IBM WebSphere Partner Gateway Enterprise and
Advanced Editions

Hub Configuration Guide

Version 6.0

IBM WebSphere Partner Gateway Enterprise and
Advanced Editions

Hub Configuration Guide

Version 6.0

Note!

Before using this information and the product it supports, read the information in Appendix E, "Notices," on page 289.

28June2005

This edition applies to WebSphere Partner Gateway Enterprise Edition (5724-L69), version 6.0, and Advanced Edition (5724-L68), version 6.0, and to all subsequent releases and modifications until otherwise indicated in new editions.

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

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

© Copyright International Business Machines Corporation 2004, 2005. All rights reserved.
US Government Users Restricted Rights – Use, duplication or disclosure restricted by GSA ADP Schedule Contract with IBM Corp.

Contents

About this book xi
Audience xi
Typographic conventions xi
Related documents xii

New in this release xiii
New in release 6.0 xiii
New in release 4.2.2 xiii

Chapter 1. Introduction 1
Overview 1
Information needed to set up the hub 2
  Overview of transports 2
  Overview of document flow definitions 3
Overview of document processing 7
Configuring document processing components with handlers 9
  Targets 9
  Document Manager 10
  Gateways 14
Overview of configuring the hub 15
  Setting up the hub 15
  Creating participants 16
  Establishing document connections 16

Chapter 2. Preparing to configure the hub 17
Creating a directory for a file-directory gateway 17
Configuring the FTP server for receiving documents. 17
  Configuring the required directory structure on the FTP server 18
  How files sent over FTP are processed 19
  Additional FTP server configuration 20
  Security considerations for the FTPS server 20
Configuring the hub for the JMS transport protocol 20
  Creating a directory for JMS 21
  Modifying the default JMS configuration 21
  Creating queues and the channel 21
  Adding a Java(TM) run time to your environment 22
  Defining the JMS configuration 22
Using FTP scripts for FTP Scripting targets and gateways 23
Using maps from the Data Interchange Services client 23

Chapter 3. Starting the server and displaying the Community Console 25
Starting WebSphere MQ 25
Starting the WebSphere Partner Gateway components 25
Logging in to the Community Console 26

Chapter 4. Configuring the Community Console 27
Specifying locale information and console branding 27
  Branding the console 27
  Changing the style sheet 28
  Localizing the data on the console 28
Setting the password policy 29
Configuring permissions 29
  How permissions are granted to users 29
  Enabling or disabling permissions 30

© Copyright IBM Corp. 2004, 2005

Chapter 5. Defining targets . . . 31
Overview . . . 31
Uploading user-defined handlers . . . 32
Setting global transport values . . . 32
Setting up an HTTP/S target . . . 33
  Target Details. . . . 33
  Target Configuration . . . 33
  Handlers . . . 34
Setting up an FTP target . . . 34
  Target Details. . . . 34
  Target Configuration . . . 34
  Handlers . . . 35
Setting up an SMTP target . . . 35
  Target Details. . . . 35
  Target Configuration . . . 35
  Schedule . . . 36
Setting up a JMS target . . . 36
  Target Details. . . . 36
  Target Configuration . . . 36
  Handlers . . . 37
Setting up a File-system target . . . 38
  Target Details. . . . 38
  Target Configuration . . . 38
  Handlers . . . 38
Setting up an FTP Scripting target . . . 39
  Creating the FTP script . . . 39
  FTP scripting commands . . . 39
  Target Details. . . . 40
  Target Configuration . . . 41
  User-Defined Attributes . . . 41
  Schedule . . . 42
  Handlers . . . 42
Setting up a target for a user-defined transport . . . 42
Modifying configuration points . . . 43
  Preprocess . . . 43
  SyncCheck. . . . 45
  Postprocess . . . 46
  Modifying the Configured List . . . 47

Chapter 6. Configuring fixed workflow steps and actions . . . 49
Uploading handlers . . . 49
Configuring fixed workflows . . . 50
  Inbound workflows. . . . 50
  Outbound workflow . . . 51
Configuring actions. . . . 51
  Modifying a user-defined action . . . 51
  Creating actions . . . 52

Chapter 7. Configuring document flows . . . 55
Overview . . . 55
  Step 1: Make sure the document flow definition is available . . . 55
  Step 2: Create interactions . . . 56
  Step 3: Create participant profiles, gateways, and B2B capabilities . . . 56
  Step 4: Activate connections . . . 56
  An example flow . . . 57
Binary documents . . . 58
EDI documents with Pass Through action . . . 59
  Creating document flow definitions . . . 59
  Creating interactions . . . 60
RosettaNet documents. . . . 60

Overview 60
RNIF and PIP document flow packages 61
Creating document flow definitions 63
Configuring attribute values 64
Creating interactions 65
Web services 68
Identifying the participants for a Web service 68
Creating document flow definitions 69
Creating interactions 72
Restrictions and limitations of Web service support 72
cXML documents 73
Overview 73
Creating document flow definitions 76
Creating interactions 76
Custom XML documents 77
Overview 77
Creating a protocol definition format 77
Creating a document definition flow 78
Creating an XML format 78
Using validation maps. 79
Adding validation maps 79
Associating maps with document flow definitions 79
Viewing documents 80

Chapter 8. Configuring EDI document flows. 81
Overview of EDI 81
The EDI interchange structure 81
Maps 83
Overview of XML and ROD documents 84
XML documents 84
ROD documents 84
Splitters and multiple documents 84
Overview of creating document flows and setting attributes 85
Step 1: Make sure the document flow definition is available 85
Step 2: Create interactions 86
Step 3: Create participant profiles, gateways, and B2B capabilities 86
Step 4: Activate connections 86
Overview of possible flows 87
EDI to EDI flow 87
EDI to XML or ROD flow 88
XML or ROD to EDI flow 88
Multiple XML or ROD documents to EDI interchange flow 89
XML to ROD or ROD to XML flow 90
XML to XML or ROD to ROD flow 91
How EDI interchanges are processed 91
How XML or ROD documents are processed 94
Setting up the EDI environment 95
Enveloper 95
Envelope profiles 96
Connection profiles 101
Control numbers 103
Control number initialization 105
Current control numbers 106
General steps for defining document exchanges 106
Importing maps 107
Setting up an EDI to EDI flow. 108
Setting up an EDI to XML or ROD flow 110
Setting up an XML or ROD to EDI flow 112
Setting up multiple XML or ROD documents in one file to EDI flow 113
Setting up an XML to ROD or ROD to XML document flow. 114
Setting up an XML to XML or ROD to ROD flow 115

Setting up acknowledgments 115
Adding an acknowledgment to the document flow 117
Viewing EDI interchanges and transactions 118

Chapter 9. Creating the Community Manager profile and B2B capabilities 119
Creating the Community Manager profile 119
Setting up B2B capabilities 120

Chapter 10. Creating gateways 123
Overview. 123
Setting up global transport values 124
Configuring a forward proxy 125
Setting up an HTTP gateway 125
Gateway Details 126
Gateway Configuration 126
Setting up an HTTPS gateway 127
Gateway Details 127
Gateway Configuration 127
Setting up an FTP gateway 128
Gateway Details 128
Gateway Configuration 128
Setting up an SMTP gateway 129
Gateway Details 129
Gateway Configuration 129
Setting up a JMS gateway 130
Gateway Details 130
Gateway Configuration 130
Setting up a file-directory gateway 132
Gateway Details 132
Gateway Configuration 132
Setting up an FTPS gateway 133
Gateway Details 133
Gateway Configuration 133
Setting up an FTP Scripting gateway 134
Creating the FTP script 134
FTP script commands 135
FTP Scripting gateways 135
Gateway Details 136
Gateway Configuration 136
User-Defined Attributes 136
Schedule 137
Configuring handlers. 137
Setting up a gateway for a user-defined transport 138
Specifying a default gateway 138

Chapter 11. Creating participants and their B2B capabilities 139
Creating participant profiles 139
Setting up B2B capabilities 140

Chapter 12. Managing connections 143
Overview. 143
Activating participant connections 143
Specifying or changing attributes. 144

Chapter 13. Setting up security for inbound and outbound exchanges. 147
Security terms and concepts 147
Security mechanisms and protocols used in WebSphere Partner Gateway 147
The iKeyman utility 148
Community Console 148
Key stores and trust stores 148

Certificate chains . . . 150
Primary and secondary certificates . . . 150
Changing the encryption strength . . . 150
Creating and installing SSL certificates . . . 151
SSL handshake . . . 151
Inbound SSL certificates . . . 152
Outbound SSL certificate . . . 154
Adding a Certificate Revocation List (CRL) . . . 156
Enabling access to CRL distribution points . . . 156
Creating and installing signature certificates . . . 157
Inbound signature certificate . . . 157
Outbound signature certificate. . . . 158
Creating and installing encryption certificates . . . 159
Inbound encryption certificate . . . 160
Outbound encryption certificate . . . 161
Configuring inbound SSL for the Console and Receiver . . . 162
Certificate overview . . . 163

Chapter 14. Finishing the configuration . . . 165
Enabling the use of APIs . . . 165
Specifying the queues used for events . . . 165
Specifying alertable events . . . 166
Updating a user-defined transport . . . 167

Appendix A. Basic examples . . . 169
Basic Configuration – Exchanging passthrough EDI documents. . . . 169
Configuring the hub . . . 169
Creating participants and participant connections . . . 171
Basic configuration - Setting up security for inbound and outbound documents . . . 174
Setting up SSL authentication for incoming documents . . . 175
Setting up encryption . . . 177
Setting up document signing . . . 178
Extending the basic configuration . . . 180
Creating an FTP target . . . 180
Setting up the hub to receive binary files . . . 180
Setting up the hub for custom XML documents . . . 181

Appendix B. EDI examples . . . 185
EDI to ROD example . . . 185
De-enveloping and transforming an EDI interchange . . . 185
Adding a TA1 to the exchange . . . 190
Adding an FA map . . . 194
EDI to XML example . . . 197
Importing the transformation map . . . 198
Verifying the transformation map and document flow definitions . . . 198
Configuring the target . . . 199
Creating the interactions. . . . 199
Creating the participants . . . 199
Creating the gateways . . . 200
Setting up B2B capabilities . . . 201
Activating the connections . . . 202
XML to EDI example . . . 202
Importing the transformation map . . . 203
Verifying the transformation map and document flow definitions . . . 203
Configuring the target . . . 203
Creating the interactions. . . . 204
Creating the participants . . . 204
Creating the gateways . . . 205
Setting up B2B capabilities . . . 206
Creating the envelope profile . . . 207

Creating the XML format . . . 207
Activating the connections . . . 208
Configuring attributes . . . 208
ROD to EDI example . . . 209
Importing the transformation map . . . 209
Verifying the transformation map and document flow definitions . . . 210
Configuring the target . . . 210
Creating the interactions . . . 211
Creating the participants . . . 211
Creating the gateways . . . 212
Setting up B2B capabilities . . . 213
Creating the envelope profile . . . 214
Activating the connections . . . 214
Configuring attributes . . . 215

Appendix C. Additional RosettaNet information . . . 217
Deactivating PIPs . . . 217
Providing failure notification . . . 217
0A1 PIP . . . 217
Updating contact information . . . 217
Editing RosettaNet attribute values . . . 218
Creating PIP document flow packages . . . 219
Creating the XSD files . . . 219
Creating the XML file . . . 226
Creating the package . . . 228
About validation . . . 229
Cardinality . . . 229
Format . . . 229
Enumeration . . . 230
PIP document flow package contents . . . 230
0A1 Notification of Failure V1.0 . . . 230
0A1 Notification of Failure V02.00 . . . 231
2A1 Distribute New Product Information . . . 231
2A12 Distribute Product Master . . . 233
3A1 Request Quote . . . 233
3A2 Request Price and Availability . . . 234
3A4 Request Purchase Order V02.00 . . . 235
3A4 Request Purchase Order V02.02 . . . 236
3A5 Query Order Status . . . 238
3A6 Distribute Order Status . . . 239
3A7 Notify of Purchase Order Update . . . 240
3A8 Request Purchase Order Change V01.02 . . . 241
3A8 Request Purchase Order Change V01.03 . . . 242
3A9 Request Purchase Order Cancellation . . . 244
3B2 Notify of Advance Shipment . . . 244
3B3 Distribute Shipment Status . . . 245
3B11 Notify of Shipping Order . . . 246
3B12 Request Shipping Order . . . 247
3B13 Notify of Shipping Order Confirmation . . . 248
3B14 Request Shipping Order Cancellation . . . 249
3B18 Notify of Shipping Documentation . . . 250
3C1 Return Product . . . 251
3C3 Notify of Invoice. . . . 252
3C4 Notify of Invoice Reject . . . 253
3C6 Notify of Remittance Advice . . . 253
3C7 Notify of Self-Billing Invoice . . . 254
3D8 Distribute Work in Process . . . 255
4A1 Notify of Strategic Forecast . . . 256
4A3 Notify of Threshold Release Forecast . . . 257
4A4 Notify of Planning Release Forecast . . . 258
4A5 Notify of Forecast Reply . . . 258

4B2 Notify of Shipment Receipt . . . 259
4B3 Notify of Consumption . . . 260
4C1 Distribute Inventory Report V02.01 . . . 261
4C1 Distribute Inventory Report V02.03 . . . 262
5C1 Distribute Product List. . . . 263
5C2 Request Design Registration . . . 263
5C4 Distribute Registration Status . . . 264
5D1 Request Ship From Stock And Debit Authorization . . . 265
6C1 Query Service Entitlement . . . 266
6C2 Request Warranty Claim . . . 267
7B1 Distribute Work in Process . . . 267
7B5 Notify Of Manufacturing Work Order. . . . 268
7B6 Notify Of Manufacturing Work Order Reply . . . 269

Appendix D. Attributes . . . 271
EDI attributes . . . 271
Envelope profile attributes . . . 271
Document flow definition and connection attributes . . . 275
Data Interchange Services client properties . . . 281
AS attributes . . . 283
RosettaNet attributes . . . 285
Backend Integration attribute . . . 287

Appendix E. Notices . . . 289
Programming interface information . . . 291
Trademarks and service marks . . . 291

Index . . . 293

About this book

This document describes how to configure the IBM $^{(R)}$ WebSphere $^{(R)}$ Partner Gateway server.

