be used with full XPath XML formats. To enable large files to be processed, set the large file processing option when defining the document family.

The Large file options list includes the following options:

- None
- Use large file processor
- Use namespace-aware large file processor

Select a large file option if you are writing XML formats for large documents that cannot be handled using the full XPath processor. The namespace-aware option specifies that the element paths include namespace prefixes when they appear in a document.

Note: This option cannot be changed once the family is created. This is because the document family might already include XML formats that will be made incorrect if the family type is changed.

Formats in a family with the large file processing option selected have limited XPath processing power. When using the large file processing option on a document family, the following limitations are placed on the expressions used in the XML formats that are stored in the family:

1. Only simple element paths that begin at the root of the document can be used.
2. Element paths cannot include namespace prefixes even though they can appear in the documents.

Enabling or disabling actions

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

To enable or disable the actions, perform the following steps:

- Click **Hub Admin > Hub Configuration > Actions** to display the Actions window.
- Change the Status (**Enabled** or **Disabled**) of the action. Click **Save**.

Managing handlers

The **HandlersList** window displays all the handlers that are available for use with an action, receiver, destination, 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

About this task

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**, enter the name of an XML file that represents the handler you want to import, or use the **Browse** option 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

About this task

To delete a handler, follow these steps:

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

Configuring the content-type attribute in handlers

About this task

In some cases, the Document Manager may not be able to route some EDI-X12 documents with text/plain attributes until they are configured. The Handlers such as **BinaryChannelParseHandler**, **XMLRouterBizHandler**, **EDIRouterBizProcessHandler** support comma-separated content-type values. For these handlers, the text/plain content-type has to be added manually.

Note: Do not change the handler values unless advised to do so by an IBM representative.

Perform the following steps to add the text/plain attribute to these handlers.

1. Click **Hub Admin > Fixed Workflow > ChannelParseFactory**.
2. Select **EDIRouterBizProcessHandler** and click the **Edit** icon.
3. In the configured list, select **EDIRouterBizProcessHandler** and click **Configure**.
4. Edit the content-types attribute by adding **text/plain** to the content type.
5. Click **Save**.

Managing maps

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

Updating validation maps

About this task

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 required.
3. Click the **Upload map** icon to load the updated map to the system.

Viewing validation maps Where used

About this task

Use this procedure to view the usage of validation maps, that is, where all the validation map is being used:

1. Click **Hub Admin > Hub Configuration > Maps > Validation Maps**.
The validation maps currently in the system are displayed.
2. Click **Where used** icon to list all the routing objects that use the validation map.

Deleting validation maps

About this task

Use this procedure to delete validation maps:

1. Click **Hub Admin > Hub Configuration > Maps > Validation Maps**.
The validation maps currently in the system are displayed.
2. Click **Delete** icon.

Note: A warning message is displayed to verify whether the selected validation map is used by any of the document definitions. If the validation map is not used by any of the routing objects, the warning message is not displayed.

3. Click **OK** in the warning message window to confirm deletion. Before deletion the validation map is dereferenced from the document definitions. Click **Cancel** to abort delete operation.

Managing transformation maps

About this task

Use the Manage Transformation Maps 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.
1. Click the **Details** icon to display details about a map.

2. Click the **Download map** icon to download a transformation map to your local computer. This is useful when you have to update a map.
3. Click the **Upload map** icon to upload an updated map to the system.

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

Managing EDI FA maps

About this task

Use the Manage EDI Functional Acknowledgment Maps page to view a list of functional acknowledgment (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.
1. Click the **View details** icon to display details about a map.
 2. Click the **Where used** icon to see where a FA map is used.
 3. Click the **Delete** icon to delete an 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.

See the *WebSphere Partner Gateway Hub Configuration Guide* for descriptions of each Envelope Profile Attribute for the EDI standards.

Editing envelope profile records

About this task

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 *WebSphere Partner Gateway Hub Configuration Guide* for attribute descriptions.

4. Update the envelope profile attribute values, and click **Save**. See the *WebSphere Partner Gateway Hub Configuration Guide* for attribute descriptions.

Creating envelope profile records

About this task

1. Click **Hub Admin > Hub Configuration > EDI > Envelope Profile**.
2. Click **Create** in the Envelope profiles window.
3. Type a value for the following fields:
 - 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 list that is applicable to the new profile. This is a required field.

After selecting a value in the EDI Standard list, the envelope profile attributes specific to that standard (General, Interchange, Group, or Transaction) are automatically displayed.

5. Update the envelope profile attribute values, and click **Save**. See *WebSphere Partner Gateway Hub Configuration Guide* for attribute descriptions.

Deleting envelope profile records

About this task

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

About this task

Use the Enveloper page to view and edit the Lock and 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 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) 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. 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. See the *WebSphere Partner Gateway Hub Configuration Guide* for more information about Connection Profiles.

Editing connection profiles

About this task

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 attribute values for the connection profile.
3. Click the **Edit** icon and edit the attributes.
4. Click **Save**.

Creating connection profiles

About this task

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

Deleting connection profiles

About this task

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

Control number initialization

About this task

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 partners 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 partners. See the *WebSphere Partner Gateway Hub Configuration Guide* for more information about control numbers and control number masks.

1. Click **Hub Admin > Hub Configuration > EDI > Control Number Initialization**.
2. Type the search criteria in the **Partner Name** field. The criteria can be either the name of a partner or wildcard search criteria. If you are not searching for EDI-capable partners, clear the **EDI-capable** check box. By default, the check box is selected. If you are searching for EDI-capable partners, 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 partner.
4. The partner'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**.

Current control numbers

About this task

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

1. Click **Hub Admin > Hub Configuration > EDI > Current Control Numbers**
2. Use the following options to search for one or more From partners and to search for one or more To partners.

- **partner Name:** The name of a specific partner. The search function is case sensitive, so enter the partner name exactly as it appears in the system.

Note: Select both From partner and a To partner.

- **Find EDI-capable:** By default, this check box is selected. If you are not searching for EDI-capable partners, clear the EDI-capable check box. If you are searching for EDI-capable partners, 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 partner. To search for

all partners, leave the Partner Name field blank, and click **Search**. To search for a specific partner, type the name in the **Partner Name** field, and then click **Search**.

- **Display Current Status:** Click to display the control-number status values for the selected partner-pair.
3. Click the **Edit** icon to make changes.

CAUTION:

Use the Edit and Reset All options for special circumstances only, as they can cause duplicate control number.

4. Do one of the following actions:
 - 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 partner-pair so that the status values are reset by the next message exchange that occurs between the partners.

Managing system configuration data

System configuration data specifies how WebSphere Partner Gateway components access system resources. These resources vary depending on your own installation. Some of this data is used to establish communication between components while other data establishes the allocation of system resources to each component.

In the WebSphere Partner Gateway, the system configuration data is saved in the database and configured by the hubadmin user through the console.

As the database is shared by all of the hub component instances, there might be times when component instances require their own configuration and not use the shared configuration data. To handle this situation, the components are always checked, using server scope, for the attribute values in the WebSphere Application Server environment before obtaining the attribute data from the central database.

Check WebSphere Application Server documentation for the steps to define variables with server scope. You can implement these actions using the WebSphere Application Server admin console, or specifically designed scripts.

Accessing the system configuration data

About this task

To access the system configuration data perform the following steps:

1. Log in as hubadmin.
2. Click **System Administration** from the menu tabs.

Note: Use the second row of navigation tabs to select from **Common Properties**, **Console Administration**, **Document Manager Administration**, **Feature Administration**, and **Receiver Administration**. Each of these tabs access configuration data screens or to additional navigation tabs. See "Appendix C - component-specific system attributes" on page 225 for detailed information about specific configuration data and how to locate it from the console.

3. Navigate to the configuration page you want to edit.
4. Click **Edit** on that page and change the data.
5. Click **Save** to save the changes to the database or **Cancel** to discard them.

After changing data, most changes are made immediately without restarting the system. Changes that require one or more components to be restarted are noted in Appendix C “Appendix C - component-specific system attributes” on page 225.

Note: You should not change any of these values unless you are very familiar with the way the WebSphere Partner Gateway product operates. Typically system configuration data is changed only by experienced systems or support engineers. If you do change this data, record the original value or values so you can revert to your original values if it becomes necessary.

Configuring the alert mail server

Alerts are text-based e-mail messages notifying partners of a system event. If you are going to use these alerts, configure the SMTP server along with the reply-to e-mail addresses. You must configure the reply-to e-mail addresses in the event there are delivery difficulties.

To locate the configuration attributes, navigate to **System Administration > DocMgr Administration > Alert Engine** within the WebSphere Partner Gateway console.

The attributes are:

- bcg.alertNotifications.mailHost
- bcg.alertNotifications.mailFrom
- bcg.alertNotifications.mailReplyTo
- bcg.alertNotifications.mailEnvelopeFrom

Additional descriptions regarding the purpose and values for these attributes are located in Table 59 on page 240.

Viewing system activity

About this task

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.

Use the Summary Service Properties window 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 > DocMgr Administration > Others > Summary Engine**. The Console displays the Summary Service Properties window.
2. On the Summary Service Properties window, click the **Edit** icon next to **Processing Interval (in Minutes)**.
3. Type 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

About this task

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 might have 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 must change the value for JMS Queue Factory Name from `WBIC/QCF` to `WBIC\\QCF` and the value for JMS Queue Name from `jms/bcg/queue/deliveryQ` to `jms\\bcg\\queue\\deliveryQ`.

To activate event publishing, follow these steps:

1. Click **System Administration > Event Processing > Event Delivery Information**.
2. In 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 *WebSphere Partner Gateway Hub Configuration Guide* for the property descriptions.
3. Click **Save**.

Managing API calls

About this task

Partners can make application programming 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**.

Note: The XML-based administrative API is deprecated.

The migration utility that is introduced by WebSphere Partner Gateway can be used instead of the administrative API to perform the creation and update tasks. Creation and update tasks formerly only performed using the administrative API can now be performed by using a migration import file that has the new or updated information.

The import file is described by the XML schema that is provided with the migration utility. You can use a development tool such as Rational Application Developer to produce an import XML file that conforms to the schema. By importing this file with the migration utility, you can load new partner definitions including contacts and business IDs for the partners. You can also update existing partner definitions by importing them with the migration utility. With the

administrative API, you can list some of the configuration artifacts in a system. A full export of the system using the migration utility provides listings of partner capabilities, partner connections, and receivers (targets) in the exported XML file.

Managing Document Manager information

You can use the admin console 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. As 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

About this task

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 > BPE-DAE**.
2. Select one of the tabs that is displayed under the BPE-DAE tab to access either the Main, Signal, or Synchronous property values.

The Document Manager Administration page shows the properties in read-only mode.

3. Click the **Edit** icon to modify the properties.
4. Click **Save**.

Supporting ebMS

WebSphere Partner Gateway supports ebXML Message Service (ebMS) mechanism. The ebMS defines the message enveloping and header document schema used to transfer ebXML messages in a communications protocol. ebMS is defined as a set of layered extensions to the base SOAP and SOAP with attachments, specifications. It contains structures for a message header used to route and deliver the message, and a payload section. ebMS focuses on transporting a payload from one party to another, which may include intermediaries. It is important to keep in mind that ebMS does not validate the business processes or the correctness of the ebXML content being sent. The function of ebMS is to assure the sender of a secure and intact transmission of the ebXML payload. ebMS uses Collaboration Protocol Agreements (CPA) to determine how and what kind of data is transmitted between two parties.

Uploading a CPA to WebSphere Partner Gateway

A CPA defines all the valid, visible, and enforceable electronic data interactions between two parties. The CPA is an agreement between two parties as to how they will exchange electronic data. If a CPA is provided, it can be uploaded into WebSphere Partner Gateway to aid in configuring the product. If a CPA has not been provided, the product can be configured manually.

There are two ways to upload a CPA: from the **Document Definition** page or from the **Hub Admin** page.

Uploading from the Document Definition page

About this task

Perform the following to upload a CPA:

1. Click **Hub Admin > Hub Configuration > Document Definition**.
2. Click the **Upload/Download Packages** link on the top of the screen.
3. Select **ebMS CPA** as the package type and click **Submit**.
4. Click the **Upload CPA** link on the top of the screen.
5. Click **Browse**, locate the appropriate file, and click **Open**.
6. Ensure that ebMS Version 2.0 is selected.
7. Click **Upload**.

After a successfully completing the upload, you will have both the internal and external partners created. The internal and external partner business-to-business capabilities are enabled, interactions and connections made, and respective destinations created as well. It is important to note that if an error occurs during a CPA upload then any configuration made during the upload is not rolled back.

Note: To prevent the accidental replacement of existing certificates, you must manually upload any certificates in the CPA that are stored in the file system.

While creating the interaction the default action is set to **Pass Through**. The following are the additional flows made for supporting ebMS:

- Ping
- Status Request

- Error

During runtime when processing an ebMS document from a Partner, WebSphere Partner Gateway validates that the ebMS interaction conforms to the ebMS configuration (for example if encryption is required) and if there is a non-conformance the document is failed. The specific failure events can be viewed in the Document or ebMS viewers.

Uploading the CPA from the ebMS page

About this task

Perform the following to upload a CPA:

1. Click **Hub Admin > Hub Configuration > ebMS**.
2. Click **Upload CPA**.
3. Click **Browse** and select the appropriate CPA package.
4. Ensure that ebMS Version 2.0 is selected.
5. Click **Upload**.

During the CPA upload process, you will be asked to select the internal partner from the partners present in the CPA.

Non-prepopulated attributes

Attribute values are set at connection level during the upload of the CPA. Some attributes however, do not have pre-populated values. The following is the list of such attributes and example values:

- Encryption Mime Parameter

Values can be:

- i. smime-type="enveloped-data"
- ii. type="text/xml" version="1.0"

- Encryption Constituent

Values can be:

- i. text/xml:application/binary:application/edi
- ii. */xml

Note: Values are separated by the colon (:) delimiter

- Packaging Mime Parameter

Values can be:

- i. type="text/xml" version="1.0"
- ii. type="multipart/related"

- Packaging Constituent

Values can be:

- i. text/xml:application/pkcs7-mime
- ii. text/xml:application/binary:application/edi

Note: text/xml must be the first element.

- Exclude from Signature

Values can be as follows:

- i. application/binary:text/xml:application/pkcs7-mime
- ii. application/pkcs7-mime

Algorithms supported by the ebMS

There are various algorithms supported by the ebMS including:

- “Digest and Signature algorithms”
- “XML encryption and SMIME encryption algorithms”

Digest and Signature algorithms

The digest algorithms supported are as follows:

- SHA1
- SHA256
- SHA512
- RIPEMD160

The signature algorithms supported are as follows:

- DSA-SHA1
- RSA-SHA1

If the signing fails because of a configuration issue, an event is logged that reads Signing Failed. Similarly if the signature verification fails, an event reading, Signature Verification Failed is logged and an ebMS error message is generated containing information as to why the signature verification process failed.

XML encryption and SMIME encryption algorithms

There are two supported protocols for ebMS encryption; XML encryption and SMIME encryption.

If you are using the XML encryption, you can use the following algorithms:

1. 3-des-cbc
2. aes-128-cbc
3. aes-192-cbc
4. aes-256-cbc

If you are using the using SMIME encryption, you can use the following algorithms:

1. 3-des-cbc
2. aes-128-cbc.
3. aes-192-cbc
4. aes-256-cbc
5. rc2-128-cbc

Configuration details for validating Webservices

This feature validates SOAP Body or Payload that is available under SOAP Envelope. Payload validation is supported only for XML Payloads in SOAP Envelope. This also enables the De-Envelope of SOAP Envelope before introducing the SOAP Body for further processing. Note that the De-Envelope of SOAP Envelope happens only in the event of asynchronous communication. See the *WebSphere Partner Gateway Hub Configuration Guide* for more information on Validating WebServices. To validate Payload under SOAP Envelope, you need to perform the following additional configurations on the top of Webservice channel configuration:

- Upload the necessary validation map to WebSphere Partner Gateway. See *Configuring document types chapter of WebSphere Partner Gateway Hub Configuration Guide* for uploading validation maps onto WebSphere Partner gateway.
- For DTD based validation, associate DTD against validation map under its respective Webservice channel. See *Configuring document types chapter of WebSphere Partner Gateway Hub Configuration Guide* for associating validation map to channel.
- For schema-based validation, optionally, you can associate the validation map under its respective Webservice channel.
- While uploading schema into WebSphere Partner Gateway, use the SystemId for file name. If you follow the WebSphere Partner Gateway schema location functionality and industry standard way of specifying the schema location in XML, it is not required to externally associate schema against validation map under the respective Webservice channel.
- Choose the built-in action SOAP Body Validate to validate SOAP Body under the Webservice request channel.
- You can optionally choose not to validate the response by setting the **Response Validation** routing object attribute to "No". On the target side, modify the routing object attribute Response Validation.
- By enabling/disabling **Content Validation** routing object attribute, the content validation over payload XML can be altered. By default, **Content Validation** is enabled.

Using non-repudiation logging

About this task

WebSphere Partner Gateway increases the configuration options for using non-repudiation by enabling a Trading Partner or internal partner to configure it at the package, protocol, and document flow levels. By using this configuration, you can start or stop non-repudiation for each connection rather than stopping all the connections.

For example, to initiate non-repudiation for an AS2 connection between a Trading partner and a internal partner perform the following steps:

1. Create a partner connection between **AS > None**.
2. List the partner connection between Trading Partner and Community Manager.
3. Edit the attributes for the AS2 package setting the NonRepudiationRequired attribute to yes.
4. Edit the attributes for the none package setting the NonRepudiationRequired attribute to no.

See the *WebSphere Partner Gateway Hub Configuration Guide* for more information about setting the non-repudiation attributes at the package, protocol, and document type.

Using message store

About this task

WebSphere Partner Gateway increases the configuration options for using message store by enabling a trading partner or internal partner to configure it at the package, protocol, and document flow levels. By using this configuration, you have

the flexibility to decide which documents are to be persisted in the message store. You can choose not to store an inbound, outbound or both inbound and outbound WebSphere Partner Gateway documents in message store.

For example, to configure the message store option for an AS2 connection between a trading partner and a internal partner, perform the following steps:

1. Create a partner connection between **AS > None**.
2. List the partner connection between trading partner and internal partner.
3. Edit the attributes for the AS2 package and set the Message Store Required attribute to Yes.
4. Edit the attributes for the none package and set the Message Store Required attribute to No.

See the *WebSphere Partner Gateway Hub Configuration Guide* for more information about setting the message store attributes at the package, protocol, and document type.

Prerequisite to setup WebSphere Partner Gateway - WebSphere Transformation Extender Integration Environment

Before you begin

Here are the prerequisites required to setup the integration environment of WebSphere Partner Gateway and WebSphere Transformation Extender:

Procedure

1. WebSphere Partner Gateway V6.2.1 is installed and running.
2. WebSphere Transformation Extender V8.2 is installed and running.
3. WebSphere Transformation Extender server must have access to the WebSphere Partner Gateway common file system.
4. Copy the **dtxpi.jar** from the WebSphere Transformation Extender installation directory into the directory <WebSphere Partner Gateway Install>\router\lib\userexts. This jar file contains the WebSphere Transformation Extender runtime classes that are required to invoke WebSphere Transformation Extender for performing the transformation.
5. Restart WebSphere Partner Gateway bcgdocmgr server to pick up the new jar files.
6. Add WebSphere Transformation Extender installation directory in the system path even if you are not using the WebSphere Transformation Extender RMI Server, instead running the environment locally. Restart WebSphere Partner Gateway to pick up the new path settings.
7. If using the WebSphere Transformation Extender RMI Server, then start the Server.
8. Open a command prompt and access WebSphere Transformation Extender install directory. Enter the command `startRMIServer.bat -verbose`. The verbose option will display the port number of the RMI Server that it is listening.
9. In WebSphere Partner Gateway console, provide values for the attributes:
 - wtx.rmihostname
 - wtx.rmiport
 - rmiuseserver

- `bcg.wtx.mapLocation`, which is under system administration tab

Chapter 5. Account administration tasks

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

- “Managing partner profiles”
- “Managing destination configurations” on page 44
- “Managing certificates” on page 51
- “Changing B2B attribute values” on page 55
- “Managing partner connections” on page 56
- “Managing exclusion lists” on page 61

Managing partner profiles

Use the Account Admin partners feature to enable users who are hub administrators to create, view, edit, and delete partner profiles. A partner profile identifies companies (partners) to the system. See the *WebSphere Partner Gateway Hub Configuration Guide* for information about creating partner profiles.

Note: Internal partner and external partner users can edit only their own partner profile.

Viewing and editing partner profiles

About this task

Follow these steps to view and edit partner profiles:

1. Click **Account Admin**.
2. Click **Search**.
3. Click the **View details** icon next to the partner whose details you want to view.
4. On the Partner Details window, click the **Edit** icon.
5. Modify the partner 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 partner to enter a new password at the next login.

6. Click **Save**.

Searching for partners

About this task

From the Partners window, you can find partners that meet your search criteria. Follow these steps to find a partner:

1. Click **Account Admin**.
2. Type the partner name or business ID in the appropriate field.
3. Click **Search**. The system finds the partners that match your criteria.
4. To change the partner status, click **Enabled** or **Disabled** in the **Status** column.
5. To view the details for a partner, click the **View details** icon next to the partner.

6. Click the **Edit** icon to edit the partner profile.
7. Click **Save**.

Deleting partners

About this task

To delete a partner, follow these steps:

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

Managing destination configurations

Destinations 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 destination configuration. For information about creating destinations, see the *WebSphere Partner Gateway Hub Configuration Guide*.

Required information for destination configuration

The transport type determines the parameter information required for destination setup. In Table 4, the boxes marked with an X require configuration information, boxes marked with the letter O are optional. See Table 5 on page 45 for the destination parameter descriptions.

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

Table 4. Required transport information

Required transport information	HTTP transport	HTTPS transport	FTP transport	FTPS transport	FTP Scripting transport	File Directory transport	JMS transport	SMTP transport
Authentication 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
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			
Receiver URI	X	X	X	X		X	X	X
User Id					O			
User Name	O	O	O	O		O	O	O

Table 4. 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
Validate Client IP	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>				
Validate Client SSL Cert		<input type="radio"/>						

Note:

1. When the Authentication Required option of a destination is on, and the user name and password provided, the destination passes the user name and password to the external system that it connects to for document delivery. For a JMS destination, 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 destinations

About this task

To view and edit destinations, follow these steps:

1. Click **Account Admin > Profiles > {Partner} > Destinations**.
2. Click **Online** or **Offline** in the **Access** column to change the access of a destination.
3. Click **Enabled** or **Disabled** in the **Status** column to change the status of a destination.
4. Click the **View details** icon to view destination details.
5. Click the **Edit** icon.
6. On the Destination Detail window, edit the destination parameters that are described in Table 5.
7. Click **Save**.

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

Table 5. Destination parameter descriptions

Parameter	Description
Authentication Required	If enabled, user name and password are supplied with JMS or SMTP messages.
Auto Queue	If auto queue is enabled, then if the document delivery fails the first time, the destination is put offline and the document and subsequent documents are queued for delivery later. The destination has to be put online manually. If auto-queue is disabled, and if the document delivery fails, retries are done. The destination is not put offline.
Calendar Based Scheduling	When this option is selected, the documents associated with that destination 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 seconds (2 minutes).

Table 5. Destination parameter descriptions (continued)

Parameter	Description
Description	Optional description of the destination.
FTPS Mode	Select Yes or No to control whether a secure connection is used.
Destination Name	Name used to identify the destination. Note: Destination Name is a user-defined free format field. While uniqueness is not required, users should use different names for individual destinations to avoid potential confusion.
Interval Based Scheduling	When this option is selected, the destination processes the documents at the specified interval of 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. As the Receiver component decides the JMS message type mapping, the value of JMS Message type is optional.
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 the concurrent connections can be made.
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 users who are hub administrators.
Online / Offline	Indicate whether the destination is online or offline. If offline, documents are queued until the destination is placed online.
Password	Password for secure access through the partner 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 destination 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.
Status	Indicates whether the destination is enabled or disabled. If disabled, documents passing through the destination fail processing.
Receiver URI	Uniform Resource Identifier (URI) of the partner.
Thread Nbr	Number of documents that should be processed simultaneously.
Transport	Protocol for routing documents (see "Required information for destination configuration" on page 44).
Use Unique File Name	Creates a unique file name.
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 destination and replaced in the script file.
User Id	Required to access the FTP server.

Table 5. Destination parameter descriptions (continued)

Parameter	Description
User Name	User name for secure access through the partner firewall.
Validate Client IP	Validates the IP address of the sending partner before processing the document. Used with the destination that is selected as a source destination for a connection.
Validate Client SSL Cert	Validates the sending partner's digital certificate against the business id associated with the document before processing the document. Used with the destination that is selected as a source destination for a connection.

Viewing and editing default destination

About this task

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

1. Click **Account Admin > Profiles > {Profiles} > Destinations**.
2. Click **View Default Destinations** in the upper right corner of the window. The Console displays a list of all Operation Modes with their associated destinations.
3. To view information associated with a default destination, click the **View details** icon next to the destination.
4. Edit the information as required, then click **Save**.

Viewing destination Where used

About this task

To view the details of where all a particular destination is employed, use the following procedure:

1. Click **Account Admin > Profiles > {Partner} > Destinations**.
2. From the destination list, click **Where used** icon against the appropriate destination. The list of where all the selected destination is being used is displayed.

Note: This screen is provided with paging info as there could be many channels using the destination. Every page will hold a maximum of 10 connections.

Deleting destination

About this task

This delete destination feature is available for all the destinations except for default destination. To delete a destination, use the following procedure:

1. Click **Account Admin > Profiles > {Partner} > Destinations**.
2. From the list of destinations, click the **Delete** icon that is against the destination to be deleted.

Note: The **Delete** icon will not be available for the default destination. Also, a warning message is displayed if the destination is used by any channel. In case you need information about the usage of the destination, see "Viewing destination Where used."

3. Click **OK** in the warning window to confirm deletion.

Uploading transports

About this task

Use the following procedure to upload a transport.

1. Click **Account Admin > Profiles > {Partner} > Destinations**.
2. Select **Manage Transport Type**.
3. Click **Browse** and select the transport.
4. Select whether to commit the new transport to the database.
5. Select whether to overwrite the existing data.
6. Click **Upload**.

Deleting transports

About this task

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

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

Transport and destination retries

When delivery of a document to a partner destination 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 destination.

Transport retries

Transport retries are built-in, low-level retries that apply to all destinations. 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 Console under **System Administration > DocMgr Administration > Delivery Manager**. The default values are 3 retries at 3 second intervals. If the retry interval is set to 0 then no Transport retry is attempted, but the destination retry will still occur.

Destination retries (also called document retries)

Destination retry parameters (the number of retries and the interval between retries) are configured by the user in the destination properties. If the retry interval is set to 0 then no retry occurs regardless of the settings for Transport retry. Typically the destination retry interval is longer than the built-in transport retries. The intent is to specify 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 destination.

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

- First attempt fails
- Destination retry 1 fails
 - Transport retry 1 fails
 - Transport retry 2 fails
 - Transport retry 3 fails
- Destination retry 2 fails
 - Transport retry 1 fails
 - Transport retry 2 fails
 - Transport retry 3 fails
- Destination retry 3 fails
 - Transport retry 1 fails
 - Transport retry 2 fails
 - Transport retry 3 fails
- Document fails delivery

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

Retry example

The following example is an interaction for a retry using an HTTP destination.

Configuration

Transport: retries = 2, interval = 3000 ms (3 seconds)

Console HTTP Destination: retries = 3, interval = 20 seconds, Connection timeout = 120 seconds.

1. The Delivery Manager calls the HTTP Destination Sender. The HTTP Destination Sender then sends the request but does not get the response within the connection time out value of 120 seconds (from the Connection time out value specified).
2. Console Gateway retry 1 of 3.

The Delivery Manager checks the Console Gateway level retries. If it is greater than 0, then the delivery Manager waits for the specified Console interval (in this case, 20 seconds).

 - a. The HTTP Destination Sender sends the request, but does not get the response within the connection timeout of 120 seconds (from the Connection timeout).
 - b. The Delivery Manager waits for the specified Sleep per Transport properties interval of 3000 ms.
 - c. The HTTP Destination Sender sends the request, but does not get a response within the connection timeout of 120 seconds (from the Connection timeout).

This is Transport retry 1 of 2.
 - d. The Delivery Manager waits for the specified Sleep per Transport properties interval of 3000 ms.
 - e. HTTP Destination Sender sends the request, but does not get the response within the connection timeout of 120 seconds (from the Connection timeout).

This is Transport retry 2 of 2.
3. Console Gateway retry 2 of 3.

The Delivery Manager waits for the specified Console interval of 20 seconds before starting Console Gateway retry 2 of 3.

- a. The HTTP Destination Sender sends the request, but does not get the response within the connection timeout of 120 seconds (from the Connection timeout).
- b. The Delivery Manager waits for the specified Sleep per Transport properties interval of 3000 ms.
- c. The HTTP Destination Sender sends the request, but does not get the response within the connection timeout of 120 seconds (from the Connection timeout).

This is Transport retry 1 of 2.

- d. The Delivery Manager waits for the specified Sleep per Transport properties interval of 3000 ms.
- e. The HTTP Destination Sender sends the request, but does not get the response within the connection timeout of 120 seconds (from the Connection timeout).

This is Transport retry 2 of 2.

4. Console Gateway retry 3 of 3.

The Delivery Manager waits for the specified Console interval of 20 seconds before starting Console Gateway retry 3 of 3.

- a. The HTTP Destination Sender sends the request, but does not get the response within the connection timeout of 120 seconds (from the Connection timeout).
- b. The Delivery Manager waits for the specified Sleep per Transport properties interval of 3000 ms.
- c. The HTTP Destination Sender sends the request, but does not get the response within the connection timeout of 120 seconds (from the Connection timeout).

This is Transport retry 1 of 2.

- d. The Delivery Manager waits for the specified Sleep per Transport properties interval of 3000 ms.
- e. The HTTP Destination Sender sends the request, but does not get the response within the connection timeout of 120 seconds (from the Connection timeout).

This is Transport retry 2 of 2.

At this point, if the document has not been sent, the document is moved to the Gateway failed directory.

For the previous scenario, the following overall time intervals occur:

120 seconds (Item 1 on page 49) – Console Gateway Connection timeout.
Item 1 subtotal = 120 seconds

20 seconds (Item 2 on page 49) – Console Gateway Interval (Console retry 1 of 3)
120 seconds (Item 2a on page 49) – Console Gateway Connection timeout.
3 seconds (Item 2b on page 49) – Transport Interval (Transport retry 1 of 2)
120 seconds (Item 2c on page 49) – Console Gateway Connection timeout.
3 seconds (Item 2d on page 49) – Transport Interval (Transport retry 2 of 2)
120 seconds (Item 2e on page 49) – Console Gateway Connection timeout.
Item 2 subtotal = 386 seconds

20 seconds (Item 3 on page 49) – Console Gateway Interval (Console retry 2 of 3)
120 seconds (Item 3a on page 50) – Console Gateway Connection timeout.
3 seconds (Item 3b on page 50) – Transport Interval (Transport retry 1 of 2)
120 seconds (Item 3c on page 50) – Console Gateway Connection timeout.
3 seconds (Item 3d on page 50) – Transport Interval (Transport retry 2 of 2)
120 seconds (Item 3e on page 50) – Console Gateway Connection timeout.
Item 3 subtotal = 386 seconds

20 seconds (Item 4 on page 50) – Console Gateway Interval (Console retry 3 of 3)
120 seconds (Item 4a on page 50) – Console Gateway Connection timeout.
3 seconds (Item 4b on page 50) – Transport Interval (Transport retry 1 of 2)
120 seconds (Item 4c on page 50) – Console Gateway Connection timeout.
3 seconds (Item 4d on page 50) – Transport Interval (Transport retry 2 of 2)
120 seconds (Item 4e on page 50) – Console Gateway Connection timeout.
Item 4 subtotal = 386 seconds

Total time interval for all items = 1278 seconds (approximately 21 minutes)

In the instance where the connection does not time out but is refused, the preceding scenario is still started but the 120 second Connection time out period does not occur since the connection was immediately refused.

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 destination (for example, all HTTP destinations make use of the forward proxy). For each individual destination 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 *WebSphere Partner Gateway Hub Configuration Guide* for more information about 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. A digital certificate contains user identification information and user's public key. It binds the key to the user name, and is either self-signed or signed by a Certifying Authority.

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 and 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 internal partners and external partners. They are also used for encryption and decryption.

You can specify a primary and a secondary certificate 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.

Digital certificates are uploaded and identified during the configuration process.

If a certificate is expired or revoked, it is disabled and is reflected as such in the console. However, this is not applicable to the certificates uploaded as Root/Intermediate certificates. If the primary certificate is expired, 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.

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 and SSL Client certificate types. It cannot be set for other types. In the internal partner profile, it can be set for Digital Signature and SSL Client certificate types, and not for Encryption. In the external partner profile, it can be set for Encryption, and not for Digital Signature, SSL Client, and server. If the same certificate is to be used for different purposes, for example, for Digital Signature and Encryption in Hub Operator profile, it must 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 check boxes can be set in the same certificate entry. If the certificate is designated as an FTP Server and/or SFTP Server certificate, the Certificate Type must be SSL Server and one of or both the check boxes for FTP Server Authentication and SFTP Server Authentication must be selected.

Secondary certificates can also be loaded twice, once for Digital Signature and again for SSL Client. If so, the same pattern has to be followed for the secondary certificates. For example, if the primary certificates were loaded as different certificates for Digital Signature and for SSL Client, then secondary certificates has to 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 is not built and the transaction is unsuccessful. The CA certificates can be obtained from the Certificate Repositories maintained by the Certificate Authorities. 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 about loading the certificates, see the *WebSphere Partner Gateway Hub Configuration Guide*.

The Certificate Management view allows you to modify certificate sets that are used for a specific participant connection. An option to filter is provided. Modify the certificate sets that are used in the connection. Alternatively, this can be done from the participant connection itself. Steps to manage Certificates sets:

1. In the Console, navigate to **Profile > {Partner} > Certificate > Certificate Management**
2. If you have logged in as a Hub Operator, then choose an internal partner and external partner. Make sure that both the values are not "ALL".
3. Click **Search** to filter partners or subset of partners.

Note: The **From** and **To** packages are preloaded based on the partners. The subsets will also be displayed in the table based on your selection. The table columns have SSL client, Digital Signature (this will be disabled when the **From** partner is set to "ALL") and encryption (will be disabled if the **To** partner is set to "ALL". The rows have operation type).

4. Update the Certificate sets and click **Save**. The changes will be reflected at the connection level.

Configuring the certpath related properties

The certpath properties can be configured using the WebSphere Application Server admin console and the WebSphere Partner Gateway console. Access these properties by clicking **System Configuration > DocMgr Configuration > Security**. The properties are displayed using a read-only view. If you want to edit them, click the **Edit** icon. The following descriptions are brief summaries of the configuring process used with the certpath related properties.

bcg.CRLDir

This property contains the name of the directory where the CRLs are stored. The default value is:

<WebSphere Partner Gateway Install Dir>/common/security/crl

bcg.checkRevocationStatus

This property specifies if the revocation status is checked. The valid values for this property are true, false and blank.

If the value is set to either true or blank, the revocation status of the digital certificates is checked. If the value is set to false, the revocation status is not checked.

The default value and recommended setting of this property is true.

bcg.build_complete_certpath

This property specifies if the certpath is built to the root certificate or to the issuer certificate. The valid values for this property are true, false and blank.

If the value is set to true or blank, the certpath is built to the root certificate. If the value is set to false, the certpath is built to the issuer certificate only.

The default value and recommended setting of this property is true.

Configuring CRLDP

Configuring CRL DP (Certificate Revocation List Distribution Point) requires you to:

- Set the Java Virtual Machine to enable or disable CRLDP
- Set the HTTP proxy host and port

Changing the Java Virtual Machine settings for CRLDP:

About this task

To view and change the Java Virtual Machine configuration for an application server process, use the Java Virtual Machine page of the Administrative console or use the WebSphere Application Server Admin console to change the configuration through scripting.

1. In the Administrative console, select **Servers > Application Servers > <server> > Java and Process Management > Process Definition > Java Virtual Machine**.
2. Specify values for the Java Virtual Machine settings as mentioned below and click **OK**.
3. When the next page displays, click **Save** on the console task bar to save the changes to the master configuration
4. Restart the application server.

For more details on configuring the Java Virtual Machine, see the WebSphere Application Server documentation.

To enable the use of CRLDP, set the `com.ibm.security.enableCRLDP` Java Virtual Machine property in the **Generic JVM Properties** field to true as follows:

```
-Dcom.ibm.security.enableCRLDP=true
```

To disable the use of CRL DP, set the `com.ibm.security.enableCRLDP` Java Virtual Machine property in the **Generic JVM Properties** field to false as follows:

```
-Dcom.ibm.security.enableCRLDP=false
```

Setting HTTP Proxy host and port for CRL DP: Set the following Java Virtual Machine properties in the **Generic JVM Properties** field:

```
-D http.proxyHost=<proxy host name or ip address>
```

```
-D http.proxyPort=<proxy port number>
```

To remove the HTTP proxy host and port, remove the following properties from the Java Virtual Machine properties in the **Generic JVM Properties** field:

```
-D http.proxyHost
```

```
-D http.proxyPort
```

Note: Whenever one of these properties changes, the change must be made for all the servers on which WebSphere Partner Gateway applications are running.

Viewing and editing digital certificates

About this task

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 Partner 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 6. Digital Certificate Parameters

Parameter	Description
Certificate name	Specify the name of the certificate.
Description	Provide brief description about the certificate.
Status	Select Enabled to show the status (valid or invalid) of the certificate. Select Disabled to disable the certificate.

Disabling a digital certificate

About this task

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

About this task

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

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

1. Click **Account Admin > Profiles > {Partner} > B2B Capabilities**. The Console displays the B2B capabilities window.
2. Click to individually expand a node to the appropriate Document Definition level or select a number from 0–4 or All to expand all displayed Document 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 partner connections

Partner connections are the mechanism that enables the system to process and route documents between the internal partner and its various partners. Connections contain the information necessary for the proper exchange of each document type including RosettaNet Trading Partner Agreement attributes, transport protocol, document processing action, operation mode, and partner destination. A document cannot be routed unless a connection exists between the internal partner and one of its partners.

The system automatically creates connections between the internal partners and external partners 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 following components:

- Attributes
- Action
- Destination
- Operation Mode
- Certificates
- Connection Profile

Once the system creates a connection, all components can be modified to tailor its routing and processing functionality. Table 7 describes each component.

Table 7. Manage partner 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 partners 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 passthrough routing. You can select the appropriate action for each connection.
Destination	Each connection contains a destination and a return destination. The return destination contains the URI and transport information of the partner initiating a document flow. Business signals such as receipt acknowledgments and general exceptions are sent to the initiating partner through the return destination. The destination options Validate Client IP and Validate Client SSL Cert apply to the return destination. The destination contains the URI and transport information of the partner receiving a document type.

Table 7. Manage partner components (continued)

Component	Description
Operation Mode	Operation Mode identifies the nature of a document being exchanged. A connection can contain multiple operation modes to accommodate the routing and processing of the same document to more than one system. This improves connection efficiency by multiplying the use of a single connection for production, test, or routing to multiple systems within one organization.
Certificates	Certificates are configured for connections. The configured certificates are used during encryption, signing, and SSL client authentication. Certificates can be configured for different operation modes.
Connection Profile	A connection profile contains EDI attributes that are used for a particular connection.

Connection duplication

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

- Source Partner
- Source package and version
- Source protocol and version
- Source document type and version
- Source Activity (if defined)
- Source Action (if defined)
- Target Partner

For example if there are two connections with the same source partner, source document and target partner, both connections cannot be activated even if the target document is different in each of the connections. In this case, one of the connections must be deactivated.

Note: EDI documents can have multiple connections as described if an additional Connection profile is associated with them. The values configured for a Connection Profile is used to add additional criteria for uniquely identifying the connection.