Audience

This document is intended for the person responsible for configuring the WebSphere Partner Gateway server, also known as the hub. To configure the hub, you should be the Hub Admin. The Hub Admin has the ability to use all the features of the WebSphere Partner Gateway Community Console to configure and operate the hub.

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.
italics	Text in italics indicates emphasis, book titles, new terms and terms that are defined in the text, variable names, or letters of the alphabet used as letters.
`Italic monospace font`	Text in italic monospace font indicates variable names within monospace-font text.
ProductDir	*ProductDir* represents the directory where the product is installed. All IBM WebSphere Partner Gateway product pathnames are relative to the directory where the IBM WebSphere Partner Gateway product is installed on your system.
`%text%` and *`$text`*	Text within percent signs (%) indicates the value of the Windows$^{(R)}$ `text` system variable or user variable. The equivalent notation in a UNIX$^{(R)}$ environment is $*text*, indicating the value of the *text* UNIX environment variable.
Underlined colored text	Underlined colored text indicates a cross-reference. Click the text to go to the object of the reference.
Text in a blue outline	(In PDF files only) 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.

© Copyright IBM Corp. 2004, 2005

Table 1. Typographic conventions (continued)

Convention	Description
`[ ]`	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, <*server_name*><*connector_name*>tmp.log.
`/, \`	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 this documentation or read it directly online at the following site:
http://www.ibm.com/software/integration/wspartnergateway/library/infocenter

Note: Important information about this product may be available in Technical Support Technotes and Flashes issued after this document was published. These can be found on the WebSphere Business Integration Support Web site, http://www.ibm.com/software/integration/wspartnergateway/support. Select the component area of interest and browse the Technotes and Flashes sections.

New in this release

New in release 6.0

WebSphere Partner Gateway (which was known as WebSphere Business Integration Connect in previous releases) has the following new features:

- The ability to de-envelope EDI transactions and to validate and transform EDI transactions within those envelopes
- The ability to envelope individual EDI transactions before they are delivered
- The ability to receive multiple record-oriented-data (ROD) and XML documents or EDI interchanges in a single file and to split them into individual documents or interchanges
- The ability to translate among any combination of ROD, XML, and EDI documents
- The introduction of a new transport--FTP Scripting, which can be used for both targets and gateways to communicate with value added networks (VANs) as well as other FTP servers
- The ability to support more than one certificate for certain functions, so that if the primary certificate expires, the secondary certificate can be used
- The ability to send documents from an HTTP or HTTPS gateway through a proxy server to participants

Note that WebSphere Partner Gateway version 6.0 does not support the RC5 algorithm.

New in release 4.2.2

Version 4.2.2 is the first release of the *Hub Configuration Guide*.

© Copyright IBM Corp. 2004, 2005

Chapter 1. Introduction

After you install WebSphere Partner Gateway and before any documents can be exchanged between the Community Manager and participants, you must configure the WebSphere Partner Gateway server (the hub).

This chapter covers the following topics:

- "Overview"
- "Information needed to set up the hub" on page 2
- "Overview of document processing" on page 7
- "Configuring document processing components with handlers" on page 9
- "Overview of configuring the hub" on page 15

Overview

The goal is to enable the Community Manager to send a document or set of documents (electronically) to a participant or to receive a document or set of documents from a participant. The hub manages the receipt of the documents, the transformation to other formats (if required), and the delivery of the documents. The hub can also be configured to provide security for incoming and outgoing documents.

The documents exchanged between the hub and the participant are typically in a standard format and represent a specific business interaction. For example, the participant might sent a purchase order request as a RosettaNet 3A4 PIP, a cXML OrderRequest document, or an EDI-X12 interchange with an 850 transaction. The hub transforms the document into a format that can be used by an application at the Community Manager. Similarly, a Community Manager back-end application might send a purchase order response in its own custom format that is transformed into a standard format. The transformed document is then sent to the participant.

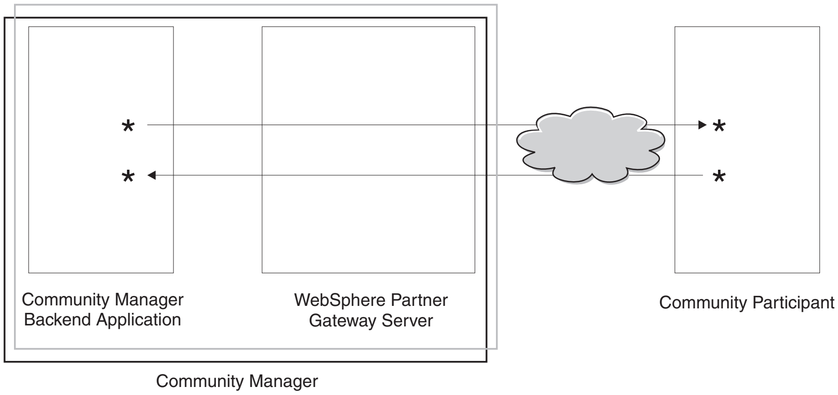

Community Manager Backend Application
WebSphere Partner Gateway Server
Community Participant
Community Manager

Figure 1. How documents flow through the hub

In this guide, you will see how to configure the hub and then how to set up the participants. You will also learn how to configure security for the hub.

© Copyright IBM Corp. 2004, 2005

Notice in Figure 1 on page 1 that the WebSphere Partner Gateway server and the Community Manager back-end application are all owned by the Community Manager. The Community Manager is the company that owns the hub, but the Community Manager is also a participant of the hub. As you will see in later chapters, you define a profile for the Community Manager just as you do for participants.

Note: This document shows you how to create connections that flow from the Community Manager back-end application to a participant gateway and from a participant to the Community Manager gateway. After the documents arrive at the Community Manager gateway, you will probably want to integrate them with a back-end application, such as WebSphere InterChange Server or WebSphere MQ Broker. The tasks required to integrate between WebSphere Partner Gateway and such back-end applications are defined in the *Enterprise Integration Guide*.

Information needed to set up the hub

You need some information about the types of exchanges in which the Community Manager will participate in order to set up the hub. For example, you need the following information:

- Which types of documents (for example, EDI-X12 or custom XML) will the Community Manager and its participants be sending through the hub?
- Which types of transports (for example, HTTP or FTP) will the Community Manager and its participants use to send the documents?
- Will a document coming into the hub need to be split into multiple documents, or will individual documents coming into the hub need to be grouped before being sent on?
- Will the documents be transformed before being delivered?
- Will the documents be validated before being delivered?
- Will the documents be encrypted or digitally signed or use some other security technique?

When this information is determined, you are ready to begin setting up the hub.

After you define the hub, you can define your participants, using information (such as IP address and DUNS numbers) that is supplied to you by the participants. As noted earlier, you also define the Community Manager as a special type of participant of the hub.

Overview of transports

Documents can be sent from participants to the WebSphere Partner Gateway (the hub) over a variety of transports. A participant can send documents over public networks using HTTP, HTTPS, JMS, FTP, FTPS, FTP Scripting, SMTP, or a file directory. A participant can send documents over a Value Added Network (VAN), a private network, using the FTP Scripting Transport. You can create your own transport, as well.

Note: When the file-directory transport is used between a participant and the hub, the administrator should take care of all the security-related issues.

Similarly, the hub sends documents to back-end applications over a variety of transports. The most commonly used transports between the hub and back-end applications are HTTP, HTTPS, JMS, and file-directory.

Figure 2 shows the various transports that can be used.

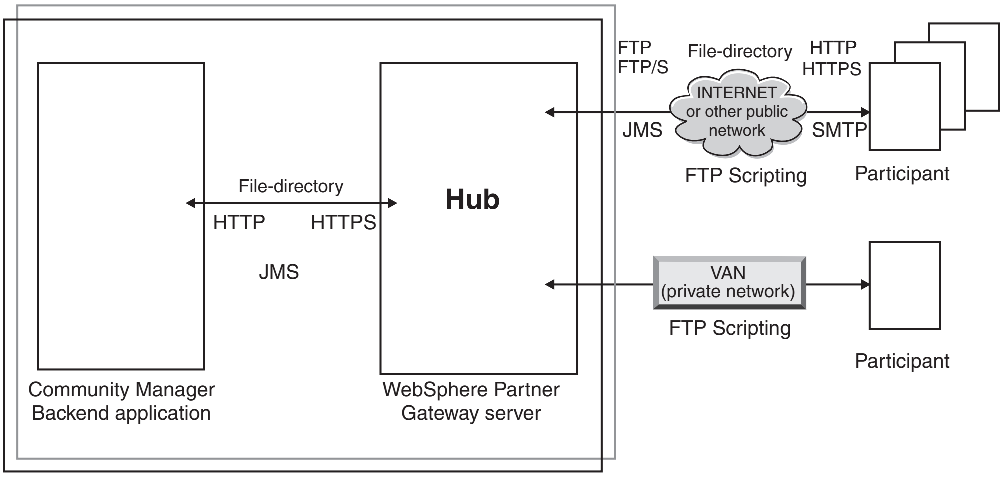


Figure 2. Transports supported by WebSphere Partner Gateway

The type of transport used to send and receive documents affects the setup of targets and gateways. A target is an entry point into the hub--the place where documents sent by participants or back-end applications are received at the hub. A gateway is an entry point into the participant's computer or the back-end system--the place where the hub sends documents. To prepare to use the FTP, FTPS, FTP Scripting, JMS, and file-directory transports, you have to do some setup work, as described in Chapter 2, "Preparing to configure the hub," on page 17.

Overview of document flow definitions

When you set up the interchange of documents between the participants and the Community Manager, you specify several things about the document:

- The *packaging* that surrounds the document
- The business *protocol* that defines the document
- The type of *document flow*

The packaging of the document, the protocol of the document, and the document flow make up the *document flow definition*. The document flow definition gives information to the hub about how to process the document. For example, suppose you use the system-supplied document flow definition of:

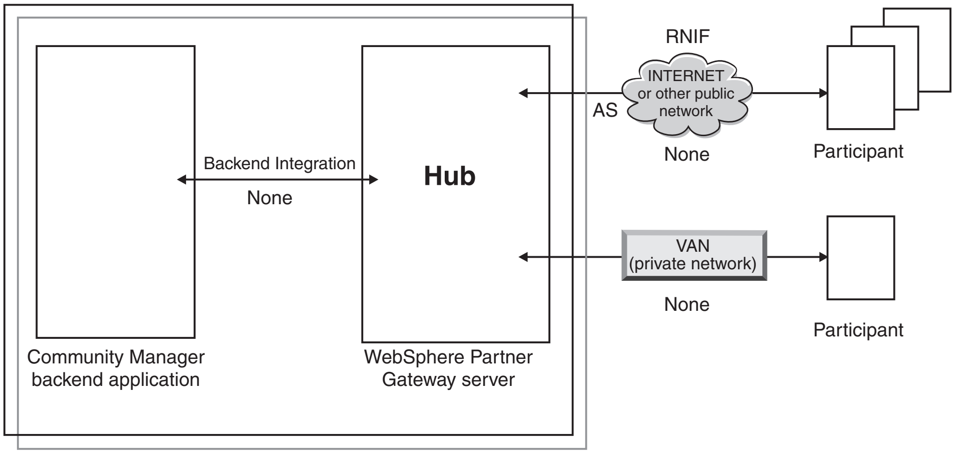
- Packaging: AS
- Protocol: EDI-X12
- Document flow: ISA

The hub extracts the AS header information (and uses it to help determine the source and destination of the document). It knows where to find, within the document, certain information, based on its placement in the document. The three parts of the document flow definition have attributes assigned to them. You can modify or add to the system-supplied attributes.

Packaging

The packaging provides information that pertains to the transmission of the document. As mentioned in the previous section, if the packaging is AS, the hub uses information in the AS header to determine the source and destination for the document. If a participant is sending a RosettaNet PIP to the Community Manager, the PIP is packaged as RNIF.

Figure 3 shows you the packaging types that can be set for documents exchanged between the hub and a community participant and between the hub and a back-end application.



RNIF
INTERNET or other public network
AS
None
Participant
Backend Integration
None
Hub
VAN (private network)
None
Participant
Community Manager backend application
WebSphere Partner Gateway server

Figure 3. Document packaging types

Packages are associated with specific protocols. For example, a participant must specify RNIF packaging when sending a RosettaNet document to the hub.

Backend Integration: As shown in Figure 3, Backend Integration is available only between the hub and the back-end application. When you specify Backend Integration packaging, documents sent by the hub to the back-end system have special header information added. Similarly, when a back-end application sends documents with a packaging of Backend Integration to the hub, it must add header information. The Backend Integration package, and the requirements for the header information, are described in the *Enterprise Integration Guide*.

AS: The AS package is available only between participants and the hub. The AS package can be used for documents that adhere to the AS1 or AS2 standards. AS1 is a standard used for securely transmitting documents over SMTP, and AS2 is a standard used for securely transmitting documents over HTTP or HTTPS. Documents sent by a participant with a packaging of AS have either AS1 or AS2 header information. Documents sent to a participant that expects AS1 or AS2 headers must be packaged (at the hub) as AS.

None: The None package can be used to send and receive documents between the hub and participants and between the hub and a back-end application. No header information is added (or expected) when a document is packaged as None.

RNIF: The RNIF package is provided on the installation medium. You upload the RNIF package (along with any PIPs you want exchanged), as described in "RosettaNet documents" on page 60. The RNIF package is used to send RosettaNet documents from the participant to the hub or from the hub to the participant.

N/A: Some document flows either end in WebSphere Partner Gateway or originate internally from WebSphere Partner Gateway. For document flows ending in WebSphere Partner Gateway, no packaging is required. Document flows originating internally from WebSphere Partner Gateway do not have source packaging. Therefore, for such flows, the packaging is specified as N/A.

For most one-way transmissions between the participant and the Community Manager (or vice versa), WebSphere Partner Gateway receives a document from a participant and sends it to the Community Manager. In WebSphere Partner Gateway, when creating the participant connection, you specify the packaging in which WebSphere Partner Gateway will receive the document and the packaging WebSphere Partner Gateway will use to send the document. In Figure 4, a document packaged as AS is flowing from a participant to the Community Manager back-end. The document is delivered to the Community Manager gateway with no transport headers. In Figure 4, one action is associated with the exchange of documents.

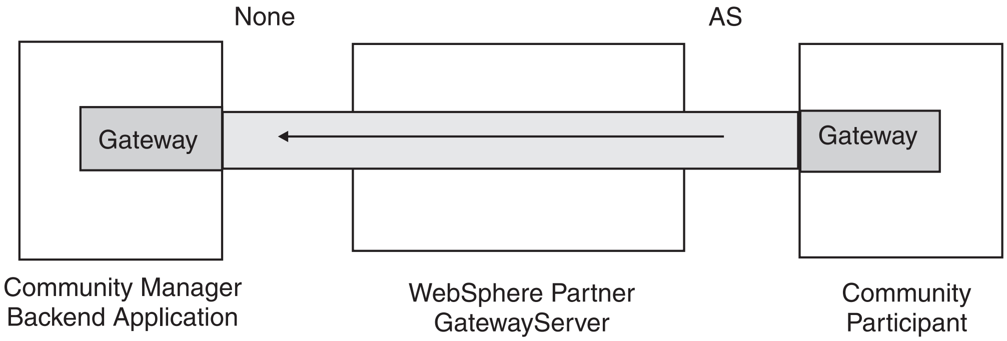

None
AS
Gateway
Gateway
Community Manager Backend Application
WebSphere Partner GatewayServer
Community Participant

Figure 4. Typical one-way connection

Certain protocols, however, involve multiple activities (such as de-enveloping and transformation), some of which occur as intermediate parts of the overall exchange. For example, if a participant sends an EDI interchange to the hub, for eventual delivery to the Community Manager, the interchange is de-enveloped and the individual EDI transactions are processed. The original EDI interchange has a package associated with it when it is sent from the participant. However, because the interchange itself is not delivered to the Community Manager (it is de-enveloped within the hub and no additional processing of the interchange occurs), packaging of the interchange does not apply. When you set up the interaction for the de-enveloping step, therefore, you enter a package on the sending side but you specify N/A for the receiving side.

The process for setting up the document flow definitions required for an EDI exchange is described in Chapter 8, “Configuring EDI document flows,” on page 81.

Protocols

The protocols that are provided with the system are:

- Binary

  The Binary protocol can be used with AS, None, and Backend Integration packages. A binary document contains no data about the source or destination of the document.
- EDI-X12, EDI-Consent, EDI-EDIFACT

  These EDI protocols can be used with the AS or None packages. As described in “N/A” on page 4, if the EDI transaction or interchange originates from the hub or ends at the hub, you specify N/A for the package. X12 and EDIFACT are EDI standards used for the exchange of data. EDI-Consent refers to content types other than X12 or EDIFACT.

- Web Service

  Web service requests can be used only with the None package.
- cXML

  cXML documents can be used only with the None package.
- XMLEvent

  XMLEvent is a special protocol used to provide event notification for documents flowing to and from a back-end application. It can be used only with the Backend Integration package. This protocol is described in the *Enterprise Integration Guide*.

When you upload RNIF packages, you also get the associated protocols (RosettaNet and RNSC). RosettaNet (which is the protocol used between the participant and the hub) is associated with the RNIF package. RNSC (which is the protocol used between the hub and the Community Manager back-end application) is associated with the Backend Integration package.

For EDI transactions or XML or ROD documents that will be transformed, you import a transformation map from the Data Interchange Services client. In the Data Interchange Services client, dictionaries are defined for the protocol associated with this transformation. A dictionary contains information about all of the EDI document definitions, segments, composite data elements, and data elements that make up the EDI Standard. For detailed information about a particular EDI Standard, consult the appropriate EDI Standards manuals. For information about the Data Interchange Services client, refer to the *Mapping Guide* or to the online help provided with the Data Interchange Services client.

Note: The sender and receiver IDs must be part of the ROD document definition associated with the transformation map. The information necessary to determine the document type and dictionary values must also be present in the document definition. Make sure that the Data Interchange Services client mapping specialist is aware of these requirements when creating the transformation map.

You can create custom protocols to define exactly how you want a document to be structured. For XML documents, you can define an XML format, as described in “Custom XML documents” on page 77.

Document Flow

The document itself can be in a variety of formats. The system-supplied document flows and their associated protocols are:

- Binary, which can be used with the Binary protocol
- ISA, which represents the X12 interchange (envelope) and which is associated with the EDI-X12 protocol
- BG, which represents the EDI Consent envelope and which is associated with the EDI-Consent protocol
- UNB, which represents the EDIFACT envelope and which is associated with the EDI-EDIFACT protocol
- XMLEvent, which can be used with the XMLEvent protocol

The following list describes other types of documents and the source of their definition:

- A RosettaNet PIP (which you upload from the installation medium), which can be used with the RosettaNet protocol
- A Web service (which you upload as a WSDL file), which can be used with the Web Service protocol
- A cXML document (which you create by specifying the type of cXML document)
- A specific EDI standard transaction, which you import from the Data Interchange Services client
- A record-oriented-data (ROD) or XML document, which you import from the Data Interchange Services client

You can also create your own document flows, as described in “Custom XML documents” on page 77.

Overview of document processing

Before you begin setting up the hub, it is helpful to review the components of WebSphere Partner Gateway and how they are used to process documents.

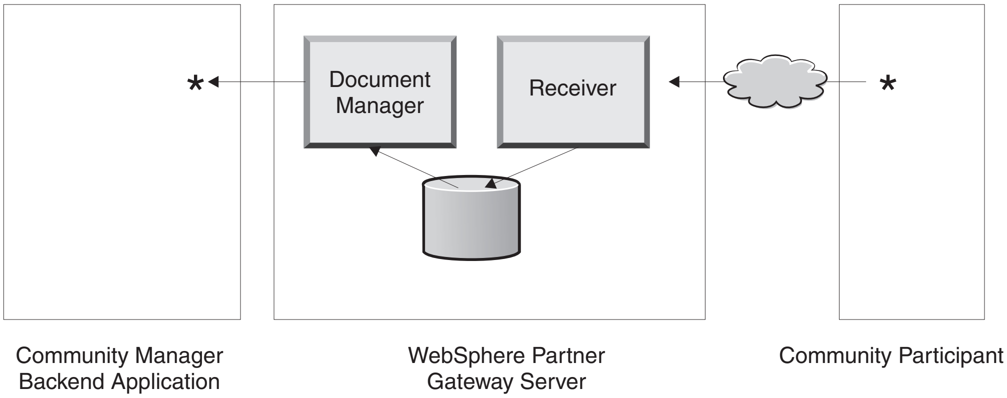

Document Manager
Receiver
*
*
Community Manager Backend Application
WebSphere Partner Gateway Server
Community Participant

Figure 5. The Receiver and Document Manager components

Figure 5 is an example of how a document is sent from a participant, received at the hub, processed at the hub, and sent to a Community Manager back-end application.

Note: For purposes of illustration, the drawings in this document show one Receiver and one Document Manager, installed on the same server machine. (Not shown is the third component, the Console, which is the interface to WebSphere Partner Gateway.) You can, in fact, have multiple occurrences of these components, and they can be installed on different servers. All components must use the same common file system. See the *Installation Guide* for information about the different topologies that can be used to set up WebSphere Partner Gateway.

A document is received into WebSphere Partner Gateway by the Receiver component. The Receiver is responsible for monitoring transports for inbound documents, retrieving the documents that arrive, performing some basic processing on them, and then queueing them so that the Document Manager can retrieve them.

Receivers are transport-specific. Instances of transport-specific receivers are known as *targets*. You set up a target for each type of transport the hub will support. For example, if participants are going to send documents over HTTP, you set up an HTTP target to receive them.

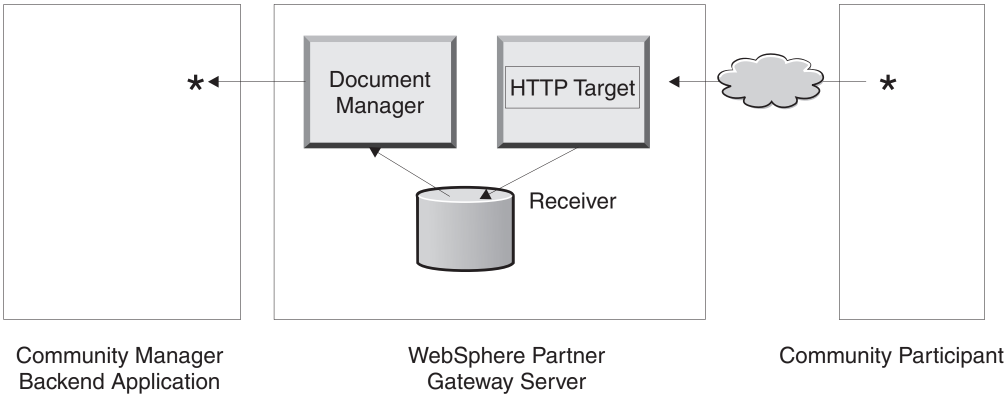

*
Document Manager
HTTP Target
*
Receiver
Community Manager Backend Application
WebSphere Partner Gateway Server
Community Participant

Figure 6. An HTTP target

If the Community Manager back-end application is going to send documents over JMS, you set up a JMS target at the hub to receive them.

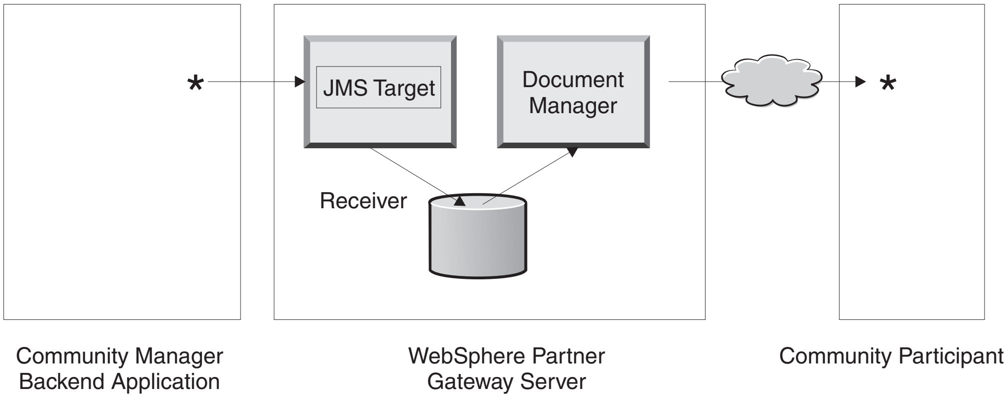

*
JMS Target
Document Manager
*
Receiver
Community Manager Backend Application
WebSphere Partner Gateway Server
Community Participant

Figure 7. A JMS target

As described in “Overview of transports” on page 2, WebSphere Partner Gateway supports a variety of transports, but you can also upload your own user-defined transport to define a target (as described in “Setting up a target for a user-defined transport” on page 42).

The Receiver sends the document to a shared file system. For multiple documents that are in a single file (for example, XML or ROD documents or EDI interchanges sent together), the target splits the documents or interchanges before sending them to the shared file system. The Document Manager component retrieves the document from the file system and determines the routing information and whether any transformation is required.

For example, the Community Manager might send an EDI-X12 document with None packaging to the hub, for delivery to a participant that is expecting the EDI-X12 document with AS2 packaging. The participant provides the HTTP URL where the AS2-packaged document should be delivered, and the Document Manager packages the document as expected by the participant. The Document Manager uses the configuration of the gateway for that participant (which must have been set up for the HTTP URL where the participant expects to receive AS2 documents) to send the document to the participant.

Configuring document processing components with handlers

This section describes, in more detail, the components of WebSphere Partner Gateway and shows you the various points at which you can (or must) change the system-supplied behavior of the components for processing a business document.

You use *handlers* to change the system-supplied behavior of targets, gateways, fixed workflow steps, and actions. There are two types of handlers--those supplied by WebSphere Partner Gateway and those that are user-defined. See the *Programmer Guide* if you want information about creating handlers.

After a handler is created, you upload it to make it available. You upload only user-defined handlers. The handlers supplied by WebSphere Partner Gateway are already available.

The sections that follow describe the processing points at which you can specify handlers.

Targets

Targets have three *configuration points* for which handlers can be specified--Preprocess, SyncCheck, and Postprocess.