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 Receiver. See “Performing a basic search for connections” on page 58.
- 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 59.

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 has to be unique.
- Do not mix a production destination with a test destination when selecting source and receiver; otherwise, an error occurs. Both the source and the target has to be production or test destinations.

1. Click **Account Admin > Connections > Partner 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 has to be unique.

4. Click **Search** to find the connections that match your criteria.
5. Click the appropriate item as necessary:
 - Click **Deactivate** icon to disable a connection.
 - Click **Enabled** icon to enable a connection.
 - Click **Attributes** to display the Connection Attributes window, where you can view and change connection attributes. For more information, see “Changing partner attribute values” on page 60.
 - Click **Actions** to display the Connection Details page, where you can view and change the Action. For more information, see “Selecting a new action” on page 60.
 - Click **Destinations** to display the Connection Management Destinations window, where you can view and change the Return Destinations or Destinations. For more information, see “Changing the destination or return destination” on page 60.
6. To activate a connection, click **Activate**. The Console displays the Manage Connections window. This window shows the package, protocol, and document type for the Source and Receiver, as well as options for viewing and changing partner-connection status and parameters.

Performing a basic search for connections

About this task

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 destination with a test destination when selecting source and target; otherwise, an error occurs. Both the source and the target must be production or test destinations.
1. Click **Account Admin > Connections > Partner 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 type for the Source and Receiver, as well as options for viewing and changing partner-connection status and parameters.
6. Click the appropriate item as necessary:
 - Clicking the **Deactivate** icon disables a connection.
 - Clicking the **Enabled** icon enables a connection.
 - Clicking **Attributes** displays the Connection Attributes window, where you can view and change connection attributes. For more information, see “Changing partner attribute values” on page 60.

- 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 60.
- Clicking **Destinations** displays the Connection Management Destinations window, where you can view and change the Return Destinations or Destinations. For more information, see “Changing the destination or return destination” on page 60.

Performing an advanced search for connections

About this task

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 destination with a test destination when selecting Source and Target; otherwise, an error occurs. Both the Source and the Target must be production or test destinations.
 1. Click **Account Admin > Connections > Partner 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 8:

Table 8. Advanced Search window

Parameter	Description
Search By Partner 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 Type	Document type used by the Source.
Target Document Type	Document type used by the Target.
Connection Status	Enables the search for enabled and disabled connections.

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

Changing connection configurations

About this task

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

1. Click **Account Admin > Partner Connections**. The Console displays the Manage Connections window.
2. Perform a basic search for connections (see “Performing a basic search for connections” on page 58) or advanced search for connections (“Performing an advanced search for connections”).

3. See the appropriate section:
 - “Changing partner attribute values”
 - “Selecting a new action”
 - “Selecting a new transformation map”
 - “Changing the destination or return destination”
 - “Disabling or deactivating a connection.”

Changing partner attribute values

About this task

To change partner attribute values, use the following procedure.

1. Click **Attributes** for either the Source or Target partner.
2. In the **Scope** list, select **Connection** if the attribute changes will apply to all the operation modes associated with the connection, or select an operation mode to which the changes will apply.
3. Click the **Expand** icon and expand the node to the Document Definition whose attribute values will be changed.
4. Update the attribute value.
5. Click **Save**.

Selecting a new action

About this task

To select a new action, use the following procedure.

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

Selecting a new transformation map

About this task

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

1. Click **Actions**.
2. Select the new transformation map from the list.
3. Click **Save**.

Changing the destination or return destination

About this task

To change the return destination or destination, use the following procedure.

1. Click **Destination**.
2. Select the destination or return destination from the list.
3. Click **Save**.

Disabling or deactivating a connection

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

For EDI documents, there can be several connections that apply to the same partners. 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 *WebSphere Partner Gateway Hub Configuration Guide*.

Managing exclusion lists

An exclusion list lets the hub administrator configure the Document Manager to restrict RosettaNet notifications sent to the internal partner 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 internal partner by a partner that cannot complete a particular document type.
- Backend Event
A system-generated XML file sent to notify the internal partner that the partner has received a business document successfully.

Adding partners to the exclusion list

About this task

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

1. Click **Account Admin > Exclusion List**. The Console displays the Exclusion List window.
2. Select a partner from the **Partner Name** list. The Console displays a list of partners and their business ID and exclusion status. **Send All Notifications** is selected by default.

Editing the exclusion list

About this task

There might be times when you must edit the Exclusion List. For example, you might want to restrict a notification from being routed to the internal partner.

1. Click **Account Admin > Exclusion List**. The Console displays the Exclusion List window.
2. Select a partner from the **Partner Name** list. The Console displays a list of partners, their business ID and exclusion status.
3. Click the **Edit** icon next to the notification you want to edit.
4. Select the check box below the notification to restrict the notification from being routed to the internal partner. Select **Send All Notifications** to remove all routing restrictions.

Chapter 6. Administering partner migration

The configuration migration utility enables you to selectively export, and import WebSphere Partner Gateway configuration data like the preferences, features, connection details, and B2B capabilities. This differs from other data-moving options like database backup and restore because data is selectively extracted when it is exported with the utility and a database backup is not normally selective.

The configuration migration utility exports selected partner and system definitions into an XML file and a set of supporting files. You can subsequently import these files into another system, moving the configuration across systems.

Note: When transferring data from one system to another, both systems must use the same version of WebSphere Partner Gateway.

The migration utility is used primarily to move configuration data from a development and testing system to a production system, but you can also load configuration data from an XML file that you create based on the XML schema provided.

There are two options available for running the migration utility:

1. A command line interface is provided so the migration utility can be started using a script.
2. An API is provided so user-written Java programs can invoke the migration utility. See the *WebSphere Partner Gateway Programming Guide* for more information about using the API.

The migration utility is implemented as a standalone Java application that calls WebSphere Partner Gateway remotely. The utility is packaged in a .zip file named `BCGMigrationUtil.zip`. This file is installed by the hub installer in this directory:
`hub installation/console/support`.

Using the migration utility from the command line

About this task

Before you can use the migration utility, you must extract the `BCGMigrationUtil.zip` file on the workstation where you will run the utility. After the utility files are extracted to your local file system, perform the following prerequisite steps:

1. The console component for the WebSphere Partner Gateway system that you will export from or import into must be running. Note that the utility can be run on a different workstation than where the console component is installed. This is because the utility accesses the console using the IIOP (EJB) protocol over a network. Connectivity between the workstations is required, and the IIOP port (typically 58809) of the console has to be available from the workstation where the utility runs.
2. You must have Java 5 available on the workstation where the utility will run. In your machine install JDK1.5.

When you run the command line script to start the utility, it obtains the system environment variable `JAVA_HOME` for this location. If `JAVA_HOME` is

undefined, then the script will prompt for you to enter the home location for Java 5. For example, you can use the copy of Java 5 that is installed for use by WebSphere Application Server. To do this, you would use the value *<WebSphere Install Dir>\java*.

Another system environment variable named `MIGRATION_PATH` can be set to point to the location where `BCGMigrationUtil.zip` was extracted. If the `MIGRATION_PATH` is undefined, then the script will prompt you to enter a path to this directory. The directory that `MIGRATION_PATH` points to is the directory called `bcgmigrate` under the directory where the `.zip` file is extracted. For example, if you want to extract the files to the directory `c:\IBM\migration`, then you should set `MIGRATION_PATH` to `c:\IBM\migration\bcgmigrate`.

Note: Ensure that you have **Execute** file permission for `bcgmigrate.bat/bcgmigrate.sh` to run `bcgmigrate` command. This is applicable for UNIX platform.

3. If you are exporting data, an export options file is required. The export options file specifies what types of data are to be extracted by the utility. Configuration data can be exported for the following items in a system:

- Enveloper schedules
- Event codes
- Transport and operation modes
- Handler definitions (metadata only, user-written executable code jar files are transferred manually)
- Fixed workflow definitions (metadata only, user-written executable code jar files are transferred manually)
- Variable workflow definitions (metadata only, user-written executable code jar files are transferred manually)
- Proxy configurations and Envelope profiles
- Connection profiles and Validation maps and Transformation maps
- FA maps and Receiver instance data
- XML document families and formats
- Routing definitions (packages, protocols, and document types)
- Partner profile data (including contacts, addresses, EDI control number data, and destination data)
- B2B Capabilities for partners
- Partner connections
- Alert notifications
- Group configuration
- User configuration
- FTP user configuration
- Certificates
- Error flow configuration
- System admin properties
- Archiver configuration

A sample export options file named `export.zip` is available in the directory *migration utility root/samples/export*. This file exports all of the supported configuration data types from a system. The options file can be an XML file or a `.zip` file holding an XML file. The XML must conform to the XML schema `bcgMigrationExport.xsd` located in *migration utility root/schemas* directory.

Note: Ensure that the dependency requirements between export types are met. These dependencies are outlined further in the topic *Migrating configuration type dependencies*.

4. If you are importing data, you must have data to import. The import file can be produced by exporting data, or you can write your own that contains definitions you want to load into a system. After exporting, the exported data is contained in a .zip file. The .zip file includes an XML file that conforms to the XML schema `bcgMigrationImport.xsd` located in *migration utility root/schemas* directory. This XML file includes data that can be used by the import code to re-create the configuration types you exported.

The .zip file also includes these files:

- The exported validation, transformation, and FA maps
- `RoutingObjects.zip` containing the internal representations of the exported routing objects (packages, protocols, and document types).

Follow these steps to write your own import file:

- Create an XML file that conforms to `bcgMigrationImport.xsd`.

You must be sure that the dependency requirements between import types are met. For more information regarding dependencies see, *Configuration type dependencies*.

- If any maps or routing objects are described in the import XML, create a .zip file with the XML file in the root directory for the .zip file.

The directories are as follows:

- The routing objects are in a file called `RoutingObjects.zip` within the `RoutingObjects` directory in the root.
- The transformation maps are in the `TransformationMaps` directory in the root.
- The validation maps are in the `ValidationMaps` directory in the root.
- The FA maps are in the `FAMaps` directory in the root.

Note: If you are importing any file directory receivers, the receiver system cannot already have the file directory used by the receiver in its file system. Be sure to delete any such directories before importing.

5. The migration utility has to log on to the console that you are using. The WebSphere Partner Gateway user account must have permission to export or import configurations. The hub administrator user has this permission. If you want to use an account other than hub administrator or a user who is a member of the "Hubadmin" group, you must enable the permission to use the migration module for the user. By default this permission is disabled.

The hub administrator specifies the input file from which the data is imported, and also specifies whether the existing information should be overwritten or not. The configuration migration utility then enables you to import configuration, if you are profiled for overwriting the configuration, that is already present on a system.

Any new information, that is not already existing is added to the database. If override option is set to true, then the information in the database is overwritten by the input data. If the option is not set to true, then the information in database is not overwritten by the input data. If any exception occurs, then import operation stops and an error event is logged to the log file.

Invoking from the command line

You can migrate configuration data from one WebSphere Partner Gateway instance to another WebSphere Partner Gateway instance using a command line utility. After completing the prerequisite steps to use the utility, you can invoke the utility by running the batch file `bcgmigrate.bat` or shell script `bcgmigrate.sh`. These files are located in:

- **For Windows:** `\<migration utility root>\bcgmigrate\bin\`
- **For Linux/UNIX:** `/<migration utility root>/bcgmigrate/bin/`

Note: The user should either belong to Hubadmin group or another group under Operator that has the migration module permission enabled.

If you issue the script with no arguments, a help prompt is displayed with the required arguments and syntax.

The command line invocation syntax for Windows is as follows:

```
bcgmigrate [-h hostname:bootstrap_port] [-a import|export] -f filename with path  
-u userid -p password [-r root_path [-o] [-d 1..5] ]
```

For a UNIX system, the invocation is similar, except you use `bcgmigrate.sh` instead of `bcgmigrate`.

Legend:

- `-h` is the hostname:bootstrap port where the console component is running
- `-a` is the activity (which can be either import or export). By default, it is export.
- `-f` is the fully qualified file name of the export option file or the import configuration file.
- `-u` is the WebSphere Partner Gateway user ID that has migration permission
- `-p` is the WebSphere Partner Gateway user password
- `-o` is the overwrite option

Note: The overwrite option is only used by the import activity. If you do not include `-o` then only new configurations are created and existing configuration data is not changed. Including `-o` means existing configuration may be overwritten if they are different within the imported data.

- `-d` is the debug level from 1 to 5 where 5 provides the most debug output. The `-d` argument is optional and can be omitted. If it is omitted, only errors are logged.
- `-r` is the root path where exported data is stored and the log file is written. The `-r` argument is optional and can be omitted. If it is omitted, exported data is written under the directory specified by the `-f` option.

Example command for export

The following is an example command for export on a Windows system:

```
bcgmigrate -h localhost:58809 -a export -f D:\partnerMigration\export.xml  
-u hubadmin -p admin123 -r d:\partnermigration\output -d 5
```

For a UNIX system, the invocation is similar, except you use `bcgmigrate.sh` instead of `bcgmigrate.bat` and directory path has forward slash.

The output for the example is saved under the root directory specified by the `-r` option.

The output is written to a .zip file named BCGMigration_<IP or host name provided in -h option>.zip. Logs are written to the file BCGMigration.log. If the -r option is not specified for an export, then the output will be placed in the directory configured in -f option.

Example command for import

The following is an example command for import on a Windows system:

```
bcgmigrate.bat -h localhost:58809 -a import
-f D:\partnerMigration\BCGMigration_localhost.zip -u hubadmin -p admin123
-r d:\partnermigration\output -d 5
```

For a UNIX system, the invocation is similar, except you use bcgmigrate.sh instead of bcgmigrate.bat. Once the import is completed, the logs are written to the file BCGMigration.log. If the -r option is not specified for an import, then the output will be placed in the directory configured in -f option.

Mapping of XML element with Console

The exported file or the file to be imported will be in XML format. The XML elements may not depict the exact name on the console. The following table shows the mapping between console screen and root elements in the XML file. The table contains only the views and element names and not the individual fields on the screen. If the element name is a link in the view, it is represented in italics.

Table 9. Map of XML element with Console

Element name in XML	Console view
EnveloperSchedulingInfo	Hub Admin > Hub Configuration > EDI > Enveloper.
TransportTypeInfo	Hub Admin > Hub Configuration > Receivers > <i>Manage Transport Types</i> and Account Admin > Partner > Destinations > <i>Manage Transport Types</i> .
DestinationTypeInfo	Account Admin > Partner > Destinations > <i>create destination</i> . Operation Mode is represented by DestinationTypeInfo.
HandlerInfo	Hub Admin > Hub Configuration > Handlers. There are four more sub menus Action, Fixed Workflow, Destination, and Receiver.
FixedWorkflowStepInfo	Hub Admin > Hub Configuration > Fixed Workflow > Inbound and Hub Admin > Hub Configuration > Fixed Workflow > Outbound. Each step is represented as FixedWorkflowStepInfo.
WorkflowInfo	Hub Admin > Hub Configuration > Actions. Each Action in the list page is represented as WorkflowInfo
EnvelopeProfileInfo	Hub Admin > Hub Configuration > EDI > Envelope Profile. Each envelope profile in the list page is represented by EnvelopeProfileInfo.
MapInfo	Hub Admin > Hub Configuration > Maps > Validation Maps. Each map in the list page is represented as MapInfo. There will be an inner tag routingNameList. It represent the routing object names to which the validation map is linked.

Table 9. Map of XML element with Console (continued)

Element name in XML	Console view
TransformMapInfo	Hub Admin > Hub Configuration > Maps > Transformation Maps. Each map in the list page is represented as TransformMapInfo.
FAMapInfo	Hub Admin > Hub Configuration > Maps > FA Maps. Each map in the list page is represented as FAMapInfo. There will be an inner tag routingNameList. It represents the routing object names to which the FA map is linked.
ReceiverInfo	Hub Admin > Hub Configuration > Receivers. Each receiver in the list page is represented by ReceiverInfo.
ProtocolFamilyInfo	Hub Admin > Hub Configuration > XML formats. Each document family is represented by ProtocolFamilyInfo.
RoutingObjectPkgInfo	Hub Admin > Hub Configuration > Document Definitions. The RoutingObjectPkgInfo is just a place holder. There will be a folder RoutingObject and a zip file RoutingObjects.zip under it. This is the zip file which contains all the package information in xml format. The xml file is same as that of downloaded package from Hub Admin > Hub Configuration > Document Definitions > Upload/Download Packages.
ValidObjInteractInfo	Hub Admin > Hub Configuration > Document Definitions > Manage Interactions > Search. Each Interaction in the list is represented by ValidObjInteractInfo.
PartnerInfo	Account Admin > Partner . PartnerInfo represents each partner in the list.
ContactInfo	Account Admin > Partner > Contacts. ContactInfo represents each contact in the list.
PartnerAddressInfo	Account Admin > Partner > Addresses. PartnerAddressInfo represents each address in the list.
ParticipantControlInfo	Hub Admin > Hub Configuration > EDI > Control Number Initialization > Search. ParticipantControlInfo represents each partner's initial control numbers.
ConnectionProfileInfo	Hub Admin > Hub Configuration > EDI > ConnectionProfile. Each connection profile in the list page is represented by ConnectionProfileInfo.
GatewayInfo	Account Admin > Partner > Destinations. The details of each destination listed is represented in GatewayInfo.
DefaultGatewayInfo	Account Admin > Partner > Destinations > View Default Destinations. Each row in the view represents DefaultGatewayInfo.

Table 9. Map of XML element with Console (continued)

Element name in XML	Console view
CapabilityInfo	Account Admin > Partner > B2B Capabilities . The bright rows in the tree with either enabled or disabled state are represented by CapabilityInfo. There is an edit attribute icon that takes the attributes. These attributes are also part of CapabilityInfo in the form of ROAttrValueInfo.
ChannelInfo	Account Admin > Participant Connections > Search. Each row that is active is activated or deactivated. Initially all the connections are in deactivated state. They are available for connection creations. Once it is activated, the actual connections are created. Though it is deactivated, the connection still exists. The connections that are not even activated once are not actual connections.
ProxyConfigInfo	Account Admin > Destinations > Forward Proxy Support. Each row in the list page is represented by ProxyConfigInfo.
EventCodeInfo	Hub Admin > Hub Configuration > Event Codes.
AlertInfo	Account Admin > Alerts.
CertificateInfo	Account Admin > Partners > Certificates. CertificateInfo represents the details of each certificate.
SetMgmtInfo	Account Admin > Partners > Sets. SetMgmtInfo represents the details of each set. Also, Account Admin > Partners > Certificate Management contains the details of the certificate management configurations for packages and partners.
SetDestTypeInfo	Account Admin > Connections > Participant Connections > Certificates. SetDestTypeInfo represents the details of certificates sets used in the connections.
GroupInfo	Account Admin > Partners > Groups. GroupInfo represents each group in the list.
UserInfo	Account Admin > Partners > Users. UserInfo represents each user in the list.
FTPUserInfo	Account Admin > Profiles > Users > FTP User. You can also access FTPUserInfo by navigating to Account Admin > FTP User Management. FTPUserInfo represents each FTP user in the list.
ErrorFlowInfo	Account Admin > Error Flows. ErrorFlowInfo represents each error flow in the list.
SystemAdminInfo	System Administration
ArchiverInfo	Hub Admin > Hub Configuration > Archiver > Archiver Configuration.

Exporting partner migration

The command line utility retrieves the location of option file. The option file should be in XML format or ZIP format and must be located in the same machine. Export option file does not have any attributes for tags. If the option file is in the form of a zip, the zip file should contain an XML file. The input from POJO can be an InputStream instead of a file. The result will be stored in another XML file in the same folder with the name BCGMigration_HostName.xml. As the same file can be used as input for import function, a common name, BCGMigration_HostName.xml is used. A POJO can also call the partner migration utility to export the configuration. The option file or input stream is one of the inputs. Internal identifiers such as the id, rowTS and time stamp is not exported during export. Only the logical identifiers such as name, description is exported. The configurations like Handler Types that does not have user defined configuration is not exported. Export option file contains the following options:

1. Partner – each partner is specified by the tag. This option exports partner profile information such as partner information, IP address, business ids, contacts and addresses. When partner option is provided, the following options also can be provided in inner tags:
 - a. Gateways – All or None. When Gateways are exported, the Default Gateways is also exported.
 - b. B2B Capabilities – All or None
 - c. Connections – All or None
 - d. Initial Control Numbers – All or None
 - e. Group configuration – All or None
 - f. User configuration – All or None
 - g. FTP user configuration – All or None
 - h. Certificates – All or None
 - i. Error flow configuration – All or None
 - j. Archiver configuration – All or None
2. Global configuration
 - a. Targets – All or None
 - b. Enveloper
 - c. Transport Types
 - d. Destination Types
 - e. Handlers – All or None
 - f. Handler attributes – All or None for a handler
 - g. Actions – All or None
 - h. Fixed workflow – All or None
 - i. EnvelopeProfiles – All or None
 - j. Validation maps – All or None
 - k. Transformation maps – All or None
 - l. EDI FA Maps – All or None
 - m. EDI FA Maps – All or None
 - n. Global DFDs – All or None
 - o. Interactions – All or None
 - p. XML Format Family – All or None
 - q. Connection profile - All or None

- r. Proxy configuration – All or None
- s. Event Codes – All or None
- t. Alert Notifications – All alert notifications or selected alert notifications or None.
- u. System admin properties – All or None

Considerations when creating your own import data

If you decide to create your own import file or to edit an import file that was created by the export utility, there are several things that you must consider. Not only does your XML file need to conform to the XML schema for an import file, but there are rules about the content of the file that are not controlled by the schema.

Manual validation of the import file

If you invoke your migration utility from the command line using the partner migration script, your data is not validated as it is not using the console. For instance, it is possible to create an incorrect partner ID using a migration script whereas this is not possible using the console. Data entered into the console is validated by the console. For example, you may enter a DUNS ID containing alphabetic characters from the command line, but this is not possible from the console because a DUNS ID must contain numeric characters only.

Remember: It is important to manually validate all of your data before you enter it from the command line.

Migration configuration type dependencies

Configurable items can be broadly classified into three sections based on dependencies, namely Independent Items, First level dependent items, and Complex dependent items. Some configuration types have no dependencies. For example, a partner definition can be created without referring to any other configured entity in the system. Independent items are the configurable items that do not have any dependency before importing them into the target system.

Other configuration types cannot exist by themselves because they depend on other entities in the system. For example, a destination is associated with a partner, so it cannot exist unless the partner also exists.

To ensure that dependency items are always available, the content and ordering of the items in export and import files are important. When an export is performed, any item that has dependencies must be exported after any dependency items. The XML file reflects this ordering. Using the same logic, when the import is performed, the dependency items are imported before the dependent items.

If you selectively export configuration types, you must ensure that you specify dependency types for all dependent types. It is also important if you create an import file using the schema definition. The schema enforces the ordering, but not the content. So if you define an import file incorrectly, for example, you forget to provide a dependency item or incorrectly defining a dependency item, that item will fail when you attempt an import of it.

Independent configuration items

The following configurable types are independent. Other configuration types depend on these items, but these items do not directly depend on other system items.

- Enveloper Scheduling
- Event codes
- Transport types
- Destination types
- Envelope profiles
- Connection Profiles
- Proxy configurations
- Validation maps
- FA Maps
- Partners
- System admin properties

It is important to note that validation maps and FA maps are independent items when considered individually. But to be useful, they have to be linked to routing object definitions in the system. If the routing objects are not imported, the maps might exist in the system without the links. Because this is an indirect dependency, the migration utility can export and import map types without the routing object that refer to them.

Dependent configuration items

First level dependent items are the configurable items that have dependency on independent items or on one of first level dependent items. The import may either fail or generate unexpected runtime behavior if the dependent items are not imported. The following configuration types are First level dependent items:

- Routing objects
Routing objects are dependent on import of envelope profile and FA Map. The validation map is imported as a part of routing objects. If the routing objects of the source system has association with any of the profiles or maps, the runtime behavior may not be as expected. If the routing objects of the source system do not have any association with envelope profiles and FA maps, the runtime behavior will be as expected even if the envelope profiles and FA Maps are not imported.
- Handlers
Transport types
- FA Map links
FA Map links require FA Map import and routing object import. If the routing objects are not imported, the links will be created with the existing routing objects. If the routing object does not exist, the link will not be created.
- Validation map links
Validation map links require Validation map import and routing object import. If the routing objects are not imported, the links will be created with the existing routing objects. If the routing object does not exist, the link will not be created
- Fixed workflow
Handlers
- Variable workflow (actions)
Handlers
- Contacts
Partners

- Addresses
Partners
- Control number initialization
Partners
- XML families and format
Routing objects
- Destinations
Transport types, destination types, and handlers
- Transformation maps
Routing objects
- User configuration
Partners and Group configuration
- FTP User Configuration
User configuration, Group configuration, and Partners
- Group configuration
Partners
- Certificates
Partners, Certificate sets, Destination types, and Routing objects

Complex dependent items are the configurable items that are dependent on independent items and are more complex than first level dependent items. The following configuration types are Complex dependent items:

1. Interactions – are dependent on routing object , actions and transform map. If either routing object or action is not imported, Interaction will not be imported.
2. Receivers – are dependent on transport type import, destination type import and handler import. Receiver import will not be performed if any of the mentioned imports are not performed. Importing receiver without the above configurable items may cause the import activity exit.
3. Gateways – are dependent on transport type import, destination type import and handler import. Gateway import will not be performed if any one of the mentioned imports are not performed. Importing Gateways without the above configurable items may cause the import activity exit.
4. B2B Capabilities – B2B Capabilities migration is one of the most complex dependent items. It is dependent on routing object import, FA Map import, envelope profile import and Partner import. If either partner import or routing object import is not performed, then B2B capabilities will not be imported.
5. Connection – Connection is the most complex dependent item. Connection import is dependent on routing object import, interaction import, partner import, B2B capabilities import, gateways import, actions import, and connection profile import. If any one of the listed configurable items is not imported, importing connections may cause exit of import activity
6. Alert Notifications – are dependent on routing objects, partners, event codes, and contacts.
7. Error flow configuration - are dependent on routing objects, partners, and event codes.
8. Archiver configuration - are dependent on routing objects and partners.

Validation map and FA Map are routing object attributes. Transform map is an attribute of interaction. Transform map is linked to a “from routing object id” and “to routing object id” in the detail view of transform map. Validation map and FA

Map can be linked to a particular routing object id in their detail view. When a map is linked, it can be used as an option for association. Assume that the validation map attribute is configured for routing object AS-Binary. MapA and MapB are linked to AS-Binary. If the AS-Binary edit attribute view under document flow definitions has validation map, then the value will be “select a map from the list” and the drop-down will have MapA and MapB. One of the map can be selected and associated as the attribute.

So linking makes the map eligible to be one of the options and association makes the map suitable for use at runtime. The same holds true for FA Map and Transform map. Transform map is slightly different as it is used at interaction instead of routing object. But the concept of linking and association is same.

Export/Import order

The generated XML file during export and the input XML file during import should follow the sequence. The order is arranged such that independent items are imported first followed by partners and partner dependant items.

1. Enveloper
2. Event Codes
3. Transport Types
4. Destination Types
5. Handler Info
6. Handler Attributes
7. Fixed Workflow
8. Actions
9. Proxy Configuration
10. Envelope Profiles
11. Connection Profiles
12. Validation Maps
13. Transform Maps
14. EDI FA Maps
15. Targets
16. XML format family
17. Routing Objects
18. FA Map links
19. Validation Map links
20. Transform Map links
21. Interactions
22. Partners
23. Group configuration
24. Contacts
25. Addresses
26. Control Number Initialization
27. Alert Notifications
28. B2B Capabilities
29. Connections
30. Gateways
31. Certificates

32. User configuration
33. FTP users
34. Error flow configuration
35. Archiver configuration
36. System Admin properties

BCG and DIS Import

BCG migration utility also imports maps and routing objects. When the production system has maps and routing objects imported through DIS tool, the BCG migration utility will overwrite, if overwrite option is enabled. If you import the run time environment (maps and routing objects) through DIS client, DIS import must be performed after BCG Import, so that the target production system will have the configuration required at run time.

Non-migratable configurations

The following configuration data are not migrated:

- CPA
The Community Partner Agreement (CPA) is meant only for production system. It does not exist on the test system.
- Reports and logs are not migrated. They are not configuration items.
- Also, EDI Map data and related information is not migrated.

Limitations of the migration utilities

- If any error occurs during migration, the transactions are not rolled back. In case of import, errors occur due to the following reasons:
 - The exported file is edited manually and the required information is removed.
 - The manually created import file does not have all the required information for each object.
 - The newly configurable item is created when the utility is executed.
 - An existing configurable item is updated when the utility is executed
- Only partner migrations and connections can be migrated selectively. All other migrations must be migrated as a whole.
- If an export is made from a source system that uses a different file system type than the receiver system, the XML document contained in the exported output requires manual updates to correct any file-system specific `<targetURL>` elements. These elements must be corrected to match the receiver file system environment before the import is performed.

Forward proxy migration

Forward proxies are used by HTTP/S destinations, as a placeholder during the import process. The production environment (receiver system) might not have the same proxies as those of the test environment (source system). After the import, the administrator might have to change the proxy related information to reflect that of the production environment. If the test environment is same as that of production environment, the administrator need not make changes.

Note: The overwrite option is disabled for forward proxies. So if a forward proxy exists on the receiver system, the import utility will not change it.

Chapter 7. LDAP support for logon authentication

In addition to using WebSphere Partner Gateway partner registry for console authentication, WebSphere Partner Gateway supports Lightweight Directory Access Protocol (LDAP) container-based authentication that uses the WebSphere Application Server authentication mechanism. WebSphere Application Server supports 3 types of authentication:

1. LDAP registry
2. Local operating system registry
3. Custom registry

WebSphere Partner Gateway uses WebSphere Application Server LDAP registry authentication. By enabling the container managed authentication in applications like WebSphere Partner Gateway which are deployed in WebSphere Application Server, the administrator can manage user authentication in a central location outside of the WebSphere Partner Gateway application.

Using LDAP

Use LDAP when Container based authentication is selected:

- During installation.
- By setting the attribute `bcg.ldap.containerauth` located in **Console System Administration > Common Properties** to True.

Enabling the container managed authentication mechanism

To enable the container managed authentication mechanism, set the `bcg.ldap.containerauth` property value to True in the WebSphere Partner Gateway console, then configure the WebSphere Application Server **Global Security** setting to use LDAP. After you have enabled the authentication, users are authenticated against the LDAP server when logging into WebSphere Partner Gateway.

Note: When LDAP is enabled during the installation process, the administrator must ensure that the configured LDAP server is given a user named `hubadmin`. This is a valid logon user name for LDAP authentication regardless of whatever logon type is chosen.

Enabling J2EE security

About this task

If you are enabling J2EE security in addition to WebSphere Application Server global security, create a policy file (for example: `wpg.policy`) for the Java Runtime Environment (JRE) granting the necessary security permissions. To add this file into the JRE, perform the following steps:

1. Make an entry in the `java.security` file residing in the `WASND_ROOT/java/jre/lib/security` folder.

The syntax for the new entry in the `java.security` file is:

```
policy.url.3=file:///fully_qualified_path/wpg.policy
```

2. Restart all of the Java processes.

User names and groups

Groups provide superuser permissions to all users who are members of the Hubadmin group. By using groups, more than one user can have Hub Administrative responsibilities while maintaining password security.

Because unique user names are required on an LDAP server, user names must be unique on WebSphere Partner Gateway as well. If you are creating a new user and the user name already exists in the same or a different partner, you will see an error message stating, A User with this name already exists. In this situation, input another user name into the console and continue. If you are migrating to a new version of WebSphere Partner Gateway wherein there is no restriction on user names, then a double asterisk ** is displayed next to any duplicate user name indicating that it already exists in the same or another partner. Change one of the user names so that they are unique from one another.

Note: New users and groups, which are added to the LDAP server and WAS Admin console, must also be added in the WebSphere Partner Gateway console in order to be active.

Stopping the use of LDAP authentication

You might have to stop LDAP authentication under the following circumstances:

- The LDAP server stops or permanently goes down.
- Container based authentication was chosen when installing WebSphere Partner Gateway but the LDAP server is not ready.

Notes for UNIX users:

1. UNIX users who use DB2 must log in as the db2instance user and use the db2instance username and password to run the script.
2. UNIX users who use Oracle must log in as the oracle user and use the username and password given at the time of installation to run the script.

To stop WebSphere Partner Gateway from using LDAP for accessing passwords and instead use the WebSphere Partner Gateway database to store passwords, run the following script:

- `bcgResetAuthentication.bat` for Windows
- `bcgResetAuthentication.sh` for UNIX

This script requires the following input parameters:

- database schema owner user ID
- database schema owner password

The script requires these parameters to connect to the WebSphere Partner Gateway database.

Note: If you are using a DB2 database, start the script from a DB2 command line.

This script is located in the `{dbloader install location}/scripts/{database type}` directory.

This script:

- Sets the attribute `bcg.ldap.containerauth` located in the **Console System Administration > Console Properties > Common Attributes** to False.

- Resets the hubadmin user ID password to the installation default and the database is now used to store passwords.

Note: After these scripts are run, any passwords that were configured in LDAP must be reentered for each defined user using the WebSphere Partner Gateway Console.

Sample LDAP configuration

The following section has the instructions on how to configure the WebSphere Application Server so that it can connect to the LDAP Servers for the authentication of the deployed application. However, this section does not address LDAP Server administration which is specific to the site where it is installed. For more complete information about configuring the LDAP Servers or the administration of the LDAP Server, see the WebSphere Application Server documentation.

Configuring the WebSphere Application Server for the standalone IBM Tivoli Directory Server

About this task

To configure a standalone LDAP server for WebSphere Partner Gateway, you can install the IBM Tivoli Directory server and configure the WebSphere Application Server to authenticate users in the LDAP server.

1. Install the IBM Tivoli Directory server. Follow the instructions in the installation guide that comes with IBM Tivoli Directory server.

Installation Tips:

- The username used to install the product should be the same as the DB2 instance name and must be a member of the administrators and the DB2Admin groups.
- The directory server name should be the same as the DB2 name.
- Create a user named DB2 and include the user name into the administrators and DB2admin groups.
- Login as the DB2 user and install.

After you have successfully installed the IBM Tivoli Directory server, continue with the next step to start creating users for the LDAP server.

2. Start the LDAP directory server using the following command:

```
idsslapd -I db2
```

3. Start the WebSphere Application Server that comes with LDAP.
4. Access the WebSphere Application Server admin page for LDAP using the following address:

```
http://<ip>:12000/IDSWebApp/IDSjsp/Login.jsp
```

5. Login using console administration ID:

```
Username: superadmin
```

```
Password: secret
```

6. Go to **Console Administrator > Manage console server** and add your LDAP server from the list.
7. Logoff the console administration ID.

8. Select your LDAP server and login using the administrator username and password.
9. Go to **Server Administration > Manage server properties > Suffices** and add a suffix (for example, o=ibm, c=us).
10. Click **Apply**.
11. Go to **Directory Management-Add an entry** and select **Organization in Structural object classes**.
12. Click **Next**.
13. In the present screen, select the default values (aixAuxAccount) and click **Next**.
14. Specify the following settings:
 - Relative DN='o=ibm'
 - Reqd attributes= o='ibm'
 - Parent DN= 'c=us'

Note: The values provided for the settings are shown as an example.

15. Click **Finish**.
16. Create a user and add a directory entry under 'o=ibm,c=us'.
For example, to add user 'cn=user1,o=ibm,c=us':
 - a. Select the 'Person' structural object class so that you get 'password' as an optional attribute.
 - b. Specify sn='user1',cn='user1'.
 - c. In the optional attributes, specify the password=<password>.

After installing the LDAP server and creating a user, configure the WebSphere Application Server with this LDAP server with the following steps:

17. Click on **Security > Secure administration, applications, and infrastructure**.
18. In the right pane of the page click **Security Configuration Wizard**. The wizard opens to step 1 of 4 for configuration.
19. For step 1, select **Enable application security** and click **Next** to go to step 2 of the configuration wizard.
20. For step 2, select **standalone LDAP registry** and click **Next** to go to step 3 of the configuration wizard.
21. For step 3 of the wizard, you specify the following information about the LDAP server that is running and click **Next**.
 - a. Primary administrative user name: user created in LDAP (for example, cn=user1,o=ibm,c=us)
 - b. Type of LDAP server: IBM_Tivoli Directory_Server
 - c. Host: <IPaddress of LDAP server>
 - d. Port: <port of your LDAP server> (for example, 389)
 - e. Base Distinguished Name: o=ibm,c=us
 - f. Bind distinguished name (DN): <ldapadmin name> (for example: cn=root).
 - g. Bind password: <ldap admin password>
22. For step 4, a summary of the configuration information specified on the previous pages is shown. Verify the information and click **Finish** and **Save** configuration.
23. Restart the WebSphere Application Server.
Stop the server using the following command:
stopserver <servername> -username <ldap_username> -password <ldap_password>

Restart the server using the following command:

```
startserver <servername> -username <ldap_username> -password <ldap_password>
```

Now the user can login using any username created in the IBM Tivoli Directory server.

Specifying LDAP users to use the WebSphere Partner Gateway Console

About this task

After authentication in LDAP server, you must associate the LDAP user with the Hubuser role. Only users who are members of this role can enter the application after authentication. To define LDAP users as a member of this role:

1. Start the WebSphere application server that has the Console application deployed.
2. Select **Applications > Enterprise Applications** and then click **BCGConsole**
3. On the right side of the page, in the **Additional Properties** pane, click **Security role to user/group mapping**.
4. You can either specify that all successfully authenticated users are made member of the Hubuser role or that only certain users are to be included.
 - To include all authenticated users, select **All Authenticated?** under the role named **Hubuser**.
 - To include certain users only, click **Look up users** and include only selected users to be a member of **Hubuser** role.

Chapter 8. Support for IPv6

Internet Protocol version 6 (IPv6) is an extension over the current IPv4 protocol. IPv6 features support for 128 bit address as opposed to the 32 bit address supported by IPv4. Except the change in address format, no other configuration changes are required for IPv6 in the Community Console.

The difference between IPv4 and IPv6 configuration is a change in IP address or URL format.

- If you are using the IPv4 protocol then write the address as in this example:
9.183.12.12.
- If you are using the IPv6 protocol then write the IP in brackets ('['and ']') as in this example: [0::9.183.12.12]
- If you are using the IPv6 protocol and an HTTP address then write the IP within the square brackets ('['and ']') as in this example: http://
[::FFFF:129.144.52.38]:80/index.htm
- If it is IPv6 and FTP address then write the IP within the square brackets ('['and ']'), as in this example: ftp://[::FFFF:129.144.52.38]:80/index.htm

Enabling tunneling IPv6 over IPv4

The IPv6 protocol cannot be used throughout the entire Internet so you must encapsulate IPv6 packets within IPv4 and "tunnel" through networks where only IPv4 is available.

RHEL Linux 3

About this task

To enable tunneling on an RHEL Linux 3 platform, follow the steps below:

1. Login as the Root user.
2. Add the line `add - NETWORKING_IPV6=yes` to the file `etc/sysconfig/network`.
3. Save the file and exit.
4. Add the following lines to the file `etc/sysconfig/network-scripts/ifcfg-eth0`.
 - a. `add - IPV6INIT=yes`
 - b. `add - IPV6T04INIT=yes`
5. Save the file and exit.
6. Issue `ifconfig` from the command prompt.

The system automatically generates an IPv6 address. Use this address for configuring receivers and destinations in WebSphere Partner Gateway.

Windows 2003/XP

To configure IPv6 on a Windows 2003/XP system, follow the Microsoft guidelines at <http://www.microsoft.com/windowsserver2003/techinfo/overview/ipv6faq.mspx>. If you are operating on a IPv6 supported Windows platform consult your system administrator to enable the tunneling feature.