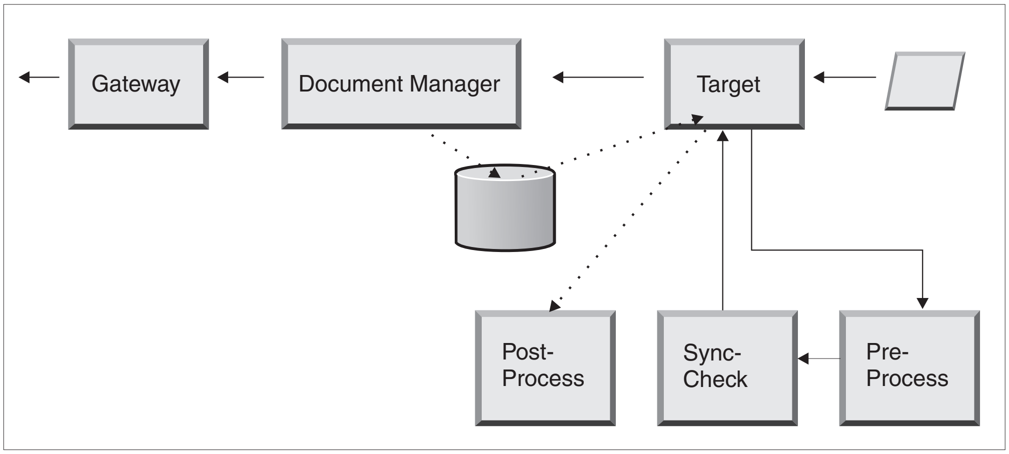


Figure 8. Target configuration points

The processing occurs in the following order:

1. The Receiver calls the Preprocess and SyncCheck steps after it receives the document.
2. It then calls the Document Manager to process the document.
3. In the case of synchronous flows, the Document Manager provides a Sync Response. The Receiver then calls the Postprocess step with the response returned from the Document Manager.

The steps are described in the following sections:

- Preprocess

  The Preprocess step is generally used for any processing on the document that needs to be accomplished before the document can be processed by the

Document Manager. For example, if you will be receiving multiple ROD documents in a single file, you configure the ROD splitter handler when you define the target. The ROD splitter, along with two other system-supplied splitters, are available for you to use when you set up a target. If you create additional handlers for the preprocess step, those handlers are also available.

See "Preprocess" on page 43 for information about configuring the Preprocess configuration point.

- SyncCheck

  SyncCheck is used to determine whether WebSphere Partner Gateway should process the document synchronously or asynchronously. For example, in the case of AS2 documents received over HTTP, it determines whether an MDN (message disposition notification) should be returned synchronously over the same HTTP connection. WebSphere Partner Gateway supplies a variety of handlers for synchronous checking. The list of handlers varies, depending on the transport associated with the target.

  SyncCheck applies only to those transports (such as HTTP, HTTPS, and JMS) that support synchronous transmission.

  Note: For AS2, cXML, RNIF, or SOAP documents that will be used in synchronous exchanges, you must specify the associated SyncCheck handler on the HTTP or HTTPS target.

  See "SyncCheck" on page 45 for information about configuring the SyncCheck configuration point.

- Postprocess

  Postprocessing is used for processing the response document that the hub sends as the result of a synchronous transaction.

  See "Postprocess" on page 46 for information about configuring the Postprocess configuration point.

Document Manager

Documents received by targets are picked up by the Document Manager from the common file system for further processing. The Document Manager uses participant connections to route the documents. All documents flowing through the Document Manager go through a series of workflows: fixed inbound workflow, variable workflow, and fixed outbound workflow. At the end of the inbound workflow, the participant connection is determined. The participant connection specifies the action to perform on this document. After executing the variable workflow, the Document Manager executes the fixed outbound workflow on this document.

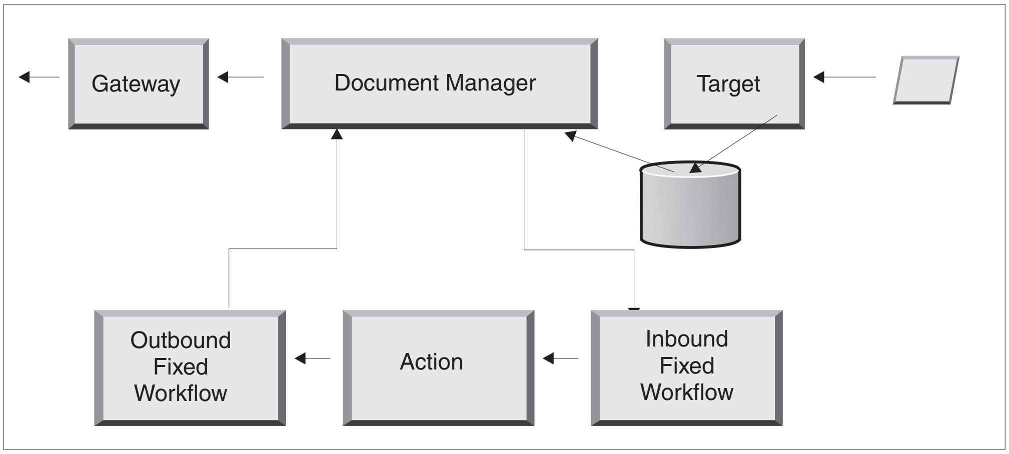


Figure 9. Fixed workflows and actions

Figure 9 shows the path that a document such as a RosettaNet PIP or a Web service would take. Some documents, however, require several configured flows. For example, an EDI interchange can consist of multiple transactions. The first flow uses an action to de-envelope the set of individual transactions. Each of these transactions is reintroduced and processed in its own configured flow.

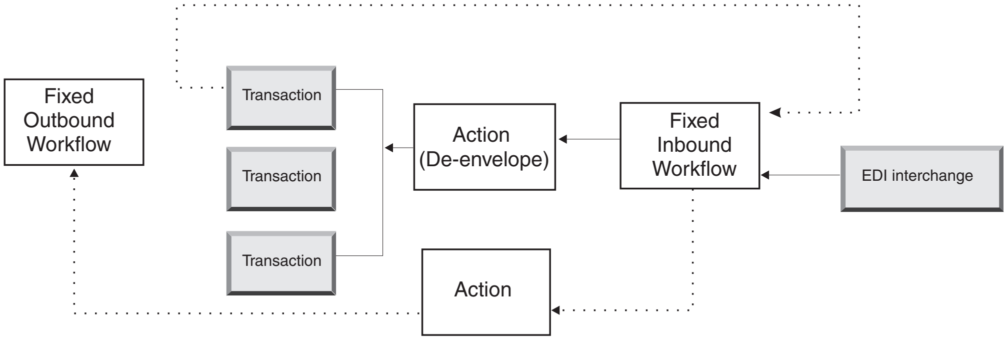


Figure 10. Fixed workflows and actions for an EDI interchange

Inbound fixed workflow

The Inbound fixed workflow consists of the standard set of processing steps performed on all documents coming into the Document Manager from a Receiver. The workflow is fixed because the number and types of steps are always the same. Through user exits, however, you can provide customized handlers for processing the following steps: Protocol Unpackaging and Protocol Processing. The last step of inbound fixed workflow performs participant connection lookup, which determines the variable workflow that executes for this business document.

For example, if an AS2 message is received, the message is decrypted, and the sender and receiver business IDs are retrieved. The inbound fixed workflow steps convert the AS2 document into plain text for further processing by WebSphere Partner Gateway and extract information to determine the action for the message.

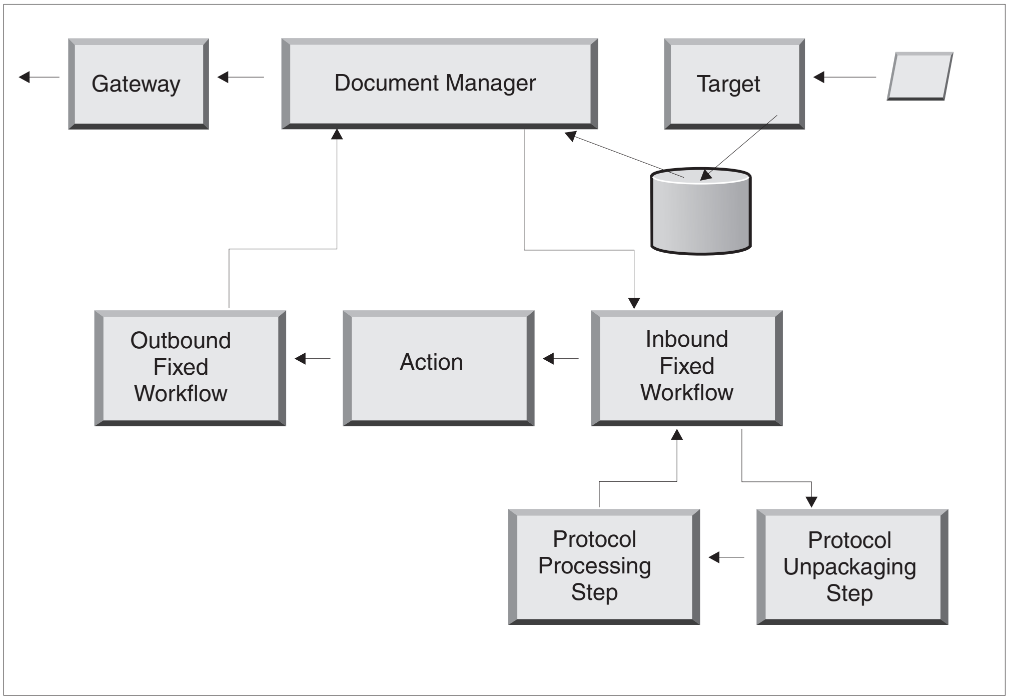


Figure 11. Inbound fixed workflow steps

Protocol Unpackaging: During Protocol Unpackaging, a document is unpackaged so that it can be further processed. This process can include decryption, decompression, signature verification, extraction of routing information, user authentication, or business document parts extraction.

WebSphere Partner Gateway provides handlers for RNIF, AS, Backend Integration, and None packaging. If handlers for other packaging types are necessary, they can be developed as user exits. Refer to the *Programmer Guide* for information about writing user exits.

You cannot modify the Protocol Unpackaging step; however, you can add business logic to the step by adding handlers.

See “Configuring fixed workflows” on page 50 for information about configuring this step.

Protocol Processing step: Protocol Processing involves determining protocol-specific information, which might include parsing the message to determine routing information (such as the sender ID and the receiver ID), protocol information, and document flow information. WebSphere Partner Gateway provides processing for a variety of protocols, as listed in “Protocol processing handlers” on page 50. Processing for other protocols—for example, CSV (comma-separated value)—can be provided with a user exit.

You cannot modify the Protocol Processing step; however, you can add business logic to the step by adding handlers.

See “Configuring fixed workflows” on page 50 for information about configuring this step.

You can use the default handler that applies to the protocol for your document, or you can specify a different handler for the Protocol Unpackaging and Protocol Processing fixed workflow steps.

Actions

The next step in the processing sequence occurs based on the actions that have been set up for the document exchange. Actions consist of a variable number of steps that can be performed on the document. Examples of actions are validation of a document (so that it conforms to a particular set of rules) and transformation of the document to the format required by the recipient.

If the document has no specific steps required, it can use the system-supplied Pass Through action, which makes no changes to the document.

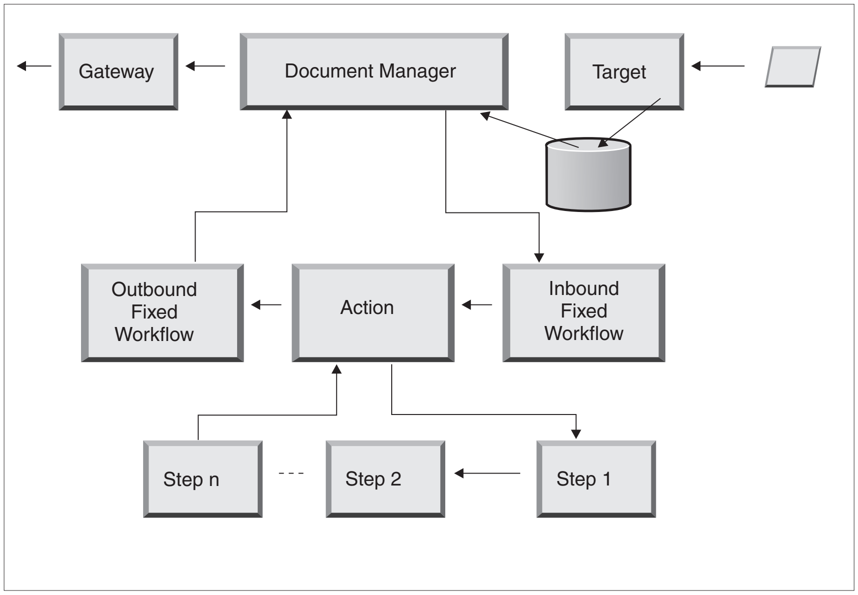


Figure 12. Action steps

You cannot modify a system-supplied action. You can, however, create an action (and add handlers to the configured list) or copy a system-supplied action and then modify the list of handlers.

See "Configuring actions" on page 51 for information about creating or copying a system-supplied action or configuring a user-defined action.

Outbound fixed workflow

The Outbound Fixed Workflow consists of one step—the packaging of the document with its protocol information. For example, if a document has been set up to be received by a back-end application using Backend Integration packaging, certain header information is added to the document before it is passed to the gateway.

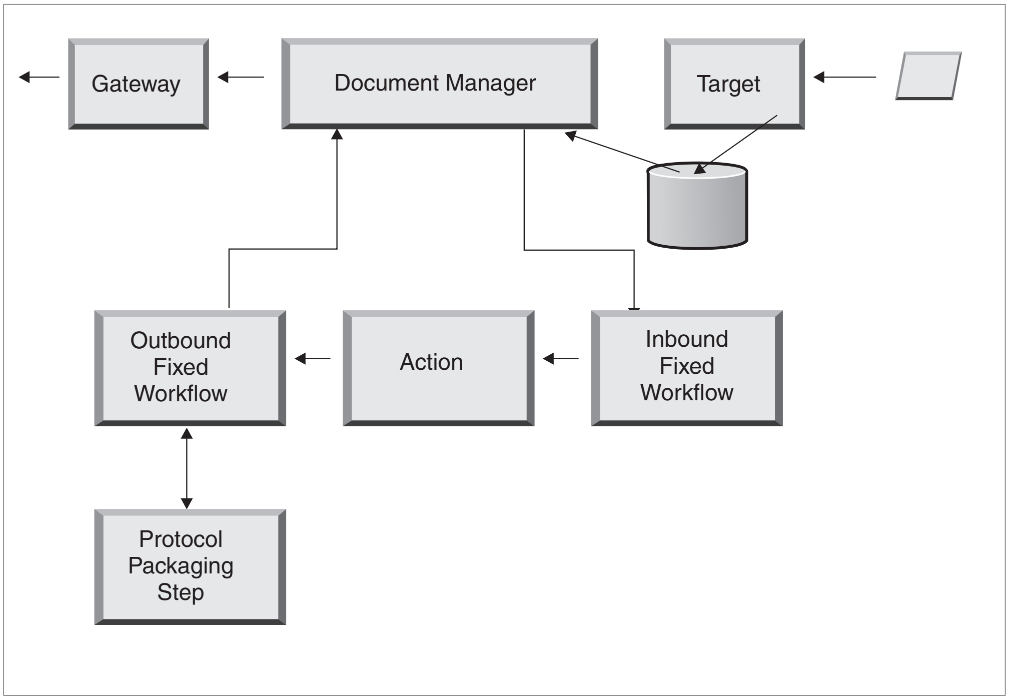


Figure 13. Outbound fixed workflow steps

WebSphere Partner Gateway provides handlers for a variety of packages and protocols, as listed in “Outbound workflow” on page 51. If other packaging handlers are required, they can be developed as user exit steps. Typically these steps take care of one or more of the following processes:

- Assembling or enveloping
- Encrypting
- Signing
- Compressing
- Setting business-protocol-specific transport headers

You cannot modify the Protocol Packaging step; however, you can add business logic to the step by adding handlers.

See “Configuring fixed workflows” on page 50 for information about configuring this workflow step.

Gateways

After the document leaves the Document Manager, it is sent, from the Gateway, to the intended recipient. The Gateway has two configuration points—Preprocess and Postprocess.

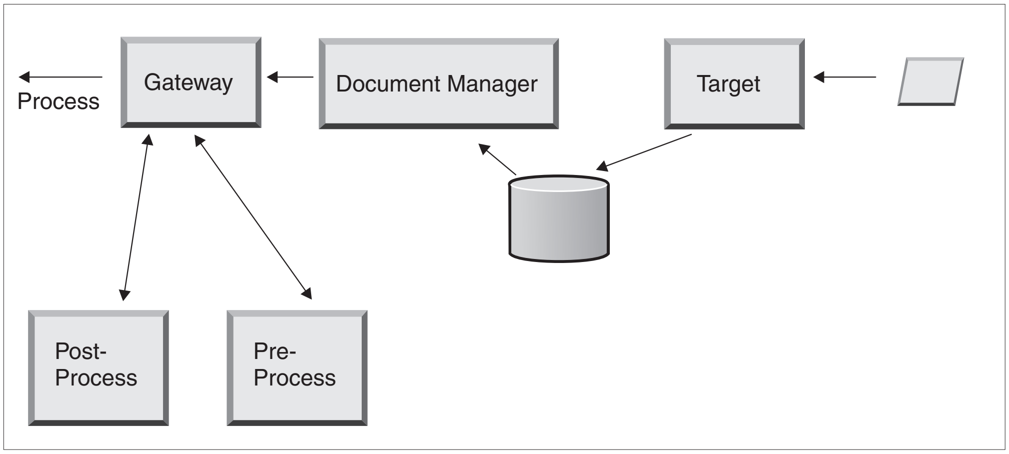


Figure 14. Gateway configuration points

- Preprocess

  Preprocess affects the processing of a document before it is sent to the recipient. (Process is the actual sending of the document.) No handlers are supplied by the system to configure the Preprocess step; however, you can upload a user-defined handler.
- Postprocess

  Postprocess acts on the results of the document transmission (for example, on the response it receives from the recipient during a synchronous transmission). No handlers are supplied by the system to configure the Postprocess step; however, you can upload a user-defined handler.

See "Configuring handlers" on page 137 for information about configuring the Preprocess and Postprocess steps.

Overview of configuring the hub

After you have analyzed your business needs, as described in "Information needed to set up the hub" on page 2, you set up the hub and create your participant profiles. This section provides a high-level overview of the tasks involved.

Note: As you are configuring the hub, refer to the *Administrator Guide* for information on event codes and for troubleshooting tips.

Setting up the hub

As the Hub Administrator, you perform the following tasks to set up the hub:

1. Perform any preliminary setup (if required) for the transports you are using. The preliminary setup is described in Chapter 2, "Preparing to configure the hub," on page 17.
2. Optionally, customize the console and change the default password and permissions policy. These tasks are described in Chapter 4, "Configuring the Community Console," on page 27.
3. Create targets for the types of transports that will be used to receive documents at the hub (from the Community Manager and from participants). Creating targets is described in Chapter 5, "Defining targets," on page 31.

Note: If you will be configuring the target with user-defined handlers, you must upload the handlers before creating the target. Uploading handlers is described in "Uploading user-defined handlers" on page 32.

4. Configure any inbound workflow steps or actions. This is an *optional* step and is needed only by those who have specific requirements for document processing not provided by WebSphere Partner Gateway. If you do not need to change the system-supplied behavior of workflows or actions, skip this step. Configuring workflow steps and actions is described in Chapter 6, "Configuring fixed workflow steps and actions," on page 49.

   Note: You must upload the user-defined handlers before configuring workflows or actions. Uploading user-defined handlers is described in "Uploading handlers" on page 49.
5. Create document flow definitions (or verify that the ones you need are already available) to define the types of documents you can send or receive at the hub.
6. Create interactions to indicate the valid combination of two document flow definitions.

   Creating document flow definitions and creating interactions are described in Chapter 7, "Configuring document flows," on page 55 and Chapter 8, "Configuring EDI document flows," on page 81.
7. Create a profile for the Community Manager, providing information about the Community Manager and establishing the types of documents that the Community Manager can send and receive (the B2B capabilities of the Community Manager). Creating the profile is described in Chapter 9, "Creating the Community Manager profile and B2B capabilities," on page 119.

Creating participants

After you set up the hub, you create a profile for each participant that will be exchanging documents with the Community Manager. Only the Hub Admin can create participants.

As the Hub Admin, you can also set up the B2B capabilities of participants, establish the gateways for participants, and set up security profiles for participants. These steps can alternatively be performed by the participants themselves.

Creating participants is described in Chapter 11, "Creating participants and their B2B capabilities," on page 139. Creating gateways is described in Chapter 10, "Creating gateways," on page 123. Setting up security profiles is described in Chapter 13, "Setting up security for inbound and outbound exchanges," on page 147.

Establishing document connections

After you configure the hub and create participant profiles, you are ready to set up connections. Connections indicate the valid combinations of senders and receivers and the documents they can exchange. Managing connections is described in Chapter 12, "Managing connections," on page 143.

Chapter 2. Preparing to configure the hub

In the next few chapters, you will be setting up the targets and gateways described in Chapter 1, “Introduction.” Depending on the types of transports you will be using to receive documents into targets and to send them from gateways, you have to do some setup work.

This chapter covers the following topics:

- “Creating a directory for a file-directory gateway”
- “Configuring the FTP server for receiving documents”
- “Configuring the hub for the JMS transport protocol” on page 20

It also provides a brief overview of the FTP scripts needed for the FTP Scripting targets and gateways, and it describes the Data Interchange Services client, which can be used to create transformation, validation, and functional acknowledgment maps for EDI, XML, and record-oriented-data (ROD) documents.

- “Using FTP scripts for FTP Scripting targets and gateways” on page 23
- “Using maps from the Data Interchange Services client” on page 23

If you are not planning to set up any of these types of targets or gateways, skip this chapter and go to Chapter 3, “Starting the server and displaying the Community Console.”

Creating a directory for a file-directory gateway

If you are going to use a file-directory gateway to send documents to the Community Manager, you must first create a directory on the file system used by the Community Manager.

For example, suppose you wanted to create a directory named FileSystemGateway under the c:\temp directory of a Windows installation. These are the steps you would perform:

1. Open Windows Explorer.
2. Open the C:\temp directory.
3. Create a new folder named FileSystemGateway.

Configuring the FTP server for receiving documents

Note: This section applies only to receiving documents over FTP or FTPS from participants. Sending documents to participants is described in “Setting up an FTP gateway” on page 128 and “Setting up an FTPS gateway” on page 133.

If you are going to use FTP or FTPS as a transport for incoming documents, you must have an FTP server installed. If you are planning to use FTP and do not currently have a server installed, do so now before continuing. Make sure that one of the following scenarios is true for your installation:

- The FTP server is installed on the same machine on which WebSphere Partner Gateway is installed.
- The bcguser on the WebSphere Partner Gateway machine has read/write access to the location where the FTP server will be storing files.

© Copyright IBM Corp. 2004, 2005

Configuring the required directory structure on the FTP server

After the FTP server is installed, the next step is to create the required directory structure under the home directory of the FTP server. WebSphere Partner Gateway requires a particular directory structure that the Receiver and Document Manager components use to correctly identify the participant sending the incoming document. The structure is illustrated in Figure 15.

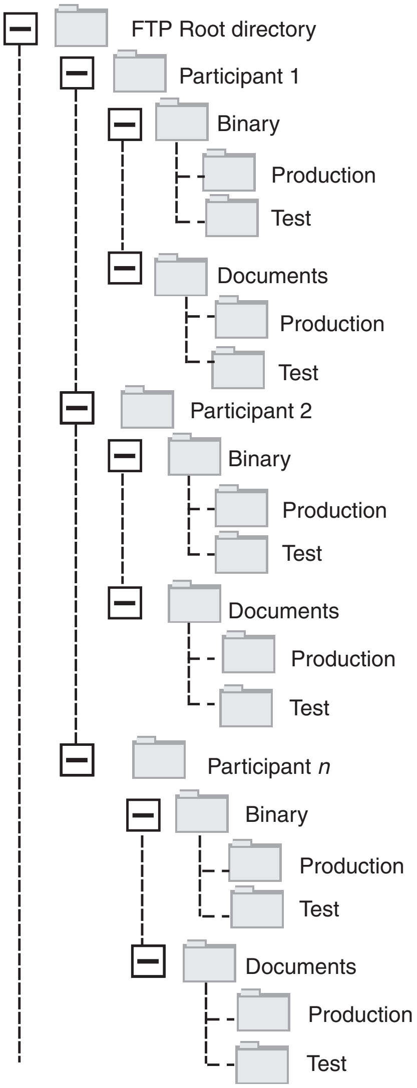


Figure 15. FTP Directory structure

Each participant directory contains a Binary directory and a Documents directory. Both the Binary and Documents directories contain a Production directory and a Test directory.

The Documents directory is used when a participant sends an XML document containing complete routing information (using FTP) to the hub. This requires the creation of a custom XML definition.

The Binary directory is used when a participant sends any other documents (using FTP) to the hub.

For each participant who will use FTP to send or receive documents, create the following folders from the root directory of your FTP server:

1. Create a folder for the participant.

   Note: The name of the folder should match the name you specify for **Company Login Name** when you create the participant. Creating participants is described in "Creating participant profiles" on page 139.
2. Create subfolders under the participant folder named `Binary` and `Documents`.
3. Create subfolders under the Binary and Documents folders called `Production` and `Test`.

How files sent over FTP are processed

It is important to understand how binary and XML files are processed by the FTP server.

Binary files

Binary files have a required file name structure, because the files are not inspected at all by the Document Manager.

The file name structure is: *<To_ParticipantID><Unique_Filename>*

When a binary file is detected by the Receiver, it is written to shared storage and passed to the Document Manager for processing.

The name of the directory in which the file was detected is used to evaluate the From Participant Name, and the first part of the file name is used to evaluate the To Participant Name. The position of the directory in the directory structure is used to evaluate whether the transaction is a Production or Test transaction.

For example, a file named 123456789.abcdefg1234567 is detected in the `\ftproot\partnerTwo\binary\production` directory. The Document Manager knows the following information:

- The `From Participant Name` is `partnerTwo` (because the file was found in the partnerTwo part of the directory tree).
- The `To Participant Name` is `partnerOne` (because the first part of the file name is 123456789, which is the DUNS ID for partnerOne).

  Note: Here and throughout this book, all DUNS numbers are meant to be examples only.
- The Transaction type is Production.

The Document Manager looks for a Production participant connection from partnerTwo to partnerOne for:

- Package: None (N/A)
- Protocol: Binary (1.0)
- Document Flow: Binary (1.0)

The Document Manager then processes the file.

XML files

An XML file has no file name requirements because the file is inspected by the Document Manager and the routing information is extracted from the document itself.

When an XML file is detected by the Receiver, it is written to the shared storage and passed to the Document Manager for processing.

The Document Manager compares the XML file to the XML Formats that have been defined and selects the required XML Format. (Setting up XML formats is described in "Custom XML documents" on page 77.) The From Participant Name, To Participant Name, and the Routing information are extracted from the XML File.

The position of the directory in the directory structure is used to evaluate whether the transaction is a Production or Test transaction.

The Document Manager then uses this information to locate the correct participant connection before processing the file.