HP-UX 11i

About this task

To enable tunneling on an HP-UX 11i , follow the steps below:

1. Login as the Root user.
2. To enable tunneling add the line `IPV6_TUNNEL="1"` to the file `/etc/rc.config.d/netconf-ipv6`.
3. Assign the following parameters in the file `/etc/rc.config.d/netconf-ipv6`:
`IPV6_DESTINATION[0]=`
`IPV6_GATEWAY[0]=" "` (if set to 1 the gateway is remote, if set to 0 the gateway is local)
`IPV6_ROUTE_COUNT[0]=`
`IPV6_ROUTE_ARGS[0]=`

See the comment text in the `netconf-ipv6` file and the `route(1m)` man page for more information.

4. Save the file and exit.
5. The changes can be activated in one of the following two ways:
 - By rebooting the system.
 - By issuing the `ifconfig` and `route` commands to make equivalent configuration settings.

Enabling IPV6

About this task

To configure IPV6, change the Java Virtual Machine parameter for runtime support in the WebSphere Application Server console. To change the Java Virtual Machine parameter:

1. Log in to the WebSphere Application Server Admin console.
2. Go to **Servers > Application servers** and select server.
3. Select each server and change the `java.net.preferIPv4Stack` property using the following process:
 - a. Select the server (`bcgdocmgr`, `bcgreceiver`, or `bcgconsole`).
 - b. On the Configuration page, expand **Java and Process Management** in the Server infrastructure section of the page and select **Process Definition**.
 - c. On the Process definition configuration page, select **Java Virtual Machine** in the Additional Properties section.
 - d. Select **Custom Properties**.
 - e. Change the property `java.net.preferIPv4Stack` to false.
 - f. Click **Apply** and then **Save** to complete this configuration.
 - g. Repeat this process for each server.
4. After you have changed the `java.net.preferIPv4Stack` for each server, a Full Resynchronization of the node is required for Full Distributed Mode. To resynchronize the node, go to **System Administration > nodes** and select **bcnode**. Click **Full Resynchronize**.

Note: The synchronization can take approximately 5 to 10 minutes.

5. Restart all of the servers.

Configuring attributes

About this task

If the workstation where the Document Manager is installed is configured with IPv6 and documents are sent using a destination based on IPv6 protocol, then the IPv6 address of the workstation must be configured. To configure the workstation address:

1. Log in to the WebSphere Gateway Console.
2. Go to **System Administration > DocMgr Administration > Delivery Manager Attributes**.
3. Click the **Editing publishing info properties** icon.
4. Type the IPv6 address of the local workstation where the hub is running in the `bcg.router.ipv6.address` property.

Note: If more than one instance of document manager exists, leave the property `bcg.router.ipv6.address` blank.

5. Click **Save**.
6. For Receiver, go to **System Administration > Receiver Administration > Others**.
7. Type the IPv6 address of the local workstation where the hub is running in the `bcg.receiver.ipv6` property.

Note: If more than one instance of receiver exists, leave the property `bcg.receiver.ipv6` blank.

8. Click **Save**.

Chapter 9. Managing the Destination Queue

The Destination Queue lets you view documents queued for delivery from any destination in the system. You can also:

- View all Partner destinations that have documents queued for delivery.
- Display documents in a queue.
- Enable or disable destinations.

The Destination Queue hold messages that are waiting to be sent from WebSphere Partner Gateway to partner destinations.

The Destination 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 Destination Queue, you can:

- See a list of all destinations containing documents queued for delivery
- View a document that has been in a destination queue for an extended amount of time (30 seconds or more). You can also view document details to troubleshoot documents from the queue.

Note: If you are implementing an FTP Scripting Destination with an interval or calendar 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 destination details to ensure proper operation. Documents backing up in a Destination Queue can indicate a fault in the delivery manager or destination.
- Confirm destination status. An offline destination causes documents to collect in the queue until the destination is placed online. Destination status does not affect connection functionality, and documents continue to be processed and placed in the queue for delivery.
- Limit the size of the Destination Queue list with the **Partner Name** and **Destination** fields.

Viewing the Destination Queue

About this task

To view a list of documents residing in the destination queue, use the following procedure:

1. Select **Viewers > Destination Queue**. The Console displays the Destination Queue window.
2. Input the parameters shown in Table 10 on page 88.

Table 10. Destination Queue window

Criteria	Description
Partner Name	To complete this field you can: <ol style="list-style-type: none"> 1. Specify the Partner name. 2. Specify part of the partner name in this field and click Show Partners. Select the partner from the partner list. 3. Specify the wildcard * and click Show Partners. Select the partner from the partner list.
Destination	Clicking Show Partners displays a Partner field on the page. The Partner field lists all the available partners in alphabetical order. The first item in this list is All, which is selected by default. The rest of the list is an ordered list of destination transports. On this list, you can select only a single destination. The default is All. Note: The Destination list is automatically populated with the selected partner's destinations and the list is presented in alphabetical order.
Queued at least	Minimum number of minutes a document has been waiting in the destination queue. For example, if 6 minutes is selected, all destinations containing documents that have been waiting for delivery for 6 minutes or more will be displayed. The default is 0.
Sort By	Sort search results by Partner (default) or Destination Name.
Refresh	Turn refresh on or off (default).
Minimum Queued	Minimum number of documents in a destination queue. The default is 1.
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 Rate	Number of seconds the Console waits before updating displayed data.

3. Click **Search**. The system finds all documents in the destination that match your search criteria. **Table 11** shows the information returned from the search.

Table 11. Results after destination queue search

Criteria	Description
Partner	Trading partner associated with destination
Destination	Name of the destination
Queued	Number of documents in the destination queue waiting for delivery. Link to destination details
State	Shows whether the destination is online or offline

Note: For the Console to display a destination, the destination must meet all the requirements of the search criteria.

Viewing queued documents

About this task

To view documents queued for a specific Partner:

1. Click **Viewers > Destination Queue**.
2. From the Destination Queue Search window, click **Documents Search**.
3. From the Queue Documents Search window, specify the search criteria (see Table 12 on page 89).

Table 12. Queue Documents Search window

Criteria	Description
Partner Name	To complete this field you can: <ol style="list-style-type: none"> 1. Specify the Partner name in the field. 2. Specify part of the partner name in this field and click Show Partners. Select the partner from the list. 3. Specify the wildcard * and click Show Partners. Select the partner from the partner list. <p>Note: Clicking Show Partners displays a Partner field on the page. The Partner field lists all the available partners in alphabetical order.</p>
Destination	The first item in this list is All, which is selected by default. The rest of the list is an ordered list of destination transports. On this list, you can select only a single destination. The default is All. <p>Note: The Destination list is automatically populated with the selected partner's destinations and the list is presented in alphabetical list.</p>
Sort By	Select whether the list should be sorted by Partners (the default), by Destinations, Reference ID, or Queued timestamp (the time the document was last sent).
Reference ID	Type the unique identification number assigned to the document by the system.
Direction	Click Ascend to display documents starting with the oldest time stamp or beginning of the alphabet, or Descend to display documents starting with the most recent time stamp or end of the alphabet.
Document ID	Type the unique identification number assigned to the document by the source partner.
Results Per Page	Specifies the number of documents displayed on a page.
Maximum Documents Allowed	Specifies the number of records to be displayed.

4. Click **Search**. The results of the queues search are displayed.

Stopping the processing of documents from the destination queue

About this task

Using the Destination Queue, you can make a request to WebSphere Partner Gateway to stop processing the document. When you click **Stop process** icon, your request to stop processing the document is submitted and the status of the document is shown as Stop Submitted. This status means that the request to stop processing the document has been submitted.

The following procedure describes how to stop processing the documents.

1. Click **Viewers > Destination Queue**.
2. From the Destination Queue window, click **Documents Search**.
3. Complete the parameters in the window (see Table 12).
4. Click **Search**. The results of the queues search are displayed.
5. Click the **Stop process** icon to stop the processing of the document.

Note: If the document is already processed by document manager when you click **Stop process** icon, the Stop Process action from console will not have any impact.

Viewing destination details

About this task

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

1. Click **Viewers > Destination Queue**.
2. From the Destination Queue window, type the search criteria (see Table 10 on page 88).
3. Click **Search**.
4. From the list of destinations, click the document count link in the **Queued** column to open the **Queued Documents Search** screen.
5. Click **Search** in Queued Documents Search. The Destination details and a list of queued documents are displayed.

Changing destination status

About this task

To place a destination online or offline, use the following procedure:

1. Click **Viewers > Destination Queue**.
2. From the Destination Queue window, type the search criteria (see Table 10 on page 88).
3. Click **Search**.
4. From the list of destinations, click the document count link in the **Queued** column. Destination details and a list of queued documents appear.
5. Click **Online** in **Destination Info** to place a destination offline, or click **Offline** to place destination online. (You must be logged in as hubadmin to change destination status.)

Chapter 10. Analyzing document flows

Use the Document Analysis tool to get a detailed overview of the number of documents in the system sorted by state:

- Received
- In Progress
- Failed
- Successful

You can focus your search using the following criteria:

- Date
- Time
- Type of process (To or From)
- Operation Mode
- Protocol
- Document type
- Process version

The Document Volume Report helps manage, track, and troubleshoot the flow of your business documents by locating and viewing the failed documents and investigating the reason for these failures. The report displays the volume of documents processed by the system within a specific time period, and 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 Partner Connection tool is used to test the connection to the destination.

Features covered in this chapter include:

- “Document Analysis tool”
- “Document Volume Report” on page 93
- “Test Partner Connection” on page 94
- “EDI Reports” on page 98
- “FTP Reports” on page 100

Document Analysis tool

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 13. 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: <ul style="list-style-type: none">• 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 external partner or internal partner.
Failed	Document processing was interrupted because of 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 receiver partner.

Viewing documents in the system

About this task

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 lists.

Table 14 describes the values that you can specify to determine which documents are displayed.

Table 14. 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 Partner	The partner that initiated the business process (internal partner only).
Receiver Partner	The partner that received the business process (internal partner only).
Search On	Search on From document type or To document type.
Operation Mode	For example, All, Production, Test, CPS Partner, or CPS Manager. Test is only available on systems that support the test Operation Mode.
Package	Describes document format, packaging, encryption, and content-type identification.
Protocol	Document protocol available to the partners.
Document Type	Specific business process.
Sort By	Sort results by From Partner Name or To Partner Name.
Refresh	Controls if the search results are refreshed periodically (internal partner only).
Refresh Rate	Controls how often search results are refreshed (used by internal partner only).

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

Viewing process and event details

About this task

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 lists.
3. Click **Search**. The system displays the Document Analysis Summary.
4. Click the **View details** icon next to the Source and Receiver Partners that you want to view. The system displays a list of all documents for the selected partners. 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 15. 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 because of an error.
Successful	The final message that completes document processing has been transmitted from the system to the receiver partner.

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

About this task

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 lists.

Table 16. 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 Partner	The partner that initiated the business process (internal partner only).
Receiver Partner	The partner that received the business process (internal partner only).
Search on	Search on From document type or To document type.
Operation Mode	Production or test. Test only available on systems that support the test Operation Mode.
Package	Describes document format, packaging, encryption, and content-type identification.
Protocol	Type of process protocol, for example, XML, EDI, flat file.
Document Type	Specific business process.
Sort By	Sort results by this criteria (Document Type or Receiver Document Type).
Results Per Page	Number of records displayed per page.

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

Exporting the Document Volume Report

About this task

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

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

Printing reports

About this task

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

Test Partner Connection

The Test Partner Connection feature is used to test the destination or Web server. If you are the internal partner, you can also select a specific partner. The test consists of sending a blank POST request to a destination or URL. For example, the request is similar to entering the Yahoo Web address (www.yahoo.com) into your browser address field. Nothing is sent; it is an empty request. The response received from the destination 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 Partner Connection feature works with HTTP that does not require any connection parameters.

To test a partner connection:

1. Click **Tools > Test Partner Connection**.
2. From the Test Partner Connection window, select the test criteria from the lists.

Table 17. Test Partner Connection values

Value	Description
To Partner	The name of a specific To Partner to be tested (internal partner only).
From Partner	The name of a specific From Partner to be tested (external partner only). This field is only available if Ping ebMS is selected in the Command field.
Destination	Displays available destinations based on the to partner selected.
URL	Dynamically populated based on the destination selected.
Command	Post, Get or Ping ebMS. For more information about Ping ebMS, see "Pinging ebMS partners."

3. Click **Test**. The system displays the test results. For information about the status code returned, see "Web Server result codes."

Pinging ebMS partners

About this task

From the Test Partner connection page, you can ping ebMS partners. This means that you can send a ping message to a partner, and, if the partner is up and ready to receive, the partner responds with a pong message. Once you upload a CPA, the ping-pong connection is created.

For the Ping to work connections have to be defined with the partner involved. For details, see the section for pinging ebMS partners in the *WebSphere Partner Gateway Hub Configuration Guide*.

To ping an ebMS partner, complete the following steps:

1. Click **Tools > Test Partner Connection**.
2. For **Command**, select **PING ebMS**.
3. Select **From Partner** and **To Partner**.
4. Optionally, select a **Destination** or type a **URL**.
5. Click **Test** to send a ping message.

To determine the status of the ping message, click **Ping Status**. The status for the last ping request then displays under Results.

Note: The last ping request may have been initiated from the Test Partner Connection or from a Document Viewer re-send of an existing Ping document.

Web Server result codes

The following sections describe the server result codes:

200 Series

- 200 - OK
Successful transmission. This is not an error.
- 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 vendor-acquired 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 might 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 user name 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)
- Users guessing file names
- Bad links from your site or other sites
- 405 - Method Not Allowed
The method specified in the request line cannot be used 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 might not be completed because of 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 fulfilling the request. Something went wrong with the Web server and it cannot give you a meaningful response. There is typically nothing that can be done from the browser end to fix this error; the server administrator checks the error log for the server 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 Destination

The server received an unusable response from the destination or upstream server it accessed in attempting to fulfill the request.

- 503 - Service Temporarily Unavailable

The server is currently unable to handle the request because of a temporary overloading or maintenance of the server. The server is out of resources.

- 504 - Destination Time Out

The server did not receive a timely response from the destination or upstream server it accessed in attempting to complete the request.

- 505 - HTTP Version Not Supported

EDI Reports

Use EDI Reports to search overdue electronic data interchange (EDI) functional acknowledgments (FA). You can also search for rejected electronic data interchange (EDI) transactions. The following sections detail the procedure to use EDI Reports.

EDI FA Overdue Search

About this task

The EDI FA Overdue Search page provides search criteria for performing a search for overdue electronic data interchange (EDI) functional acknowledgments (FA).

Note: Any records, returned by previous EDI FA overdue searches, that were removed from the resulting reports will be ignored by later searches. Therefore, removed records are not displayed in later reports. Records can be removed from a report by selecting **Ignore Selected Records** on the EDI FA Overdue Report page. Only the hub administrator can remove records from a report.

To search for the EDI FA Overdue records, do the following:

1. Click **Tools > EDI Reports**. The EDI FA Overdue Search screen is displayed.
2. Select one or more search criteria from the drop-down list:

Table 18. EDI FA Overdue Search Criteria

Value	Description
Start date & time	The date and time the transaction was initiated.
End date & time	The date and time the transaction was completed.
Source Partner	The partner that initiated the transaction.
Target Partner	The partner that received the transaction.
Search on	Search on Source document type or Target document type.
Package	Describes document format, packaging, encryption, and content-type identification.
Protocol	Type of process protocol, for example, XML, EDI, flat file. The protocols displayed vary depending on the value you select in the Package field.
Document type	Specific document type. The types displayed vary depending on the value you select in the Protocol field.
Reference ID	Specifies a transaction ID.

Table 18. EDI FA Overdue Search Criteria (continued)

Value	Description
Sort By	Specifies the criteria for sorting the search results. The defaults are Overtime Due and Descend. Use Descend to display the most overdue FAs first. Select Ascend to display the least overdue FAs first.
Results Per Page	Specifies the number of transaction search results to display on each page.

3. Click **Search** to display the EDI FA Overdue Search report.

Viewing EDI FA Overdue reports

Depending on the search criteria selected on the EDI FA Overdue Search page, the search result is displayed in the EDI FA Overdue Report page.

The following data, when applicable, is displayed in the EDI FA Overdue report.

Table 19. EDI FA Overdue Report

Value	Description
Date	The Date on which the EDI was sent from the source partner to the target partner.
Time	The time (GMT) at which the EDI was sent from the source partner to the target partner.
ActivityID	The unique ID (UID) of the transaction.
Source Trading Partner	The partner that sent the transaction.
Source Package	The source package of the transaction.
Source Protocol	The source protocol of the transaction.
Source Document Type	The source document type of the transaction.
Target Trading Partner	The partner that sent the transaction.
Target Package	The target package of the transaction.
Target Protocol	The target protocol of the transaction.
Target Document Type	The target document type of the transaction.
Interchange Number	The interchange number of the transaction.
Group Number	The group number of the transaction.
Transaction Number	The identifying number of the transaction.
FA Due By	The date that the FA for the transaction was due.
Overdue By	The amount of time that the FA is overdue.
Ignore Selected Records	When you select this option for a record, that particular record is removed from the report. Once a record is removed from a report, that record is ignored by later EDI FA overdue searches, and therefore, is not displayed in the resulting reports. Only the hub administrator can remove records from a report.

EDI Rejected Transaction Search

About this task

The EDI Rejected Transaction Search page contains criteria for performing searches for electronic data interchange (EDI) transactions that have a functional acknowledgment (FA) containing an error code. Transaction records without FAs are not returned by an EDI rejected transaction search.

To search for the EDI Rejected records, do the following:

1. Click **Tools > EDI Reports > EDI Rejected Report**.
2. Select one or more search criteria from the drop-down list:

Table 20. EDI Rejected Transaction Search Criteria

Value	Description
Start date & time	The date and time the transaction was initiated.
End date & time	The date and time the transaction was completed.
Source Partner	The partner that initiated the transaction.
Target Partner	The partner that received the transaction.
Search on	Search on Source document type or Target document type.
Package	Describes document format, packaging, encryption, and content-type identification.
Protocol	Type of process protocol, for example, XML, EDI, flat file. The protocols displayed vary depending on the value you select in the Package field.
Document type	Specific document type. The types displayed vary depending on the value you select in the Protocol field.
Reference ID	Specifies a transaction ID.
Sort By	Specifies the criteria for sorting the search results. The defaults are Overtime Due and Descend. Use Descend to display the most overdue FAs first. Select Ascend to display the least overdue FAs first.
Results Per Page	Specifies the number of transaction search results to display on each page.

3. Click **Search** to view the EDI Rejected Transaction report.

Viewing EDI Rejected Transaction reports

Depending on the search criteria selected on the EDI Rejected Transaction Search page, the search result is displayed in the EDI Rejected Transaction Report page.

The following data, when applicable, is displayed in the EDI Rejected Transaction report.

Table 21. EDI Rejected Transaction Report

Value	Description
Date	The Date on which the EDI was received.
Time	The time (GMT) at which the EDI transaction was sent from the source partner to the target partner.
ActivityID	The unique ID (VUID) of the transaction.
Source Trading Partner	The partner that sent the transaction.
Source Package	The source package of the transaction.
Source Protocol	The source protocol of the transaction.
Source Document Type	The source document type of the transaction.
Target Trading Partner	The partner that received the transaction.
Target Package	The target package of the transaction.
Target Protocol	The target protocol of the transaction.
Target Document Type	The target document type of the transaction.
Interchange Number	The interchange number of the transaction.
Group Number	The group number of the transaction.
Transaction Number	The identifying number of the transaction.
Status Code	The status code of FA.
Status Text	The status text of FA.

FTP Reports

FTP Reports provide details on the Statistics and Connections of FTP and SFTP servers.

Statistics

About this task

The Statistics page will display the FTP and SFTP Server Status in Read Only Mode.

Note: The statistics will not be displayed if the FTP / SFTP Server or the FTP / SFTP Management Server is not available.

To view the FTP and SFTP server status, do the following:

1. Click **Tools > FTP Reports > Statistics**. The FTP Statistics page is displayed.
2. Select *FTP server* or *SFTP Server* for **Server type**.
3. The following server status information is displayed:

Table 22. FTP and SFTP Statistics

Value	Description
Server start time	Start time of the FTP or SFTP Server.
Number of directories created	Number of directories created by users using mkdir.
Number of directories removed	Number of directories removed by users using rmdir.
Number of file uploaded	Number of files uploaded by all users.
Number of files downloaded	Number of files downloaded by all users.
Number of files deleted	Number of files deleted by all users using delete command.
Uploaded Bytes	Total number of bytes uploaded.
Downloaded Bytes	Total number of bytes downloaded.
Current logins	Displays existing logins.
Total Logins	Total logins since the last reset.
Total failed logins	Total number of logins failed.
Current Connections	Current connections since the last reset.
Total Connections	Total connections since the last reset.

4. Click **Reload** to refresh current login.
5. Click **Reset** to reset the values.

Connections

About this task

View FTP Connections by following the steps mentioned below:

1. Click **Tools > FTP Reports > Connections**.
2. Select *FTP server* or *SFTP server* from **Server type**. Based on your selection, all the FTP or SFTP Server connections are displayed
3. The following connection information is displayed in the report:

Table 23. FTP Connections

Value	Description
Login Name	The login userid for this connection. If this is blank, it means that the user has only established a connection but has not logged in.
Login Time	The time when the user logged in. If this is blank, it means that the user has only established a connection.

Table 23. FTP Connections (continued)

Value	Description
Last Access Time	The time when the user last accessed this connection. If this is blank, it means that the user has only logged in and not issued any command yet.
Client Address	The client IP from which the user has logged in.

Note: Click the Delete icon against the appropriate FTP or SFTP Server to disconnect it.

Chapter 11. 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”
- “AS Viewer” on page 106
- “RosettaNet Viewer” on page 109
- “Document Viewer” on page 111
- “ebMS Viewer” on page 120
- “Destination Queue” on page 122

Note: Data time is stored in the system using Greenwich mean time (GMT) value but is displayed using the user's time zone setting.

The RosettaNet and AS Viewers include additional search criteria for the hub administrator. For more information, see the *WebSphere Partner Gateway Hub Configuration Guide*.

Event Viewer

Use the Event Viewer to view and research events.

An event informs you about some significant occurrence in the system. Events of type Error and Severe indicate that something unusual has happened in the system. It can let you know that a system operation or function was successful (for example, a partner was successfully added to the system). An event can also identify a problem (for example, the system cannot process a document). Most types of documents are resent multiple times, so when a document fails and generates an event, you can use this information to investigate and correct the problem preventing similar failures in the future.

WebSphere Partner Gateway includes predefined events.

The **Alerts** feature in the Account Admin module allows you to do the following:

- Create event-based alerts
- Identify the events that impact the system

The **Contacts** feature in the Account Admin module identifies staff members that the system notifies if those events occur.

Note: The administrator has to associate alerts with the events that are considered vital. If this association does not take place during the configuration, no alert notifications will be generated through WebSphere Partner Gateway.

The Event Viewer displays events based on specific search criteria. Using these criteria, you can locate a specific event and determine why it occurred. Use the Event Viewer to search for events by time, date, event type (debug, information, warning, error, and critical), event code, and event location.

Data available through the Event Viewer includes event name, time stamp, user, and partner 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 24.

Table 24. 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 because of a noncritical anomalies in document processing or system functions that enable the operation to continue.
Error	Error events occur because of anomalies in document processing that cause the process to terminate.
Critical	Critical events are generated when services are terminated because of a system failure. Critical events require intervention by support personnel.

Searching for events

About this task

1. Click Viewers > Event Viewer

Check boxes for Event severity are organized from left to right and Debug is located on the left 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 Debug events are selected, all event types are displayed.

Note: Debug events cannot be viewed by all users.

2. Select the search criteria from the lists.

Table 25. 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.
Partners	Select all partners or a specific partner.
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).

Table 25. Event search criteria (continued)

Value	Description
Sort by	Sort results by: <ul style="list-style-type: none"> • Event Name • Time Stamp • Type • Source Partner • Source IP
Descend or Ascend	The default is Time Stamp. Descend displays the most recent time stamp or the beginning of the alphabet first.
	Ascend displays either the oldest time stamp or the end of the alphabet first.
Results per page	The default is Descend. 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 (internal partner only).

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

Tip: The event list can be refiltered based on the event type selected at the top of the Event Viewer window. The next window refresh reflects the newly selected event type.

Viewing event details

About this task

1. Click **Viewers > Event Viewer**.
2. Select the search criteria from the 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, if any exist.

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.

Error events

You can have a detailed information of any error/warning event that appear in your viewer page of your console. This self help will provide the cause, diagnosis, and solution for the problem.

The following example provides the necessary details when connection parse XML failure occurs:

```
BCG240065-Connection Parse XML Failure XML connection parsing failed: {0}
```

Problem Cause: The Connection Parse XML Failure error is generated due to the following reason: The information from the incoming document is not sufficient for parsing the connection.

Explanation: Hub should parse the incoming document for getting the attributes required to find the connection for the incoming XML document. Either the connection is not configured or the proper values are not present in the incoming XML.

Solution: To solve this problem, do the following:

- Check whether the connection is configured properly.
- Check whether the incoming document contains all the required attributes for identifying the connection.

Technical support: For further information on this error event, visit our technical support site at: [WebSphere Partner Gateway technical support site](#).

Detailed information about events: To view the details of the event, click on the event code provided.

AS Viewer

Use the AS Viewer to view packaged B2B transactions and B2B process details that use the Applicability Statement 1, 2, or 3 (AS1, AS2, or AS3) 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. AS3 is a standard for data transmission using FTP.

AS2 and AS3 describe how to connect, deliver, validate, and reply to data. They do not interact with the content of the document, only the transport. AS2 and AS3 create a wrapper around a document so that it can be transported over the Internet using HTTP or HTTPS for AS2, or FTP for AS3. Together, the document and wrapper are called a message. AS2 provides signing and encryption around the data carried within HTTP packets. Similarly, AS3 does this for the data transported using the FTP transport. AS2 and AS3 provide an encryption base with guaranteed delivery. AS1, AS2 and AS3 provide signing and encryption functionality. Compression functionality is also provided.

An important component of both AS2 and AS3 is the receipt mechanism, which is referred to as a 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 the decryption fails for an incoming encrypted AS2 document, a failure MDN is not sent on the same connection. To correct this issue, a partner connection must be activated, whether used or not between the two partners. The connection created must be a AS to None connection, that is, a connection by activating the AS B2B capability on one partner and None B2B capability on the other, thus creating a connection and activating it. Ensure that the source gateway on the AS side is a SMTP gateway (in case of AS1) or HTTP destination (in case of

AS2) or FTP gateway (in case of AS3), which is configured to the MDN address. Thus the decryption failure MDN is sent back over this AS to none binary connection.

Searching for messages

About this task

1. Click **Viewers > AS Viewer**. The system displays the AS Viewer window.
2. Select the search criteria from the lists, described in Table 26.

Table 26. AS 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 Partner	Identifies the source (initiating) and the target (receiving) partners (internal partner only).
Partner	Identifies if the search applies to all partners or the internal partner (partner only).
My role is the	Identifies if the search looks for documents in which the Partner is the Target or Source (partner only).
AS Source Business ID	Business identification number of the source partner defined in the AS header.
Payload Source Business ID	Business identification number of the source partner, defined by the content of the payload.
Operation Mode	Production or test. Test is only available on systems that support the test operation mode.
Package	Describes the document format, packaging, encryption, and content-type identification.
Protocol	Document format available to the partners, for example, RosettaNet XML.
Document Type	The specific business process.
Message ID	ID number assigned to the AS packaged document. Search criteria can include the asterisk (*) wildcard. The maximum length is 255 characters.
Document ID	Specifies a document ID.
Synch/Asynch	All, Synchronous, and Asynchronous. Search for documents received in synchronous mode, asynchronous mode, or both modes.

Table 26. AS Viewer search criteria (continued)

Value	Description
MDN Status	<p>Identify one or more MDN status from the MDN Status multi-selection box. Possible options are:</p> <p>All Display all results; do not filter on MDN Status.</p> <p>MDN Not Required Display all AS transactions where no MDN exists and no MDN is required.</p> <p>MDN Processed Display all AS transactions with successful MDNs.</p> <p>Waiting for MDN Display all AS transactions that are waiting for an MDN, but have not timed out yet, and are not considered missing (not received).</p> <p>MDN Not Received Display all AS transactions that have timed out while waiting for an MDN.</p> <p>MDN Disposition Error Display all AS transactions that have an MDN returned with a disposition error.</p> <p>Unknown Specifies that the database has not been updated with the MDN state.</p>
Sort by	<p>Sort results by:</p> <ul style="list-style-type: none"> • Target Timestamp • Source Document Definition • Target Document Type • Message ID • MDN Status • Document ID <p>The default is Target Timestamp.</p>
Descend or Ascend	<p>Descend displays the most recent time stamp or the beginning of the alphabet first.</p> <p>Ascend displays either the oldest time stamp or the end of the alphabet first.</p> <p>The default is Descend.</p>
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

About this task

1. Click **Viewers > AS Viewer**. The system displays the AS Viewer Search window.
2. Select the search criteria from the 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 27 on page 109.

Table 27. Message details

Value	Description
Message ID	ID number assigned to the AS 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 Partner	Partner initiating a business process.
Target Partner	Partner receiving the business process.
Source Time Stamp	Date and time the document begins processing.
Operation Mode	Either test or production. Test is only available on systems that support the test Operation Mode.
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 information: <ul style="list-style-type: none"> • Automatic-action/MDN-sent-automatically; processed. • Automatic-action/MDN-sent-automatically; processed/Warning;duplicate-document. • Automatic-action/MDN-sent-automatically; processed/Error;decryption-failed. • Automatic-action/MDN-sent-automatically; failed:unsupported MIC-algorithms.

5. (Optional) Click the **Document details** icon to view more information about the document.

RosettaNet Viewer

RosettaNet is a group of companies that created an industry standard for e-business transactions. Partner 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 internal and external partners.

The RosettaNet Viewer displays the required order of sub-transactions for successfully completing 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

About this task

1. Click **Viewers > RosettaNet Viewer**.
2. From the RosettaNet Viewer Search window, select the search criteria from the list, described in Table 28.

Table 28. RosettaNet search criteria

Value	Description
Start Date and Time	The date and time that the process was initiated.

Table 28. RosettaNet search criteria (continued)

Value	Description
End Date and Time	The date and time that the process was completed.
Source and Target Partner	Identifies the source (initiating) and the target (receiving) partners (internal partner only).
Partner	Indicates whether the search applies to all partners or the internal partner (partner only).
My role is the	Indicates whether the search looks for documents in which the partner is the Target or Source (partner only).
Source Business ID	Business identification number of initiating partner, for example, DUNS.
Operation Mode	Production or test. Test is only available on systems that support the test operation mode.
Protocol	Protocols available to the partners.
Document Type	The specific business process.
Process Instance ID	Unique identification number assigned to the process. Criteria can include asterisk (*) wildcard.
Sort by	Sort results by: <ul style="list-style-type: none"> • Target Timestamp • Document Type
Descend or Ascend	The default is Target Timestamp. Descend displays the most recent time stamp or the beginning of the alphabet first. Ascend displays either the oldest time stamp or the end of the alphabet first.
Results Per Page	The default is Descend. 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

About this task

1. Click **Viewers > RosettaNet Viewer**. The system displays the RosettaNet Viewer Search window.
2. Select the search criteria from the lists.
3. Click **Search**. The system displays the results of your search, described in Table 29.

Table 29. Document processing details

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

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

About this task

Use this procedure to view a raw document associated with a RosettaNet transaction.

Procedure

1. Click **Viewers > RosettaNet Viewer**. The system displays the RosettaNet Viewer Search window.
2. Select the search criteria from the 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 Type to display the raw document.

Results

Restrictions:

1. 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. To view the complete file, you can download the file to the local disk, using the copy option.
2. The Raw Document Viewer might not display document attachments. To view any attachments, click the **Copy** link in the Raw Document Viewer to copy the file, including any attachments, to your local disk.

Tips:

- To troubleshoot documents that have failed processing, see “Viewing data validation errors” on page 117.
- 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 re-send failed or successful documents.

Searching for documents

About this task

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

2. Select the search criteria from the lists, described in Table 30.

Table 30. Document Viewer search criteria

Value	Description
Start Date	Date the document type process was initiated.
Start Time	Time the document type process was initiated.
End Date	Date the document type process was completed.
End Time	Time the document type process was completed.
Source Partner	Represents the partner that initiated the document type. The default is All.
Target Partner	Represents the partner that received the document type. The default is All.
Search on	Indicates whether to search on source document type or target document type. The default is Source document type.
Operation Mode	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 partners.
Document Type	The specific document type for which this document is included. A document type is the third level of a document definition falling below Package and Protocol.
Original File Name	The initial name assigned to the file.
Document ID	Created by the source partner. 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 partner.
Filter	Search for documents received in synchronous mode. This means that the connection between the initiator and the Hub stays open until the transaction is complete, including request and acknowledgment or request and response.
Sort By	Sort results by: <ul style="list-style-type: none"> • Target Timestamp • Source Document Type • Target Document Type • Document ID • Search Fields 1 to 10
Results Per Page	The default is Target Timestamp.
Descend or Ascend	Number of records displayed per page. Descend displays the most recent time stamp or the beginning of the alphabet first. Ascend displays either the oldest time stamp or the end of the alphabet first. The default is Descend.

3. To search using the user defined search fields, specify the search criteria in the fields labeled **Search field 1** through **Search field 10**.

User defined search fields can be defined for the document in your system when configuring XML Formats, EDI Transformation maps, or can be defined in custom user exits. For more information about configuring XML Formats, see

the *WebSphere Partner Gateway Hub Configuration Guide*. For help on creating user exits, see the *WebSphere Partner Gateway Programmers Guide*.

If custom search fields have not been defined for the documents in the system, then leave the search fields blank.

Note: User defined search data is only saved for documents exchanged after the configuration is complete. Documents exchanged prior to this configuration do not contain user defined search data.

4. Click **Search**. The system displays the results of your search, described in Table 31.

Note: The term partners is used on the Viewer windows to identify a hub community member, including the internal partner.

Table 31. Document details

Value	Description
Partners	Source (From) and Target (To) partners involved in the business process.
Time Stamps	Date and time the document begins and ends processing.
Document Type	Business process that is being transacted.
Operation Mode	Test or production. Test is only available on systems that support the test operation mode.
Synchronous	Identifies that the document was received in synchronous mode. This means that the connection between the initiator and the Hub stays open until the transaction is complete, including request and acknowledgment or request and response.

Viewing document details, events, and raw documents

About this task

1. Click **Viewers > Document Viewer**. The system displays the Document Viewer Search window.
2. Select the search criteria from the lists.
3. Click **Search**. The system displays a list of documents.
4. Click the **View details** icon next to the document you want to view.
 - 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 115 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.
 - To view the User Defined Search fields which have been assigned to this document, click the **Show** link in the User Defined Search Fields section.
 - To view the Duplicate ID fields which have been assigned to this document, click the **Show** link under the Duplicate ID Fields section.

Note: If this document was returned as a duplicate document, then the duplicate ID fields are empty. If there is any data in these fields, then the data must be unique for all documents in the system.

The document processing information is displayed when you view document details, described in Table 32.

Table 32. 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 partner.
Doc Time Stamp	Date and time document was created by partner.
Operation Mode	Destination the document passed through.
Connection Document Definition	Actions performed on a document by the system to ensure its compatibility with business requirements between partners.
Source and Target	Source and Target partners involved in business process.
In Time Stamp	Date and time the document was received by the system from the partner.
End State Time Stamp	Date and time the document was successfully routed by the system to the Target Partner.
Source and Target Business ID	Business identification number of Source and Target partners, for example, DUNS.
Source and Target Document Type	The specific business process transacted between Source and Target partners.

Restrictions:

1. 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. To view the complete file, you can download the file to the local disk, using the copy option.
2. The Raw Document Viewer might not display document attachments. To view any attachments, click the **Copy** link in the Raw Document Viewer to copy the file, including any attachments, to your local disk.

Tips:

1. If the system displays a Duplicate Document event, view the previously sent original document by clicking on the **View previously sent original document** icon next to the Duplicate Document event, then click the **View original** document icon.
2. For information about troubleshooting documents that have failed processing, see “Viewing data validation errors” on page 117.

Mass document resend

About this task

Perform the following steps in the document viewer search results screen to resend multiple documents:

1. Follow the steps in Searching for document section.
2. In the resultant screen of document viewer, select either **Inbound** or **Outbound** check box to resend all the documents in that category. Alternatively, you can resend the documents individually by selecting the check box against it.

- Note:** At a time, you can send either Inbound or Outbound and not both.
3. Click **Resend**.

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 an external partner or an internal partner. 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 for an EDI transaction” on page 116
- “Locating the target interchange for an EDI child transaction” on page 116

See the *WebSphere Partner Gateway Hub Configuration Guide* for more information about de-enveloping and enveloping EDI Interchanges.

Viewing EDI document source transactions About this task

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 lists.
3. Click **Search**. The system displays a list of documents.
4. Click the **View details** icon next to the Document ID.
5. Click **Target Document Children** section to view the document children details.

Viewing EDI document target transactions About this task

WebSphere Partner Gateway envelopes outgoing EDI transactions in an interchange.

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 **Target** in the **Document Children** section to view the document children details.

Locating the source interchange for an EDI transaction

About this task

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 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 for an EDI child transaction

About this task

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 lists.
3. Click **Search**. The system displays a list of documents.
4. Click the **View details** icon next to the Document ID.
5. Click **Information** 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.

Document Validation Errors

To view document validation errors click the **View document** icon in the Document details page under the Document Viewer tab. The document validation error page displays the following fields:

- XML field: Displays the XPath expression of the XML element causing the error.
- Value description: Displays the erroneous value that is not being accepted for the element shown.
- Error description: Describes the error condition and the correct element value expected.

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 33.

Table 33. 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:

```

<?xml version="1.0" encoding="UTF-8"?><!DOCTYPE Pip3 A7PurchaseOrderUpdateNotification
SYSTEM "3A7_MS_V02_00_PurchaseOrderUpdateNotification.dtd">
<Pip3A7PurchaseOrderUpdateNotification>
  <fromRole>
    <PartnerRoleDescription>
      <GlobalPartnerRoleClassificationCode>Seller</GlobalPartnerRoleClassificationCode>
      <PartnerDescription>
        <ContactInformation>
          <ContactName>
            <FreeFormText>John</FreeFormText>
            <FreeFormText>John</FreeFormText>
          </contactName>
          <EmailAddress>John@example.com</EmailAddress>
          <telephoneNumber>
            <CommunicationsNumber>+1-234-567-8998-8</CommunicationsNumber>
            </telephoneNumber>
            <facsimileNumber>
              <CommunicationsNumber>+1-234-567-8998-7</CommunicationsNumber>
              </facsimileNumber>
            </ContactInformation>
          <BusinessDescription>
            <GlobalBusinessIdentifier>123456789</GlobalBusinessIdentifier>
            <GlobalSupplyChainCode>Information Technology</GlobalSupplyChainCode>
          <BusinessDescription>
            <GlobalPartnerClassificationCode>Carrier</GlobalPartnerClassificationCode>
          </PartnerDescription>
        </PartnerRoleDescription>
      </fromRole>
    </Pip3A7PurchaseOrderUpdateNotification>
  </Pip3A7PurchaseOrderUpdateNotification>

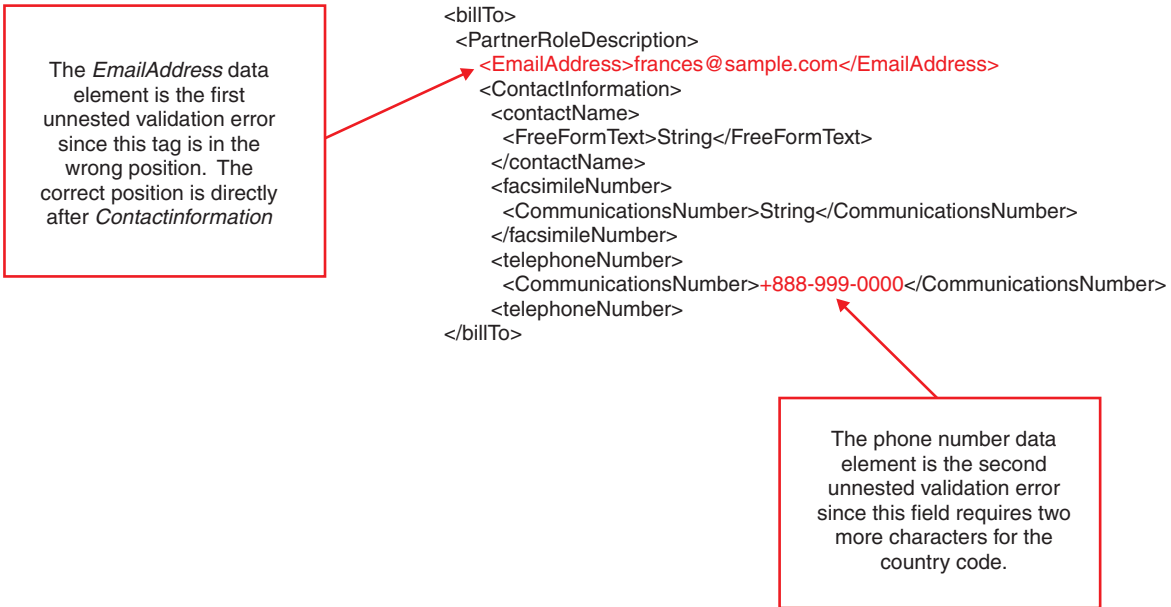
```

The *ContactInformation* data element is the first validation error since this tag is in the wrong position. The correct position is directly after *PartnerRoleDescription*

The *FreeFormText* data element is the second validation error since this tag has been duplicated.