Additional FTP server configuration

After creating the required directory structure, you configure your FTP server for each of the participants in the hub community. The way you configure the FTP server depends on which server you are using. Refer to the FTP server documentation, and perform the following tasks:

1. Add a new group (for example, Participants).
2. Add a user to the newly created group for each participant who will be sending or receiving documents over FTP.
3. For each participant, set up the FTP server to map the incoming participant to the respective directory structure you created for the participant in the earlier section "Configuring the required directory structure on the FTP server" on page 18. Refer to your FTP server documentation for additional information.

Security considerations for the FTPS server

If you are using an FTPS server to receive incoming documents, the security considerations for the SSL sessions are handled solely by the FTPS server and client that the participant is using. There is no specific security configuration for WebSphere Partner Gateway on incoming FTPS documents. WebSphere Partner Gateway retrieves the documents from the FTP target (which is described in "Setting up an FTP target" on page 34) after the server has successfully negotiated the secure channels and received the document. Refer to the FTPS server documentation to determine which certificates are needed (and where they are needed) to successfully configure a secure channel that the participant can contact.

For server authentication, provide the certificate of the Receiver to the participants. If the certificate is issued by a Certifying Authority (CA), also provide the CA certificate chain. If client authentication is supported by the FTPS server, the client authentication certificates of the participants should be specified in the FTPS server. Consult the FTPS server documentation for information about specifying client authentication and client authentication certificates.

Configuring the hub for the JMS transport protocol

This section describes how to set up the hub to use the JMS transport. If you will be using the JMS transport to send documents from the hub or to receive documents at the hub, follow the procedures in this section. If you will not be using the JMS transport, skip this section.

Note: The procedures in this section describe how to use the JMS implementation of WebSphere MQ to set up the JMS environment. The procedures also describe how to set up local queues. If you want to set up transmission and remote queues, refer to the WebSphere MQ documentation.

In later sections of this document, you will learn how to set up JMS targets or gateways (or both). These tasks are described in “Setting up a JMS target” on page 36 and “Setting up a JMS gateway” on page 130.

Creating a directory for JMS

You first create a directory for JMS. For example, suppose you wanted to create a directory named JMS in the c:\temp directory of a Windows installation. These are the steps you would follow:

1. Open Windows Explorer.
2. Open the C:\temp directory.
3. Create a new folder named JMS.

Modifying the default JMS configuration

In this section, you update the JMSAdmin.config file, which is part of the WebSphere MQ installation, to change the context factory and provider URL.

1. Navigate to the `Java\bin` directory of WebSphere MQ. For example, in a Windows installation, you would navigate to: C:\IBM\MQ\Java\bin
2. Open the JMSAdmin.config file using a plain text editor, such as Notepad or vi.
3. Add the character # to the front of the following lines:
   ```
   INITIAL_CONTEXT_FACTORY=com.sun.jndi.ldap.LdapCtxFactory
   PROVIDER_URL=ldap://polaris/o=ibm,c=us
   ```
4. Remove the character # from the front of the following lines:
   ```
   #INITIAL_CONTEXT_FACTORY=com.sun.jndi.fscontext.RefFSContextFactory
   #PROVIDER_URL=file:/C:/JNDI-Directory
   ```
5. Change the `PROVIDER_URL=file:/C:/JNDI-Directory` line to equal the name of the JMS directory you set up in “Creating a directory for JMS.” For example, if you set up the `c:/temp/JMS` directory, the line would look like this:
   ```
   PROVIDER_URL=file:/c:/temp/JMS
   ```
6. Save the file.

Creating queues and the channel

In this section, you use WebSphere MQ to create the queues you will use to send and receive documents and the channel for this communication. It is assumed that a queue manager has been created. The name of the queue manager should be substituted where <*queue_manager_name*> appears in the following steps. It is also assumed that a listener for this queue manager has been started on TCP port 1414.

1. Open a command prompt.
2. Enter the following command to start the WebSphere MQ command server:
   ```
   strmqcsv <queue_manager_name>
   ```
3. Enter the following command to start the WebSphere MQ command environment:
   ```
   runmqsc <queue_manager_name>
   ```
4. Enter the following command to create a WebSphere MQ queue to be used to hold incoming documents sent to the hub:
   ```
   def ql(<queue_name>)
   ```
   For example, to create a queue named JMSIN, you would enter:
   ```
   def ql(JMSIN)
   ```

5. Enter the following command to create a WebSphere MQ queue to be used to hold documents sent from the hub:

   ```
   def ql(<queue_name>)
   ```

   For example, to create a queue named JMSOUT, you would enter:

   ```
   def ql(JMSOUT)
   ```

6. Enter the following command to create a WebSphere MQ channel to be used for documents sent to and from the hub:

   ```
   def channel(<channel_name>) CHLTYPE(SVRCONN)
   ```

   For example, to create a channel named java.channel, you would enter:

   ```
   def channel(java.channel) CHLTYPE(SVRCONN)
   ```

7. Enter the following command to exit the WebSphere MQ command environment:

   ```
   end
   ```

Adding a Java(TM) run time to your environment

Enter the following command to add a Java run time to your system path:

```
set PATH=%PATH%;<ProductDir>\_jvm\jre\bin
```

where *ProductDir* refers to the directory where WebSphere Partner Gateway is installed.

Defining the JMS configuration

To define the JMS configuration, perform the following steps:

1. Change to the WebSphere MQ Java directory (directory (<*path_to_Websphere_MQ_installation_directory*>\java\bin)
2. Start the JMSAdmin application by typing the following command:

   ```
   JMSAdmin
   ```

3. Define a new JMS Context by typing the following commands from the InitCtx> prompt:

   ```
   define ctx(<context_name>)
   ```

   ```
   change ctx(<context_name>)
   ```

   For example, if the *context_name* is JMS, the commands look like this:

   ```
   define ctx(JMS)
   ```

   ```
   change ctx(JMS)
   ```

4. From the InitCtx/jms> prompt, enter the following JMS configuration:

   ```
   define qcf(connection_factory_name)
       tran(CLIENT)
       host(<your_IP_address>)
       port(1414)
       chan(java.channel)
       qmgr(<queue_manager_name>)
   ```

   ```
   define q(<name>) queue(<queue_name>) qmgr(<queue_manager_name>)
   ```

   ```
   define q(<name>) queue(<queue_name>) qmgr(<queue_manager_name>)
   ```

   ```
   end
   ```

The previous steps created the .bindings file, which is located in a subfolder of the folder you specified in step 5 on page 21. The name of the subfolder is the name you specified for your JMS context.

As an example, the following JMSAdmin session is used to define the queue connection factory as `Hub`, with an IP address of `sample.ibm.com` where the MQ queue manager resides (<*queue_manager_name*> of sample.queue.manager). The example uses the JMS queue names and channel name created in "Creating queues and the channel" on page 21. Note that user input follows the > prompt.

```
InitCtx> define ctx(jms)
InitCtx> change ctx(jms)
InitCtx/jms> define qcf(Hub)
    tran(CLIENT)
    host(sample.ibm.com)
    port(1414)
    chan(java.channel)
    qmgr(sample.queue.manager)
InitCtx/jms> define q(inQ) queue(JMSIN) qmgr(sample.queue.manager)
InitCtx/jms> define q(outQ) queue(JMSOUT) qmgr(sample.queue.manager)
InitCtx/jms>end
```

In this example, the .bindings file would be located in the following directory: c:/temp/JMS/JMS, where c:/temp/JMS is the PROVIDER_URL and JMS is the context name.

Using FTP scripts for FTP Scripting targets and gateways

The FTP Scripting transport allows you to send data to any FTP service, including a Value Added Network (VAN). You control the operations on the FTP server using a script file that contains FTP commands.

You specify this script when you create the FTP Scripting target or gateway. WebSphere Partner Gateway substitutes the actual values you enter when you create the target or gateway for the placeholders in the FTP script.

The operations defined in the input script are translated into actions on the FTP server. The input script is made up of a group of supported FTP commands. Parameters for these commands can take the form of a variable, which will be filled in at runtime.

For information about creating an FTP script for an FTP Scripting target, see "Setting up an FTP Scripting target" on page 39. For information about creating an FTP script for an FTP Scripting gateway, see "Setting up an FTP Scripting gateway" on page 134.

Using maps from the Data Interchange Services client

To perform EDI de-enveloping, transformation, and validation or to make transformations between ROD, XML, and EDI, you need to import the associated maps from the Data Interchange Services client. Data Interchange Services is a separately installed program that typically resides on a different computer from the one on which WebSphere Partner Gateway runs.

The Data Interchange Services mapping specialist creates maps describing how specific documents should be transformed and validated. For example, you might have a purchase order created by a back-end application that you want transformed and sent to a community participant as a standard EDI X12 purchase order (850). The Data Interchange Services mapping specialist would write a map detailing how to transform each field or piece of data from your program to the X12 format. The map would then be exported directly to WebSphere Partner Gateway, or it would be exported to a file, which you would then import using a command script.

Detailed information about how to import maps from the Data Interchange Services client is provided in “Importing maps” on page 107.

Chapter 3. Starting the server and displaying the Community Console

This chapter shows you how to start the WebSphere Partner Gateway server and display the Community Console. It includes the following topics:

- "Starting WebSphere MQ"
- "Starting the WebSphere Partner Gateway components"
- "Logging in to the Community Console" on page 26

Starting WebSphere MQ

If you have not already done so, start WebSphere MQ by following one of these procedures:

- For UNIX-based systems:
  1. Enter:
     ```
     su mqm
     ```
  2. Enter:
     ```
     strmqm bcg.queue.manager
     ```
  3. Enter:
     ```
     runmqlsr -t tcp -p 9999 -m bcg.queue.manager &
     ```
  4. Wait about 10 seconds and press Enter to return to the command prompt.
  5. Enter:
     ```
     strmqbrk -m bcg.queue.manager
     ```
- For Windows-based systems:
  1. Enter:
     ```
     strmqm bcg.queue.manager
     ```
  2. Enter:
     ```
     runmqlsr -t tcp -p 9999 -m bcg.queue.manager
     ```
     The Listener runs in this window; therefore, leave it open.
  3. Open a new window and start the JMS Broker (the publish-subscribe broker) with the following command:
     ```
     strmqbrk -m -bcg.queue.manager
     ```

Starting the WebSphere Partner Gateway components

To start the server, you must start each of the three components of WebSphere Partner Gateway: the Console, the Document Manager, and the Receiver.

1. Change to the directory \<*ProductDir*\bin.
2. Type the following command to start the Console:
   - For UNIX-based systems:
     ```
     ./bcgStartServer.sh bcgconsole
     ```
   - For Windows-based systems:
     ```
     bcgStartServer bcgconsole
     ```
3. Type the following command to start the Receiver:
   ```
   ./bcgStartServer.sh bcgreceiver
   ```

© Copyright IBM Corp. 2004, 2005

or

```
bcgStartServer bcgreceiver
```

4. Type the following command to start the Document Manager:

   ```
   ./bcgStartServer.sh bcgdocmgr
   ```

   or

   ```
   bcgStartServer bcgdocmgr
   ```

After starting the components, start the help system. Type the following command to start the help system:

```
./bcgStartHelp.sh
```

or

```
bcgStartHelp.bat
```

After the components are started, log in to the Community Console, as described in "Logging in to the Community Console."

For information about starting the Data Interchange Services client, refer to the *Mapping Guide*.

Logging in to the Community Console

The Community Console is the access point to WebSphere Partner Gateway. Most of the tasks you will perform in setting up the hub require that you be logged in as the Hub Administrator (hub admin), which is the super-user of the system.

Make sure you know the IP address of the computer on which the Console component is running. You will enter that address in the HTTP command.

1. From a browser, type the following URL:

   ```
   http://<IP_address>:58080/console
   ```

2. Enter the following information:
   a. For **User Name**, type `hubadmin`
   b. For **Password**, type `Pa55word`

      Note: If you have already signed on to the Community Console and changed the default password of Pa55word, enter your new password in the **Password** field.
   c. For **Company Login Name**, type `Operator`

You see the Participant Search page, which is always the first page displayed when you log in to the Community Console.

You will use this page later in the book to define participants.

If you click **Search** now, you will see that one participant, the Community Operator, is listed. The Community Operator is defined automatically by WebSphere Partner Gateway.

Note: If you have not changed your password from the default of Pa55word, you will be prompted to do so before the Participant Search page is displayed.

Chapter 4. Configuring the Community Console

This chapter describes how to configure the Community Console to specify what participants see, how they log in to the console, and what access they have to various console tasks. This chapter includes the following topics:

- "Specifying locale information and console branding"
- "Setting the password policy" on page 29
- "Configuring permissions" on page 29

You do not have to perform any of these tasks if you want to use the default settings supplied by WebSphere Partner Gateway.

Specifying locale information and console branding

By default, the pages of the Community Console are presented in the English language. IBM provides translations of the content in other languages as a set of files that can be uploaded. Other console items that are provided by IBM for different locales are the banner graphics. Optionally, you can upload your own logo graphics. You can also upload your own custom style sheet used to format the text on the pages.

You perform these tasks using the Locale Upload page. To display the Locale Upload page:

1. Click **Hub Admin > Console Configuration > Locale Configuration**.
2. Click **Create**.
3. Select a locale from the **Locale** list.

The Console displays the Locale Upload page.

From the Locale Upload page, you can choose to perform the following tasks:

- Brand the console, by uploading a unique banner or logo (or both)
- Upload files that IBM provides so that you can localize the content of the elements on the console

Branding the console

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

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

The images must be .JPG format files and must conform to certain specifications, so that they will fit in the Community Console window.

- To see the specifications required for the banner and logo, click **Image Specifications** on the Locale Upload window.
- To see samples of a header or logo image, scroll down to the **Sample Images** portion of the page and click **sample_headerback.jpg** or **sample_logo.jpg**.

© Copyright IBM Corp. 2004, 2005

- To download samples of a banner and logo to use as a template for creating your own banner and logo, click **Sample images (header background and company logo)**.

After you have created the banner or logo (or both), perform the following steps:

1. To upload the customized banner, perform either of the following tasks:
   - In the **Banner** field, type the path and name of the image file you want to use for the header/banner.
   - Click **Browse** to navigate to the .jpg file containing the banner, and select it.
2. To upload the customized logo, perform either of the following steps:
   - In the **Logo** field, type the path and name of the file you want to use for the company logo.
   - Click **Browse** to navigate to the .jpg file containing the logo, and select it.
3. Click **Upload**.

Note: When you replace the header background and company logo, you must restart the Community Console for the changes to take effect.

Changing the style sheet

If you want to specify a style sheet that is different from the default (for example, if you want different sized fonts or colors), perform the following tasks:

1. Perform one of the following tasks:
   - In the **CSS** field, type the path and name of the file that contains the customized style sheet.
   - Click **Browse** to navigate to the file containing the style sheet, and select it.
2. Click **Upload**.

Localizing the data on the console

If you receive resource bundles or other locale files from IBM, you can use the Locale Upload page to upload them. Resource bundles include the following information:

- **Console Labels**, which contain text strings that represent all the text on the interface
- **Event Descriptions**, which contain text strings used to display event details (for example, “An attempt was made to create a duplicate connection”)
- **Event Names**, which contain text strings representing event names (for example, “Connection already exists”)
- **EDI Event Descriptions**, which contain text strings used to display EDI event details (for example, “FA Reconciliation Failure. No activity ids found for the transactions found in the EDI Acknowledgement. “)
- **EDI Event Names**, which contain text strings representing EDI event names (such as “FA Reconciliation Failure”)
- **Extended Event Text**, which contain text strings that provide additional information about events (for example, the cause of the event and troubleshooting information)

To upload a resource bundle or other locale file:

1. For each resource bundle or file, perform either of the following tasks:
   - Type the path and name of the file.
   - Click **Browse** to navigate to the file, and select the file.

2. When you have finished uploading the files, click **Upload**.

Setting the password policy

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

You can change the following elements of the password policy:

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

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

  The special characters supported by the system are as follows: ’#’, ’@’, ’$’, ’&’, ’+’.
- Name Variation Checking, which, when selected, prevents the use of passwords that comprise an easily guessed variation of the user’s login or full name. This field is selected by default.

To change the default values:

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

Configuring permissions

Permissions represent privileges that a user must have to access various Console modules.

How permissions are granted to users

Before you configure permissions, it is helpful to understand how permissions are granted to individual users. All three types of entities in the hub community, the Community Operator, the Community Manager, and participants, have an Admin user. When you create a Community Manager or participant, you are actually creating the Admin user for that entity. (In the case of the Community Operator, the Hub Admin is automatically created, as is another Admin user for the hub.)

When you create the participant (as defined in "Creating participant profiles" on page 139), you provide the participant with login information (such as the name to use to log in and the password). After the participant logs in, the participant creates additional users within the organization. The participant also creates groups and assigns users to those groups. For example, an organization might want to have a group for people who monitor document volume. The participant would create a Volume group and add users to it.

Note: As the Hub Admin user, you can also define the users and groups for a participant.

The Admin user for the participant would then assign permissions to that group of users. For example, the Admin user might decide that the Volume group should see only the Document Volume and Document Analysis reports. The Admin user, using the Group Details page, would enable the document reports module but disable all other modules for the Volume group.

The setting you, as the Hub Admin, make on the Permissions page determines whether a module is listed on the Group Details page.

Some modules are restricted to certain members of the hub community (for example, the Hub Admin). Therefore, even if you enable one of these modules for use by a participant, the module will not be displayed on the Group Details page for the participant.

Enabling or disabling permissions

From the Permission List page, you can determine which permissions will be available to assign to groups of users by enabling or disabling the permissions. You cannot, however, define new permissions.

To change the default permissions:

1. Click **Hub Admin > Console Configuration > Permissions**. The Permission List is displayed.
2. If you want to change the defaults, perform the following steps:
   a. Click the current setting (**Enabled** or **Disabled**) to change the setting.
   b. When you are prompted to confirm the change, click **OK**.

Chapter 5. Defining targets

This chapter describes how to set up targets on WebSphere Partner Gateway. It covers the following topics:

- "Overview"
- "Uploading user-defined handlers" on page 32
- "Setting global transport values" on page 32
- "Setting up an HTTP/S target" on page 33
- "Setting up an FTP target" on page 34
- "Setting up an SMTP target" on page 35
- "Setting up a JMS target" on page 36
- "Setting up a File-system target" on page 38
- "Setting up an FTP Scripting target" on page 39
- "Setting up a target for a user-defined transport" on page 42
- "Modifying configuration points" on page 43

Overview

As described in "Overview of document processing" on page 7, the Receiver is responsible for accepting inbound documents from a specific transport. A target is an instance of the Receiver configured for a particular deployment.

Documents received at a target on the hub can come from community participants (for eventual delivery to the Community Manager) or from a Community Manager back-end application (for eventual delivery to participants).

Figure 16 shows a WebSphere Partner Gateway server with four targets set up. Two of the targets (HTTP/S and FTP/S) are for documents coming from participants. These two targets represent an HTTP URI and an FTP directory. You provide information about these targets to your participants to indicate where they should send documents to you. The other two targets (JMS and file directory) are for documents originating from the Community Manager back-end application. These targets represent a queue and a directory.

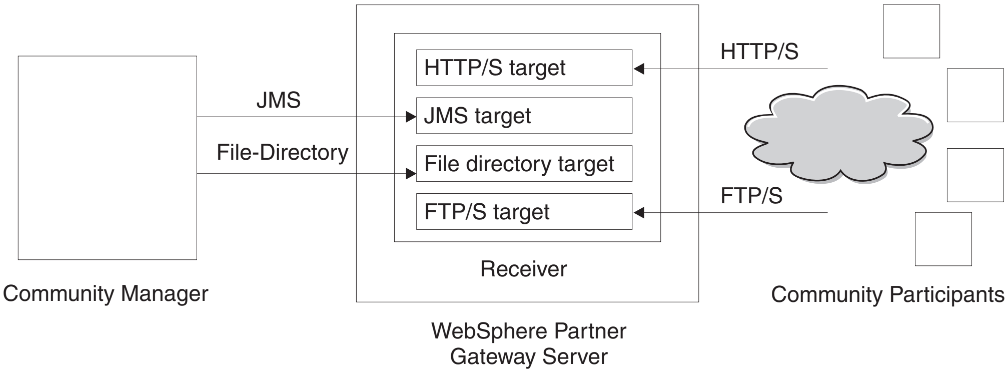


Figure 16. Transports and associated targets

© Copyright IBM Corp. 2004, 2005

You set up at least one target for each type of transport over which documents will be sent to the hub. For example, you will have an HTTP target to receive any documents sent over the HTTP or HTTPS transport. If your community participants will be sending documents over FTP, you will set up an FTP target.

The Receiver component detects when a message arrives at one of the targets. Some targets detect messages by polling their transports at regular intervals or on a scheduled basis to determine if new messages have arrived. The WebSphere Partner Gateway targets that are polling-based are: JMS, FTP, SMTP, File, and FTP Scripting. The HTTP/S target is callback-based, which means that it receives notification from the transport when messages arrive. User-defined transports can be either polling-based or callback-based.

Uploading user-defined handlers

You can modify configuration points for targets by specifying a handler for the target. The handler can be supplied by WebSphere Partner Gateway or it can be a user-defined handler. This section describes how to upload a user-defined handler. Use this section only for user-defined handlers. Handlers supplied by WebSphere Partner Gateway are already available for use.

To upload a handler, perform the following steps:

1. From the main menu, click **Hub Admin > Hub Configuration > Handlers**.
2. Select **Target**.

   The list of handlers currently defined for targets is displayed. Notice that handlers provided by WebSphere Partner Gateway have a Provider ID of **Product**.
3. From the Handler List page, click **Import**.
4. On the Import Handler page, specify the path to the XML file that describes the handler, or use **Browse** to search for that XML file.

After a handler is uploaded, you can use it to customize the configuration points of targets.

Setting global transport values

You set global transport attributes that apply to all HTTP/S and FTP Scripting targets. If you are not defining HTTP/S or FTP Scripting targets, this section does not apply to you.

1. Click **Hub Admin > Hub Configuration > Targets** to display the Target List.
2. Select **Global Transport Attributes** from the Target List.
3. If the default values are appropriate for your configuration, click **Cancel**. Otherwise, continue with the remaining steps in this section.
4. Click the **Edit** icon next to **Global Attributes Listed by Category**.
5. Review and, if necessary, change **FTP Scripting Transport** and **FTP Scripting - Targets and Gateways** values.

   The FTP Scripting transport uses a locking mechanism that prevents more than one FTP Scripting instance from accessing the same target at the same time. When an FTP Scripting transport is ready to send documents, it requests this lock. Default values are supplied for such things as how long a target instance waits to obtain the lock and how many times it attempts to retrieve it if the lock is in use. You can use these default values or change them. To change one or more of the values, type the new value or values. You can change:

- **FTP Scripting Transport** values
  - **Lock Retry Count**, which indicates how many times the target will attempt to obtain a lock if the lock is currently in use. The default is 3.
  - **Lock Retry Interval (Seconds)**, which indicates the amount of time that will elapse between attempts to obtain the lock. The default is 260 seconds.
- **FTP Scripting - Targets and Gateways** values
  - **Maximum Lock Time (Seconds)**, which indicates how long the target can hold the lock. The default is 240 seconds.
  - **Maximum Queue Age (Seconds)**, which indicates how long the target will wait in a queue to obtain the lock. The default is 740 seconds.

6. Review and, if necessary, change the **HTTP/S Transport** values. You can change:
   - **Maximum Synchronous Timeouts (Seconds)**, to indicate the number of seconds a synchronous connection can remain open. The default is 300 seconds.
   - **Maximum Simultaneous Synchronous Connections**, to indicate how many synchronous connections the system will allow. The default is 100 connections.
7. Click **Save**

Setting up an HTTP/S target

The Receiver component has a predefined bcgreceiver servlet that is used to receive HTTP/S POST messages. You create one or more HTTP targets to access the messages received by the servlet.

The following steps describe what you need to specify for an HTTP/S target.

1. Click **Hub Admin > Hub Configuration > Targets** to display the Targets List page.
2. From the Target List page, click **Create Target**.

Target Details

In the **Target Details** section, perform the following steps:

1. Type a name for the target. For example, you might call the target HttpTarget1. This is a required field. The name you enter here will be displayed on the Targets list.
2. Optionally indicate the status of the target. **Enabled** is the default. A target that is enabled is ready to accept documents. A target that is disabled cannot accept documents.
3. Optionally enter a description of the target.
4. Select **HTTP/S** from the **Transport** list.

Target Configuration

In the **Target Configuration** section, perform the following steps:

1. Optionally, specify the gateway type. The gateway type defines the nature of the transmission. For example, if you want to test a document exchange before putting it into production, you would enter **Test**. The default is **Production**.
2. Enter the URI for the HTTP/S target. The name must begin with **bcgreceiver**. For example, you might enter bcgreceiver/submit. Documents coming into the server over HTTP/S would then be received at bcgreceiver/submit.

Note: The **Sync Routing** values are already filled in, and you cannot edit them from this page. To modify these values, you use the Global Transport Attributes page, as described in "Setting global transport values" on page 32.

Handlers

If you will be receiving files containing multiple EDI interchanges or XML or ROD documents that need to be split, configure the appropriate splitter handler in the Preprocess configuration point.

If you will be sending or receiving certain types of business documents (RosettaNet, cXML, SOAP, and AS2) through a synchronous exchange, specify a handler for the associated protocol in the SyncCheck configuration point. You can also modify the Postprocess configuration points for the target.

To modify a configuration point, go to "Modifying configuration points" on page 43. Otherwise, click **Save**.

Setting up an FTP target

An FTP target polls your FTP server at a set interval to look for new documents.

The following steps describe what you need to specify for an FTP target.

1. Click **Hub Admin > Hub Configuration > Targets** to display the Targets List page.
2. From the Target List page, click **Create Target**.

Target Details

In the **Target Details** section, perform the following steps:

1. Type a name for the target. For example, you might call the target FTPTarget1. This is a required field. The name you enter here will be displayed on the Targets list.
2. Optionally indicate the status of the target. **Enabled** is the default. A target that is enabled is ready to accept documents. A target that is disabled cannot accept documents.
3. Optionally enter a description of the target.
4. Select **FTP Directory** from the **Transport** list.

Target Configuration

In the **Target Configuration** section, perform the following steps:

1. In the **FTP Root Directory** field, enter the root directory of the FTP server. The Document Manager automatically polls the participant sub-directories within the FTP root directory for document routing. This field is required. Refer to "Configuring the FTP server for receiving documents" on page 17 for information about setting up the directory for an FTP server.

   Note: Type the directory path ending at the root FTP directory. Do not include the participant sub-directories.
2. Optionally, enter a value for **File Unchanged Interval** to indicate the number of seconds the file size must remain unchanged before the Document Manager retrieves the document for processing. This unchanged interval period ensures that a document has completed its transmission (and is not still in transit) when the Document Manager retrieves it. The default value is 3 seconds.

3. Optionally enter a value for **Thread Nbr**, to indicate the number of documents the Document Manager can process simultaneously. The default value of 1 is recommended.
4. Optionally enter a value for **Exclude File Ext** to indicate the types of documents the Document Manager should ignore (exclude from processing) if it finds the documents in the FTP directory. For example, you might want the Document Manager to ignore spreadsheet files, in which case you would enter the extension associated with them. After you type the extension, click **Add**. The extension is then added to the list of file extensions to be ignored. The default is that no file types are excluded.