The *John* data element is the third validation error since this field requires a minimum of six characters.

Example of non-nested XML validation errors:



For details on viewing validation errors in a raw document, see “Viewing raw documents” on page 111.

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

About this task

This topic describes information for stopping an in-process document, which is partially sent from one partner to another. The purpose of stopping an in-process partially sent document is to track the progress of the document that is being delivered to the receiving partner, and thereupon, resolve any issues that might occur during the transfer process. To stop a document that is being delivered, click **Stop Process**. Upon clicking **Stop Process** for a document in the console, the system starts the process of stopping the document and as a result, the **Stop submitted** icon displays. When the Hub operator clicks **Stop Process**, the delivery of current document stops, and as a result of this, the document is not delivered to the receiving partner. When the delivery of the partially sent document is stopped, an error event is logged. This error event displays useful information for troubleshooting to the Hub operator.

Note: It can take up to an hour or so for the system to stop the document. During this time, the Document Viewer continues to display the document with "in progress" status.

Re-sending failed and successful documents

You can re-send failed documents after correcting the cause of the failure. Additionally, you can re-send 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 backend system.

There are two basic types of documents that administrators can re-send:

- **In** documents are those that come into WebSphere Partner Gateway, either from the Backend or the partner. 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 partner. These documents can fail either in the BPE or Delivery Manager.

To re-send a failed **In** document, select **In** document and click **Resend**. 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 re-send failed **Out** documents, select the **Out** document and click **Resend**. 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 ensures 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 because of incorrect certificate configurations for partner or hub.
- For a Delivery Manager failure:
 - If the problem was because of an error in the BPE flow, the **In** document should be resubmitted. This ensures that any corrections in the BPE flow will get picked up. For example, if the destination information was incorrect.
 - If the failure was caused by something else, for example, the destination transport was down, then a resubmit 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 re-send, 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 re-send.

When re-sending the **In** document, the document goes through the complete workflow processing steps. For example, if a document is an AS2 Request from the partner and an MDN is required, then an MDN is sent to the partner even though an MDN might have already been sent the first time the document was processed. Also duplicate document ID checking is bypassed. However, depending on the business protocol, a "duplicate document ID is detected" warning might still be issued.

To re-send a document:

1. Click **Viewers > Document Viewer**. The system displays the Document Viewer Search window.
2. Select the search criteria from the lists.
3. Click **Search**. The system displays a list of documents.
4. Select the document or documents that you want to re-send.

Note: If you are re-sending an ebMS Ping document, a new Ping document is created.

5. Click **Resend**.

You will receive a confirmation message after the re-send is processed.

ebMS Viewer

The ebXML Message Service (ebMS) mechanism provides a standard way to exchange business messages among ebXML Trading Partners. It provides a reliable means to exchange business messages without relying on proprietary technologies and solutions. An ebXML message contains structures for a message header (necessary for routing and delivery) and a payload section. An ebXML message is a communication protocol independent MIME/Multipart message envelope.

Searching for ebMS processes

About this task

1. Click **Viewers > ebMS Viewer**. The system displays the ebMS Viewer Search screen.
2. Select the search criteria from the lists.

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 Partner	Identifies the sending partner.
Target Partner	Identifies the receiving partner.
Source Business ID	Business identification number of initiating partner.
Operation Mode	Production, test, RN simulator external partner or RN simulator internal partner. Test is only available on systems that support the test operation mode.
Protocol	Protocols available to the partners.
Document Type	The name of the source document type used to route the document.
Conversation ID	Unique id to identify the conversation.
Sort by	Sort results by: <ul style="list-style-type: none"> • Target Timestamp • Document Type <p>The default is Target Timestamp.</p>

Value	Description
Descend or Ascend	Descend displays the most recent time stamp or the beginning of the alphabet first. Ascend displays either the oldest time stamp or the end of the alphabet first. The default is Descend.
Results Per Page	Display <i>n</i> number of results per page.

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

Viewing ebMS process details

About this task

1. Click **Viewers > ebMS Viewer**. The system displays the ebMS Viewer Search window.
2. Select the search criteria from the lists.
3. Click **Search**. The system displays the results of your search, described in Table 34.

Table 34. ebMS processing details

Value	Description
Partners	Partners involved in the business process.
Time Stamps	Date and time the first document begins processing.
Document Type	The specific business process, for example ebMS (2.0): ALMService.
Operation Mode	Indicates the nature of the document being exchanged.
Synchronous	
Process Status	The status of the process as indicated by the receiver.
Conversion ID	Unique number assigned to the process by the initiating partner.
Source Partner	Initiating partner.
Target Partner	Receiving partner.

4. Click the **View details** icon next to the ebMS process you want to view. The system displays details and associated documents for the selected process, including the Conversation Status. The Conversation status indicates what process is next (for example, Waiting for confirmation acknowledgment). If the Conversation Status is complete, then all the children have been processed.
5. Click the **View details** icon next to the document you want to view. The system displays the document and associated event details. To view the complete file, you can download the file to the local disk, using the copy option.

Viewing raw documents

About this task

Use this procedure to view a raw document associated with an ebMS transaction.

Procedure

1. Click **Viewers > ebMS Viewer**. The system displays the ebMS Viewer Search window.
2. Type or select the search criteria.

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 Type to display the raw document.

Results

Restrictions:

1. 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.
2. The Raw Document Viewer might not display document attachments. To view any attachments, click the **Copy** link in the Raw Document Viewer to copy the file, including any attachments, to your local disk.

Tips:

- To troubleshoot documents that have failed processing, see “Viewing data validation errors” on page 117.
- The raw document viewer displays the HTTP header with the raw document.

Requesting and viewing the status of a document

About this task

Use this procedure to request the status for a document.

Note: Status can be requested only if the document status is still pending and the Request Status feature is enabled.

1. Click **Viewers > ebMS Viewer**. The system displays the ebMS Viewer Search window.
2. Type or select the applicable search criteria.
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. Select a document in the details list, and then click **Request Status**.
6. When the system receives the status, the **View Status** displays on the page. Click **View Status**.

If the document is still pending, then the status displays the last state of the document with the timestamp

Destination Queue

The Destination Queue lets you view documents queued for delivery from any destination in the system. Using the Destination Queue you can view all destinations that have documents queued for delivery, display and remove documents in a queue, and enable or disable destinations. See Chapter 9, “Managing the Destination Queue,” on page 87 for more information.

Chapter 12. Simulating production traffic

The RosettaNet Partner Simulator (RN PS) can be used before and after the Hub Community goes live to simulate production traffic (requests, responses, and acknowledgments) between the internal partner and an external partner, which is referred to as the Virtual Test Partner (VTP) in this description of the RN PS.

The purpose of the RN PS is:

- To give you a way to simulate an external partner sending an RN request to the internal partner through the hub.
- To give you a way to simulate the internal partner enterprise system sending RosettaNet Service Content (RNSC) through the hub to an external partner.

The internal partner uses the RN PS to verify that documents are formatted correctly and contain valid business content.

The RN PS gives the internal partner the ability to test their backend systems (Document Managers and receivers) without initiating the test from their own backend applications, and without requiring a partner to transmit data. As a result, they can test without engaging test systems or technical support personnel.

To initiate the test, the internal partner uploads a test document. This feature only accepts RNIF v2.0, DTD based PIP; 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.

If a RN document is posted to WebSphere Partner Gateway using the RN PS, then a acknowledgment is generated. If a 3A4 confirmation is sent to RN PS, the Document Manager closes the exchange with an 0A1.

Note that the installation process creates a sink destination (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” on page 124
- “Setting up test scenarios” on page 124
- “Uploading and viewing your requests and responses” on page 127
- “Initiating and viewing document type” on page 127

Preparing to test

About this task

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 internal partner, or a request or response from a partner:

1. Review the connections that you have configured to confirm that the test scenario appears to be configured correctly. In particular, make sure that the destinations that are configured in the connection are active.
2. Verify that your receivers are enabled and configured with the appropriate URL for incoming messages. Different traffic occurs on different receivers.

This requirement only applies when you are testing a document that requires a response. For more information about receivers, see the *WebSphere Partner Gateway Hub Configuration Guide*.

3. Verify the Business IDs 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 internal partner, 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 RN PS to test the scenarios shown in Table 35 between you and your partners.

Table 35. Test scenarios

Scenario	Destination for Connection	URL
One-way outbound from an internal partner to an external partner.	VTP_Owner	VTP_OWNER
Simulating internal partner.		
One-way inbound from an external partner to an internal partner.	VTP_TP	Not applicable in this scenario.
Simulating external partner.		
Two-way outbound from an internal partner to an external partner (Upload Request).	VTP_Owner	VTP_OWNER
Simulating internal partner.		
Two-way inbound from an external partner to an internal partner (Upload Request).	VTP_TP	VTP_TP
Simulating external partner.		

Table 35. Test scenarios (continued)

Scenario	Destination for Connection	URL
Two-way outbound from an internal partner to an external partner (Upload Response).	VTP_TP	VTP_TP
Simulating external partner.		
Two-way inbound from an external partner to an internal partner (Upload Response).	VTP_Owner	VTP_Owner

Sample scenarios

This section describes the steps involved in configuring the RN PS to simulate two one-way RosettaNet (RN) interactions. The steps for setting up RN interactions are described here in the context of setting up the RN PS. For more information about configuring RN in general, see the *WebSphere Partner Gateway Hub Configuration Guide*.

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

Internal partner

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

The sink destination should be specified as the default RN PS partner and RN PS Manager destination for the internal partner.

External partner

Set up an HTTP sink destination for the partner just as you did for the internal partner.

RosettaNet PIP XML files

The 3A4 interaction is the scenario described here. The external partner to internal partner simulation uses XML that contains the 3A4 Purchase Order Request content.

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

See the *WebSphere Partner Gateway Hub Configuration Guide* for related information. When you create the files, remember that the to and from Ids must match those of the internal partner and the external partner in the appropriate places in these files.

Configuring the Console and Router Servers

About this task

If you plan to use encryption or signing in your simulation, you must have 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 PKCS#8 and DER files to the `common/security/vtp` directory.
2. Copy the DER file to the `common/security/ca` directory.

3. If it is a self-signed certificate, with the console started, the CA certificate should be uploaded as Root and Intermediate certificate. If it is a CA signed certificate, the CA certificate should be uploaded as Root and Intermediate certificate. If the certificate path is to be built till root, then all the CA certificates in the certificate chain should be uploaded.
4. Modify the console configuration to point to the certificate and keystore files.
 - a. Use the console to view the RN PS properties by navigating to **System Administration > Console Administration > RN Simulator**.
 - b. Click on the **Modify** icon to place the screen into edit mode. Enter the following with values that are appropriate for your system. You must use der and p8 file formats as shown.


```
bcg.console.certs.vtp.CertificateDir=C:/<INSTALL DIR>/common/security/vtp
bcg.certs.vtp.Certificate=testcert.der
bcg.certs.vtp.PrivateKey=testkey.p8
bcg.certs.vtp.Passwd=password
bcg.certs.vtp.VerifySig=false
bcg.vtp.RouterIn=C:/<INSTALL DIR>/common/router_in
```
 - c. Click the **Save** button to save the changes that you have made.
5. If the console server is running, restart it. If it is not running, start it now.
6. Check to be sure that the Document Manager configuration is set up correctly.
 - a. Use the console to view the Document Manager security properties by navigating to **System Administration > DocMgr Administration > Security**.
 - b. Click the **Modify** icon to place the screen into edit mode.
 - c. Change the value of the `bcg.certs.vtp.CertificateDir` property to point to the same directory that the console pointed to step 4b. Save the property setting.

Note: These directories are named in the context of the server where the components are installed. The document manager and console should map a file system to the same directory.
7. If the Document Manager server is running, restart it. If it is not running, start it now.

Configuring 3A4 Connectivity

About this task

If you are familiar with RosettaNet routing, configure RosettaNet connectivity between an external partner and an internal partner using the following steps.

If you are not familiar with RosettaNet routing, see the *WebSphere Partner Gateway 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 interactions for 3A4 purchase order requests and confirmations to be routed through the hub.

3. Configure the internal partner and external partner B2B capabilities to be the Source and Receiver of partner 3A4 requests and confirmations that use RNSC content.
4. Establish the partner connections between the internal partner and the external partner 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 RosettaNet Partner Simulator to exercise all of the internal routing function. Select the **RosettaNet Partner Simulator** page and then click **Browse**. Select a file from the file system containing the content that you want to route, and then click **Route**.

The document is read from the file system and uploaded to the hub. It is passed to the Document Manager for routing, and the connection that you have configured in the hub is 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 second feature window, View Document Type, 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 Type window to examine the document. It is not necessary to edit a response.

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

After the upload completes, the RN PS 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 for the Document Manager to handle the message before attempting to view the results.

Initiating and viewing document type

About this task

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 type:

1. Click **RosettaNet Partner Simulator > Initiate Document Type**. 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 RN PS.
4. If you are simulating a one-way scenario, the test is complete.

Searching for an open document

About this task

1. Click **RosettaNet Partner Simulator > View Document Flows**.
2. Click the **View details** icon to view and open Document Type. The system displays the Open RN PS Document Type window.
3. Click the **Display raw document** icon to view the raw document.

Responding to an open document

About this task

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 receiver's URL. See Table 36 for test scenario information.

Table 36. Test scenarios

Scenario	Destination for Connection	URL
Two-way outbound from the internal partner to an external partner (Upload Request). Simulating internal partner.	VTP_TP	VTP_TP
One-way inbound from an external partner to the internal partner. Simulating external partner.	VTP_OWNER	VTP_OWNER
Two-way outbound from the internal partner to an external partner (Upload Response). Simulating external partner.	VTP_OWNER	VTP_OWNER
Two-way inbound from an external partner to the internal partner (Upload Response).	VTP_TP	VTP_TP

2. Click **RosettaNet Partner Simulator > View Document Type**.
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 Type** to view the document.

Removing an open document

About this task

1. Click **RosettaNet Partner Simulator > View Document Type**.
2. Click **Remove** next to the displayed document. The document is deleted from the system.

Chapter 13. Archiving

WebSphere Partner Gateway provides an Archiver utility for archiving and purging data from the system. Using WebSphere Partner Gateway console, you can schedule the archiver task to run automatically without manual intervention. In case of failure, the report and the corresponding error event generated will help you take corrective actions.

The archiver task will be configured while installing the WebSphere Partner Gateway hub. You can enable or disable the archiver task using the console. The console also allows you to restore the data backup, and search for a specific document by providing the required parameters in the filter criteria.

As a WebSphere Partner Gateway system administrator, you can perform or monitor the following operations:

- “Archiver configuration”: you can view and modify the archiver task.
- “Archiver runtime tasks” on page 134: list of runtime activities that occur while archiving.
- “Archiver reports” on page 135: view the status of each archiver task
- “Archiver Restore” on page 137: you can restore the data, which is already archived
- “User intervention for archiving” on page 139: if the automatic archiver schedule fails due to some reason, you can manually archive the data.

Archiver configuration

An archiver task is a scheduled process that is executed automatically at the configured time. This task is configured while installing WebSphere Partner Gateway components. As a system administrator, you can view and modify the archiver configuration details. Also, you can export or import the WebSphere Partner Gateway archiver configuration.

View archiver task

About this task

To view the archiver task, login as administrator and follow these steps:

Procedure

1. Click **Hub Admin > Hub Configuration > Archiver > Archiver Configuration**.
2. The following information is displayed:

Table 37. Archiver Configuration

Section	Field	Description
General	Task Name	Name of the archiver task, which is constant and cannot be edited.
	Description	Brief description of the task, which is constant and cannot be edited.
	Last Execution Time	Date and time of the task that was last executed. This field is updated automatically depending on the archiver execution time, and cannot be edited.
	Next Execution Time	Date and time of the task that is scheduled to be executed next. This field is updated automatically depending on the archiver execution time, and cannot be edited.
	Status	<p>Status of the task displayed in non-editable mode, which can be any one of the following values:</p> <ul style="list-style-type: none"> • Scheduled: by default the status is scheduled. It means that the task is scheduled to be run. • Running: displayed when the archiver task is executing • Stopping: displayed when you click 'Stop' on the console. • Being Scheduled: displayed when the configuration changes are saved to the database • Disabling: displayed when you click 'Disable' on the console • Disabled: displayed when you disable the task • Disabled_Failed: displayed if a task fails while running. Click 'Resume' to schedule the task <p>If the status is Disabled, Stopping, or Running, then the following parameters will be in non-editable mode.</p>

Table 37. Archiver Configuration (continued)

Section	Field	Description
Purging	Data Retention Period in days	The number of days of data (specified in this field) will be retained in the system, and the rest will be archived or purged.
	Copy NonRep data	By default, this value will be checked, which indicates that the non-repudiation data will be backed up to the archive location specified. You can un-check this value if you do not want to backup the data.
	NonRep File Archive Location	This field will be visible if the Copy Non Rep data checkbox option is selected. Specify the destination directory to backup the non-repudiation files. The default destination is: <common_file_system_location>/dataBackup
	NonRep Database Archive Location	This field will be visible if the Copy checkbox option is selected. Specify the destination directory to backup the database. The default destination is: <DBLoader>/dbBackup in case of DB2 <ORACLE_HOME>/oradata/<ORACLE_SID>/dbBackup in case of Oracle. Note: You need to provide a fully qualified path, where the database user has write permissions.
Purging Schedule	Daily, Weekly, or Custom schedule	The schedule for the archiver task to run, which can be daily, weekly, or user specified. The time specified will be in HH:MM (GMT) format.
Archive criteria	The following parameters are used to optionally filter the data to be archived. These will be used only to backup the data, and not for purging, that is, data will be purged regardless of these values. This section will be visible only if the 'Copy NonRep data' checkbox is selected.	
	Sending Partner	Name of the sending partner. Default value is All.
	Package	The package name and version that needs to be archived. Default value is All.
	Protocol	The protocol name and version that needs to be archived. Default value is All.
	Document Type	The document type and version that needs to be archived. Default value is All.

Archiver task modification

About this task

Follow these steps to modify the archiver task:

Procedure

1. Click **Hub Admin > Hub Configuration > Archiver > Archiver Configuration**. The Archiver Task is displayed in the view mode.
2. Click **Edit** icon to modify the required parameters. Refer to section Table 37 on page 132 for details on the parameters.
3. **Save** the archiver configuration. The status will change to **Currently being scheduled**.
4. An event is published to trigger the scheduler component. The scheduler reads the task configuration and updates the WebSphere Application Server configuration. The database tables are updated with the configuration information, which will be used during execution of archiver task and reporting.
5. The status then changes to **Scheduled** from **Currently being scheduled**.

What to do next

You can also reset a failed archiver task by selecting **Resume scheduling**.

Export and Import of archiver configuration

About this task

For detailed procedure on exporting and/or importing archiver configuration, refer to the chapter Chapter 6, “Administering partner migration,” on page 63

Archiver runtime tasks

During run time, the archiving activity is done as follows:

1. The archiver task is started by the system.
2. The configuration is read and the appropriate data is archived to the backup locations.
3. The common file system is cleaned up and data is purged from the database tables.

Here is the archiver runtime flow:

1. The Scheduled Archiver task runs as per the configured schedule.
2. The Archiver marks itself as **Running** in the database. The same status is displayed (at that instance) on the console.
3. The archiver reads the stored configuration from the database. The configuration is stored in the database during the state transition from 'Currently being scheduled' to 'Scheduled'.
4. If the 'Copy' attribute is selected in the archiver configuration, then:
 - a. The archiver takes the backup of the non-repudiation store from the database. The rows from LG_MSG_ARCHIVE table are exported to files in the directory specified in the database archive destination. It also exports the rows from the LG_CERT_ARCHIVE table.
 - b. The archiver copies the contents of the non-repudiation folder to the backup location.

Note: The criteria to back up the data is based on the configuration of the archiver task.

5. The archiver cleans-up the files from the Common File System. All files older than the cutoff date specified are deleted.

6. The archiver purges the data from the tables in the database. The data that is updated or created earlier than the cutoff date is deleted.
7. The archiver task is then marked as 'Successful' and the timestamp is updated in the reporting database tables.

Exception scenarios

If any error occurs during any of the mentioned runtime phases, the archiver task stops executing. In such a scenario, the following activities occur:

- The archiver logs the associated error in the server log file.
- There is an error event associated with the archiver task, and it is logged in the database.
- You can set up an 'Alert' for an error event, so that an alert is generated whenever a particular error occurs.
- The 'Archiver Task' will stop further scheduling and you must manually reset the configuration for the archiver after correcting the error.

Important: Data purging occurs whenever the archiver task is run without providing write permissions to the specified location of File Destination. Though the export of LG_MSG_ARCHIVE data is incomplete as expected, data purging must not happen. When the archiver is in disabled_failed state, if there are issues in copying non-rep data to the file system, manually back up the non-rep files.

Archiver reports

To view the archiver report, login as administrator and navigate to **Hub Admin > Hub Configuration > Archiver > Archiver Configuration** . The page lists the existing archiver task instances, that have run in the past.

The following information is displayed when you access the archiver report:

- Date/Time Started: Date and Time
- Date/Time Completed: Date and Time
- Status: Successful, Failed, Stopped, or Running
- Number of rows purged, along with start and end time, from the following tables:

Table 38. Data Purging Tables

Data	Table
Message Archive	LG_MSG_ARCHIVE

Table 38. Data Purging Tables (continued)

Data	Table
Activity Logging	LG_ACTIVITY_RNDTL
	LG_ACTIVITY_RNHDR
	LG_AS_DTL
	LG_AS_HDR
	LG_STATUS_ACTIVITY
	LG_B2BPROCESS_HDR
	LG_VALIDATION
	LG_ACTIVITY_DTL
	LG_ACTIVITY_ENDSTATE
	BP_PROCESS_LOG
	LG_DELIVERY_LOG
	LG_SYNCH_REQ_RESP
	LG_ACTIVITY_EVENT
	LG_ACTIVITY
	LG_STACKTRACE
	LG_EVENT
	LG_ACK
	LG_CHAIN
	LG_EDIFACT_RECONCILE
	LG_ENVELOPE_INCLUSION
State Engine	BP_RNSTATEHDRAUDITLOG
	BP_RNMSGDIGEST
	BP_SPONSOR_STATE
	BP_RNSTATEDTL
	BP_RNSTATEHDR
	BP_AS_STATE_DTL
	BP_AS_STATE_HDR
	BP_STATE_HDR
	BP_RM_STATE_DTL
	BP_RM_STATE_HDR
	BP_SPONSOR_STATE_EBMS
	BP_DUPCHECK
	LG_SUMMARY_MI
	LG_SUMMARY_RN
	LG_SUMMARY_RN_MI
	LG_EVENT_EVENTSUMMARY
	LG_EVENTSUMMARY
	LG_ACTIVITY_SUMMARY
	LG_SUMMARY

- Number of rows purged from LG_MSG_ARCHIVE
- Configuration settings enabled for that particular task
- Purging schedule that was configured
- Archive criteria used, such as Sending partner, Package, Protocol, and Document type. This is displayed only if the CopyNonRep data is selected while running the archiver task.

Archiver Restore

WebSphere Partner Gateway allows you to restore the data, which has been archived and purged from the system.

Before you begin

You will be able to restore only if the WebSphere Partner Gateway file system and database are available, and at least one archive and purge task is successfully completed.

About this task

To restore, do the following:

Procedure

1. Login as administrator and navigate to **Hub Admin > Hub Configuration > Archiver > Archiver Restore**.
2. Specify the date range by entering the **Start Date** and **End date**.
3. Provide the **NonRep File Archive Location** directory where the data is stored. This location will be searched for the files backed up from the NONREP folder during archiving. The default value will be taken from the latest configuration for the archiver task. The restore will fail, if it fails to read from the path specified e.g. If directory does not exist.
4. Provide the **NonRep Database Archive Location** directory. This location will be searched for the files backed up from the NONREP folder during archiving. The default value will be taken from latest configuration for the archiver task. The restore will fail, if it fails to read from the path specified e.g. directory does not exist.
5. Select the **Append** checkbox if you wish to append the data while restoring. If the checkbox is not selected, then the existing data will be overwritten by the new data. By default, this checkbox will not be selected.
6. Click **Restore**. The console will publish the event to the server.
7. Here are the server side activities:
 - a. The data is restored in the LG_MSG_RESTORE and LG_CERT_ARCHIVE tables. From the export log table, the server thread searches for the files that have the data for specified sub-volumes and reads those during the restore operation. Upon completion of the data restore, it will update the log table with flag set to 'Imported'.
 - b. The files are copied to dataRestore subfolder of Common File System in the appropriate sub-volume(s). The data is read from the backup files, which contain the documents processed on the days specified in the date range and are found on the backup locations.
8. Click **Refresh** to view the status of the restore task. On completion of the task, the status is displayed as **Successful** on the console. If there is a failure, then the status is displayed as **Failed**.

Restoring archived data of WebSphere Partner Gateway V6.1 and earlier

About this task

The console based restore (from archive) feature in WebSphere Partner Gateway V6.2 does not support the backup database archives taken on WebSphere Partner Gateway versions prior to V6.1. However, it supports the restoration of non repudiation file archives taken prior to WebSphere Partner Gateway V6.1. If the database is on DB2 and the archive backup was taken on WebSphere Partner Gateway V6.1 or later, then you can restore them using the 'restore' feature provided in WebSphere Partner Gateway V6.2. In the case of Oracle database, when you try to restore the data, an error occurs:

```
"Exception while doing the db restore
java.sql.SQLException: ORA-20999: 20002 AR_IMPORT_DATA ORA-29913: error
  in executing ODCIEXTTABLEOPEN callout
ORA-29400: data cartridge error
KUP-11010: unable to open at least one dump file for load
ORA-06512: at "BCGAPPSD.AR_IMPORT_DATA", line 338"
```

The workaround is to convert the format of the Oracle export files. To do this, you need to have another (separate from the production) installation of WebSphere Partner Gateway V6.2. Steps to be followed to restore the database archives taken on WebSphere Partner Gateway V6.1 or later:

Procedure

1. Use the 'bcgDBNonRepImport' script to import the table data into LG_MSG_ARCHIVE table.
2. Run the archiver from the console. This will create the database export files in the format supported by WebSphere Partner Gateway V6.2, which can be restored using the console. The steps to restore the archived data are same as described for DB2 database in the previous section. To restore V6.0 non repudiation file backup through the WebSphere Partner Gateway V6.2 console, the last modified date of the directory must fall within the start date and end date range selected in the Archiver Restore screen. This is because the V6.0 non rep directory structure is not in the YYYYMMDD format.

Searching the restored documents

About this task

You can search for the required restored document by specifying the search criteria. Here are the steps to follow:

Procedure

1. Login as administrator and navigate to **Hub Admin > Hub Configuration > Archiver > Archiver Restore > Search Restored Documents**.
2. Use the following filter criteria to search for a particular document:
 - Date range
 - Source Partner
 - Package
 - Protocol
 - Document type
 - Results Per Page

3. Click **Search**. The list of archiver tasks, along with the corresponding details are retrieved from the LG_MSG_RESTORE table and presented in a tabular format. The following information is displayed:
 - View Raw Message, click to view the raw message details of a particular record
 - Sending Partner, click on the partner name to view the complete partner profile
 - Package
 - Protocol
 - Document Type
 - Subvolume
 - Certificate name, click on the certificate name to view the certificate details.
4. Click **Reset** to revert to default system specified values.

User intervention for archiving

During some instances, the automatic archiver schedule might cease to work due to various reasons. In such instances, you can manually archive the required data. Following sections details the process to manually archive the data.

Initiating the archiver task to run from console

As WebSphere Partner Gateway administrator, you can initiate the archiver task from the console for immediate execution. This initiation will be irrespective of the scheduled tasks.

Here are the steps:

1. Navigate to **Hub Admin > Hub Configuration > Archiver > Archiver Configuration** and click **Run Now**.

Note: If the task is already running, Run Now link will be disabled.

2. The server starts to execute the task. If the **Copy** option is selected while configuring, the data gets copied to the specified location.

Stopping a running archiver task

Here are the steps to abort a running archiver task:

1. Navigate to **Hub Admin > Hub Configuration > Archiver > Archiver Configuration**. The page lists the existing archiver task with the status as 'Running'.
2. Click **Stop** to abort the task.
3. Click **Yes** when you get a prompt to confirm your operation. The status will be displayed as 'Stopping'.
4. The server stops the task completely and updates the status in the report tables in the database. It also publishes the event to schedule the next task.
5. The scheduler will schedule the archiver task for the next execution and the status will be updated to 'Scheduled'.

Note: If you try to stop the running task, it is possible that the data will be archived and/or purged partially. You will not be able to roll back the operation. As a result, the database tables may have an inconsistent set of data for the period before the cutoff date that was specified during the purge

operation. The same will be depicted on the console too. These discrepancies will be corrected with the next successful purge operation, which needs to have a cutoff date greater than or equal to the one that was specified while stopping the archiver task.

Archiver Restrictions

Due to native database support for server side export and/or import, WebSphere Partner Gateway Archiver and Restore functionality will be restricted on the following versions:

- Oracle 9i does not support export or import through database calls. You need to perform export (and import) of database data using the scripts provided - bcgDBNonRepExport and bcgDBNonRepImport .
- DB2 version 8 does not support import using database calls. Hence you need to perform the import of database tables using the script provided - bcgDBNonRepImport.

Chapter 14. Using logging and tracing features

One of the tasks of the WebSphere Partner Gateway administrator is to help diagnose problems that arise when documents are being processed. Logging and tracing are the tools that are used in the diagnosis of the problems. The administrator needs to know how to configure the system so it can provide the information needed to diagnose problems.

WebSphere Application Server provides sophisticated logging and tracing capabilities that are available to applications that it hosts. WebSphere Partner Gateway components are applications that are hosted by WebSphere Application Server, and they use the WebSphere log and trace capabilities.

WebSphere Application Server documentation contains general information about configuring logging and tracing, but in order to use it for WebSphere Partner Gateway, there are many specific things that you need to know. In this chapter, you will find a summary of the important items you need to know about using the WebSphere Application Server console to control logging and tracing. In addition to this general information, you will also find the specific items about using logging and tracing to solve WebSphere Partner Gateway problems.

Log and trace files

The log and trace files used for WebSphere Partner Gateway are described in this section:

SystemOut.log and SystemErr.log

Log messages are written whenever an application writes to the standard output stream or standard error stream. Application developers can write messages to these streams to provide general information about the status of the programs. For example, when an application is starting up, log messages are often provided to verify that the subsystems used by the application have been accessed, and that the application itself has started. When Exceptions occur, these are recorded in the form of a log message by the application that detected the Exception. The stack trace showing the state of the system when an Exception occurred is saved by writing it to the standard error stream.

Log messages are written to the following WebSphere Application Server files:

- `SystemOut.log` which records messages written to the standard output stream.
- `SystemErr.log` which records messages written to the standard error stream.

There is not a way to filter log messages so that only some are written and others are omitted. Since they are always written, log messages tend to be short and general in nature. Often they are useful because they do provide information about the status of the system and they can give you hints about what kind of detailed tracing you should use when a problem occurs.

Trace file

Unlike log messages, trace messages are only written by applications when

the system is configured to write them. WebSphere Partner Gateway applications provide numerous trace messages that can be used to get detailed information about the operation of the system. The trace messages are written to a trace file by themselves, without any of the log messages. The Messages logged in SystemOut.log and SystemErr.log are also included in the trace file. The WebSphere Application Server console is used to filter trace messages based on two criteria:

- The severity of the message
- The origin of the message.

You can configure WebSphere Application Server with the name of the trace file, the format of the trace file, the way that the trace file is managed, and the type of messages that are written to the trace file. Each WebSphere Partner Gateway application has default settings for these configuration values.

Note: The transactions submitted by WebSphere Partner Gateway and WebSphere Business Integration Connect product users are recorded in different time zones, as users are from different geographies. To maintain a common reference time zone for these transactions, WebSphere Partner Gateway and WebSphere Business Integration Connect performs time conversion for *bcg*.logs* internally and records it in GMT. However, no option is provided to change the time zones in these logs to avoid overlapping and conflicts. For SystemOut, SystemErr, and *bcg_server* log files, the timezone is in UTC (Universal Coordinated Time).

Log file management

The log files SystemOut.log and SystemErr.log are located on the workstation where the application is deployed under the path *<WebSphere Partner Gateway install dir>/wasND/profiles/<profile-name>/logs/<server-name>*.

Managing the log files means controlling the amount of disk space they can use. Some way of limiting the size is necessary; otherwise they can grow out of control and eventually affect your system's status. To control the file sizes, they are maintained as a set of circular log files. You can configure the number of files in the set and the size that each file can grow to before logging is moved to the next file in the set. This limits the total disk space that can be taken up by the log files.

Before configuring the log files, determine if your WebSphere Partner Gateway system was installed using simple mode or distributed mode. See the *WebSphere Partner Gateway Installation Guide* for more information about simple and distributed mode systems. Knowing the mode used for installation is important because the way that you access the WebSphere Application Server is different for simple and distributed modes.

For a simple mode system, the WebSphere Application Server admin console is found by browsing to `http://<server-address>:58090/admin`, where the server address is for the workstation where the system is installed. Port 58090 is the default used by the installer, however this port may be different if the default port was not used during installation.

If you are using a distributed mode system, the WebSphere Application Server admin console for the deployment manager. Find this by browsing to `http://<deployment-mgr-address>:55090/admin`. Port 55090 is the default used by the installer, however this may be different if the default port was not used during installation.

For both modes, the steps to configure the circular log files used by a server are the same.

1. Locate the server in the console by clicking on **Servers/Application servers** in the left pane to list the server names in the right pane.
2. View the details of the server that you want to configure by selecting the server name in the list.
3. Scroll down until you see the **Troubleshooting** heading near the bottom of the page. Click **Logging and Tracing** under **Troubleshooting**.
4. Click **JVM logs** to see the details of the logging configuration.
5. The tabbed window that displays contains a tab called **Configuration** and one called **Runtime**.

Note:

- a. Changes made on the **Configuration** page take effect after the server is restarted. These changes persist across server restarts.
- b. Changes on the **Runtime** page take effect immediately but do not persist across server restarts unless **Save runtime changes to the master configuration** is selected.

Key features of the **Configuration** page are that:

- You are presented two sections on the page, one to configure for standard output logging and the other to configure standard error logging.
- You can change the name and the path to the files that are used to store the log messages for the server.
- You can change the format used for the log messages. Both of the formats provide the message that the application writes. The difference between the basic and advanced formats is how much *meta-information* is provided with each message. *Meta-information* is information such as the time the log was written (basic and advanced) and the name of the thread (advanced only) that wrote the information.
- You can control how the circular logging is configured. Options are provided to set the size, number of files in the ring, and rollover triggering method (file size or time).

The key feature of the **Runtime** page is that you can view the log files by clicking **View** for a specific file. The line numbers that are displayed can be changed by entering a range of line numbers and refreshing the viewer page.

For a complete description of these features, see the WebSphere Application Server documentation.

Trace file management

Managing trace files includes:

- Controlling the amount of disk space that trace files can consume
- Setting the names and paths for the trace files
- Setting the trace file format
- Determining which WebSphere Partner Gateway components write trace information to the files
- Setting the trace level for the selected components.

You set the trace configuration using the WebSphere Application Server admin console.

Configuring tracing in a simple mode system

About this task

Setting up trace for a simple mode system is slightly different than for a distributed mode system. To configure tracing for a simple mode system, use the WebSphere Application Server admin console by browsing to `http://<server-address>:58090/admin`.

The port 58090 is the default used by the installer, however this might be different if the default port was not used during installation.

1. Locate the simple mode server named `server1` in the console by clicking on **Servers/Application servers** in the left pane to view the list of server names in the right pane.
2. View the details of `server1` by clicking its name in the list.
3. Scroll down until you see the **Troubleshooting** heading near the bottom of the page. Click **Logging and Tracing** under **Troubleshooting**.
4. Click **Diagnostic trace** to see the details of the tracing configuration.

By default, the trace file for the simple mode WebSphere Partner Gateway applications is configured as shown in Table 39. Because all of the WebSphere Partner Gateway applications are deployed to `server1`, all the trace messages are written to the same trace file. The trace file is written to the default directory of `<WebSphere Partner Gateway install dir>/wasND/profiles/<profile-name>/logs/<server-name>`. This is the same default directory where the log files are written.

Table 39. Simple mode trace configuration

Application	Trace file name	Format	Number of files	Maximum file size
All applications (Console, Receiver, and Document Manager)	trace.log	Basic	1	20 Mb

By default, the simple mode installer does not set the logging level. The logging level controls the amount of tracing information that is provided by components. If you want any tracing for the WebSphere Partner Gateway applications, you must specify logging levels. To change the logging levels, see “Setting log detail levels” on page 146.

Setting tracing in a distributed mode system

About this task

To manage the trace files on a distributed mode installation, use the WebSphere Application Server admin console for the deployment manager. Find this by browsing to `http://<server-address>/55090/admin`.

The port 55090 is the default used by the installer, however the port can be different if the default port was not used during installation.

1. Locate the server that you want to trace by clicking on **Servers/Application servers** in the left pane to view the list of server names in the right pane.
2. To view the details of the server you want to configure, select the server name in the list.

3. Scroll down until you see the **Troubleshooting** heading near the bottom of the page. Click **Logging and Tracing** under **Troubleshooting**.
4. Click **Diagnostic trace** to view the details of the tracing configuration.

By default, trace files for the distributed mode of WebSphere Partner Gateway applications are configured as shown in Table 40. The trace files are written in `<WebSphere Partner Gateway install dir>/wasND/profiles/<profile-name>/logs/<server-name>` directory. This is the same place that the log files are written by default.

Table 40. Distributed mode trace configuration

Application	Trace file name	Format	Number of files	Maximum file size
Receiver	bcg_receiver.log	Advanced	10	10 Mb
Document manager	bcg_router.log	Advanced	10	50 Mb
Console	bcg_console.log	Advanced	10	50 Mb
Messaging server	trace.log	Basic	1	20 Mb

The installer sets the logging level for all components of the WebSphere Partner Gateway applications to log severe level trace messages. The logging level controls the amount of tracing information that is provided by components. To change the logging levels, see “Setting log detail levels” on page 146.

Tracing tasks common to both types of systems

About this task

1. Locate the server in the console by clicking on **Servers/Application servers** in the left pane to list the server names in the right pane.
2. View the details of the server that you want to configure by selecting the server name in the list.
3. Scroll down until you see the **Troubleshooting** heading near the bottom of the page. Click **Logging and Tracing** under **Troubleshooting**.
4. Click **JVM logs** to see the details of the logging configuration. The window has two pages: **Configuration** and **Runtime**.

Note:

- a. Changes made on the configuration page take effect after the server is restarted. These changes persist across server restarts.
 - b. Changes made on the runtime page take effect immediately but do not persist across server restarts unless **Save runtime changes to configuration** is selected.
5. The **Configuration** and **Runtime** pages both contain a link on the right side called **Change Log Detail Levels**. This is where you can:
 - Enable WebSphere Partner Gateway components to write to the trace file
 - Select the logging level for each enabled component. The logging level controls the amount of tracing information that is provided by components. To set the log detail levels, see “Setting log detail levels” on page 146.

Key features that you should understand on the Configuration page are:

- The tracing is not written to the file named until you select **Enable Log**, save the change, and restart the server. To enable the log, go to **Logging and Tracing > Diagnostic Trace Service**.

- Trace messages can be written to a memory buffer or to a file. You specify this by choosing one of the **Trace Output** radio buttons.
 - If you select the **memory buffer** option, you must have a way to take what is in memory and put it into a file so you can see the messages.
 - If you use the **trace file** option, you configure a circular log similar to the way the system circular logging is configured. By using circular logging, you can limit the growth of the trace files so they do not consume too much of your file system resource. You can also configure the path and file name for the trace files.
 - The **trace output format** option can either be **Basic** or **Advanced**. Trace files can also be written using a binary format called the **Log Analyzer** format. By specifying the log analyzer format, you can open a trace output file using the Log Analyzer tool. The Log Analyzer tool is an application included with the WebSphere Application Server. See the WebSphere Application Server documentation for more information about the Log Analyzer.

The key benefit of the **Runtime** page is that you can dynamically change the trace logging without restarting the server. You can reflect any changes that you make at runtime into the persistent configuration if you select **Save runtime changes to configuration** before saving.

For a complete description of these features, see the WebSphere Application Server documentation.

Setting log detail levels

When problems occur, services and support personnel may ask for trace files to help understand the nature of the problem. As the administrator of the system, you will configure the system to obtain the tracing that is useful for diagnosing problems. That is the purpose of setting the logging levels. When you set the logging level for a server:

- You determine which WebSphere Partner Gateway components (Java classes) write trace messages.
- You determine the types of messages that are included in the trace file using an importance scale with five levels.

Trace messages are classified using severity levels that are derived from levels used by WebSphere Partner Gateway version 6.0 and earlier. These old severity levels are mapped to WebSphere Application Server severity levels according to Table 41. This table illustrates how to use the new levels to achieve the same level of trace.

Table 41. WebSphere Application Server severity levels

Version 6.1 severity level	Version 6.2 severity level
FATAL	FATAL
ERROR	SEVERE
WARN	WARNING
INFO	INFO
DEBUG	FINEST

Log detail levels are accessed using a link that is provided on the Diagnostic tracing **Configuration** and **Runtime** pages for an application server. When you click this link, you are presented with a page that shows a tree-view of

components. Components are represented by the Java package names for the classes that can provide trace information when they are issued by the application server.

Note: The Java package names for WebSphere Partner Gateway classes all begin with the prefix `com.ibm.bcg` so you can locate the individual components by looking for packages that use this prefix.

There are three ways to set log detail levels:

- To set log details at the component level using the component tree:
 1. Select the item.
 2. Choose the level of tracing you require.
 3. Click **OK** on the page to make the change
- To set log details at the group level using the group tree:
 1. Select the group name.
 2. Choose the level of tracing you require.
 3. Click **OK** to make the change

Note: There are groups of components that represent WebSphere Partner Gateway subsystems like the receiver or the document manager state engine. You can view the subsystems by clicking the **Groups** link. The WebSphere Partner Gateway group names can be identified because they all start with the prefix `BCG`. Each of the group names describes the purpose of the classes and packages that are in the group.

- To Set log details by directly entering package and class names. The names that are in the tree views are only a fraction of all the packages and classes that make up WebSphere Partner Gateway applications. You might be asked to obtain tracing for classes that are not in these lists.

If you change the configuration page, be sure to save the configuration to the master configuration according to the message that displays at the top of the page.

Identifying WebSphere Partner Gateway trace messages

If you configured tracing with the Advanced format, each trace message includes the class name, method name, originator, thread id, thread name, and other information for the message. The Basic log format contains necessary information like timestamp, thread id, source class, source method, severity level and log message.

Note: In the event of failure, Websphere Partner Gateway does not log events related to First Failure Data Capture (FFDC) feature. Do not refer to the FFDC logs unless directed by the product support or by any specific troubleshooting instruction.

EDI, XML, ROD subcomponent tracing

There might be times to enable tracing for some EDI, XML and ROD (flat file) components that are used in relation to validation maps and transformation maps created by the DIS Client. These are enabled from the WebSphere Partner Gateway Console > System Administration > Feature Administration > EDI Properties. For the trace level settings and purpose of each property, see Table 55 on page 234

Interpreting WebSphere Application Server log and trace messages

Messages and errors from the WebSphere Application Server console processes display in the WebSphere Partner Gateway logs. Some of these messages might appear to be errors, but they are informational and do not pose a problem for the WebSphere Partner Gateway application. The level value is set from configuration data when the logger is created and can be changed at run time from the administrative console. Use the following information to interpret the WebSphere Application Server messages you might encounter in your system output logs.

WebSphere Application Server event types

A one character field that indicates the type of the message or trace event. Message types are in upper case. Possible values include:

- | | |
|----------|--|
| F | A fatal message |
| E | A error message |
| W | A warning message |
| A | A audit message |
| I | A informational message |
| C | A configuration message |
| D | A detail message |
| O | A message that was written directly to SystemOut.log by the user application or internal components. |
| R | A message that was written directly to SystemErr.log by the user application or internal components. |
| Z | A placeholder to indicate that the type was not recognized. |

Integrated FTP Server logging

This section describes the integration of success and failure event messages for the FTP Server actions. When WebSphere Partner Gateway Partner intends to send a document to WebSphere Partner Gateway Integrated FTP server, Integrated FTP server produces a client connect notification event. The appropriate connection event message is logged into WebSphere Partner Gateway database after examining the FTP server response codes.

Success and failure event messages for FTP Server actions

The event messages produced by the FTP Server for various actions such as establishing connection, user login, file upload, file download and disconnect are logged as events in WebSphere Partner Gateway database. These events can be viewed from WebSphere Partner Gateway console using the existing event viewer.

The possible response codes for connect event are:

- 220 Service ready for new user.
- 530 No server access from the IP.
- 530 Maximum number of server connections has been reached.

After the connection is established, the user information is authenticated. After user authentication is performed, FTP Server produces a client login notification

event. The appropriate login event message is logged into WebSphere Partner Gateway database. The possible response codes for user authentication are:

- 501 Syntax errors in parameters or arguments
- 503 Login with USER first.
- 202 Already logged-in
- 21 Maximum number of anonymous login has been reached.
- 421 Maximum number of login has been reached.
- 230 User logged in, proceed

After the user login is successful, Partner FTP Sender attempts to put the document to the FTP Server. Once the file is uploaded, FTP Server produces an upload end notification event. The possible response codes for upload start event are:

- 150 File status okay; about to open data connection.
- 226 Transfer complete.
- 550 Invalid paths.
- 550 Permission denied.
- 425 Can't open data connection.
- 426 Data connection error.
- 551 Error on output file.

Once the document is successfully uploaded to the FTP Location, the FTP connection is disconnected. FTP server produces a disconnect notification event. This event is logged into WebSphere Partner Gateway database.

Logging and exception information related to Integrated FTP Server

The FTP server code internally produces logging and exception information. This information is available in the log files generated on the system where the FTP Server is installed. These log files are checked and analyzed separately to obtain details on any error or debug information. The log file format is similar to the formats used by other components of WebSphere Partner Gateway.

Integrated SFTP Server logging

This section describes event messages for the SFTP Server actions. When WebSphere Partner Gateway Partner intends to send a document to WebSphere Partner Gateway Integrated SFTP server, Integrated SFTP server produces a client connect notification event. The appropriate connection event message is logged into WebSphere Partner Gateway database after examining the SFTP server response codes. In the Events code page of the console, the range of SFTP events is from BCG620001 to BCG620008.

Chapter 15. FTP and SFTP Server Configuration Management

The FTP Server configuration properties are stored in WebSphere Partner Gateway database. In the console, navigate to **System Administration > FTP Administration**.

From the **Server Start/Stop** page of the console, you can start and stop the FTP and SFTP servers.

The FTP Server configuration is divided into six tabs:

- **Event Properties**

The Event properties page displays the editable configuration properties for logging FTP Server event messages.

- **Listener Properties**

The Listener Properties page lists all the editable properties.

- **Connection Properties**

The Connection Properties page list all the editable properties.

- **IP Restrictor Properties**

The IP Restrictor allows you to restrict access to FTP Server using IP addresses. Click **Add** to add new IP address. IP address can be specified with wild cards, namely *, ?, and -. The order of the rules is important. When a client contacts the server, the rules are evaluated from top to bottom. Click **Save** to save the changes. The FTP server will restart for the changes to take effect. If all the passive ports are in use by client connection, then the next client will have to wait till a port is available. The allowed range is from 0-65535. Using **config.data-connection.passive.ports** property, passive ports can be specified either as single port, multiple ports or a range of ports.

- **Database Properties**

The Database Properties page allows you to enter the database properties like **Host name, User name, Password, and Port**. These values will automatically be saved in FTP server.

- **Other Properties**

The Other Properties page list all the editable properties.

The **SFTP Properties** page contains the port, maximum authentication requests, and authentication time out values of the SFTP server:

FTP and SFTP user management

Use FTP user management page to manage FTP and SFTP users. In the console, navigate to **Account Admin > FTP User Management**. You can perform the following tasks using FTP user management page:

- Search for FTP and SFTP users across partners based on the required search criteria.
- Edit FTP and SFTP user information.
- Create FTP and SFTP users.
- View and edit FTP and SFTP configuration information.

Chapter 16. Relocation and Redeployment of WebSphere Partner Gateway

Typically, when the IP address or host name of the WebSphere Partner Gateway environment changes, the system configuration files need to be updated in all machines where WebSphere Partner Gateway components are installed.

WebSphere Partner Gateway 6.2.1 provides you an option to automatically update the configuration files if the IP address, host name, data source details, or port number of a server component or deployment manager changes. The following changes are supported post deployment of WebSphere Partner Gateway:

- “Changing host name and IP address of WebSphere Partner Gateway” on page 154
- “Changing the host name and port number of database” on page 155. When you change the host name or port number of the database, update the same in the datasource defined in WebSphere Application Server, which is used by WebSphere Partner Gateway to connect to the database.
- “Changing the port numbers” on page 155

This chapter also provides example scenarios considering different installation and deployment topologies.

Note: The commands mentioned in this chapter is not case sensitive.

Limitations

While automatically updating host name or IP address, here are few things to keep in mind:

- Ensure that you take a backup before changing the parameters. If you backup the existing configuration using *backupconfig.bat*, you will be able to restore that configuration, if required. Refer to “Prerequisites” for more details.
- You need to manually change certain properties such as FTP host, database source user name and password.

Prerequisites

Simple mode

Before starting relocation and redeployment, ensure that you backup the existing configuration as described below:

1. Stop the application server
2. Run the command `<WPG Components Installed Path>/WASND/Profiles/<ProfileName>/bin/backupConfig.bat`

Distributed mode

1. Stop all application servers, nodes, and deployment manager
2. Run the following commands to backup the configuration files of deployment manager and the components installed on deployment manager:
 - `<Deployment Manager Installed Path>/WASND/Profiles/<ProfileName>/bin/backupConfig.bat`

- <WPG Components Installed Path>/WASND/Profiles/<ProfileName>/bin/backupConfig.bat. Run this command on all machines where WebSphere Partner Gateway components are installed.

Restoring the configuration details

You will be able to restore the configuration details only if you backup the configuration using the steps mentioned in the above section. Run the following commands to restore the configuration:

- <Deployment Manager Installed Path>/WASND/Profiles/<ProfileName>/bin/restoreConfig.bat
- <WPG Components Installed Path>/WASND/Profiles/<ProfileName>/bin/restoreConfig.bat

Changing host name and IP address of WebSphere Partner Gateway

The following sections provide detailed steps to change host name or IP address of WebSphere Partner Gateway components. Refer to the appropriate section based on WebSphere Partner Gateway installation mode.

Note: Stop the server before you start executing the steps provided for changing the host name and IP address.

Simple mode

Follow these steps:

1. Ensure that you backup the configuration files before making any significant changes. Refer to “Prerequisites” on page 153 section for more details.
2. Change the data source; execute `bcgChangeDataSource.bat\sh` with new Host name/IP address and Port number as the input parameters, that is `bcgChangeDataSource.bat\sh <New IP/Hostname> <PORTNUMBER>`. This executable is available in the folder <Installation directory of simple mode>/bin.
3. Change the host name; execute `bcgChangeNodeHostname.bat\sh` with new Host name/IP address as the input parameter, that is `bcgChangeNodeHostname.bat\sh <New IP/Hostname>`. This executable is available in the folder <Installation directory of simple mode>/bin.

Note: Up on successful completion of host name/IP address change, the application servers will start automatically.

Distributed mode

Follow these steps:

1. Ensure that you backup the configuration files before making any significant changes. Refer to “Prerequisites” on page 153 section for more details.

Note: Stop the Deployment Manager, Node agent before executing the steps provided for changing host name and port number.

2. Change the DMGR profile; execute `bcgChangeDmgrHostname.bat\sh` with new Host name/IP address as the input parameter, that is `bcgChangeDmgrHostname.bat\sh <New IP/Hostname>`. This executable is available in the folder <Installation directory of Deployment Manager>/bin. This command changes the host name/IP address of DMGR profile and starts the deployment manager.

3. Change node associations with new DMGR hostname; execute `bcgChangeDmgrHostname.bat\sh` with new Host name/IP address and SOAP port as input parameters, that is `bcgChangeDmgrHostname.bat\sh <New IP/Hostname> <SOAP PORTNUMBER>`. This executable is available in the folder `<Installation directory of hub>/bin`.
4. Change the host name of the WebSphere Partner Gateway components; execute the following:
 - a. `bcgChangeNodeHostname.bat\sh` with with new Host name/IP address and Current node name as the input parameters, that is, `bcgChangeNodeHostname <New IP/Hostname> <Node name of the machine>`. The executable is available in the folder `<BCG_DMGR_HOME>/bin`.
 - b. In the machine where WebSphere Partner Gateway components, run `bcgChangeNodeHostname.bat\sh` with new Host name/IP address, DMGR host name, and DMGR SOAP port as the parameters. The command will be `bcgChangeNodeHostname <New IP/Hostname> <Dmgr IP/hostname> <DMGR SOAP port>`. This executable is available in the folder `<BCG_Hub_HOME>/bin`.

Note: After successful completion of host name/IP address change, the deployment manager starts automatically. However, you need to manually start the node and application servers.

Changing the host name and port number of database

Refer to the appropriate section for detailed steps to change the host name and port number of database. Ensure that you backup the configuration files before making any significant changes. For more details, see “Prerequisites” on page 153 section.

Simple mode

Run the command `bcgChangeDataSource.bat\sh <New IP/Hostname> <PORTNUMBER>`. This executable is available in the folder `<BCG_SIMPLE_HOME>/bin`.

Distributed mode

To change the host name and port number of:

- MAS database: run the command `bcgChangeMASDataSource.bat\sh <New IP/Hostname> <PORTNUMBER>`. This executable is available in the folder `<BCG_HUB_DMGR>/bin`.
- WebSphere Partner Gateway Application database: run the command `bcgChangeDataSource.bat\sh <New IP/Hostname> <PORTNUMBER>`. This executable is available in the folder `<BCG_HUB_DMGR>/bin`.

Note: If you wish to change just one parameter, specify `<None>` for the parameter that should not be changed. For example, to change just the IP address, run the command `bcgChangeDataSource 9.182.10.12 NONE`.

Changing the port numbers

Ensure that you backup the configuration files before making any changes. Refer to “Prerequisites” on page 153 section for more details.

To change the port number, run the command `bcgChangePorts.bat <PortType> <Portno> <ServerType> <HostName>`. The port type must be any of the following values:

- BOOTSTRAP_ADDRESS
- SIB_ENDPOINT_ADDRESS
- WC_defaulthost

The port number must be any value in the range 0 to 65535.

Server type must be any of the following values:

- simple
- console
- router
- receiver
- simpledistributed

Relocation and redeployment examples

Depending on the WebSphere Partner Gateway installation and deployment topology, you will have to run the relocation and redeployment scripts on one or more machines. The following sections describe various scenarios where the changes have to be updated, and the steps to update the same.

Example 1: Simple distributed installation

Here is a scenario where WebSphere Partner Gateway is installed in a simple distributed mode. Assumptions are:

- Machine A - Database is installed
- Machine B - Deployment manager and WebSphere Partner Gateway components are installed. Hostname of this machine is being updated.

Follow these steps to change the host name or IP address:

1. Ensure that you backup the configuration files before you make any significant changes. Refer to “Prerequisites” on page 153 section for details.
2. Change the host name or IP address of DMGR profile as described below:
 - a. In **Machine B** where deployment manager is installed, execute `bcgChangeDmgrHostname.bat\sh` with new Host name/IP address as the input parameter, for example, `bcgChangeDmgrHostname.bat 9.1.1.1`. The executable is available in the folder <Installation directory of Deployment Manager>/bin. This command changes the host name/IP address of DMGR profile and starts the deployment manager.
 - b. In **Machine B**, access the Node where WebSphere Partner Gateway components are installed. Execute `bcgChangeDmgrHostname.bat\sh` with new Host name/IP address and SOAP port as input parameters, for example, `bcgChangeDmgrHostname.bat 9.1.1.1 55880`. The executable is available in the folder <<Installation directory of hub>/bin>.

The host name/IP address of the deployment manager for the node on Machine B is now changed. All the changes from the deployment manager will be synchronized to this node.

Note: If there are multiple nodes, run these scripts for each node.

3. Change the host name/IP address of the node on which the WebSphere Partner Gateway components are installed. Follow these steps:
 - a. In **Machine B** where deployment manager is installed, execute `bcgChangeNodeHostname.bat\sh` with new Host name/IP address and

Current node name as the input parameters, for example, `bcgChangeNodeHostname.bat 9.1.1.2 bcgnode_B`. The executable is available in the folder `<Installation directory of Deployment Manager>/bin`.

- b. In **Machine B**, access the Nodes where all WebSphere Partner Gateway components are installed. Execute `bcgChangeNodeHostname.bat\sh` with new Host name/IP address, DMGR host name, and DMGR SOAP port as the parameters, for example, `bcgChangeNodeHostname.bat 9.1.1.2 9.1.1.1 55880`. The executable is available in the folder `<Installation directory of hub>/bin`.

Note: Manually start the nodes and application server. DMGR is started automatically.

Example 2: Fully distributed installation

In this scenario, the assumptions are:

- Machine A - Database is installed and the port number of this is being updated.
- Machine B - Deployment Manager is installed and the IP address is being updated.
- Machine C - Components are installed and IP address is being updated.

Follow these steps to change the host name or IP address of deployment manager and WebSphere Partner Gateway components:

1. Ensure that you backup the configuration files before you make any significant changes. Refer to “Prerequisites” on page 153 section for details.
2. Change the host name or IP address of DMGR profile as described below:
 - a. In **Machine B** where deployment manager is installed, execute `bcgChangeDmgrHostname.bat\sh` with new Host name/IP address as the input parameter, for example, `bcgChangeDmgrHostname.bat 9.1.1.1`. The executable is available in the folder `<Installation directory of Deployment Manager>/bin`. This command changes the host name/IP address of DMGR profile and starts the deployment manager.
 - b. In **Machine C**, access the Node where WebSphere Partner Gateway components are installed. Execute `bcgChangeDmgrHostname.bat\sh` with new Host name/IP address and SOAP port as input parameters, for example, `bcgChangeDmgrHostname.bat 9.1.1.1 55880`. The executable is available in the folder `<Installation directory of hub>/bin`.

The host name/IP address of the deployment manager for the node on Machine C is now changed. All the changes from the deployment manager will be synchronized to this node.

Note: If there are multiple nodes, run these scripts for each node.

3. Change the host name/IP address of the node on which the WebSphere Partner Gateway components are installed. Follow these steps:
 - a. In **Machine B** where deployment manager is installed, execute `bcgChangeNodeHostname.bat\sh` with new Host name/IP address and Current node name as the input parameters, for example, `bcgChangeNodeHostname.bat 9.1.1.2 bcgnode_C`. The executable is available in the folder `<Installation directory of Deployment Manager>/bin`.
 - b. In **Machine C**, access the Nodes where all WebSphere Partner Gateway components are installed, execute `bcgChangeNodeHostname.bat\sh` with

new Host name/IP address, DMGR host name, and DMGR SOAP port as the parameters, for example, `bcgChangeNodeHostname.bat 9.1.1.2 9.1.1.1 55880`.

4. Change the hostname and port of the database. Ensure that DMGR is up and running before executing the following steps:
 - a. In **Machine C** where WebSphere Partner Gateway components are installed, execute `bcgChangeDataSource.bat \sh` with new Host name/IP address and port as the parameters. For example, `bcgChangeDataSource.bat 9.1.1.2 55880`. Ensure that you provide new host name/IP address and new port number of the application database that is installed on **Machine A**.
 - b. In **Machine C** where WebSphere Partner Gateway components are installed, execute `bcgChangeMASDataSource.bat \sh` with new Host name/IP address and port as the parameters. For example, `bcgChangeMASDataSource.bat 9.1.1.2 55880`. Ensure that you provide new host name/IP address and new port number of the MAS database that is installed on **Machine A**.

Note: Manually restart all the servers.

Chapter 17. Troubleshooting

This chapter provides troubleshooting information you can use to identify and resolve problems. See “Appendix B - failed events” on page 191 for a list of failed events and their corresponding descriptions.

Topics in this chapter include:

- “Avoiding long processing time on large encrypted AS documents” on page 160
- “Avoiding long processing time for large encrypted documents” on page 161
- “Avoiding out-of-memory errors” on page 161
- “Collating data for multiple languages” on page 162
- “Ensuring sufficient virtual memory for DB2 agents” on page 163
- “Fixing DB2 SQL errors” on page 163
- “IBM service log unreadable” on page 165
- “WebSphere Application Server informational messages” on page 165
- “Increasing the Receiver timeout setting” on page 165
- “Optimizing database query performance” on page 166
- “Resolving event 210031” on page 166
- “Documents routed twice when network is lost or document manager server shutdown abruptly” on page 167
- “0A1 generated with data validation errors” on page 167
- “EDI reports export the first 1000 records only” on page 167
- “Console does not start after a server restart” on page 167
- “FTPScripting Receiver receives StringIndexOutOfBoundsException” on page 168
- “Receiver Failure to read Configuration File” on page 168
- “Configuring Users to receiving Alerts Notification” on page 168
- “Resolving ClassNotFoundException for User Exit classes” on page 169
- “Reprocessing events and business documents that fail to log to the database” on page 169
- “Disabling JIT in a WebSphere Application Server when WebSphere Partner Gateway produces a javacore” on page 170
- “Defining a custom transport type” on page 170
- “Resolving WebSphere Partner Gateway errors BCG210031 and BCG240415” on page 170
- “Creating File directory destination on a drive other than C:” on page 171
- “Preventing partner transactions from being processed by WebSphere Partner Gateway” on page 171
- “Fixing the browser ERROR: 500” on page 172
- “Downloading CRL for SSL transactions” on page 172
- “Databinding in JMS Exports/Imports within WebSphere Process Server” on page 173
- “Fixing test partner connection for SSL connections” on page 174
- “Fixing errors BCGEDIEV0056 and BCG210001” on page 174
- “Fixing ORA-00988 error” on page 174

- “Configuring Content-Types attribute for the fixed workflow handlers” on page 174
- “Fixing BCG210013 error” on page 175
- “Increasing buffer size to prevent document transmission low performance” on page 176
- “WebSphere Partner Gateway hub installer logs error messages” on page 176
- “DB password required error in bcgHubInstall.log” on page 177
- “Using revocation check and using CRL DP support” on page 177
- “Returning document volume report search information about the console” on page 177
- “Loading the native library” on page 178
- “Fixing error TCPC0003E and CHF0029E” on page 178
- “CA certificate expiration” on page 179
- “VBaseException in the SystemOut.log” on page 180
- “Reporting file size for documents greater than 2 GB” on page 180
- “SSL handshake fails because no certificate received” on page 180
- “Fixing the hanging threads warning” on page 181
- “Stopping the Document Manager exception” on page 181
- “Fixing WebSphere MQ messages” on page 182
- “java.security.InvalidKeyException: Illegal key size or default parameter” on page 183
- “The MDN status of 'unknown' for AS transactions” on page 183
- “Servers fail to start after applying fixes” on page 183
- “Correcting the shortcut ports for WebSphere Application Server” on page 184
- “Avoiding duplicate document delivery when there is more than one router” on page 184
- “Rendering of tab headings on displays with resolution greater than 1024” on page 185
- “Documents not processed when using Oracle 9i Release 2” on page 185
- “Document processing when the database goes down” on page 185
- “java.lang.NoClassDefFoundError with reprocessDbLoggingErrors.bat” on page 186
- “Recovery process when queue and disk is full or unavailable” on page 186
- “Workflow Handler Runtime Error” on page 186
- “Error while invoking WebSphere Transformation Extender Map” on page 187
- “IBM Support Assistant (ISA) Plugin” on page 187
- “Partner Migration Utility with LDAP” on page 187
- “AS signature failure for interop content type” on page 188

Avoiding long processing time on large encrypted AS documents

About this task

Large encrypted AS documents can 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" to increase memory size and speed up processing of encrypted documents.

Avoiding long processing time for large encrypted documents

Large files can be compressed before sending. Large file support with an order of size in GBs has been extended for AS2 and AS3. In version 6.2, the maximum file size processed using byte arrays is configurable. When the amount of memory allocated is more than the available heap size, `OutOfMemoryError` occurs. If the size of data is less than the available memory, `OutOfMemoryError` may still occur if the memory allocated increases available memory. You can specify the maximum file size that can be used with byte arrays using the property `bcg.maximumFileSizeForByteArrays`. When you log in as a hub operator, navigate to **System Administration** tab > **Common Attributes** tab. Overwrite the default value of `bcg.maximumFileSizeForByteArrays` property to specify the maximum file size to be used with byte arrays. Increase the value of this property for better performance. To avoid out of memory errors, the value of property `bcg.maximumFileSizeForByteArrays` must be set such that very large files are processed using streams rather than as byte arrays. For example, if RAM size is 512 MB, then the value of `bcg.maximumFileSizeForByteArrays` property can be set to 20 MB. All documents of size greater than 20 MB will be processed using streams and not using byte arrays. Documents of size less than 20 MB will be processed in memory.

Avoiding out-of-memory errors

Areas that can contribute to the out of memory conditions are:

- Document Manager memory configuration
This configuration specifies the amount of memory the underlying Java application has allocated to work with.
- Document Manager workload
You can configure the number of threads subcomponents can use. If the configured thread number is high and there is a heavy work load then more memory is required to handle all of the documents.
- Document structure of the documents that are being processed
Depending on the document structure more memory can be required to process a document, especially for large documents. Areas affected are security (encryption, decryption, signing, signature verification) and XML Transformation and Validation processing steps (especially those documents with large text values).

For more information on `OutOfMemoryError` due to large file size, see "Avoiding long processing time for large encrypted documents."

Document Manager memory configuration

About this task

To improve performance and avoid out of memory errors, you can increase the size of the initial and maximum heap sizes for the Websphere Partner Gateway components. From the Websphere Application Server admin console:

1. Navigate to Application Servers.
2. Select the Websphere Partner Gateway component.
3. Select **Java and Process Mgmt** > **Process Definition** > **Java Virtual Machine**.

4. Update the values for **Initial Heap Size** and **Maximum Heap Size**
5. Restart Websphere Partner Gateway.

Document Manager workload

The number of processing threads used can be configured for several subcomponents by setting system properties. The default values for these properties are low but they might have been modified by the administrator. Look for properties involving thread configuration in the configuration tables in “Appendix C - component-specific system attributes” on page 225.

Document structure

Large documents can come either from the external partner or the internal partner (backend application). Determine if there are ways to reduce the document sizes, such as reduced batch sizes or using smaller documents.

Increasing the heap size

About this task

Whenever sending a large number of documents (approximately 40) that have a size of 50MB with encryption, signing, and compression over AS3, it is necessary to increase the heap size. If the heap size is not increased, documents can fail with the error `OutOfMemory`.

The `OutOfMemory` error is the result the working memory not being sufficient for the Websphere Partner Gateway to route the documents in bulk. Therefore, it is recommended that you increase the heap size. To increase the heap size parameters for the DocMgr server, perform the following steps:

1. Log into the WebSphere Application Server admin console.
2. From the WebSphere Application Server admin console, select **java and process management > Process Definition > Java virtual machine** for the `bcgDocMgr` server.
3. Set the **initial heap size** to 1024.
4. Set the **max heap size** to 1536. If the system has more than 2GB, then max heap size can be set to a value higher than 1536 value.

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, review this section.

DB2

Since version 6.0, WebSphere Partner Gateway configures DB2 to use 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 contact DB2 directly.

Oracle

Oracle databases use dynamic changing for collation sequences. In order to use this functionality, WebSphere Partner Gateway changes the value of the `NLS_SORT` session variable depending on the locale of the current user. Table 42 on page 163

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 42. 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.
```

Fixing DB2 SQL errors

See the following sections to fix specific DB2 SQL messages:

- “SQLCODE -444 error” on page 164
- “SQLCODE -289 error” on page 164
- “SQLCODE -1225 error” on page 164
- “SQL 0964C Transaction log full error on the BCGMAS database” on page 164

SQLCODE -444 error

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. Consult your database administrator or see 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 can decrease the values of STMTHEAP and APPLHEAPSZ for your WebSphere Partner Gateway 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
```

Consult your DBA or see your DB2 administrator's guide before changing any settings.

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

SQLCODE -289 error

A DB2 error code -289 indicates that the database has run out of space on the file system. Check with the database administrator about adding additional capacity on the database server.

Alternatively WebSphere Partner Gateway data can be archived to a different storage location to free up disk space.

SQLCODE -1225 error

You can receive the SQLCODE -1225 error followed by a stack trace in the WebSphere Partner Gateway server logs when DB2 resources are running low on the system. The following is an example of the SQLCODE error.

```
java.sql.SQLException: com.ibm.db2.jcc.c.SQLException:
DB2 SQL error: SQLCODE: -1225, SQLSTATE: 57049, SQLERRMC: null
```

This error is typically occurs when transaction rates are high (large number of documents per second) and DB2 is not able to sustain this rate. The database administrator might want to monitor and tune the database to accommodate these high transaction periods. To improve the performance of the database logging, you can tune the following DB2 parameters:

- LOGPRIMARY
- LOGSECOND
- LOGFILESIZ

SQL 0964C Transaction log full error on the BCGMAS database

WebSphere Partner Gateway creates the BCGMAS database with the following default configuration values:

```
LOGFILSIZ=1024
LOGPRIMARY=13
LOGSECOND=4
```

The amount of space required for the DB2 transaction log is dependent on a number of factors, including the peak rate of documents being processed by WebSphere Partner Gateway during a given time period. If you observe that WebSphere Partner Gateway seems to quiesce while documents are still in the queue, check the FFDC logs for the BCGMAS server. If you find that the BGMAS server failed with error SQL 0964C, increase the size (LOGFILESIZ) and number (LOGPRIMARY, LOGSECOND) of transaction logs for the BCGMAS database.

IBM service log unreadable

In previous releases of WebSphere Partner Gateway logs were viewable using a text editor or the more command. In the current release, several of the logs are in a binary format and cannot be read with a text editor or by using the more command at the command line. If your service log output appears garbled when using either of these methods, convert the service log from binary format into plain text by issuing the showlog command from the workstation where the tool resides as shown below.

```
showlog -format CBE-XML-1.0.1 filename
```

Where *filename* is the file name of the service log file. Note that if the service log is not in the default directory you must fully qualify the service log file name.

This showlog command produces output in Common Base Event XML format. For more examples of Showlog scripts, go to http://publib.boulder.ibm.com/infocenter/wasinfo/v6r1/index.jsp?topic=/com.ibm.websphere.base.doc/info/aes/ae/ttrb_viewsvclog.html.

WebSphere Application Server informational messages

Some WebSphere Application Server messages recorded as errors in WebSphere Partner Gateway system output logs are actually informational in nature and not indicative of a WebSphere Partner Gateway problem. For more information about interpreting WebSphere Application Server log and trace messages, see “Interpreting WebSphere Application Server log and trace messages” on page 148.

Increasing the Receiver timeout setting

About this task

If a partner 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 because of the slow transmission rate from the partner.

From the WebSphere Application Server admin console:

1. Navigate to Applications.
2. Select the WebSphere Partner Gateway Receiver component.
3. Select **Web Container > Web Container Transport Chain**.
4. Modify the timeout settings for the WebSphere Partner Gateway Receiver ports.

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 time-outs 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.

Another method of updating the DB2 access plan is to use the reorgchk command. From a DB2 command window, run the following commands:

1. db2 connect to <database name>
2. db2 -v reorgchk update statistics on table all
3. db2 connect reset

Note: Ensure that you stop all Websphere Partner Gateway components before starting this procedure. You should also stop and restart the database instance after you finish the reorgchk.

Resolving event 210031

About this task

You can receive event 210031 while a document is performing non-repudation when one of the following occurs:

- Database or network (connection) went down.
- Network connection to common file system went down.
- Common file system disk space is full.

To resolve this event, perform the following checks before initiating a re-send on the failed document with event code 210031.

1. Check that the WebSphere Partner Gateway database and network to the DB workstation is up and established.
2. Check that there is network connectivity between the common file system and the WebSphere Partner Gateway components.
3. Check that the common file system disk has enough free space to write the documents.

Documents routed twice when network is lost or document manager server shutdown abruptly

If the system running your Document Manager abruptly loses its network connection or shuts down while processing a document that has not yet had its status updated, the document may be sent twice. The system administrator should take steps to avoid unexpected shutdowns or abnormal outages of the document manager workstation.

0A1 generated with data validation errors

About this task

The 0A1 specification 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 the 0A1. GlobalSupplyChainCode must be either in the 3A7 document or added as attribute to 0A1 in Document Definition.

To add the attribute:

1. Click **Hub Admin > Hub Configuration > Document Definition**. The Console displays the Manage Document Definitions window.
2. Click **Package: RNIF > Protocol: Rosettanet > DocumentType: 0A1**, and click 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 list.
5. Click **Save**.

EDI reports export the first 1000 records only

The export function of the 2 EDI Reports FA Overdue and Rejected Transactions exports the first 1000 records only in order to minimize unexpected system shutdowns because of memory overflow issues. If the number of records to export from the reports is over 1000, export the records directly from the related database view: LG_EDI_Overdue_FA_VW or LG_EDI_Rejected_Tx_VW.

Console does not start after a server restart

If you have installed WebSphere Partner Gateway, started the console server and logged into the console successfully, but find that once you have restarted the server your console does not display and runs in a loop, ensure that your tracing level is not set to "WAS.*=finest". This setting is used to perform the finest logging of all WebSphere Application Server related classes. The default connection time out for the WebSphere Partner Gateway console to start is set at 180 seconds and if the WebSphere Application Server tracing level is set to "finest" the processing time it takes to log all of that information along with making the requisite database connections causes the system to time out. Alter the setting and restart the console server.

Note: Setting the tracing level to "finest" can affect system performance.

FTPScripting Receiver receives StringIndexOutOfBoundsException

If you receive a `StringIndexOutOfBoundsException` while connecting to a Pro FTP server, request the partner to remove all blank lines from the Welcome Message for the FTP server. This FTP server send this message whenever a client connects to the FTP server.

Error scenario

The following example shows blank lines in the Welcome Message.

```
ftp myftp.mycompany.com
Connected to myftp.mycompany.com
220-
<blank line>
You have connected to myftp.mycompany.com FTP Server.
<blank line>
Please enter userid and password to login
<blank line>
220 MYCOMPANY FTP Server ready.
User (myftp.mycompany.com:(none)):
```

Working scenario

The following example shows the Welcome Message with the blank lines removed.

```
ftp myftp.mycompany.com
Connected to ftp myftp.mycompany.com
220-You have connected to myftp.mycompany.com FTP Server.
Please enter userid and password to login
220 MYCOMPANY FTP Server ready.
User (myftp.mycompany.com:(none)):
```

Receiver Failure to read Configuration File

If the Receiver failed to read the configuration file, the following error message is displayed:

```
Unable to update the Receiver Config file java.io.IOException: A file
or directory in the path name does not exist.
```

This error occurs when the WebSphere Partner Gateway Receiver is starting and it does not have a connection to the database and it is attempting to read the configuration information from the `BCGReceiverConfiguration.xml` file. The `BCGReceiverConfiguration.xml` file is located in a folder specified by the attribute `bcg.receiver.configpath` on the System Administration Page of the console.

Ensure that the path specified by `bcg.receiver.configpath` is correct.

Configuring Users to receiving Alerts Notification

If the SMTP configuration has not been provided in the System Administration page of the WebSphere Partner Gateway console, the configured alerts are not sent to the Users because document manager fails to locate the necessary SMTP configuration.

To configure the alerts, update the values of the following two attributes:

- On the **System Administration > DocMgr Administration > Alert Engine page**, update the `bcg.alertNotifications.mailHost` attribute
- On the **System Administration > DocMgr Administration > Delivery Manager page**, update the `bcg.delivery.smtpHost` attribute

Optionally, you can change the value of the attributes `bcg.alertNotifications.mailFrom` and `bcg.alertNotifications.mailReplyTo`.

Resolving ClassNotFoundException for User Exit classes

The `ClassNotFoundException` error can occur when a required class is not found for the following user exits:

- Receiver user exits
- Custom Actions user exit
- Sender user exits

If the `ClassNotFoundException` error occurs, verify the following information:

1. If the user exits are related to Receiver user exits, check that the corresponding jar or classes are present in either of the following folders:
 - `<WebSphere Partner Gateway Install Dir>/Receiver/lib/userexits`
 - `<WebSphere Partner Gateway Install Dir>/Receiver/lib/userexists/classes`
2. If the user exits are related to the document manager, check that the corresponding jar or classes are present in the following folders:
 - `<WebSphere Partner Gateway Install Dir>/Router/lib/userexits`
 - `<WebSphere Partner Gateway Install Dir>/Router/lib/userexists/classes`
3. If the jar or class files for the user exits are present in the correct location, verify that the corresponding user exits shared library has the correct entries. To do this:
 - a. Open the WebSphere Application Server Admin Console.
 - b. Go to **Environment > Shared Libraries**.
 - c. Look for `BCG_RCVR_USEREXISTS` and `BCG_ROUTER_USEREXISTS`.
 - d. Edit the shared library information in these attributes and ensure that the corresponding jars or classes are added to the class path.

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

If WebSphere Partner Gateway fails to log an event or a document status to its database, the data is placed into the `DATALOGERRORQ` queue for later reprocessing when the problem is resolved.

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

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

To run the `reprocessDbLoggingErrors.sh` or `reprocessDBLoggingErrors.bat` utility:

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

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

2. Run the utility from the command line:
./reprocessDbLoggingErrors.sh or reprocessDBLoggingErrors.bat

Disabling JIT in a WebSphere Application Server when WebSphere Partner Gateway produces a javacore

About this task

When WebSphere Partner Gateway components (Receiver, Document Manager, or Console) end abruptly and produce a javacore, it is typically because of a problem with the Java JIT compiler. If this behavior occurs, disable JIT from the WebSphere Application Server Admin Console.

To disable JIT from WebSphere Application Server:

1. Logon to WebSphere Application Server Admin console.
2. Under Servers, click Servers and select the WebSphere Partner Gateway Server.
3. On the configuration page, select **Java and Process Management > Process Definition**.
4. In Additional Properties select **Java Virtual Machine**.
5. Select the **Disable JIT** check box.

Defining a custom transport type

When defining a custom transport type, do not create an attribute with name URI. This conflicts with a WebSphere Partner Gateway reserved keyword. You will not be able to create and save any destination of that transport type.

For example: `<tns2:AttributeName>URI</tns2:AttributeName>` should not be used.

Resolving WebSphere Partner Gateway errors BCG210031 and BCG240415

WebSphere Partner Gateway continually attempts to process the same document, issuing the following errors:

```
BCG210031: Unable to Non-Rep document {0}
BCG240415: AS Packager Error: {0}
```

The following is an example of the messages that the router.log file contains:

```
17 Oct 2005 17:55:30,681 ERROR [BPEEngine] [main Thread 1]
- Error in nonRepProcess
17 Oct 2005 17:55:30,681 ERROR [BPEEngine] [main Thread 1]
- java.io.FileNotFoundException:
/opt/wbi/ca/common/data/Inbound/process/917/fa/xxx
(A file or directory in the path name does not exist.)
at java.io.FileInputStream.open(Native Method)
at java.io.FileInputStream.<init>(FileInputStream.java(Inlined Compiled Code))
at java.io.FileInputStream.<init>(FileInputStream.java(Inlined Compiled Code))
at com.ibm.bcg.util.NonRepudiationDbImpl.copyFile(NonRepudiationDbImpl.java
(Compiled Code))
at com.ibm.bcg.util.NonRepudiationDbImpl.store(NonRepudiationDbImpl.java(Compiled Code))
at com.ibm.bcg.server.BPEBean.doNonRepudiation(BPEBean.java(Compiled Code))
at com.ibm.bcg.server.BPEBean.processDocument(BPEBean.java(Compiled Code))
```



```
ASPackaging Exception:java.io.FileNotFoundException:
/opt/wbi/ca/common/data/Inbound/process/917/fa/xxx
(A file or directory in the path name does not exist.)
at java.io.FileInputStream.open(Native Method)
at java.io.FileInputStream.<init>(FileInputStream.java(Inlined Compiled Code))
at java.io.FileInputStream.<init>(FileInputStream.java(Inlined Compiled Code))
at com.ibm.bcg.util.Util.readFile(Util.java(Compiled Code))
at com.ibm.bcg.ediint.ASPackaging.process(ASPackaging.java(Compiled Code))
at com.ibm.bcg.ediint.ASPackaging.process(ASPackaging.java(Inlined Compiled Code))
at com.ibm.bcg.ediint.ASPackagingHandler.process(ASPackagingHandler.java(Compiled Code))
at com.ibm.bcg.server.HandlerProcessWrapper.process(HandlerProcessWrapper.java (Compiled Code))
at com.ibm.bcg.server.DocumentProcessor.process(DocumentProcessor.java(Compiled Code))
at com.ibm.bcg.server.BPEBean.processDocument(BPEBean.java(Compiled Code))
```

These errors are produced when the affected document (identified in the log files by a unique identifier or UUID) is cycling in the system through the main_inboundq queue and the data\inbound\serialize folder.

To resolve this error:

1. Stop the document manager.
2. Clear the queues.
3. Remove the affected UUID entry in both main_inboundq and data\inbound\serialize folder.
4. If the operation does not succeed the first time, possibly because of some timing condition, clear the system again.
5. The router.log should now be clear of the error and the router CPU usage should go back to normal.

Creating File directory destination on a drive other than C:

If a WebSphere Partner Gateway File Directory Destination address is defined for a drive other than C: , WebSphere Partner Gateway returns the error Destination Directory does not exist. The console will accept the creation of the File Directory Destination, but generates an error similar to the following occurs at runtime:

```
17 Oct 2005 19:00:12,844 INFO [FileSender] [Gw_1_2] -
Exception in delivering the message in first attempt.
Exception is: java.lang.Exception: Destination directory '/wsi_gateway/inbound/tradingpartner01';
does not exist at com.ibm.bcg.delivery.FileSender.getFileSystemProperties(FileSender.java:244)
```

```
17 Oct 2005 19:00:12,844 ERROR [SenderFramework] [Gw_1_2] - First attempt failed: reason: java.lang.
Exception : Destination directory '/wsi_gateway/inbound/tradingpartner01' does not exist
```

To define a folder on a drive other than C:, use three forward slashes instead of two. For example:

```
file:///d:\HubMgrGateway
```

Preventing partner transactions from being processed by WebSphere Partner Gateway

To prevent document processing to and from a Partner, the WebSphere Partner Gateway administrator must deactivate the connections created for that specific partner in the WebSphere Partner Gateway Console Connections window.

Although disabling the Partner profile prevents the entity from be listed in the Partner Connections menu, this does not close the active channels between that partner and the internal partner.

Fixing the browser ERROR: 500

About this task

The browser can show ERROR: 500 and SRVE0026E: [Servlet Error]-[action]: java.lang.NullPointerException error in the SystemOutlog file. These errors can occur after you:

1. Install WebSphere Partner Gateway.
2. Start the console.
3. Log in as hubadmin, and change the default password.

If these errors occur because, either cookies are turned off in the browser or the firewall settings for cookies is too strict. To resolve the error:

1. Change the firewall security level to medium/medium high.
2. Enable cookies on the browser.

The browser ERROR: 500 can also occur as the result of one of the servers being down.

1. Verify all the WebSphere Partner Gateway servers are up.
2. If they are all up, review the logs to determine what caused the error.
If WebSphere Partner Gateway is installed in C:\IBM\WPG:
 - Console logs are in C:\IBM\WPG\bcghub\was\profiles\bcgconsole\logs\bcgconsole.
 - Receiver logs are in C:\IBM\WPG\bcghub\was\profiles\bcgreceiver\logs\bcgreceiver.
 - Document manager logs are in C:\IBM\WPG\bcghub\was\profiles\bcgdocmgr\logs\docmgr.
3. In the each folder, check the SystemErr log. This file should have the time stamp of the latest access attempt.
4. Scroll down to the bottom of the file to see the latest log entries and review the error messages.

Downloading CRL for SSL transactions

About this task

SSL transactions can fail when using certificates if the CRL is not available. If the problem exists, the SSL transaction using certificates fails with error event:

BCG240024: "CertPath validation Failed".

The router log for event 240024 points to the fact that the revocation status of the certificate "could not be determined".

To address this error, do the following steps:

1. Download the CRL list from the Certificate Authority site, specified in the certificate CRL Distribution Point field on the Details tab or made available by a Certificate Authority download site.

For example: <http://SVRSecure-crl.verisign.com/SVRTrialRoot2005.crl>

2. Copy the CRL into the WebSphere Partner Gateway common/security/crl folder.

Note: Alternatively, with CRL DP you can retrieve CRLs from CRL DP at runtime.

Databinding in JMS Exports/Imports within WebSphere Process Server

When using WebSphere Partner Gateway Databinding in JMS Exports/Imports within WebSphere Process Server, there are certain messages which are providing the wrong/irrelevant information. When using WebSphere Partner Gateway Databinding in JMS Exports/Imports within WebSphere Process Server the following messages are printed out:

```
[11/1/05 14:14:07:426 PST] 00000080 SystemOut 0 <<com.ibm.bcg.dataBinding.Utility>>
warning : Error in the element JMS-IBM-MsgTypeMsg :
Class 'BCGPackagingHeaders' does not have a feature named 'JMS-IBM-MsgType'
```

```
[11/1/05 14:14:07:426 PST] 00000080 SystemOut 0 <<com.ibm.bcg.dataBinding.Utility>>
warning : Error in the element JMS-IBM-PutTimeMsg :
Class 'BCGPackagingHeaders' does not have a feature named 'JMS-IBM-PutTime'
```

```
[11/1/05 14:14:07:426 PST] 00000080 SystemOut 0 <<com.ibm.bcg.dataBinding.Utility>>
warning : Error in the element JMS-IBM-Character-SetMsg :
Class 'BCGPackagingHeaders' does not have a feature named 'JMS-IBM-Character-Set'
```

```
[11/1/05 14:14:07:426 PST] 00000080 SystemOut 0 <<com.ibm.bcg.dataBinding.Utility>>
warning : Error in the element JMSXDeliveryCountMsg :
Class 'BCGPackagingHeaders' does not have a feature named 'JMSXDeliveryCount'
```

```
[11/1/05 14:14:07:426 PST] 00000080 SystemOut 0 <<com.ibm.bcg.dataBinding.Utility>>
warning : Error in the element JMS-IBM-EncodingMsg :
Class 'BCGPackagingHeaders' does not have a feature named 'JMS-IBM-Encoding'
```

```
[11/1/05 14:14:07:426 PST] 00000080 SystemOut 0 <<com.ibm.bcg.dataBinding.Utility>>
warning : Error in the element JMS-IBM-PutAppITypeMsg :
Class 'BCGPackagingHeaders' does not have a feature named 'JMS-IBM-PutAppIType'
```

```
[11/1/05 14:14:07:426 PST] 00000080 SystemOut 0 <<com.ibm.bcg.dataBinding.Utility>>
warning : Error in the element JMSXGroupSeqMsg :
Class 'BCGPackagingHeaders' does not have a feature named 'JMSXGroupSeq'
```

```
[11/1/05 14:14:07:426 PST] 00000080 SystemOut 0 <<com.ibm.bcg.dataBinding.Utility>>
warning : Error in the element JMS-IBM-System-MessageIDMsg :
Class 'BCGPackagingHeaders' does not have a feature named 'JMS-IBM-System-MessageID'
```

```
[11/1/05 14:14:07:426 PST] 00000080 SystemOut 0 <<com.ibm.bcg.dataBinding.Utility>>
warning : Error in the element JMSXGroupIDMsg :
Class 'BCGPackagingHeaders' does not have a feature named 'JMSXGroupID'
```

```
[11/1/05 14:14:07:426 PST] 00000080 SystemOut 0 <<com.ibm.bcg.dataBinding.Utility>>
warning : Error in the element x-out-filenameMsg :
Class 'BCGPackagingHeaders' does not have a feature named 'x-out-filename'
```

```
[11/1/05 14:14:07:436 PST] 00000080 SystemOut 0 <<com.ibm.bcg.dataBinding.Utility>>
warning : Error in the element JMS-IBM-PutDateMsg :
Class 'BCGPackagingHeaders' does not have a feature named 'JMS-IBM-PutDate'
```

```
[11/1/05 14:14:07:436 PST] 00000080 SystemOut 0 <<com.ibm.bcg.dataBinding.Utility>>
warning : Error in the element JMSXUserIDMsg :
Class 'BCGPackagingHeaders' does not have a feature named 'JMSXUserID'
```

```
[11/1/05 14:14:07:436 PST] 00000080 SystemOut 0 <<com.ibm.bcg.dataBinding.Utility>>
warning : Error in the element JMS-IBM-FormatMsg :
Class 'BCGPackagingHeaders' does not have a feature named 'JMS-IBM-Format'
```

```
[11/1/05 14:14:07:436 PST] 00000080 SystemOut 0 <<com.ibm.bcg.dataBinding.Utility>>
warning : Error in the element JMSXAppIDMsg :
Class 'BCGPackagingHeaders' does not have a feature named 'JMSXAppID'
```

The preceding messages are not errors and can be safely ignored.

Fixing test partner connection for SSL connections

If the Tools/Test partner Connection fails when a Gateway https URL is selected, the following error message displays:

```
Exception during http POST-: null
```

This error can occur when using either the POST or GET commands.

The Console Tools/Test partner Connection only works with HTTP.

Fixing errors BCGEDIEV0056 and BCG210001

About this task

An EDI transformation map can fail with the Check Channel error and errors BCGEDIEV0056 and BCG210001 on Oracle systems and produce the warning event:

```
Warning BCGEDIEV0056 Event "Translation Table Lookup Warning":  
A translation table lookup returned no entry while deenveloping a message.  
Next: "Check Channel Error - Channel lookup failed. Not enough channel info
```

This error occurs when the Oracle database is not created with the Unicode character set but is incorrectly set to Windows 1252 or similar non-Unicode code page.

To verify the character set on Oracle:

1. Connect to the oracle database.
2. Select NLS_CHARACTERSET from v\$nls_parameters.
3. The value returned should be AL32UTF8.

Verify this on your Oracle systems.

There is not a direct way of modifying the character set of the database once it has been created. The solution is to re-create the database with the database character set and the national character set as Unicode.

Fixing ORA-00988 error

This error occurs because of an Oracle limitation. If a password beginning with a number is not entered within quotation marks, then you see:

```
ORA-00988: missing or invalid password(s)
```

To resolve this error enter any password that begins with a number for an Oracle database in quotation marks (for example, "123456ABC") in the WebSphere Partner Gateway installation panels.

Configuring Content-Types attribute for the fixed workflow handlers

About this task

WebSphere Partner Gateway might fail to route an EDI document received through HTTP. An EDI document is sent with the content-type as text/plain and you should ensure that the Fixed Workflow handlers are configured correctly.

The Content-Types attribute can be set by the following steps:

1. Go to **Hub Admin > Hub Configuration > Fixed Workflow > InBound**.
2. Click **com.ibm.bcg.server.ChannelParseFactory**.
3. Click **Edit**.
4. In the configured list, select EDIRouterBizProcessHandler and click **Configure**.
5. Edit Content-Types attribute by adding text/plain content type.

This applies the EDI handler and the document gets processed as EDI. These content types value should be separated by a comma.

The Content-Types attribute is used for a particular set of handlers. These handlers are

- BinaryChannelParseHandler
- XMLRouterBizHandler
- EDIRouterBizProcessHandler
- cXMLChannelParseHandler

These handlers are populated with a default list of content types. To modify the content types, perform the following steps:

1. Go to **Hub Admin > Hub Configuration > Fixed Workflow > InBound**.
2. Click **com.ibm.bcg.server.ChannelParseFactory**.
3. Click **Edit**.
4. In the configured list, select the handler and click **Configure**.
5. Edit the Content-Types attribute by adding the new content type. Ensure that the content-type values are separated by a comma.

Note: It is recommended not to change these content-type values unless advised.

Fixing BCG210013 error

About this task

Unable to receive inbound document because of the following error:

BCG210013 - Connection Not Fully Configured

If all other configurations appear to be correct, the most common cause of this is an incorrect receiver specification.

1. Check that there are no spaces in front of the receiver URL definitions.
2. Try to narrow down the problem trying to send a test EDI message using other business IDs available for the partners. Try to see if this is a business ID specific problem.
3. If the previous step fails, then take a debug trace of the error scenario as follows:
 - a. Shut down WebSphere Partner Gateway.
 - b. Change the debug setting for the receiver and router to FINEST for WebSphere Partner Gateways using the following command:

```
"*=info:com.ibm.bcg.*=finest"
```
 - c. Delete (or backup to a different folder), the current logs in these directories:
 - In simple mode installation, the logs are located in the following directory:

*<WebSphere Partner Gateway Install Dir>/wasND/Profiles/
bcgprofile/logs/server1*

- In distributed mode installation, the logs are located in the following directories.
 - *<Hub Installation Directory>\wasND\Profiles\bcgprofile\logs\bcgreceiver*
 - *<Hub Installation Directory>\wasND\Profiles\bcgprofile\logs\bcgdocmgr*
- d. Restart WebSphere Partner Gateway.
- e. Run the error scenario only once.
- f. Compress and send all logs in folders mentioned in the above two steps, along with a screen capture of the error message taken from the console viewer, to IBM customer support.

Increasing buffer size to prevent document transmission low performance

About this task

WebSphere Partner Gateway document transmission time can increase exponentially, up to 40 minutes. This is caused by the default buffer size in DB2 being defined too small, resulting in documents being processing getting added to the queue.

To increase the buffer size:

1. Open the DB2 Command Line Processor: **Start > Programs > IBM DB2 > Command Line Tools > Command Line Processor.**
2. Connect to the database using the command:
`DB2 > connect to bcgapps user <username> using <password>`
3. Increase the buffer size using the command:
`DB2 alter bufferpool buff32k immediate size 12500`

This will increase the specific buffer size from 500 (default) to 12500

WebSphere Partner Gateway hub installer logs error messages

When running the WebSphere Partner Gateway LaunchPad, errors similar to the following might be displayed:

```
Jun 14, 2005 8:13:04 PM java.util.prefs.FileSystemPreferences$3 run
WARNING: Could not create system preferences directory.
        System preferences are unusable.
Jun 14, 2005 8:13:31 PM java.util.prefs.FileSystemPreferences
        checkLockFile0ErrorCode
WARNING: Could not lock System prefs. Unix error code 270913688.
Jun 14, 2005 8:14:01 PM java.util.prefs.FileSystemPreferences
        checkLockFile0ErrorCode
WARNING: Could not lock System prefs. Unix error code 270931432.
Jun 14, 2005 8:14:32 PM java.util.prefs.FileSystemPreferences
        checkLockFile0ErrorCode
WARNING: Could not lock System prefs. Unix error code 270937824.
```

These messages can be safely ignored.

DB password required error in bcgHubInstall.log

During the installation of WebSphere Partner Gateway hub, the installer logs the following error messages in bcgHubInstall.log:

```
com.ibm.bcg.install.ismp.wizard.conditions.JdbcDatabaseConnectCondition, err,  
ERROR: dbPassword is required
```

This error message does not cause any side effects. Servers can be started successfully and the documents can be routed successfully. This error message can be safely ignored.

Using revocation check and using CRL DP support

If certpath validation fails because the "revocation status could not be determined", this might indicate that the CRL is unavailable. CRLs can be made available in a local folder or can be retrieved automatically from the CRL Distribution Point (CRL DP). Enable CRL DP support if CRLs are to be retrieved from the CRL DP.

If the access to the CRL DP uses a proxy server, then the proxy server host and port must also be provided. For self-signed certificates, revocation check is not being done.

See "Configuring the certpath related properties" on page 53 for more information.

Returning document volume report search information about the console

About this task

A WebSphere Partner Gateway document volume report search does not return information about the console.

When you click the **Search** in the **Console Tools > DocumentVolumeReportSearch**, nothing happens. The page does not show the typical red info message saying "No results were found based on your search criteria". The page just flashes and returns nothing.

The problem is with the browser popup blocker which prevents the resulting page (which is a popup page) from being displayed.

Turn off the popup blocker, and the page will be correctly shown.

For Mozilla Firefox:

1. Navigate to **Tools > Options > Web Features**.
2. Clear the **Block Popup Windows** field.

Internet Explorer:

1. Click **Tools**
2. Navigate to **Pop-up Manager**, and then click **Block Pop-up windows**.
3. Click **Tools** then **Internet Options**.
4. Navigate to the **Privacy** tab, and then click **Block Pop-up windows**.

Loading the native library

When WebSphere Partner Gateway components are started, the logs might show the following message:

```
java.lang.UnsatisfiedLinkError: Can't find library AIXNative
(libAIXNative.a or .so) in sun.boot.library.path or java.library.path
```

Depending on which operating system WebSphere Partner Gateway is running, the system uses one of the following libraries:

- libWin32Native.dll
- libpLinuxNative.so
- libAixNative.a
- libSolarisNative.so
- libHPNative.so

This error is returned if the library path is not set correctly, to resolve this error:

1. Log on to the WebSphere Application Server Admin console.
2. Select **Environment > Shared Libraries**.
3. Edit the following properties:
 - BCG_NAV_CONSOLE
 - BCG_NAV_RCVR
 - BCG_NAV_ROUTER_BPE
 - BCG_NAV_ROUTER_DOCMGR
4. Note the path shown under "native library path".
5. Check the specified library path to verify that the appropriate .dll or .so or .a file is present.
6. If the library is not present, copy it from another location.
7. Verify that the shared libraries are associated with each WebSphere Partner Gateway application. To verify:
 - a. On the WebSphere Application Server Admin console Applications page, click any of the WebSphere Partner Gateway applications containing bcgDocMgr.
 - b. Click **Shared Library references**.
 - c. Verify that the BCG_NAV_ROUTER_DOCMGR library is associated with the application. If is not associated with the library, assign the application.
 - d. Repeat this check for other applications:
 - For console shared library, the associated library is BCG_NAV_CONSOLE.
 - For WebSphere Partner Gateway receiver, the associated shared library is BCG_NAV_RCVR
 - For WebSphere Partner Gateway BPE application, the associated shared library is BCG_NAV_ROUTER_BPE.

Fixing error TCPC0003E and CHF0029E

The WebSphere Partner Gateway Receiver component can fail to start with TCPC0003E and CHF0029E errors in the SystemOut.log file. The errors can occur because of the following conditions:

1. The configured ports can be used by other applications, check for any port conflicts.

- Ports numbers lower than 1024 are privileged ports which are reserved for root. Unless your system has been configured to specially handle this restriction, non-root users will not be able to bind to those ports. WebSphere Partner Gateway uses the non-root user, WebSphere Partner Gateway user, to start components, but it cannot bind to privileged ports. The bcguser is an example of WebSphere Partner Gateway user.

Note: For WebSphere Partner Gateway, non-root users start the Receiver, but cannot bind to privileged ports.

Change the Receiver ports to available ports (that is, ports not used by other applications) and larger than 1024. The following example shows how to change port 80 to *nmn*.

- Stop the Receiver.
- Find and replace port number 80 to *nmn* in the following files:

Note: Backup all files before editing.

- Under *<Installed_path>*bcghub/was/profiles/bcgreceiver, edit the following files:
 - config\cells\DefaultNode\virtualhosts.xml
 - config\cells\DefaultNode\nodes\DefaultNode\serverindex.xml
 - config\templates\servertypes\APPLICATION_SERVER\serverindex.xml
 - installedFilters\wlm\bcgreceiver\target.xml
 - logs\portdef.props
- Edit *<Installed_path>*\bcghub\receiver\lib\config\bcg_receiver.properties.

Note: The port number can also be changed using the WebSphere Application Server Admin Console by going to Server > Ports page and changing the port for **WC_defaulthost**.

- Start the Receiver.
- Type the Receiver URL in your browser to ensure Receiver works, `http://<host_name>:xyz/bcgreceiver`, The correct result is that browser should report "Unsupported Operation". If instead, the browser reported "The page cannot be displayed", the Receiver did not successfully bind to the port.

CA certificate expiration

Only the certificates that are used for encryption, signature, and SSL client are disabled when they expire. The CA certificate is not disabled when it expires, but it is not used at runtime.

If the root or intermediate certificates expire between server restarts, those certificates are not included in the list of trusted certificates. Therefore, if the certpath build fails because the CA certificate is not found, a possible cause can be that the CA certificate has expired.

If a root or intermediate certificate expires in runtime, the certpath build fails and the corresponding encryption, digital signature or SSL certificates is not used in the business transaction.

The validity status of the certificate can be found in the WebSphere Partner Gateway Console. The WebSphere Partner Gateway Console displays the validity period of certificates on the Certificate List page. The validity period is shown in red if the certificate is expired.

If the CA certificate is expired, obtain a new certificate from the CA that issued the certificate. This new CA certificate should be uploaded in WebSphere Partner Gateway Console.

Note: If the uploaded certificate is a self signed certificate for Server authentication and has expired, then the certificate is disabled in the WebSphere Partner Gateway Console.

VCBASEException in the SystemOut.log

When there is an exception while configuring the hub using the console, the Console log shows the exception also as part of logging information. For example, if you try to create an interaction that already exists, you will receive the VCBASEException in the SystemOut.log file. This exception is acceptable as part of Logging.

Reporting file size for documents greater than 2 GB

When a document is greater than 2 GB in size, WebSphere Partner Gateway might show the file length as 0 KB in the document viewer. This is because of a maximum limit for the database datatype.

SSL handshake fails because no certificate received

This problem occurs during the SSLHandshake between a partner and WebSphere Partner Gateway when you are sending to a partner using SSL with Client Authentication. If the partner does not send the list of certifying authority certificates, the SSL client in WebSphere Partner Gateway does not send the client certificate. This causes the handshake failure.

To resolve the handshake failure, you modify the `java.security` file in WebSphere Application Server installations. This file is located in the `<WAS installation directory>\java\jre\lib\security` directory.

Note: For UNIX systems, use the forward slash (/) instead of the back slash (\).

The default order of providers in the `java.security` file is as follows:

```
security.provider.1=com.ibm.crypto.provider.IBMJCE
security.provider.2=com.ibm.jsse.IBMJSSEProvider
security.provider.3=com.ibm.jsse2.IBMJSSEProvider2
security.provider.4=com.ibm.security.jgss.IBMJGSSProvider
security.provider.5=com.ibm.security.cert.IBMCertPath
#security.provider.6=com.ibm.crypto.pkcs11.provider.IBMPKCS11
```

In the `java.security` file, place the IBMJSSE2 provider before the IBMJSSE provider as shown in the following example.

Note: If you implement a WebSphere Application Server fix pack after reordering the `java.security` file, your change is overwritten and the file must be reordered again.

```
security.provider.1=com.ibm.crypto.provider.IBMJCE
security.provider.2=com.ibm.jsse2.IBMJSSEProvider2
security.provider.3=com.ibm.jsse.IBMJSSEProvider
security.provider.4=com.ibm.security.jgss.IBMJGSSProvider
security.provider.5=com.ibm.security.cert.IBMCertPath
#security.provider.6=com.ibm.crypto.pkcs11.provider.IBMPKCS11
```

Restart the WebSphere Partner Gateway servers (bcgconsole, bcgreceiver and bcgdocmgr) after the java.security file is changed.

Fixing the hanging threads warning

The following is an example of a message you can receive in the SystemOut.log (/opt/IBM/bcghub/wasND/Profiles/bcgdocmgr/logs/bcgdocmgr/SystemOut.log) indicating that threads are hanging:

```
[7/19/06 14:35:16:839 EDT] 0000000f ThreadMonitor W WSVR0605W:
Thread "WorkManager.BCGBPEWorkManager : 5" (00000055) has been active for
709464 milliseconds and may be hung. There is/are 15 thread(s) in total in
the server that may be hung.
```

Note: Websphere Application Server can show the warning message stating that some of the threads might be hanging. But WebSphere Partner Gateway still processes the threads.

To resolve the message, change the following property under DocumentManager, Receiver servers:

```
com.ibm.websphere.threadmonitor.interval = 0
```

This value is located in **Custom Properties** under **Server Infrastructure > Administration**.

Stopping the Document Manager exception

Ignore the following exception if you receive it while stopping the document manager (server) when a document is processing.

```
[2/1/07 14:04:40:546 EST] 00000088 ExceptionUtil E CNTR0020E:
EJB threw an unexpected (non-declared exception during invocation of method "onMessage"
on bean "BeanId(BCGBPE#ejb/bcgBpeEJB.jar#BPMainEngineMDB, null)".
Exception data: javax.ejb.TransactionRolledbackLocalException: ;
nested exception is: com.ibm.websphere.csi.CSITransactionRolledbackException:
com.ibm.websphere.csi.CSITransactionRolledbackException:
  at com.ibm.ejs.csi.TranStrategy.commit(TranStrategy.java:742)
  at com.ibm.ejs.csi.TranStrategy.postInvoke(TranStrategy.java:181)
  at com.ibm.ejs.csi.NotSupported.postInvoke(NotSupported.java:99)
  at com.ibm.ejs.csi.TransactionControlImpl.postInvoke(TransactionControlImpl.java:581)
  at com.ibm.ejs.container.EJSContainer.postInvoke(EJSContainer.java:3876)
  at com.ibm.bcg.server.common.EJSLocalStatelessTransController_5c554616.onReceive
    (Unknown Source)
  at com.ibm.bcg.server.common.BaseMDB.onMessage(BaseMDB.java:194)
  at com.ibm.ejs.container.MessageEndpointHandler.invokeMdbMethod
    (MessageEndpointHandler.java:992)
  at com.ibm.ejs.container.MessageEndpointHandler.invoke
    (MessageEndpointHandler.java:725)
  at $Proxy0.onMessage(Unknown Source)
  at com.ibm.ws.sib.api.jmsra.impl.JmsJcaEndpointInvokerImpl.invokeEndpoint
    (JmsJcaEndpointInvokerImpl.java:201)
  at com.ibm.ws.sib.ra.inbound.impl.SibRaDispatcher.dispatch
    (SibRaDispatcher.java:708)
  at com.ibm.ws.sib.ra.inbound.impl.SibRaSingleProcessListener$SibRaWork.run
    (SibRaSingleProcessListener.java:584)
  at com.ibm.ejs.j2c.work.WorkProxy.run(WorkProxy.java:497)
  at com.ibm.ws.util.ThreadPool$Worker.run(ThreadPool.java:1469)
javax.ejb.TransactionRolledbackLocalException;
```

```

nested exception is: com.ibm.websphere.csi.CSITransactionRolledbackException:
  at com.ibm.ejs.csi.TranStrategy.commit(TranStrategy.java:742)
  at com.ibm.ejs.csi.TranStrategy.postInvoke(TranStrategy.java:181)
  at com.ibm.ejs.csi.NotSupported.postInvoke(NotSupported.java:99)
  at com.ibm.ejs.csi.TransactionControlImpl.postInvoke(TransactionControlImpl.java:581)
  at com.ibm.ejs.container.EJSContainer.postInvoke(EJSContainer.java:3876)
  at com.ibm.bcg.server.common.EJSLocalStatelessTransController_5c554616.onReceive
    (Unknown Source)
  at com.ibm.bcg.server.common.BaseMDB.onMessage(BaseMDB.java:194)
  at com.ibm.ejs.container.MessageEndpointHandler.invokeMdbMethod
    (MessageEndpointHandler.java:992)
  at com.ibm.ejs.container.MessageEndpointHandler.invoke
    (MessageEndpointHandler.java:725)
  at $Proxy0.onMessage(Unknown Source)
  at com.ibm.ws.sib.api.jmsra.impl.JmsJcaEndpointInvokerImpl.invokeEndpoint
    (JmsJcaEndpointInvokerImpl.java:201)
  at com.ibm.ws.sib.ra.inbound.impl.SibRaDispatcher.dispatch
    (SibRaDispatcher.java:708)
  at com.ibm.ws.sib.ra.inbound.impl.SibRaSingleProcessListener$SibRaWork.run
    (SibRaSingleProcessListener.java:584)
  at com.ibm.ejs.j2c.work.WorkProxy.run(WorkProxy.java:497)

```

Although you receive this exception, all of the follow objectives are met:

- Graceful recovery
- No document loss
- No duplicate document processing
- No performance degradation (after restart)
- No hung documents

Fixing WebSphere MQ messages

See the following sections to fix specific MQ messages:

- “MQJMS2007 error”
- “MQJMS2013 error” on page 183

MQJMS2007 error

About this task

If you are using JMS as a Gateway with Websphere MQ as the messaging service, you can receive the following message when putting a particular message in a queue.

```
MQJMS2007: failed to send message to MQ queue
```

The result is that the Connector fails to write a message to output queue. The cause of this error might be that the Maximum message length attribute for a queue, queue manager or channel is not set to a value that is equal to or higher than the largest message size.

To change the message length attribute for the queue, queue manager and channel:

1. Go to the Websphere MQ explorer Queue manager properties.
2. Click on the extended tab and set the maximum message length attribute to a value greater than the size of the message.
3. Go to the Channel properties.
4. Click on the extended tab and set the maximum message length attribute to a value greater than the size of the message.
5. Go to the Queue properties for the queue that was specified while creating the gateway.

6. Click on the extended tab and set the maximum message length attribute to a value greater than the size of the message.

MQJMS2013 error

About this task

During WebSphere Partner Gateway communication with WebSphere MQ, you can receive the following error:

```
MQJMS2013 invalid security authentication
```

To resolve the error, perform the following steps:

1. Check which user ID the application is being run under.
2. Check to verify that user ID being used is in the mqm group (or some other group with sufficient authority).
3. If the user ID is not in the mqm group, then add it to the mqm group and issue the runmqsc REFRESH SECURITY(*) command.

java.security.InvalidKeyException: Illegal key size or default parameter

If you try to upload the PKCS#12 file with a stronger cryptography than the one supported by default, or if you use a key with an illegal key size that is not supported by default, this exception is thrown. To resolve this error, you must obtain the unrestricted strength cryptography policy files and install them, if it is legal to do so. See the section on changing the cryptographic strength in *WebSphere Partner Gateway Hub Configuration Guide*.

The MDN status of 'unknown' for AS transactions

Upon completion of an upgrade to WebSphere Partner Gateway v6.2, the AS Viewer in the Community Console will show an unknown state for the MDN Status on AS transactions that occurred prior to the upgrade. This is a limitation of the migration procedures and utilities.

Servers fail to start after applying fixes

The servers (Dmgr, NodeAgent, and AppServers) might fail to start if you have recently applied a fix or fix pack with the Update Installer. The SystemOut.log will not contain any information about the failure. However, the startServer.log shows:

```
ADMU3011E: Server launched but failed initialization. startServer.log,
SystemOut.log(or job log in zOS) and other log files under
/home/dwhare/WebSphere61/profiles/Dmgr01/logs/dmgr should contain
failure information.
```

The problem is caused by applying a fix or fix pack as root when the WebSphere Application Server environment is set up to run as a non-root user.

Note: For existing installations, the root or non-root installer who owns the currently installed files is the only user who can perform subsequent installation or removal operations on that installation.

The reason the servers fail to start is that the OSGI cache was not updated after applying the fix pack because of an issue with the permission. To verify this, check the <WAS_PROFILE_HOME>/configuration/ directory for a log file with a string of numbers as the file name. This file will contain an error like:

```

!ENTRY org.eclipse.osgi 2006-08-24 09:04:14.597
!MESSAGE Error reading configuration:
/home/dwhare/WebSphere61/profiles/Dmgr01/configuration/org.eclipse.osgi/.manager/
.fileTableLock
(Permission denied)
!STACK 0
java.io.FileNotFoundException:
/home/dwhare/WebSphere61/profiles/Dmgr01/configuration/org.eclipse.osgi/.manager/
.fileTableLock
(Permission denied)
at java.io.FileOutputStream.openAppend(Native Method)
at java.io.FileOutputStream.<init>(FileOutputStream.java:203)
at org.eclipse.core.runtime.internal.adaptor.Locker_JavaNio.lock
(Locker_JavaNio.java:34)
at org.eclipse.core.runtime.adaptor.FileManager.lock(FileManager.java:361)
at org.eclipse.core.runtime.adaptor.FileManager.open(FileManager.java:658)
at ...

```

To resolve this problem:

1. Stop all remaining WebSphere Application Server processes that are running.
2. Change the file permissions for the WebSphere install back to the non-root user.
3. Run `<WAS_HOME>/profiles/<profile>/bin/osgiCfgInit.sh`.

Note: For Windows, execute the `osgiCfgInit.bat` command.
Start the server.

The `osgiCfgInit` command updates the contents of subdirectories in `<WAS_HOME>/configuration/`. This directory is used for caching data in the jars in `<WAS_HOME>/plugins/`.

When the data in the jars is updated (for example, when a service pack is installed), the caching data must be updated. The updating of the cache is supposed to occur the first time a command is issued in a profile after a service pack is installed. (for example, the `startServer.sh` command). However, if there is an exception, like one of the above, then the cache is not updated and must be updated manually.

Correcting the shortcut ports for WebSphere Application Server

About this task

If the ports used for the shortcut in a Windows systems are not correct when using the Start Menu entries to launch the WebSphere Application Server ND admin console, you must change the ports. To change the ports:

1. Go to **Start Menu > Programs > IBM WebSphere > Application Server Network Deployment V6.1 > Profiles > bcgprofile > Administrative console**.
2. Right click and select properties to change the values for the ports.

Avoiding duplicate document delivery when there is more than one router

There is a possibility that a duplicate document can be delivered to a gateway when processing high volumes of documents (for example, more than one hundred thousand documents in a 24 hour period) in a UNIX environment.

The duplication occurs when there is more than one router instance involved and the common file system is mounted under any UNIX environment. To avoid

duplicate document delivery during the processing of large volumes of documents, include the following attributes in the Websphere variables of each router instance:

1. `bcg.dm.checkFileLatency=true`
2. `bcg.dm.latencyWaitTime=3000`

Rendering of tab headings on displays with resolution greater than 1024

On displays that have the resolution width set to a value greater than 1024 pixels, the Community Console might misdraw the tab headings on screens such as the Document Details view.

You can ignore this behavior.

Documents not processed when using Oracle 9i Release 2

About this task

If you are using Oracle 9i Release 2, you might find that documents are not processed and the BCGMAS messaging engine logs contain the following error:

```
J2CA0056I: The Connection Manager received a fatal connection error from the Resource Adapter for resource datasources/bcgMASDS The exception received is com.ibm.websphere.ce.cm.StaleConnectionException: No more data to read from socket: java.sql.SQLException: No more data to read from socket
```

To resolve this issue, install the Oracle 10g version of the JDBC driver. This driver alleviates known incompatibilities between Oracle 9i and the WebSphere Application Server Messaging Engine.

For more details, see the IBM Technote for this issue. To find the IBM Technote:

1. Go to <http://www.ibm.com/support/us/>.
2. Type number 1239781 in the search box.
3. Select **Oracle 9i Thin driver running in cognizance with Service Integration Bus and Scheduler Service can result in J2C Connection Pool Exhaustion** from the search results list.

You can download the Oracle 10g JDBC driver from the Oracle website at:http://www.oracle.com/technology/software/tech/java/sqlj_jdbc/index.html

Document processing when the database goes down

If the database goes down while WebSphere Partner Gateway is processing the documents, then the documents will get stuck in the 'inprocess' state and the messages will be moved to `datalogerrorQ`. When the database is up, you must run the batch file **reprocessDbLoggingErrors.bat** (present under `WPG_HOME/bin`) in order to move the messages back from the `datalogerrorQ` and continue processing the documents.

java.lang.NoClassDefFoundError with reprocessDbLoggingErrors.bat

About this task

You might encounter java.lang.NoClassDefFoundError for the following reason. The reprocessDbLoggingErrors.bat file has the path to ws_runtime.jar, which is present in the directory:

```
<WAS_HOME>\deploytool\itp\plugins\com.ibm.websphere.v61_6.1.0.
```

But, after every fixpack release, the folder name com.ibm.websphere.v61_6.1.0 gets changed to the corresponding fixpack version. Hence, the batch file fails to find the ws_runtime.jar. To fix this issue, you have to set the ws_runtime.jar path, as described below:

1. Navigate to the directory:

```
<WAS_HOME>\deploytool\itp\plugins
```
2. Check the path for ws_runtime.jar.
3. Navigate to the directory:

```
<WAS_HOME>\bin
```
4. Edit the **reprocessDbLoggingErrors.bat** file directory.
5. Set the correct path for ws_runtime.jar and rerun the script.

Recovery process when queue and disk is full or unavailable

About this task

When messaging system and common file system are full or not available during processing, the Business Document Object (BDO) will be persisted temporarily under Receiver machine temp folder: WPG_HUB_INSTALL_HOME\Receiver\temp. In this case, the Hub will trigger an event 103205 with the following description:

```
Receiver Processing halted, due to following reason failed to process target:  
With Queue and File system unavailable/Full.  
Please make sure queue and disk system are available  
for processing and start the receiver.
```

If you get a message with the above description, do the following:

1. Make sure queue and common file system disk are available for processing.
2. Restart the receiver server.
3. Move the Business Document Object (BDO) persisted under receiver temp folder to (Hub's) common file system **router_in** folder.

Workflow Handler Runtime Error

While document processing, a failure error may occur and the document viewer displays 'Workflow handler runtime error'. In such a scenario, check if the WebSphere SystemErr.log file contains the following errors:

- java.net.ConnectException error:
Possible solution: If you are using the WebSphere Transformation Extender RMI Server, ensure that the server is running and is able to access the hostname and port mentioned in the exception.
- com.ibm.websphere.dtx.dtxpi.rmi.MRmiApiException: Unknown error - Loading map failed - Native function: CMpiMapSet::CMpiMapSet:
Possible solutions:

- Ensure that the architecture of both WebSphere Application Server ND and WebSphere Transformation Extender matches. For example, on a 32-bit WebSphere Application Server ND architecture, the you must have the 32-bit WebSphere Transformation Extender installed.
- Ensure that the WebSphere Transformation Extender system administration attribute `bcg.wtx.mapLocation` is correctly configured to point to the directory containing the WebSphere Transformation Extender maps.
- If you are using the WebSphere Transformation Extender RMI Server, then ensure that it access to the directory containing the WebSphere Transformation Extender map.

Error while invoking WebSphere Transformation Extender Map

While invoking WebSphere Transformation Extender map, if `java.lang.NoClassDefFoundError` occurs in `WebSphere SystemOut.log`, then ensure that the WebSphere Transformation Extender `dtxpi.jar` file is installed in the `router/lib.userexits` directory.

IBM Support Assistant (ISA) Plugin

WebSphere Partner Gateway is enabled for IBM Support Assistant (ISA). The ISA product plugin for WebSphere Partner Gateway provides features such as log collection for PMR (Problem Management Report), Searching product specific information, and so on. ISA tool allows the customers to find necessary information required for analyzing the problem and managing the service requests. Refer to <http://www-01.ibm.com/software/integration/wspartnergateway> for more information on the ISA product plugin for WebSphere Partner Gateway. To know more about ISA, refer to <http://www.ibm.com/software/support/isa>.

ISA helps customers to collect the logs, trace files and other configuration information required by the IBM support team. This information will help the support team to gain the necessary data required for analyzing and resolving the customer PMRs faster.

Partner Migration Utility with LDAP

About this task

Whenever LDAP is enabled for WebSphere Partner Gateway Partner Migration Utility, the "User does not have enough permissions" error occurs.

Note: The LDAP user performing this operation has to be a member of the `hubadmin` group.

1. Go to **System Administration > Common Properties**.
2. Change `bcg.ldap.containerauth` property to *False*.
3. Login to the console using the same credentials that you used without LDAP.
4. Go to **Account admin > Users** and create an user.
5. Add LDAP user to the `hubadmin` group only.
6. Go to **Administration > Common Properties** and set `bcg.ldap.containerauth` to *True*.
7. Log out and login again

AS signature failure for interop content type

In **System Administration > Common Attributes** page of the Console, the **excludedContentTypesForCanonicalization** property is made editable.

While performing AS2 transactions, this attribute has all the content types that are excluded from canonicalization.

To resolve the issue, add **application/pkcs7-mime** content type to **excludedContentTypesForCanonicalization** property. This is applicable only for AS2 transactions as there is no canonicalization support provided for RNIF transactions.

Restriction: This **excludedContentTypesForCanonicalization** property can be changed by the Hub administrator or by any user who belongs to the hubadmin group.

Remember: Restart the server for the changes to take effect.

Appendix A - performance considerations

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

Managing queue overflow

WebSphere Partner Gateway components use a JMS queue to asynchronously invoke each other. However, if the arrival rate of messages in a queue is greater than the processing rate of those messages, the queue will reach its maximum number of messages. If depth of the queue becomes equal to the maximum depth configured for that queue, the queue overflows. WebSphere Partner Gateway provides a mechanism of persisting the incoming documents or messages to the file system in a queue overflow situation.

Note: The maximum depth of queue might be reached during peak loads or while processing large documents. Monitor the queues during these times to ensure that the queue depth is large enough so that it does not overflow.

See “Appendix C - component-specific system attributes” on page 225 for the list of attributes used to manage queue overflow.

Generating summary data

About this task

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.

You can view and edit how often the summary data is generated with the Summary Service Properties window. 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 > DocMgr Administration > Others > Summary Engine**. The Console displays the Summary Service Properties window.
2. Click the **Edit** icon next to **Processing Interval (in Minutes)**.
3. Type 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. See Table 43 for a list of WebSphere Partner Gateway failed events and their corresponding descriptions. See Table 44 on page 202 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 43. 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 initialize, 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 unrecoverable 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 component is unable to process a document because of document or system errors.
BCG103205	Receiver Error	Receiver '{0},{1}' failed to process receiver: {2}.	Error	
BCG106004	No Default Destination Pair	Connection create failed. A pair of default destinations does not exist between partners: {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 Definition Create Error	Child level = {0} greater than or equal to parent level = {1}	Error	

Table 43. Failed events (continued)

Event code	Event name	Internal description	Severity	Extended description
BCG111001	FTP Account Create Error	FTP account create failed for partner {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	
BCG200000	No Default Destination Pair	Connection create failed. A pair of default destinations does not exist between partners: {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 because of 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 because of a failure during document transformation.
BCG200006	Protocol Transformer Input File Failure	Protocol transformer input file error: {0}	Critical	This event is generated because of 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 because of 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 because of failure when attempting to parse the document.
BCG200013	Internal Partner Provided RN Process-Instance-ID Error	{0}	Error	This event is generated when an unusable Process Instance ID is received and the configuration property indicates that the system will not generate a new Process Instance ID.

Table 43. Failed events (continued)

Event code	Event name	Internal description	Severity	Extended description
BCG200015	Internal Partner Provided RosettaNet GlobalUsageCode Error	{0}	Error	This event is generated when the x-aux-production header value is unusable 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 partner profile {0}	Error	This event is generated when a document is posted from an IP Address that is not approved for that partner.
BCG210009	SSL Certificate Validation Failure	Client SSL certificate name is not in the partner 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 partner.
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	Internal Partner Transport Unpackage Failure	Insufficient Internal Partner 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.

Table 43. Failed events (continued)

Event code	Event name	Internal description	Severity	Extended description
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 destination.
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 package 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	<p>This event is generated when the system is unable to non-repudiate the document.</p> <p>Ensure that the system has sufficient disk space, and that the following directories contain system-only files:</p> <ul style="list-style-type: none"> • <i><common information directory>/non_rep/</i> • <i><common information directory>/msg_store/</i> <p>If these two directories contain user generated files, document processing will fail.</p>
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.

Table 43. Failed events (continued)

Event code	Event name	Internal description	Severity	Extended description
BCG210033	Message Store Failed	Unable to store document plain text	Error	<p>This event is generated when the system is unable to store the document in plain text.</p> <p>Ensure that the system has sufficient disk space, and that the following directories contain system-only files:</p> <ul style="list-style-type: none"> • <i><common information directory>/non_rep/</i> • <i><common information directory>/msg_store/</i> <p>If these two directories contain user generated files, document processing will fail.</p>
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. Typically because of a database problem.
BCG210063	Destination Process Failure	Destination Process failed	Critical	This event is generated when destination processing fails. Typically because of 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

Table 43. Failed events (continued)

Event code	Event name	Internal description	Severity	Extended description
BCG210201	PIP Load During Doctype Processing Failure	Unable to load PIP for a document during Doctype processing	Critical	This event is generated when a spec for the PIP cannot be found. Should not occur unless there is a configuration problem.
BCG210202	Exception in Doctype Processing	Exception during Doctype Processing: {0}	Critical	This event is generated when the system fails when attempting to insert the DocType tag.
BCG210203	DoctypeProcess Error—No Action Found	DoctypeProcess Error—No action found	Critical	This event is generated when a spec for the PIP DocType cannot be found.
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 because the Discard envelope on Error attribute set to Yes.
BCG230004	Validation Internal Error	{0}	Critical	This event is generated because of an internal system failure during validation processing.
BCG230006	Validation Database Error	{0}	Critical	This event is generated because of 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.

Table 43. Failed events (continued)

Event code	Event name	Internal description	Severity	Extended description
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.
BCG240013	Partner 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	

Table 43. Failed events (continued)

Event code	Event name	Internal description	Severity	Extended description
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	
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 cannot be found.
BCG240068	Connection Parser RosettaNet Failure	Connection Parse RosettaNet Failure	Error	This event is generated when connection info might not be found in a RosettaNet document.

Table 43. Failed events (continued)

Event code	Event name	Internal description	Severity	Extended description
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.

Table 43. Failed events (continued)

Event code	Event name	Internal description	Severity	Extended description
BCG240422	AS document not found for this MDN	{0}	Error	This event is generated when a MDN is received and the system is unable to locate the corresponding document.
BCG240423	Input File Failure	Invalid input file passed in the document	Error	This event is generated when the system encounters an unusable 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 occurred 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 partner destination failed: {0}	Error	This event is generated when document delivery to a partner's destination fails and the document is set to a failed state.

Table 43. Failed events (continued)

Event code	Event name	Internal description	Severity	Extended description
BCG250002	Delivery Scheduler Failed	An internal error occurred in the Delivery Scheduler: {0}	Critical	This event is generated when an uncategorized internal error occurred within the Delivery Manager, because of a bad destination or document data, rather than failure to deliver.
BCG250005	FTP Delivery Failed	FTP delivery to partner destination 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, metadata and header files in {0} reject and oversize folders for document: {1}	Error	
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 Internal Partner Business Process Failed	Failed to get an instance of the Internal Partner business process because {0}	Critical	This event is generated when the system fails to locate the internal partner action for business processing.
BCG800004	Internal Partner Business Process Encounters Database Error	{0}	Critical	This event is generated because of a database error while processing the internal partner's action.

Table 43. Failed events (continued)

Event code	Event name	Internal description	Severity	Extended description
BCG800005	Internal Partner Process Encounters Internal Error	{0}	Critical	This event is generated because of an internal system error while processing the internal partner's action.
BCG700002	Archiver Task Error	Archiver Error for task {0}	Error	This event is generated when archiver task execution fails.
BCG700005	Restore Failed	Restore Failed. Error Reason {1}	Error	This event is generated when archiver restore fails.

Table 44. 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	
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	

Table 44. EDI event codes and messages (continued)

EDI Event code	Event name	Internal description	Severity	Extended description
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 44. 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 must 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 component is null	The temporary directory value provided for the receiver component is null.	Error	
BCGEDIEM0110	The BusinessDocument Array passed is null	The BusinessDocument 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	

Table 44. EDI event codes and messages (continued)

EDI Event code	Event name	Internal description	Severity	Extended description
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	
BCGEDIEM0200	Database Connection Error.	Invalid or missing database connection object in the context.	Error	
BCGEDIEM0201	I/O Error While Writing to File.	Unable to Create a File in PROCESS DIR {0}	Error	
BCGEDIEM0202	Unable to Serialize AbsDocument.	Parser Exception Occurred while trying to serialize the AbsDocument.	Error	
BCGEDIEM0203	Exception occurred while serializing AbsDocument.	Exception Occurred 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	

Table 44. EDI event codes and messages (continued)

EDI Event code	Event name	Internal description	Severity	Extended description
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	
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	

Table 44. EDI event codes and messages (continued)

EDI Event code	Event name	Internal description	Severity	Extended description
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 stack trace 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	
BCGEDIFT0120	FTP Command Timed Out	FTP Command timed out. The command being sent was: {0}	Error	
BCGEDIFT0200	IO Exception	An IO Exception has occurred.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 reply codes for processing is null	Error	

Table 44. EDI event codes and messages (continued)

EDI Event code	Event name	Internal description	Severity	Extended description
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 occurred	Exception occurred	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 44. 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	

Table 44. EDI event codes and messages (continued)

EDI Event code	Event name	Internal description	Severity	Extended description
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 occurred during parsing of XML document {0} at line {1}, column {2}. Message text from parser is: {3}	Error	
BCGEDIUP0002	Severe XML Parsing Error	A severe error occurred 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 repetitions 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	

Table 44. EDI event codes and messages (continued)

EDI Event code	Event name	Internal description	Severity	Extended description
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 (flat file) data is not supported. The character set was {0}	Error	
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	

Table 44. EDI event codes and messages (continued)

EDI Event code	Event name	Internal description	Severity	Extended description
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 (flat file) Data Format	Invalid ROD (flat file) Data Format. No Child Nodes (STRUCTURES or FIELDS) found in Record node. RecordName: {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 (flat file) DataFormat. ROD (flat file) 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	
BCGEDIUP0112	Unexpected Nodes Under Record Node	Invalid ROD (flat file) DataFormat. ROD (flat file) RECORD node: {0} has child nodes other than STRUCTURE & FIELD	Error	
BCGEDIUP0113	Unexpected Nodes Under Loop Node	Invalid ROD (flat file) DataFormat. ROD (flat file) LOOP node: {0} has child nodes other than LOOP & RECORD	Error	
BCGEDIUP0114	Unexpected Nodes Under Structure Node	Invalid ROD (flat file) DataFormat. ROD (flat file) STRUCTURE node: {0} has child nodes other than STRUCTURE & FIELD	Error	

Table 44. EDI event codes and messages (continued)

EDI Event code	Event name	Internal description	Severity	Extended description
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	
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	

Table 44. EDI event codes and messages (continued)

EDI Event code	Event name	Internal description	Severity	Extended description
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	

Table 44. EDI event codes and messages (continued)

EDI Event code	Event name	Internal description	Severity	Extended description
BCGEDIUT0501	Input Document for Transformation is Empty	The input document for the transformation is empty	Error	
BCGEDIVA0001	Mandatory Data Element Missing	Mandatory data element is missing, element name = {0}, segment name = {1}, segment position = {2}, sending trading partner id/qualifier = {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/qualifier = {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/qualifier = {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/qualifier = {3}/{4}, receiving trading partner id/qualifier = {5}/{6}, control numbers = {7}. Element type = {8}, value = {9}, validation table = {10}	Error	

Table 44. 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/qualifier = {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/qualifier = {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/qualifier = {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/qualifier = {4}/{5}, receiving trading partner id/qualifier = {6}/{7}, control numbers = {8}	Error	

Table 44. 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 one of the others must be present. Segment name = {2}, segment position = {3}, sending trading partner id/qualifier = {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/qualifier = {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/qualifier = {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 transaction set or message within current interchange or functional group, transaction set or message control number = {0}, sending trading partner id/qualifier = {1}/{2}, receiving trading partner id/qualifier = {3}/{4}, control numbers = {5}	Error	

Table 44. 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/qualifier = {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/qualifier = {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/qualifier = {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/qualifier = {3}/{4}, receiving trading partner id/qualifier = {5}/{6}, control numbers = {7}. Element type = {8}, value = {9}	Error	

Table 44. EDI event codes and messages (continued)

EDI Event code	Event name	Internal description	Severity	Extended description
BCGEDIVA0034	Invalid Time Element	Invalid time element, element name = {0}, segment name = {1}, segment position = {2}, sending trading partner id/qualifier = {3}/{4}, receiving trading partner id/qualifier = {5}/{6}, control numbers = {7}. Element type = {8}, value = {9}	Error	
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/qualifier = {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/qualifier = {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/qualifier = {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/qualifier = {2}/{3}, receiving trading partner id/qualifier = {4}/{5}, control numbers = {6}	Error	

Table 44. EDI event codes and messages (continued)

EDI Event code	Event name	Internal description	Severity	Extended description
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/qualifier = {2}/{3}, receiving trading partner id/qualifier = {4}/{5}, control numbers = {6}. Repetition number = {7}, maximum defined repetitions = {8}	Error	
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/qualifier = {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/qualifier = {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/qualifier = {1}/{2}, receiving trading partner id/qualifier = {3}/{4}, control numbers = {5}	Error	

Table 44. EDI event codes and messages (continued)

EDI Event code	Event name	Internal description	Severity	Extended description
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/qualifier = {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/qualifier = {2}/{3}, receiving trading partner id/qualifier = {4}/{5}, control numbers = {6}	Error	
BCGEDIVA0152	Functional Group Trailer Missing or Invalid	Functional group trailer missing or invalid, functional control number = {0}, sending trading partner id/qualifier = {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/qualifier = {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/qualifier = {1}/{2}, receiving trading partner id/qualifier = {3}/{4}, control numbers = {5}	Error	

Table 44. EDI event codes and messages (continued)

EDI Event code	Event name	Internal description	Severity	Extended description
BCGEDIVA0202	Interchange Trailer Missing or Invalid	Interchange trailer missing or invalid, interchange header control number = {0}, sending trading partner id/qualifier = {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/qualifier = {2}/{3}, receiving trading partner id/qualifier = {4}/{5}	Error	
BCGEDIVA0205	Interchange Trailer Count Invalid	Interchange trailer contains an invalid group or message count, interchange header control number = {0}, sending trading partner id/qualifier = {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/qualifier = {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	

Table 44. EDI event codes and messages (continued)

EDI Event code	Event name	Internal description	Severity	Extended description
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 system attributes

Configuring attributes as WebSphere Application Server ND environment variables

On the System Administration page of the WebSphere Partner Gateway Console, there are configuration attributes for specific subcomponents of the WebSphere Partner Gateway runtime. These attributes apply to all instances of their subcomponents. For more information about the attributes, see the tables in “Attribute tables” on page 230. There might be situations in which you want to change the values of an attribute for a specific instance. For example, you might want to increase the number of threads if the computer that the component instance is running on has a greater CPU capacity. To change the value of an attribute for a specific component instance from what is configured in the WebSphere Partner Gateway Console, use the Deployment Manager on the System Administration page to create an environment variable for the node and server where the component is running. The value of the environment variable will take precedence over the value configured in the WebSphere Partner Gateway Console. For detailed information about WebSphere environment variables see the WebSphere Application Server documentation.

To create a WebSphere Application Server ND environment variable perform the following steps:

1. Open your WebSphere Application Server Admin Console.
2. Navigate to **Environment**> **WebSphere Variables**.
3. From the menu, select the node and server for which you are adding the variable.
4. Click **New**.
5. Type the name of property as it displays on the WebSphere Partner Gateway System administration page and set its value.
6. Click **OK**.
7. Save the master configurations.

Editing RosettaNet attribute values

If XPath queries are not provided for a PIP, the default XPath queries listed in Table 45 are used to extract the corresponding values:

Table 45. Default XPath Queries

Default XPath queries	Extracted value
<code>thisDocumentIdentifier[0]/ProprietaryDocumentIdentifier[0]</code>	Document ID
<code>thisMessageIdentifier[0]/ProprietaryMessageIdentifier[0]</code>	
<code>thisDocumentGenerationDateTime[0]/DateTimeStamp[0]</code>	Document creation date and time stamp
<code>theMessageDatetime[0]/DateTimeStamp[0]</code>	
<code>thisMessageDateTime[0]/DateTimeStamp[0]</code>	
<code>GlobalDocumentFunctionCode[0]</code>	GlobalFunctionCode

Table 45. Default XPath Queries (continued)

Default XPath queries	Extracted value
requestingDocumentIdentifier[0]/ProprietaryDocumentIdentifier[0]	Requesting document identifier
WarrantyClaimConfirmData[0]/DocumentReference[0]/ProprietaryDocumentIdentifier[0]	
receivedDocumentIdentifier[0]/ProprietaryDocumentIdentifier[0]	
ReturnProductResource[0]/DocumentReference[0]/ProprietaryDocumentIdentifier[0]	
theOffendingDocumentIdentifier[0]/ProprietaryDocumentIdentifier[0]	
fromRole[0]/PartnerRoleDescription[0]/PartnerDescription[0]/GlobalPartnerClassificationCode[0]	From-partner Classification Code
fromRole[0]/PartnerRoleDescription[0]/PartnerDescription[0]/BusinessDescription[0]/GlobalSupplyChainCode[0]	From-partner Global Supply Chain Code
fromRole[0]/PartnerRoleDescription[0]/PartnerDescription[0]/BusinessDescription[0]/GlobalBusinessIdentifier[0]	From-partner Business ID
fromRole[0]/PartnerRoleDescription[0]/PartnerDescription[0]/BusinessDescription[0]/BusinessIdentification[0]/GlobalBusinessIdentifier[0]	
fromRole[0]/PartnerRoleDescription[0]/GlobalPartnerRoleClassificationCode[0]	From-partner Role
toRole[0]/PartnerRoleDescription[0]/GlobalPartnerRoleClassificationCode[0]	To-partner Role
toRole[0]/PartnerRoleDescription[0]/PartnerDescription[0]/BusinessDescription[0]/GlobalBusinessIdentifier[0]	To-partner Business ID
toRole[0]/PartnerRoleDescription[0]/PartnerDescription[0]/GlobalPartnerClassificationCode[0]	To-partner Classification Code
toRole[0]/PartnerRoleDescription[0]/PartnerDescription[0]/BusinessDescription[0]/GlobalSupplyChainCode[0]	To-partner Global Supply Chain Code

The XSD based PIP packages contain the corresponding XPath queries. To view or edit these values select **Hub Admin > Hub Configuration > Document Definition > Manage Document Definitions**. On this page, expand the Package: RNIF node until the action node of a PIP (for example, 'Action: Purchase Order Update Notification Action') is reached. On this page you can view, create and edit XPath queries.

To edit the XPath query, click on the **Edit RossetaNet values** icon that is displayed in the Actions column associated with the PIP. This displays the RosettaNet Attributes window where you can view, add and edit the XPath queries.

Editing FTP Administration

The FTP administration has the following properties:

- Listener Properties
- Connection Properties
- IP Restrictor
- Event properties
- Database Properties
- Other Properties

Listener properties:

The component in the FTP server that listens to clients connection, command execution and so on. The properties of this listener are default listener properties and Client auth.

Table 46. Default Listener Properties

Property name	Description
<code>bcg.ftp.config.listeners.default.class</code>	The concrete listener implementation.
<code>bcg.ftp.config.listeners.default.address</code>	The ip-address or hostname of the host that runs the ftp server.
<code>bcg.ftp.config.listeners.default.port</code>	Port of the FTP Server. This is for the default listener.
<code>bcg.ftp.config.listeners.default.implicit-ssl</code>	FTP will be used instead of SSL
<code>bcg.ftp.config.listeners.default.ssl.class</code>	Class that handles SSL
<code>bcg.ftp.config.listeners.default.ssl.ssl-protocol</code>	Default SSL Protocol. The allowed values are TLSv1, SSLv3, and SSL_TLS
<code>bcg.config.listeners.default.ssl.client-authentication</code>	If Client auth is required
<code>bcg.ftp.config.listeners.default.data-connection.class</code>	Class that handles the Data connection
<code>bcg.ftp.config.listeners.default.data-connection.idle-time</code>	Connection idle time in seconds
<code>bcg.ftp.config.listeners.default.data-connection.active.enable</code>	If active connection is enabled for this listener
<code>bcg.ftp.config.listeners.default.data-connection.active.local-address</code>	Local address to listen to in active connections
<code>bcg.config.listeners.default.data-connection.active.local-port</code>	Local port to listen to for active connections
<code>bcg.ftp.config.listeners.default.data-connection.passive.address</code>	The FTP passive address. This is the same as the ip address where the ftp server will run.
<code>bcg.ftp.config.listeners.default.data-connection.passive.ports</code>	Passive ports
<code>bcg.ftp.config.listeners.default.data-connection.ssl.class</code>	Class used for SSL

Table 47. Client Auth

Property Name	Description
<code>bcg.ftp.config.listeners.clientauth.class</code>	The concrete listener implementation
<code>bcg.ftp.config.listeners.clientauth.address</code>	The ip-address or hostname of the host that runs the ftp server Port of the FTP Server.

Table 47. Client Auth (continued)

Property Name	Description
bcg.ftp.config.listeners.clientauth.port	Port of the FTP Server. This is for the default listener
bcg.ftp.config.listeners.clientauth.implicit-ssl	FTP will be used instead of SSL
bcg.ftp.config.listeners.clientauth.ssl.class	Class that handles SSL
bcg.ftp.config.listeners.clientauth.ssl.ssl-protocol	Default SSL Protocol. The allowed values are TLSv1 SSLv3, and SSL_TLS Note: In FIPS mode, TLSv1 can be optionally set as the value for bcg.ftp.config.listeners.default.ssl.ssl-protocol property to avoid confusion. The steps are as follows: In WebSphere Partner Gateway Console, select System Administration > FTP Administration > Listener Properties > Default . In non-FIPS mode, the value can be set to "SSL_TLS", which will enable both SSLv3 and TLSv1 support.
bcg.config.listeners.clientauth.ssl.client-authentication	If Client auth is required
bcg.ftp.config.listeners.clientauth.data-connection.class	Class that handles the Data connection
bcg.ftp.config.listeners.clientauth.data-connection.idle-time	Connection idle time in seconds
bcg.ftp.config.listeners.clientauth.data-connection.active.enable	If active connection is enabled for this listener
bcg.ftp.config.listeners.clientauth.data-connection.active.local-address	Local address to listen to in active connections
bcg.config.listeners.clientauth.data-connection.active.local-port	Local port to listen to for active connections
bcg.ftp.config.listeners.clientauth.data-connection.passive.address	PASV address
bcg.ftp.config.listeners.clientauth.data-connection.passive.ports	Passive Ports
bcg.ftp.config.listeners.clientauth.data-connection.ssl.class	Class used for SSL

Connection Properties:

All connection properties are editable.

Table 48. Connection Properties

Property Name	Description
bcg.ftp.config.connection-manager.max-connection	Maximum allowed connections
bcg.ftp.config.connection-manager.max-login	Maximum logins allowed

Table 48. Connection Properties (continued)

Property Name	Description
bcg.ftp.config.connection-manager.default-idle-time	Default idle time in seconds after a connection is established to disconnect
bcg.ftp.config.connection-manager.timeout-poll-interval	Time out interval to run the polling thread which collects idle connections

IP Restrictor Properties:

This has a list of IP Addresses having restricted access.

Table 49. IP Restrictor Properties

Property Name	Description
IP Pattern	A valid IP address has to be in x.x.x.x format. Alternatively, a wild card * can also be provided.
Permission	Checkmark is the permission given to this IP Address.

Event Properties

Table 50. Event Properties

Property Name	Description
bcg.config.ftpserver.FTPSerializeFileInterval	It is the interval in milliseconds, after which the accumulated events are serialized to the file system.
bcg.config.ftpserver.eventPersistThreads	This property is the number of threads in the thread pool to perform the database updates.
bcg.config.ftpserver.FTPEventThreshold	Maximum number of FTP events that can be accumulated before persisting in database or file system.
bcg.config.ftpserver.FTPEventStoreInterval	Interval after which FTP Events will persist in database or file system.
bcg.config.ftpserver.FTPEventLoggingLevel	This will have values 0,1,2 or 3 corresponding to the event levels (debug/info, warning, error and critical). The default value for this property is 2, so by default all error and critical events will be logged. These values are used to determine the level of FTP events that are logged.

Database Properties:

Table 51. Database Properties

Property Name	Description
Hostname	Host on which the database is installed.
User / Password	User name and password to connect to the database.
Port	Port on which database server is listening.

Other Properties:

Table 52. Other Properties

Property Name	Description
bcg.ftp.config.rootdirectory	This is the FTP Root Directory. Whenever a user is created and a directory is assigned, the user directory is created within this root.

Editing SFTP Administration

The SFTP administration has the following properties:

Table 53. SFTP Properties

Property name	Description
bcg.sftp.port	The port on which SFTP Server is started.
max-auth-requests	The maximum SFTP Server login attempts allowed.
auth-timeout	The allowed idle time while logging into SFTP Server.

Attribute tables

- Attributes shared by one or more components—Table 54 on page 231
- Attributes used for processing EDI documents—Table 55 on page 234
- Attributes used to configure the console component—Table 56 on page 236
- Attributes used to configure JMS for the console component—Table 57 on page 238
- Attributes used to configure the RosettaNet simulator—Table 58 on page 239
- Attributes used to configure the alert engine—Table 59 on page 240
- Attributes used to configure the AS state engine—Table 60 on page 241
- Attributes used to configure the business process engine (BPE)—Table 61 on page 241
- Attributes used to configure processing of signals—Table 62 on page 242
- Attributes used to configure synchronous processing by the BPE and Document Acquisition Engine (DAE)—Table 63 on page 243
- Attributes used to configure the delivery manager—Table 64 on page 243

- Attributes used to configure JMS for the Document Manager component—Table 65 on page 244
- Attributes used to configure the Document Manager packaging process—Table 66 on page 246
- Attributes used to configure RosettaNet processing by the Document Manager—Table 67 on page 247
- Attributes used to configure security in the Document Manager—Table 68 on page 249
- Attributes used to configure JMS for the receiver component—Table 69 on page 249
- Attributes used to configure synchronous response handling by the receiver component—Table 70 on page 250
- Attributes used to configure the directory names used by the receiver component—Table 71 on page 250
- Attributes used to configure miscellaneous aspects of the receiver component—Table 72 on page 251
- Attributes used to configure the summary engine subcomponent of the Document Manager—Table 73 on page 251
- Attributes used to configure the sponsor engine subcomponent of the Document Manager—Table 74 on page 251
- Attributes used to configure the archiver subcomponent of the Document Manager—Table 75 on page 252
- Attributes used to configure processing of ebMS documents—Table 76 on page 252
- Attributes used to configure the reliable messaging subcomponent of the Document Manager—Table 77 on page 252
- Attributes used to configure the event engine subcomponent of the Document Manager—Table 78 on page 253
- Attributes used to configure the archive and purge process Table 80 on page 253
- Attributes required to configure WebSphere Transformation Extender Table 81 on page 253

Table 54. Attributes shared by one or more components

Entry	Default value	Possible settings	Description
bcg.ldap.containerauth	False	Boolean True or False	When the Boolean value is set to True it indicates that the users are authenticated using the WebSphere Partner Gateway local database. Or, if the Boolean value is set to False an enterprise user registry is accessed using JAAS.
bcg.ldap.jaaslogin	WSLogin	String containing login ID	Specifies the name of the JAAS system or application login configuration.
bcg.receiver.persistpath	<Hub install root>/common/router_in/	A file system path	The receiver stores inbound documents here for the DAE to pick up.

Table 54. Attributes shared by one or more components (continued)

Entry	Default value	Possible settings	Description
bcg.receiver.sync.persistpath	<Hub install root>/common/sync_in	A file system path	The receiver stores synchronous documents for the DAE to pick up.
bcg.receiver.signal.persistpath	<Hub install root>/common/signal_in	A file system path	The receiver stores RosettaNet signals here.
bcg.vms_inbound_directory.main	<Hub install root>/common/router_in	A file system path	Main router inbound directory.
bcg.bpe_temp_directory.main	<Hub install root>/common/data	A file system path	Main router data directory.
bcg.vms_inbound_directory.signal	<Hub install root>/common/signal_in	A file system path	Signal router inbound directory.
bcg.bpe_temp_directory.signal	<Hub install root>/common/data	A file system path	Signal router data directory.
bcg.vms_inbound_directory.synchronous	<Hub install root>/common/sync_in	A file system path	Synchronous router inbound directory.
bcg.bpe_temp_directory.synchronous	<Hub install root>/common/data	A file system path	Synchronous router data directory.
bcg.scheduler_initial_pool_size	10	Positive integer	This value is the initial size of the pool of threads. It is a Scheduler manager property.
bcg.scheduler_max_pool_size	50	Positive integer	This value is the maximum size of the pool of threads. It is a Scheduler manager property.
bcg.global.common.introduce.document.transport	JMS	String containing either 'FileSystem' or 'JMS'	Determines the document routing transport for moving documents internally from the receiver to the Document Manager.
bcg.global.common.introduce.document.transport.unavailable.timeout	60000	Positive integer	When JMS transport is used for internal routing between the receiver and Document Manager, this is the timeout value that determines whether an error has occurred using the transport.

Table 54. Attributes shared by one or more components (continued)

Entry	Default value	Possible settings	Description
bcg.global.common.deletetempfiles	Yes	Yes or No	If the bcg.global.common.deletetempfiles property value is set to Yes , temporary files created by WebSphere Partner Gateway are deleted. If the value is set to No , the system will not delete any of the temp files.
bcg.messagestore.threshold	100000	File size in bytes	The value of the bcg.messagestore.threshold attribute denotes the threshold value of content file size in bytes, above which message store operation will not be performed.
bcg.event_log_exclude	No default value	String	List the event codes, separated by commas, that are not to be processed.
bcg.CRLDir	<Hub install root>/common/security/crl/	String with directory path	Path to directory where certificate revocation list files are stored.
bcg.checkRevocationStatus	TRUE	String Boolean value TRUE or FALSE.	A TRUE value causes the certificate revocation list to be checked before signing, or verifying the signature, encryption, decryption, SSL client and server certificate while sending the document or while connecting to the SSL server using FTP Scripting receiver.
bcg.http.SSLDebug	FALSE	String Boolean value TRUE or FALSE.	A TRUE value for this attribute will generate SSL debug logs. The debug information will be put in the SystemOut.log file in <Hub install root>/wasND/Profiles/bcgprofile/logs/<profile name> directory.
bcg.rosettanet.encrypt.CertDbRefreshInterval	60000	Integer	CRLs and VTP certificates are reloaded periodically after this interval, which is in milliseconds. Despite its name including Rosettanet, this attribute applies to all protocols.

Table 54. Attributes shared by one or more components (continued)

Entry	Default value	Possible settings	Description
bcg.certs.vtp.CertificateDir	<Hub install root>/common/security/vtp	String with a file directory path	Directory that contains certificates used for VTP signature validation and encryption. This value should match the value in bcg.console.certs.vtp.CertificateDir which is set in the general console attribute settings.
bcg.build_complete_certpath	true	String Boolean value true or false.	A true value implies that in case of a chain of certificates, the cert path will be built all the way to the root certificate. This causes all the certificates in the chain to be validated. A false value means that the certificate path is built and validated only till the issuer certificate. It is recommended to set the value to true as you can also revoke the CA certificates. Note: You can revoke the CA certificate only if you have created it for the trading community.

Table 55. Attributes used for processing EDI documents

Entry	Default value	Possible settings	Description
traceLevel.All	0	Integer between 0 and 2	<p>This particular attribute (All) affects all of the traces. If you want a more focused trace, set the individual trace(s) for the function(s) of interest.</p> <p>0 means no logs related to corresponding functionality should be written.</p> <p>1 means only error logs should be written in the trace file.</p> <p>2 means all the logs (error and debug) should be written in the trace file.</p> <p>For example, traceLevel.Transformation = 1 means that only the errors generated during EDI Transformation should be written to trace logs.</p> <p>The trace logs are located in <Hub install root>/wasND/Profiles/bcgprofile/logs/bcgdocmgr/ The default name of the trace file is bcg_router.log.</p>

Table 55. Attributes used for processing EDI documents (continued)

Entry	Default value	Possible settings	Description
traceLevel.Transformation	0	Integer between 0 and 2	See the description for traceLevel.All.
traceLevel.Validation	0	Integer between 0 and 2	See the description for traceLevel.All.
traceLevel.Enveloper	0	Integer between 0 and 2	See the description for traceLevel.All.
traceLevel.Deenveloper	0	Integer between 0 and 2	See the description for traceLevel.All.
traceLevel.EDI-Parser	0	Integer between 0 and 2	See the description for traceLevel.All.
traceLevel.XML-Parser	0	Integer between 0 and 2	See the description for traceLevel.All.
traceLevel.ROD-Parser	0	Integer between 0 and 2	See the description for traceLevel.All.
traceLevel.EDI-Serializer	0	Integer between 0 and 2	See the description for traceLevel.All.
traceLevel.XML-Serializer	0	Integer between 0 and 2	See the description for traceLevel.All.
traceLevel.ROD-Serializer	0	Integer between 0 and 2	See the description for traceLevel.All.
traceLevel.EDI-Splitter	0	Integer between 0 and 2	See the description for traceLevel.All.
traceLevel.XML-Splitter	0	Integer between 0 and 2	See the description for traceLevel.All.
traceLevel.ROD-Splitter	0	Integer between 0 and 2	See the description for traceLevel.All.
traceLevel.ROD-Scanner	0	Integer between 0 and 2	See the description for traceLevel.All.
traceLevel.FTP-Scripting	0	Integer between 0 and 2	See the description for traceLevel.All.
traceLevel.IBMVanAckProcessor	0	Integer between 0 and 2	See the description for traceLevel.All.
traceLevel.EDIackProcessor	0	Integer between 0 and 2	See the description for traceLevel.All.

Table 55. Attributes used for processing EDI documents (continued)

Entry	Default value	Possible settings	Description
traceLevel.Utility	0	Integer between 0 and 2	See the description for traceLevel.All.
transcript.file.option	N	Y or N	If the option Y is selected then transcript files are generated in the current working directory specified under "transcripts" folder.
database.encoding	UTF-8	A file encoding	The encoding used in the database for DB2. The value has to be UTF-8, as the code set used in DB2 is UTF-8.

Table 56. Attributes used to configure the console component

Entry	Default value	Possible setting	Description
bcg.console.outbound.gatewayDirectory	<Hub install root>/common/gateways	A file system path	Root directory in the common file system under which are found the subdirectories that are used for managing destinations (gateways).
bcg.console.db.debugLevel	0	Boolean 0 or 1	A binary setting using 0 and 1 to turn database debug trace on (1) or off (0).
bcg.console.appserver.mgmt.pool.maxsize	20	Integer	Internal setting for IBM use only
bcg.console.EAIDocDir	Documents	A valid directory name	The name of the subdirectory that is created under the root directory that you specify for a file-system receiver instance.

Table 56. Attributes used to configure the console component (continued)

Entry	Default value	Possible setting	Description
bcg.console.specialChars	!#;\& /?.,	Character list	A set of characters that cannot be used in some of the fields that are configured using the console. These are used for validation of partner login data and receiver and destination (gateway) data that is entered on the console. Note: For Internationalization purposes you may want to change these values depending on the language of the OS and what is specified for directory names.
bcg.console.specialCharsDir	!#;& ?.,	Character list	A set of characters that cannot be used in directory names that are entered on the console. Note: For Internationalization purposes you may want to change these values depending on the language of the OS and what is specified for directory names.
bcg.console.file.encodings	us-ascii ascii 646 iso_646.irv:1983 ansi_x3.4-1968 iso646-us default ascii7 utf-8 utf8 unicode-1-1-utf-8 utf-16 utf16 unicode sjis \u30B7\u30D5\u30C8\u7B26\u53F7\u5316\u8868 u73FE pck gb18030 big5 windows-1256 ISO8859-8 IBM856 ISO8869-6 IBM1046	A list of Internet Assigned Numbers Authority file encoding names that are supported by the class sun.io.CharacterEncoding. Names are separated with a vertical bar character.	The list of Java aliases that correspond to the Internet Assigned Numbers Authority encodings is generated and displayed by the document viewer. The user can specify file encodings that are used to process the files. Note that a single Java alias name may apply to more than one Internet Assigned Numbers Authority name. The default setting has Internet Assigned Numbers Authority values for many of the most commonly used encodings

Table 56. Attributes used to configure the console component (continued)

Entry	Default value	Possible setting	Description
bcg.console.help.host	localhost	Host name or IP address	The host name or IP address of the help-system server used by the console.
bcg.console.help.port	58080	Integer port number	The port on the help-system server that is used to obtain help.
bcg.console.version	Version 6.2.0.0.273	String value	A character string to indicate the version of the console that is in use.

Table 57. Attributes used to configure JMS for the console component

Entry	Default value	Possible settings	Description
bcg.jms.queue.factory	jms/bcg/cf/CONCF	JNDI name	Internal setting that affects inter-component communications. This is for IBM use only.
bcg.jms.topic.factory	jms/bcg/cf/CONCF	JNDI name	Internal setting that affects inter-component communications. This is for IBM use only.
bcg.jms.jndi_factory	com.ibm.websphere.naming.WsnInitialContextFactory	Class name	Internal setting that affects inter-component communications. This is for IBM use only.
bcg.jms.context_url	corbaloc:iiop:localhost:58809	URL	Internal setting that affects inter-component communications. This is for IBM use only.
bcg.jms.topic.name	jms/bcg/topic/reloadCacheT	JNDI name	Internal setting that affects inter-component communications. This is for IBM use only.
bcg.jms.retry_connect_interval	300000	Integer	Internal setting that affects inter-component communications. This is for IBM use only.
bcg.console.jmsPosterInstance	com.ibm.bcg.shared.event.MQSeriesPoster	Class name	Internal setting that affects inter-component communications. This is for IBM use only.

Table 57. Attributes used to configure JMS for the console component (continued)

Entry	Default value	Possible settings	Description
bcg.jms.reloadCache.name	No default value	JNDI name	Internal setting that affects inter-component communications. This is for IBM use only.
bcg.oaq_log_q	jms/bcg/queue/ datalogQ	JNDI name	Internal setting that affects inter-component communications. This is for IBM use only.

Table 58. Attributes used to configure the RosettaNet simulator

Entry	Default value	Possible setting	Description
bcg.console.certs.vtp. CertificateDir	<Hub install root>/common/ security/vtp	Local file system path	Full path to the directory that holds .p8 and .der files for the RN Simulator. If this path or the names of the certificate and private key files are not correct, an error is recorded in the console SystemErr.log. This error will not affect the operation of the hub and can be treated as warning. The value of this attribute should match the setting of the attribute bcg.certs.vtp.CertificateDir, which is set in the Document Manager security settings.
bcg.console.certs.vtp.Certificate	No default value	File name	The name of the certificate file (DER, binary format) containing a public key that is used by the simulator. The name must include the file extension.
bcg.console.certs.vtp.PrivateKey	No default value	File name	The name of the private key file (PKCS8, binary format) that is used by the simulator. The name must include the file extension.
bcg.console.certs.vtp.Passwd	No default value	File name	The password used to access the key held in the PKCS8 file
bcg.console.certs.vtp.VerifySig	FALSE	TRUE FALSE	Boolean indicating whether signature verification is performed when the simulator is used
bcg.console.vtp.RouterIn	TRUE OR FALSE	A file system path	The directory in the common file system that is used to pass documents to the Document Manager

Table 59. Attributes used to configure the alert engine

Entry	Default value	Possible setting	Description
<code>bcg.alertQReceiver.maxRetries</code>	100	Integer	Maximum number of retries attempted by the alert receiver.
<code>bcg.alertQReceiver.retryInterval</code>	60000	Integer	Interval in milliseconds between each retry.
<code>bcg.volumeAlertScheduler.allowanceForProcessingReceivedDocInMins</code>	10	Integer	Time in minutes after the volume alert end time to record documents that were received before evaluating the volume alert. This helps to assure that all documents received during the interval are in the count.
<code>bcg.alertNotifications.maxNotificationsInInterval</code>	10	Integer	To avoid excessive e-mail notifications several properties are used. If there are more than <code>maxNotificationsInInterval</code> in the time interval <code>maxNotificationIntervalInMins</code> for the same alert, alerts are held and batched every <code>heldAlertsBatchTimeInMins</code> until no alerts of that type are received for <code>minNotificationQuietIntervalInMins</code> .
<code>bcg.alertNotifications.maxNotificationIntervalInMins</code>	30	Integer	See description of <code>maxNotificationsInInterval</code> .
<code>bcg.alertNotifications.minNotificationQuietIntervalInMins</code>	30	Integer	See description of <code>maxNotificationsInInterval</code> .
<code>bcg.alertNotifications.heldAlertsBatchTimeInMins</code>	30	Integer	See description of <code>maxNotificationsInInterval</code> .
<code>bcg.alertNotifications.mailHost</code>	unknown	The word <code>unknown</code> or an IP address or a host name	The IP or host name of the SMTP mail host used to send alert notifications.
<code>bcg.alertNotifications.mailFrom</code>	<code>unknown@unknown.com</code>	e-mail address	The e-mail address to use as the sender of alert notifications
<code>bcg.alertNotifications.mailReplyTo</code>	<code>unknown@unknown.com</code>	e-mail address	The e-mail address to use as the reply-to address for alert notifications
<code>bcg.alertNotifications.mailEnvelopeFrom</code>	<code>unknown@unknown.com</code>	e-mail address	The e-mail address to use for replies in the event of an incorrect e-mail addresses

Table 59. Attributes used to configure the alert engine (continued)

Entry	Default value	Possible setting	Description
bcg.alert.eventGenerator.schedule	13 1 CertificateExpiration	Integer minutes Integer hours Alert name	Multiple records should be separated by the “ ” character. Entries of each record consists of (first integer) minutes, (second integer) hour and (String) alert name. These entries must be separated by one or more spaces.
bcg.VolumeAlertScheduler.scheduleTime	10	Integer	After every given number of seconds, the volume alert generator will generate the volume alerts.
bcg.BatchAlertScheduler.scheduleTime	10	Integer	After every given number of seconds, the batch alert generator will generate the batch alerts.
bcg.NotificationAlertScheduler.scheduleTime	10	Integer	After every given number of seconds, the notification alert generator will generate the notification alerts.

Table 60. Attributes used to configure the AS state engine

Entry	Default value	Possible setting	Description
bcg.asstate.thread_count	1	Integer	Number of threads used by the AS state engine.
bcg.asstate.batchSize	1	Integer	Batch size is always set to 1. Changing this attribute will not have any effect, and the attribute is reserved for future use. Its can be interpreted as the number of rows that are returned when the state engine is triggered.
bcg.asstate.runinterval	60000	Integer	Time interval in milliseconds that determines how often the AS state engine processes requests.

Table 61. Attributes used to configure the business process engine (BPE)

Entry	Default value	Possible setting	Description
bcg.dae.main.maxLockAge	180000	Integer	Maximum lock hold time in milliseconds for the main folder.
bcg.dae.main.maxfiles.perPass	5	Integer	Maximum number of files to process per main folder poll interval.

Table 61. Attributes used to configure the business process engine (BPE) (continued)

Entry	Default value	Possible setting	Description
bcg.docmgr.channelCache.maxSize	20	Integer	When a document is processed, a Partner Connection is looked up for the document. This Partner Connection configuration information is cached in the runtime. The maximum number of Partner Connections that can be cached at any one time is determined by this attribute. Once the maximum number has been reached then older information is removed and the newer Partner Connection information is added.
bcg.in_thread_count.main	2	Integer	Number of threads for main router processing of inbound messages.
bcg.inbound_poll_interval.main	1000	Integer	Time in milliseconds between directory scans.
bcg.bpe_max_file_size	0	Integer	Maximum file size in bytes. A value of zero means that no limit is enforced.
bcg.inbound_files_per_pass.main	5	Integer	Maximum number of files picked up per scan.
bcg.duplicate.DupField1 to bcg.duplicate.DupField10	x-aux-system-msg-id (This is the default value for DupField1).	String	The name of a message header whose value provides a unique identity for a message. This may be combined with other header values to uniquely identify a message.

Table 62. Attributes used to configure processing of signals

Entry	Default value	Possible setting	Description
bcg.dae.signal.maxLockAge	180000	Integer	Maximum lock hold time in milliseconds for the signal folder.
bcg.dae.signal.maxfiles.perPass	5	Integer	Maximum number of files to process per signal folder poll interval.
bcg.inbound_poll_interval.signal	1000	Integer	Time in milliseconds between directory scans.
bcg.in_thread_count.signal	2	Integer	Number of inbound threads for signal router.

Table 62. Attributes used to configure processing of signals (continued)

Entry	Default value	Possible setting	Description
bcg.inbound_files_per_pass.signal	5	Integer	Maximum number of files to pick up in a scan.

Table 63. Attributes used to configure synchronous processing by the BPE and document acquisition engine (DAE)

Entry	Default value	Possible setting	Description
bcg.dae.synchronous.maxLockAge	180000	Integer	Maximum lock hold time in milliseconds for the synchronous folder.
bcg.dae.synchronous.maxfiles.perPass	5	Integer	Maximum number of files to process per synchronous folder poll interval.
bcg.inbound_poll_interval.synchronous	1000	Integer	Time in milliseconds between directory scans.
bcg.in_thread_count.synchronous	2	Integer	Number of inbound threads for synchronous router.
bcg.inbound_files_per_pass.synchronous	5	Integer	Maximum number of files to pick up in a scan.

Table 64. Attributes used to configure the delivery manager

Entry	Default value	Possible setting	Description
bcg.delivery.gatewayDirectory	<Hub install root>/common/gateways	String	Root directory under which the files and subdirectories used to manage destinations (gateways) are located.
bcg.delivery.smtpHost	\$ROUTER.DM. SMTP_RELAY\$	IP/Hostname	Host that is used when posting documents using SMTP.
bcg.delivery.smtpHostPort	\$ROUTER.DM. SMTP_RELAY.PORT\$	Integer	The port on the SMTP mail host that is used.
bcg.delivery.responseDir	<Hub install root>/common/sync_in	String containing directory path	The location of the synchronous response directory.
bcg.delivery.msMaxFileLockLife	180000	Integer	Maximum time in milliseconds for a file to be locked.
bcg.delivery.threadPoolMaxThreads	50	Integer	Maximum size of the thread pool used by the delivery manager.

Table 64. Attributes used to configure the delivery manager (continued)

Entry	Default value	Possible setting	Description
bcg.delivery.gatewayMaxThreads	20	Integer	Maximum number of gateway threads
bcg.delivery.gwTransportMaxRetries	3	Integer	Number of retries that will be attempted by the delivery manager for each destination level retry. This is a global setting that applies to all destinations (gateways). Each destination is also configured with its own retry number that is used each time the framework does a retry.
bcg.delivery.gwTransportRetryInterval	3000	Integer	The interval in milliseconds between delivery manager retries.
bcg.delivery.numberOfLoggers	10	Integer	—
bcg.delivery.jmstimeout	60000	Integer	When the JMS transport is used to post documents, this timeout in milliseconds is used to determine if there is a connectivity problem or not.
bcg.http.socketTimeout	120000	Integer	HTTP socket timeout in milliseconds
bcg.http.version	1.1	String	HTTP version used by the delivery manager
bcg.router.ipv6.address	No default value	String	If the computer where the Document Manager is installed is configured with IPv6 and documents are sent using a gateway based on IPv6 protocol, then the IPv6 address of the computer must be entered here.
bcg.delivery.loggerTimeOut	10000	Integer	—

Table 65. Attributes used to configure JMS for the Document Manager component

Entry	Default value	Possible setting	Description
bcg.jms.queue.factory	jms/bcg/cf/DOCMGRCF	JNDI name	Internal setting that affects inter-component communications. This is for IBM use only.

Table 65. Attributes used to configure JMS for the Document Manager component (continued)

Entry	Default value	Possible setting	Description
bcg.jms.topic.factory	jms/bcg/cf/DOCMGRCF	JNDI name	Internal setting that affects inter-component communications. This is for IBM use only.
bcg.jms.jndi_factory	com.ibm.websphere.naming.WsnInitialContextFactory	Class name	Internal setting that affects inter-component communications. This is for IBM use only.
bcg.jms.context_url	corbaloc:iiop:localhost:58809	URL	Internal setting that affects inter-component communications. This is for IBM use only. Port 58809 is the default port for a simple mode installation. Your installation may differ.
bcg.oaq_bpe_in.main	jms/bcg/queue/main_InboundQ	JNDI name	Internal setting that affects inter-component communications. This is for IBM use only.
bcg.oaq_bpe_out.main	jms/bcg/queue/deliveryManagerQ	JNDI name	Internal setting that affects inter-component communications. This is for IBM use only.
bcg.oaq_bpe_in.signal	jms/bcg/queue/signal_InboundQ	JNDI name	Internal setting that affects inter-component communications. This is for IBM use only.
bcg.oaq_bpe_out.signal	jms/bcg/queue/deliveryManagerQ	JNDI name	Internal setting that affects inter-component communications. This is for IBM use only.
bcg.oaq_bpe_in.synchronous	jms/bcg/queue/sync_InboundQ	JNDI name	Internal setting that affects inter-component communications. This is for IBM use only.
bcg.oaq_bpe_out.synchronous	jms/bcg/queue/deliveryManagerQ	JNDI name	Internal setting that affects inter-component communications. This is for IBM use only.
bcg.delivery.queue	jms/bcg/queue/deliveryManagerQ	JNDI name	Internal setting that affects inter-component communications. This is for IBM use only.

Table 65. Attributes used to configure JMS for the Document Manager component (continued)

Entry	Default value	Possible setting	Description
bcg.alertQueue.queue	jms/bcg/queue/alertQ	JNDI name	Internal setting that affects inter-component communications. This is for IBM use only.
bcg.eventAlertQReceiver.queue	jms/bcg/queue/alertEventQ	JNDI name	Internal setting that affects inter-component communications. This is for IBM use only.
bcg.syncdelivery.queue	jms/bcg/queue/syncDeliveryManagerQ	JNDI name	Internal setting that affects inter-component communications. This is for IBM use only.
bcg.logReceiver.queue	jms/bcg/queue/datalogQ	JNDI name	Internal setting that affects inter-component communications. This is for IBM use only.
bcg.dberrors.queue	jms/bcg/queue/datalogErrorQ	JNDI name	Internal setting that affects inter-component communications. This is for IBM use only.
bcg.jms.retry_connect_interval	300000	Integer	Internal setting that affects inter-component communications. This is for IBM use only.
bcg.jms.connect_pool_elements	2	Integer	Internal setting that affects inter-component communications. This is for IBM use only.
bcg.jms.connect_max_pool_elements	100	Integer	Internal setting that affects inter-component communications. This is for IBM use only.

Table 66. Attributes used to configure the Document Manager packaging process

Entry	Default value	Possible setting	Description
Wbipackaging_version	1	1.0 and 1.1	This is used for building the 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.

Table 66. Attributes used to configure the Document Manager packaging process (continued)

Entry	Default value	Possible setting	Description
DBProcDebug	1	Integer: either 0 or 1	A binary setting using 0 and 1 to turn database debugging on (1) or off (0). In the debug logs, the procedure name and the parameters passed to it are displayed.
GlobalStateEngInstanceId	Bcg	String	AS Inbound and Outbound documents are logged into DB using GlobalStateEngInstanceId. The AS state engine makes a DB call to get the last detail row of the oldest header row that is be processed using GlobalStateEngInstanceId and generates an MDN. This parameter is also used for retries.
bcg.ediint.reportingUA	WPG	String	Reporting UA is to indicate the user agent reporting the MDN.
bcg.ediint.retryWaitTmMS	5000	Integer	For AS outbound messages (with asynchronous MDN), if the MDN is not received, the AS Engine retries after this number of milliseconds.
bcg.maxBatchSize	1000	Integer	Maximum number of files to be picked up and processed, as a batch, by a gateway.

Table 67. Attributes used to configure RosettaNet processing by the Document Manager

Entry	Default value	Possible setting	Description
bcg.rosettanel.retryWaitTmMS	5000	Integer	Retry interval in milliseconds
bcg.rosettanel.strictBoundaryParse	FALSE	String Boolean value TRUE or FALSE.	Whether to strictly parse boundaries of Mime Multipart (Rosettanel) messages or not. Default value is TRUE.
bcg.rosettanel.mimeBoundaryValidate	FALSE	String Boolean value TRUE or FALSE.	If this value is set to TRUE, structural validation of mime multipart (Rosettanel) message is performed. Default value is FALSE.

Table 67. Attributes used to configure RosettaNet processing by the Document Manager (continued)

Entry	Default value	Possible setting	Description
bcg.rosettnet.globalUsageCode	Literal	String value of "Literal" or anything else.	<p>If this value is "Literal", we expect the x-aux-production HTTP header to literally be "Production" or "Test".</p> <p>If is not equal to "Literal" (for example, if you set it to a blank value), we expect the x-aux-production HTTP header to be True or False.</p> <p>All values are case insensitive.</p>
bcg.rosettnet.defaultUsageCdOnErr	1	String value of 1 or 0 that is interpreted as a Boolean.	<p>If the HTTP header 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 the attribute bcg.rosettnet.defaultGlbUsageCd.</p>
bcg.rosettnet.defaultGlbUsageCd	Test	String	Default global usage code.
bcg.rosettnet.useBuilderProcessInstanceId	1	String value of 1 or 0 that is interpreted as a Boolean.	<p>If this value equals 1, we expect the builder to provide an ID in the HTTP header x-aux-process-instance-id to be used as the process instance id for an outbound request.</p>
bcg.rosettnet.genProcessInstanceIdOnError	1	String value of 1 or 0 that is interpreted as a Boolean.	<p>If the builder provided process-instance-id is incorrect (for any reason), generate a new process-instance-id if this value is 1.</p>
bcg.rne.inbound_poll_interval	10000	Integer	RosettaNet engine polling interval in milliseconds.
bcg.rne.in_thread_count	2	Integer	Number of threads used by the RosettaNet engine to process inbound documents.
bcg.rne.work_size	50	Integer	The number of PIP messages processed per poll-interval.
bcg.0A1.fromContactName	\$ROUTER. CONTACT_NAME\$	String	Name of the 0A1 contact.
bcg.0A1.fromEMailAddr	\$ROUTER. CONTACT. MAIL_FROM\$	String	E-mail of the 0A1 contact.

Table 67. Attributes used to configure RosettaNet processing by the Document Manager (continued)

Entry	Default value	Possible setting	Description
bcg.0A1.fromPhoneNbr	\$ROUTER. CONTACT. PHONE_NO\$	String	Telephone number of the 0A1 contact.
bcg.0A1.fromFaxNbr	\$ROUTER. CONTACT.FAX_NO\$	String	Fax number of the 0A1 contact
bcg.rnif.pip.twoaction.correlation	documentid	String	The value of this property acts as correlation parameter between the 1-action and the 2-action of a two action PIP.

Table 68. Attributes used to configure security in the Document Manager

Entry	Default value	Possible setting	Description
bcg.rosettanet.signature. DigestAlgorithm	SHA1	SHA1 or MD5	The algorithm that is used to generate Message Digests. Despite its name including rosettanet, this attribute is used for both RNIF and AS. It is not used for ebMS. It applies to all the flows using PKCS7 for signing the document. ebMS does not use PKCS7 signatures.
bcg.rosettanet.signature. RejectIfFailVal	TRUE	String Boolean value TRUE or FALSE.	A TRUE value implies that a document will be rejected if the signature validation fails.
bcg.rosettanet.signature. VerifySigner	TRUE	String Boolean value TRUE or FALSE.	A TRUE value means that the signer will be validated once signature is validated. FALSE means that the signer won't be validated.
bcg.rosettanet.encrypt.Algorithm	3des	3des or des or aes or rc2-40	Encryption algorithm used for RosettaNet messages. This Property is applicable to all protocols.

Table 69. Attributes used to configure JMS for the receiver component

Entry	Default value	Possible setting	Description
bcg.jms.queue.factory	jms/bcg/cf/RCVRCF	JNDI name	Internal setting that affects inter-component communications. This is for IBM use only.
bcg.jms.topic.factory	jms/bcg/cf/RCVRCF	JNDI name	Internal setting that affects inter-component communications. This is for IBM use only.

Table 69. Attributes used to configure JMS for the receiver component (continued)

Entry	Default value	Possible setting	Description
bcg.jms.jndi_factory	com.ibm.websphere.naming.WsnInitialContextFactory	Class name	Internal setting that affects inter-component communications. This is for IBM use only.
bcg.jms.context_url	corbaloc:iiop:localhost:58809	URL	Internal setting that affects inter-component communications. This is for IBM use only. Port 58809 is the default port for a simple mode installation. Your installation may differ.
bcg.oaq_log_q	jms/bcg/queue/datalogQ	JNDI name	Internal setting that affects inter-component communications. This is for IBM use only.
bcg.jms.retry_connect_interval	300000	Integer	Internal setting that affects inter-component communications. This is for IBM use only.
bcg.jms.connect_pool_elements	2	Integer	Internal setting that affects inter-component communications. This is for IBM use only.
bcg.jms.connect_max_pool_elements	100	Integer	Internal setting that affects inter-component communications. This is for IBM use only.

Table 70. Attributes used to configure synchronous response handling by the receiver component

Entry	Default value	Possible setting	Description
bcg.receiver.sync.responseURL	/bcgsyncreceiver/SyncResponse	URI	Internal receiver URI for posting sync responses.
bcg.receiver.sync.responseURL.port	58081	Integer	Port number used with the sync response URI.

Table 71. Attributes used to configure the directory names used by the receiver component

Entry	Default value	Possible setting	Description
bcg.receiver.configpath	<Hub install root>/common/receiver/config	String with directory path	Receiver configuration XML file location, used when Database is not available.
bcg.vms_receiver_reject_dir	<Hub install root>/common/receiver/reject	String with directory path	Receiver reject directory

Table 71. Attributes used to configure the directory names used by the receiver component (continued)

Entry	Default value	Possible setting	Description
bcg.vms_receiver_tmp_dir	<Hub install root>/common/receiver/tmp	String with directory path	Receiver temporary storage directory. Receivers that use non-file transports like JMS, POP3, and HTTP place the content files with an extension of ".vcd" in this location. This is for IBM Internal Use.

Table 72. Attributes used to configure miscellaneous aspects of the receiver component

Entry	Default value	Possible setting	Description
bcg.receiver.ipv6	No default	An IPv6 address	The IPv6 address used by the receivers. This is required if the computer that hosts the receiver component uses IPv6.

Table 73. Attributes used to configure the summary engine subcomponent of the Document Manager

Entry	Default value	Possible setting	Description
bcg.summary.processingInterval	15	Integer	Time interval in minutes that determines how often event summary processing occurs.
bcg.summaryEng.thread_count	1	Integer	The number of threads that prepare the event summary.

Table 74. Attributes used to configure the sponsor engine subcomponent of the Document Manager

Entry	Default value	Possible setting	Description
bcg.sponsor.inbound_poll_interval	10000	Integer	Defines the interval in milliseconds between polls of the table for generating event notification documents (mainly XML events). For details on XML events, see <i>XMLEvent</i> section of <i>Enterprise Integration Guide</i> .
bcg.sponsor.in_thread_count	1	Integer	Number of threads that is used by the sponsor to generate the event notification documents.
bcg.sponsor.work_size	10	Integer	Number of rows per pass that are fetched from the database for generating the event notification documents.

Table 75. Attributes used to configure the archiver subcomponent of the Document Manager

Entry	Default value	Possible setting	Description
bcg.archiver.maxSubVolFiles	70000	Integer	Maximum number of sub-volumes under a volume.
bcg.archiver.runinterval	600	Integer	Time interval in seconds that determines how often the archiver service processing occurs.

Table 76. Attributes used to configure processing of ebMS documents

Entry	Default value	Possible setting	Description
bcg.ebXML.language	en-US	String	The language used in ebXML SOAP Messages
bcg.AddKeyInfo	true	Boolean true or false	This attribute is applicable only while signing ebXML message. If the value of this attribute is false, then Signature element will not contain the KeyInfo element. The KeyInfo element contains the public key used for the signature.
bcg.ebXML.version	2.0	String	The ebXML version used to package payloads as ebXML message. Currently, only 2.0 is supported.
bcg.ebms.xsd.schemaName	ebXMLSchema.xsd	String with file name	The XSD name used to validate an incoming ebXML message. The XSD is pre-populated in database while installing, with the default name. If user changes XSD file and uploads it with a different name in database then the same name should be given as value for this attribute.
bcg.ebms.validate	false	Boolean true or false	This attribute determines whether to validate an ebXML Soap message against the XSD named by the schemaName attribute. A value "true" will cause all incoming ebXML messages to be validated.

Table 77. Attributes used to configure the reliable messaging subcomponent of the Document Manager

Entry	Default value	Possible setting	Description
bcg.rm.pollInterval	300000	Integer	Time interval in milliseconds that determines how often reliable message service processing occurs.

Table 77. Attributes used to configure the reliable messaging subcomponent of the Document Manager (continued)

Entry	Default value	Possible setting	Description
bcg.rm.thread_count	3	Integer	The number of threads used by the reliable messaging service.

Table 78. Attributes used to configure the event engine subcomponent of the Document Manager

Entry	Default value	Possible setting	Description
bcg.eventeng.alertscache.size	100	Integer	The size of the alert cache.

Table 79. Other EDI properties

Entry	Default value	Possible setting	Description
transcript.file.option	N	Y/N	If the option yes is selected, transcript files are generated in the current working directory specified under "transcripts" folder
PageThreshold	1000	0-n	This property controls paging of repeating message structures in the EDI components. Set it zero to disable paging. Nonzero values specify the maximum number of occurrences of a given item which can occur before paging occurs. Paging reduces memory use at the cost of increasing processing time.

Table 80. Attributes used to configure the archive and purge process

Entry	Default value	Possible setting	Description
bcg.archive.maxThreads	4	Integer	Archiving of files is multithreaded, and a new property bcg.archive.maxThreads is introduced in WebSphere Partner Gateway 6.2.1, with a default value of four. This value specifies the maximum number of threads that is allowed while archiving.

Table 81. Attributes to configure WebSphere Transformation Extender properties

Entry	Default value	Possible setting	Description
wtx.rmihostname	localhost	Integer	IP address or the hostname of WebSphere Transformation Extender server.
wtx.rmiport	2500	Integer	RMI port number of WebSphere Transformation Extender.

Table 81. Attributes to configure WebSphere Transformation Extender properties (continued)

Entry	Default value	Possible setting	Description
rmiuseserver	No	Boolean: Yes or No	This attribute is set to Yes if the required WebSphere Transformation Extender map innovation style is RMI.
bcg.wtx.mapLocation	<Hub install root>/bcghub-distrib/common/maps	Integer	Default location of the map.

Notices

This information was developed for products and services offered in the U.S.A.

IBM may not offer the products, services, or features discussed in this document in other countries. Consult your local IBM representative for information about 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 grant you any license to these patents. You can send license inquiries, in writing, to:

*IBM® Director of Licensing
IBM Corporation
North Castle Drive
Armonk, N.Y. 10504-1785
U.S.A.*

For license inquiries regarding double-byte (DBCS) information, contact the IBM Intellectual Property Department in your country or send inquiries, in writing, to:

*IBM World Trade Asia Corporation Licensing
2-31 Roppongi 3-chome, Minato-ku
Tokyo 106-0032, Japan.*

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 the 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 measurements may have been estimated through extrapolation. Actual results may vary. Users of this document should verify the applicable data for their specific environment.

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

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

All IBM prices shown are IBM's suggested retail prices, are current and are subject to change without notice. Dealer prices may vary.

This information is for planning purposes only. The information herein is subject to change before the products described become available.

This information contains examples of data and reports used in daily business operations. To illustrate them as completely as possible, the examples 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.

COPYRIGHT LICENSE

This information contains sample application programs in source language, which illustrate 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.

Each copy or any portion of these sample programs or any derivative work, must include a copyright notice as follows:

Copyright (c) 1995-2008 International Business Machines Corporation and others
All rights reserved.

If you are viewing this information softcopy, the photographs and color illustrations may not appear.

Programming interface information

Programming interface information, if provided, is intended to help you create application software using this program. General-use programming interfaces is intended to help you 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.

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

Trademarks and service marks

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

IBM	DB2	i5/OS	MQIntegrator	Informix
the IBM logo	DB2 Universal Database	IMS	OS/400	MVS
AIX	Domino	iSeries	Passport Advantage	WebSphere
CICS	IBMLink	Lotus	SupportPac	z/OS
CrossWorlds		Lotus Notes	Tivoli	

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.

Solaris, 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 includes software developed by the Eclipse Project (www.eclipse.org)



Index

A

Account Admin activities 43
 adding Partners to the Exclusion List 61
 B2B attribute, changing 55
 changing connection configurations 59
 changing partner attribute values 60
 changing the destination or return destination 60
 connection components 56
 connection duplication 57
 deleting partners 44
 deleting transports 48
 disabling a digital certificate 55
 disabling or deactivating a connection 60
 editing the Exclusion List 61
 information for destination configuration 44
 managing certificates 51
 managing destination configurations 44
 managing exclusion lists 61
 managing partner connections 56
 managing partner profiles 43
 performing a basic search for connections 58
 performing an advanced search 59
 retrying destinations 48
 retrying transports 48
 searching for connections 57
 searching for partners 43
 selecting
 action, new 60
 Transformation map, new 60
 uploading transports 48
 viewing and editing destinations 45
 viewing and editing digital certificates 54
 viewing and editing partner profiles 43
 viewing default destinations 47

Actions
 enabling or disabling 25
 selecting a new 60

Activities
 Account Admin 43

Adding
 Partners to the Exclusion List 61

administering
 partner migration 63

Advanced search
 for connections 59

Alert mail server, configuring 33

Alerts Notification 168

API calls
 managing 34

archiving 131

AS documents, encrypted 160

AS Viewer 111

AS Viewer (*continued*)
 description 106
 package details 109
 search criteria 107
 searching for messages 107
 viewing message details 108

Attributes
 changing partner values 60

B

B2B attribute 55

Basic search, for connections 58

Browser ERROR: 500 172

Business documents
 reprocessing 169

C

Certificates
 disabling 55
 managing 51
 viewing and editing 54

Changing
 connection configurations 59
 destination status 90
 partner attribute values 60
 the source or target destination 60

ClassNotFoundException 169

Collating data 162

Community Console
 icons 16
 logging in 15
 logging out 18
 navigating through 16

Components
 connections 56

Configuration
 validate
 webservices 38

Configurations
 changing connection 59
 deleting transports 48
 destination required information 44
 managing destination 44
 uploading transports 48

Configuring
 alert mail server 33
 Document Definitions 23
 download packages 23
 IPv6 attributes 85
 receivers 22

Connection profiles
 creating 30
 deleting 30
 editing 30

Connections
 changing configurations 59
 components 56
 disabling or deactivating 60

Connections (*continued*)
 duplication 57
 managing partner 56
 performing a basic search 58
 searching for 57

Container, enabling 77

Content-type
 importing 26

Control number
 current 31
 initialization 30

Conventions, typographic 2

CPA
 Digest and Signature algorithms supported 38
 non-prepopulated attributes 37
 uploading 36

Create
 Document Volume Report 93

Critical event type 104

CRL DP 177

D

data validation errors 167

Database query performance,
 optimizing 166

DB2 agents, virtual memory 163

Deactivating a connection 60

Debug events 104

Default
 destination 47

Deleting
 importing 26
 partners 44
 receivers 23
 transports 48

Destination
 changing source or target 60
 changing status 90
 managing configurations 44
 required configuration information 44
 retries 48
 stopping documents from the queue 89
 using Queue 87
 viewing and editing 45
 viewing default 47
 viewing details 90
 viewing queued documents 88
 viewing the list 87

Details, viewing destination 90

Digital certificates
 disabling 55
 managing 51
 viewing and editing 54

Disabling
 a connection 60
 a digital certificate 55
 actions 25

- Disabling (*continued*)
 - receivers 22
- Document
 - details, Document Viewer 113
 - processing values, Document Viewer 114
- Document Analysis
 - description 91
 - search criteria 92
 - viewing documents 92
 - viewing process and event details 93
- Document Definition
 - configuring 23
- Document Manager
 - stopping 181
- Document Manager information
 - managing 35
- Document states
 - definitions 91
 - Document Volume Report 93
- Document Viewer
 - description 111
 - document details 113
 - document processing values 114
 - search criteria 112
 - values 107, 109, 113, 114
- Document Volume Report
 - create 93
 - description 93
 - document states 93
 - exporting 94
 - printing 94
 - search criteria 94
- Documents
 - routed twice 167
 - stopping from the queue 89
 - viewing queued 88
- Download packages, configuring 23

E

- ebMS
 - support 36
- ebMS Viewer 121
 - description 120
 - searching for processes 120
 - viewing process details 121
- EDI FA Overdue
 - report 99
 - search criteria 98
- EDI Rejected Transaction
 - report 100
 - search criteria 100
- EDI reports 167
- Editing
 - destination 45
 - digital certificates 54
 - partner profiles 43
 - permission details 21
 - receiver details 22
 - the Exclusion List 61
- Enabling
 - actions 25
 - IPV6 84
 - receivers 22
- Encrypted AS documents 160
- Error event type 104

- error events 105
- Error fields
 - validation errors 117
- Event codes
 - managing 20
 - saving names 21
- Event types 104
 - descriptions 104
- Event Viewer
 - description 103
 - search criteria 104
 - viewing event details 105
- Events
 - reprocessing 169
 - search criteria 104
 - searching for 104
- Exclusion List
 - adding Partners 61
 - editing 61
 - managing 61
- Exporting
 - Document Volume Report 94

F

- FTP Connections
 - report 101
- FTP Statistics
 - report 101
- FTPScripting 168

G

- Generating
 - summary data 189

H

- Handlers
 - configuring content-type 26
 - deleting 26
 - importing 26
 - managing 25
- Hub administrator tasks 19
 - configuring Document Definitions and download packages 23
 - configuring receivers 22
 - deleting receivers 23
 - enabling or disabling actions 25
 - enabling or disabling receivers 22
 - handlers
 - configuring content-type 26
 - deleting 26
 - importing 26
 - managing 25
 - managing event codes 20
 - managing password policy 19
 - managing XML formats 24
 - saving event code names 21
 - viewing and editing permission details 21
 - viewing and editing receiver details 22

I

- IBM service log 165
- Icons in the Community Console 16
- Increasing, Receiver timeout 165
- Information event type 104
- Information required for destination configuration 44
- informational messages 165
- intellectual property 255
- IPv6
 - attributes, configuring 85
 - enabling 84
 - HP-UX 11i 84
 - support 83
 - tunneling in RHEL Linux 3 83
 - tunneling over IPv4 83
 - Windows 2003/XP 83

J

- J2EE security 77
- java.security.InvalidKey 183
- javacore 170
- JIT, disabling 170
- JMS Exports/Imports 173

L

- Languages, multiple 162
- LDAP
 - enabling the container 77
 - for IBM Tivoli 79
 - J2EE security 77
 - sample configuration 79
 - stopping 78
 - support 77
 - user names and groups 78
 - users, specifying 81
 - using 77
- license, patents 255
- licensing
 - address 255
- Logging
 - non-repudiation 39
- Logging in 15
- Logging out 18

M

- Managing
 - API calls 34
 - certificates 51
 - destination configurations 44
 - Document Manager information 35
 - EDI maps 28
 - event codes 20
 - exclusion lists 61
 - FA maps 28
 - handlers 25
 - importing 26
 - maps 27
 - partner connections 56
 - partner profiles 43
 - password policy 19
 - queue overflow 189

Managing (*continued*)
 system configuration data 32
 transformation maps 27
 XML formats 24

Maps
 managing 27
 managing EDI 28
 managing FA 28
 managing transformation 27
 updating 27
messages, informational 165

N

Navigating through Community
 Console 16
New action, selecting 60
Non-repudiation
 logging 39

O

Out-of-memory errors, avoiding 161

P

Package Details
 AS Viewer 109
partner
 connection duplication 57
 searching for connections 57
Partner
 adding to Exclusion Lists 61
 advanced search for connections 59
 basic search for connections 58
 changing attribute values 60
 connection components 56
 deleting 44
 managing connections 56
 managing profiles 43
 preventing transactions 171
 searching 43
 viewing and editing profiles 43
partner migration
 administering 63
 configuration
 dependencies 71
 dependent items 72
 independent items 72
 independent items 72
 non-migratable configurations 75
 utility 63
partner migrationPartner Migration
 Utility with LDAP
 utility 187
patents 255
Performance consideration 189
Performing
 advanced search for connections 59
 basic search for connections 58
Permission
 viewing and editing details 21
Printing reports
 Document Volume Report 94
Profile
 managing partner 43

Proxy support, forward 51

Q

Queue overflow 189
Queue, stopping documents from 89
Queued documents, viewing 88

R

Raw documents
 viewing 111, 121
Receiver
 configuring 22
 deleting 23
 enabling or disabling 22
 viewing and editing details 22
Receiver timeout, increasing 165
Report
 EDI FA Overdue 99
 EDI Rejected Transaction 100
 FTP Connections 101
 FTP Statistics 101
 SFTP Statistics 101
Required information, destination
 configuration 44
Result codes
 200 series 96
 300 series 96
 400 series 96
 500 series 97
 Web Server 95
Retries
 destination 48
 transport 48
RosettaNet Viewer
 description 109
 document processing, details 110
 search criteria 109
 searching for processes 109
 viewing process details 110

S

Saving event code names 21
Search
 advanced for connections 59
 basic for connections 58
 ebMS processes 120
 for events 104
 for messages, AS Viewer 107
 for RosettaNet processes 109
Search criteria
 AS Viewer 107
 Document Analysis 92
 Document Viewer 112
 Document Volume Report 94
 EDI FA Overdue 98
 EDI Rejected Transaction 100
 Event Viewer 104
 RosettaNet Viewer 109
Searching
 for connections 57
 for partners 43
 security, J2EE 77

Selecting
 a new action 60
 transformation map 60
service log, IBM 165
Source destination, changing 60
SQLCODE
 -1225 164
 -289 164
 -444 164
 0964C 164
SSL connections 174
SSL handshake 180
Status
 viewing ebMS 122
Status, change destination 90
Stopping documents from the queue 89
Summary data 189
Support
 ebMS 36
 IPv6 83
System activity
 viewing 33, 34
System configuration data
 accessing 32
 managing 32

T

Target
 changing destination 60
Tasks
 Hub administrator 19
Test Partner Connection
 description 94
 values 95
 Web Server result codes 95
Tools
 description 91
 Document Analysis 91
 Document Volume Report 93
 Test Partner Connection 94
Transformation map
 selecting a new 60
Transformation map, selecting 60
Transport type, custom 170
Transports
 deleting 48
 forward proxy 51
 retries 48
 uploading 48
Troubleshooting
 01A 167
 Alerts Notification 168
 avoiding out-of-memory errors 161
 BCG210001 174
 BCG210013 175
 BCG210031 170
 BCG240415 170
 BCGEDIEV0O56 174
 bcgHubInstall.log 177
 browser error 500 172
 business documents 169
 CA certificate expiration 179
 CHF0029E 178
 ClassNotFoundException 169
 collating data for multiple
 languages 162

Troubleshooting (*continued*)

- content-types attribute 174
- creating on another drive 171
- CRL DP 177
- databinding in JMS 173
- DB password required 177
- DB2 virtual memory 163
- Define custom transport type 170
- document volume report 177
- documents not processed 185
- documents routed twice 167
- downloading CRL 172
- duplicate document delivery 184
- EDI reports 167
- Event 210031 166
- file size 0 KB 180
- FTPScripting Receiver 168
- hub installer errors 176
- IBM service log 165
- increasing buffer size 176
- information messages 165
- java.security.InvalidKey 183
- JIT, disabling 170
- long processing time 160
- MQ messages 182
- MQJMS2007 182
- MQJMS2013 183
- native library, loading 178
- optimizing database query performance 166
- ORA-00988 174
- out-of-memory errors 161
- preventing transactions 171
- Receiver Failure 168
- Receiver timeout setting 165
- reprocessing events 169
- revocation check 177
- server restart 167
- servers fail to start 183
- SQLCODE -289 164
- SQLCODE -444 164
- SQLCODE: -1225 164
- SQLCODE: 0964C 164
- SSL connections 174
- SSL handshake fails 180
- stopping Document Manager 181
- StringIndexOutOfBounds 168
- tab headings 185
- TCPC0003E 178
- threads, hanging 181
- VBaseException 180
- WebSphere Application Server shortcut 184

Typographic conventions 2

U

- Updating
 - maps 27
- Uploading
 - CPA 36
 - transports 48
- URI, restriction 170
- Using the Destination Queue 87

V

- Validation errors
 - viewing 117
- Values 107, 109
 - Document Viewer 113, 114
 - Test Partner Connection 95
- Viewers
 - AS Viewer 106
 - Document Viewer 111
 - ebMS Viewer 120
 - Event Viewer 103
 - RosettaNet Viewer 109
- Viewing 93, 121
 - default destinations 47
 - destination 45
 - destination details 90
 - destination list 87
 - digital certificates 54
 - document details 113
 - document processing details, RosettaNet Viewer 110
 - documents
 - Document Analysis 92
 - ebMS process details 121
 - ebMS status 122
 - EDI documents 115
 - event details, Event Viewer 105
 - events 113
 - message details, AS Viewer 108
 - partner profile 43
 - permission details 21
 - queued documents 88
 - raw documents 113
 - Raw documents 111, 121
 - receiver details 22
 - RosettaNet process details 110
 - system activity 33, 34
 - validation errors 117

W

- Warning event type 104
- Web Server result codes 95

X

- XML
 - managing formats 24



Printed in USA