   Note: Do not use a dot preceding the file name extension (for example: .exe or . txt). Use only the characters that denote the file extension.

Handlers

If you will be receiving files containing multiple EDI interchanges or XML or ROD documents that need to be split, configure the appropriate splitter handler in the Preprocess configuration point.

To modify the Preprocess configuration point, go to "Modifying configuration points" on page 43. Otherwise, click **Save**.

Setting up an SMTP target

An SMTP target polls your POP3 mail server (according to the schedule you specify) to look for new documents.

The following steps describe what you need to specify for an SMTP (POP3) target.

1. Click **Hub Admin > Hub Configuration > Targets** to display the Targets List page.
2. From the Target List page, click **Create Target**.

Target Details

In the **Target Details** section, perform the following steps:

1. Type a name for the target. For example, you might call the target POP3Target1. This is a required field. The name you enter here will be displayed on the Targets list.
2. Optionally indicate the status of the target. **Enabled** is the default. A target that is enabled is ready to accept documents. A target that is disabled cannot accept documents.
3. Optionally enter a description of the target.
4. Select **POP3** from the **Transport** list.

Target Configuration

In the **Target Configuration** section of the page, perform the following steps:

1. Optionally indicate the gateway type. The gateway type defines the nature of the transmission. For example, if you want to test a document exchange before putting it into production, you would enter **Test**. The default is **Production**.
2. Enter the location of the POP3 server where mail is delivered. For example, you might enter an IP address.
3. Optionally enter a port number. If you do not enter anything, the value of 110 is used.

4. Enter the user ID and password required to access the mail server, if a user ID and password are required.
5. Optionally enter a value for **Thread Nbr**, to indicate the number of documents the Document Manager can process simultaneously. The default value of 1 is recommended.

Schedule

In the **Schedule** section of the page, perform the following steps:

1. Select **Interval Based Scheduling** or **Calendar Based Scheduling**.
2. Perform one of the sets of steps:
   - If you select **Interval Based Scheduling**, select the number of seconds that should elapse before the POP3 server is polled again (or accept the default value). If you select the default value, the POP3 server is polled every 5 seconds.
   - If you select **Calendar Based Scheduling**, choose the type of scheduling (**Daily Schedule**, **Weekly Schedule**, or **Custom Schedule**).
     - If you select **Daily Schedule**, select the time of day (the hours and minutes) when the POP3 server should be polled.
     - If you select **Weekly Schedule**, select one or more days of the week in addition to the time of day.
     - If you select **Custom Schedule**, select the time of day and then choose **Range** or **Selective Days** for the week and the month. With **Range**, you indicate the start date and the end date. (For example, you can click **Mon** and **Fri** if you want the server polled at a certain time on weekdays only.) With **Selective Days**, you choose the specific days of the week and month.

Setting up a JMS target

A JMS target polls a JMS queue (according to the schedule you specify) to look for new documents.

The following steps describe what you need to specify for a JMS target.

1. Click **Hub Admin > Hub Configuration > Targets** to display the Targets List page.
2. From the Target List page, click **Create Target**.

Target Details

In the **Target Details** section, perform the following steps:

1. Type a name for the target. For example, you might call the target JMSTarget1. This is a required field. The name you enter here will be displayed on the Targets list.
2. Optionally indicate the status of the target. **Enabled** is the default. A target that is enabled is ready to accept documents. A target that is disabled cannot accept documents.
3. Optionally enter a description of the target.
4. Select **JMS** from the **Transport** list.

Target Configuration

In the **Target Configuration** section of the page, perform the following steps:

1. Optionally indicate the gateway type. The gateway type defines the nature of the transmission. For example, if you want to test a document exchange before putting it into production, you would enter **Test**. The default is **Production**.
2. Enter the JMS provider URL. This should match the value you entered (the file system path to the bindings file) when you configured WebSphere Partner Gateway for JMS (step 5 on page 21). You can also specify the subfolder for the JMS context as part of the JMS provider URL.

   For example, without the JMS context, you would enter `c:/temp/JMS`. With the JMS context, you would enter `c:/temp/JMS/JMS`.
3. Enter the user ID and password required to access the JMS queue, if a user ID and password are required.
4. Enter a value for JMS queue name. This is a required field. This name should match the one you specified with the `define q` command when you created the bindings file (step 4 on page 22).

   If you entered the subfolder for the JMS context in step 2, enter only the queue name here (for example, `inQ`). If you did not enter the subfolder for the JMS context in the JMS provider URL, specify the subfolder before the factory name (for example, `JMS/inQ`).
5. Enter a value for the JMS factory name. This is a required field. This name should match the one you specified with the `define qcf` command when you created the bindings file (step 4 on page 22).

   If you entered the subfolder for the JMS context in step 2, enter only the factory name here (for example, `Hub`). If you did not enter the subfolder for the JMS context in the JMS provider URL, specify the subfolder before the factory name (for example, `JMS/Hub`).
6. Optionally enter the Provider URL package.
7. Enter the JNDI factory name. If you do not enter anything, the value com.sun.jndi.fscontext.RefFSContextFactory is used. This is a required field.
8. Optionally enter a value for **Time Out**, to indicate the number of seconds the target will monitor the JMS queue for documents. This field is optional.
9. Optionally enter a value for **Thread Nbr**, to indicate the number of documents the Document Manager will process simultaneously. The default value of 1 is recommended.

For example, if you wanted to set up a JMS target to match the JMS configuration example in “Configuring the hub for the JMS transport protocol” on page 20, you would:

1. Enter the value **JMSTarget** in the **Target Name** box.
2. Enter the value **file:/C:/TEMP/JMS/JMS** in the **JMS Provider URL** box.
3. Enter the value **inQ** in the **JMS Queue Name** box.
4. Enter the value **Hub** in the **JMS Factory Name** box.

Handlers

If you will be receiving files containing multiple EDI interchanges or XML or ROD documents that need to be split, configure the appropriate splitter handler in the Preprocess configuration point.

To modify configuration points for this target, go to “Modifying configuration points” on page 43. Otherwise, click **Save**.

Setting up a File-system target

A File-system target polls a directory according to a set interval to look for new documents.

The following steps describe what you need to specify for a file-system target.

1. Click **Hub Admin > Hub Configuration > Targets** to display the Targets List page.
2. From the Target List page, click **Create Target**.

Target Details

In the **Target Details** section, perform the following steps:

1. Type a name for the target. For example, you might call the target FileTarget1. This is a required field. The name you enter here will be displayed on the Targets list.
2. Optionally indicate the status of the target. **Enabled** is the default. A target that is enabled is ready to accept documents. A target that is disabled cannot accept documents.
3. Optionally enter a description of the target.
4. Select **File Directory** from the **Transport** list.

Target Configuration

In the **Target Configuration** section of the page, perform the following steps:

1. Optionally indicate the gateway type. The gateway type defines the nature of the transmission. For example, if you want to test a document exchange before putting it into production, you would enter **Test**. The default is **Production**.
2. Enter a value for **Document Root Path** to indicate the directory where the documents will be received.
3. Optionally enter a value for **Poll Interval**, to indicate how often the directory should be polled for new documents. If you do not enter anything, the directory will be polled every 5 seconds.
4. Optionally, enter a value for **File Unchanged Interval** to indicate the number of seconds the file size must remain unchanged before the Document Manager retrieves the document for processing. This unchanged interval period ensures that a document has completed its transmission (and is not still in transit) when the Document Manager retrieves it. The default value is 3 seconds.
5. Optionally enter a value for **Thread Nbr**, to indicate the number of documents the Document Manager can process simultaneously. The default value of 1 is recommended.

Handlers

If you will be receiving files containing multiple EDI interchanges or XML or ROD documents that need to be split, configure the appropriate splitter handler in the Preprocess configuration point.

To modify the Preprocess configuration point, go to “Modifying configuration points” on page 43. Otherwise, click **Save**.

Setting up an FTP Scripting target

An FTP Scripting target is a polling target that runs according to the schedule you set. The behavior of an FTP Scripting target is governed by an FTP command script.

Unlike the FTP target, which polls a directory on your FTP server, the FTP Scripting target polls directories on another server (for example, a VAN).

Creating the FTP script

The FTP servers can have specific requirements for the commands they will accept. To use an FTP Scripting target, you create a file that includes all the FTP commands required by the FTP server to which you are connecting. (You must receive this information from the administrator of the FTP server.)

1. Create a script for the targets, to indicate the actions you want performed. The following script is an example of connecting to the specified FTP server (with the name and password specified), changing to the specified directory on the FTP server, and receiving all the files in that directory:

   ```
   open %BCGSERVERIP% %BCGUSERID% %BCGPASSWORD%
   cd %BCGOPTION1%
   mget *
   quit
   ```

   The placeholders (for example, %BCGSERVERIP%) are replaced when the target is put in service by the values you enter when you create a specific instance of an FTP Scripting target. The %BCGOPTION% in this example is the name of the directory in the `cd` command. The script parameters and their associated FTP Scripting Target fields are shown in Table 2:

Table 2. How script parameters map to FTP Scripting target field entries

Script parameter	FTP Scripting target field entry
%BCGSERVERIP%	Server IP
%BCGUSERID%	User ID
%BCGPASSWORD%	Password
%BCGOPTIONx%	Option*x*, under **User defined attributes**

2. Save the file.

FTP scripting commands

You can use the following commands when creating the script:

- ascii, binary, passive

  These commands are not sent to the FTP Server. They modify the mode of transfer (ascii, binary, or passive) to the FTP Server.
- cd

  This command changes to the specified directory.
- delete

  This command removes a file from the FTP server.
- get

  This command takes a single argument -- the name of the file to retrieve from the remote system. The requested file is then transferred into WebSphere Partner Gateway. Use this command only if you are picking up a single file and the name is known; otherwise, the `mget` command with wildcards should be used.

- getdel

  This command is the same as the `get` command, except that the file is removed from the remote system when WebSphere Partner Gateway gets the file for processing.
- mget

  This command takes a single argument, which describes a group of files to be retrieved. The description can include the standard wildcard characters ('*' and '?'). One or more files are then retrieved from the remote system.
- mgetdel

  This command takes a single argument, which describes a group of files to be retrieved and then deleted from the FTP server. The description can include the standard wildcard characters (* and ?). One or more files are retrieved and then deleted from the remote system.
- mkdir

  This command creates a directory on the FTP server.
- open

  This command takes three parameters--the FTP server IP address, the user name, and a password. These parameters map to the %BCGSERVERIP%, %BCGUSERID%, and %BCGPASSWORD% variables.

  The first line of your FTP Scripting target script, therefore, should be:

  ```
  open %BCGSERVERIP% %BCGUSERID% %BCGPASSWORD%
  ```
- quit, bye

  This command ends an existing connection to an FTP Server.
- quote

  This command indicates that everything after the QUOTE should be sent to the remote system as a command. This allows you to send commands to a remote FTP server that might not be defined in the standard FTP protocol.
- rename

  This command renames a file on the FTP server.
- rmdir

  This command removes a directory from the FTP server.
- site

  This command can be used to issue site-specific commands to the remote system. The remote system determines if the contents of this command are valid.

Target Details

The following steps describe what you need to specify for an FTP Scripting target.

1. Click **Hub Admin > Hub Configuration > Targets** to display the Targets List page.
2. From the Target List page, click **Create Target**.

In the **Target Details** section, perform the following steps:

1. Type a name for the target. For example, you might call the target FTPScriptingTarget1. This is a required field. The name you enter here will be displayed on the Targets list.
2. Optionally indicate the status of the target. **Enabled** is the default. A target that is enabled is ready to accept documents. A target that is disabled cannot accept documents.
3. Optionally enter a description of the target.

4. Select **FTP Scripting** from the Transport list.

Target Configuration

In the **Target Configuration** section of the page, perform the following steps:

1. Optionally indicate the gateway type. The gateway type defines the nature of the transmission. For example, if you want to test a document exchange before putting it into production, you would enter **Test**. The default is **Production**.
2. Enter the server IP address of the FTP server to which you are connecting. The value you enter here will replace %BCGSERVERIP% when the FTP script is run.
3. Enter the user ID and password you use to access the server. The values you enter here will replace %BCGUSERID% and %BCGPASSWORD% when the FTP script is run.
4. Indicate whether the target will operate in secure sockets layer (SSL) mode. If so, you will need to exchange certificates with your participants, as described in Chapter 13, "Setting up security for inbound and outbound exchanges," on page 147.
5. Upload the script file by following these steps:
   a. Click **Upload Script File**.
   b. Type the name of the file that contains the script for processing documents, or use **Browse** to navigate to the file.
   c. Click **Load File** to load the script file into the **Currently loaded script file** text box.
   d. If the script file is the one you want to use, click **Save**.
   e. Click **Close Window**.
6. For **Connection Timeout**, enter the number of seconds a socket will remain open with no traffic.
7. In the **Lock User** field, indicate whether the target will request a lock, so that no other instances of an FTP Scripting target can gain access to the same FTP server directory at the same time.

Note: The **Global FTP Scripting Attributes** values are already filled in, and you cannot edit them from this page. To modify these values, you use the Global Transport Attributes page, as described in "Setting global transport values" on page 32.

User-Defined Attributes

If you want to specify additional attributes, perform the following steps. The value you enter for the option will replace %BCGOPTION*x*% when the FTP script is run (where *x* corresponds to the number of the option).

1. Click **New**.
2. Type a value next to **Option 1**.
3. If you have additional attributes to specify, click **New** again and type a value.
4. Repeat step 3 as often as necessary to define all the attributes.

For example, suppose your FTP script looked like this:

```
open %BCGSERVERIP% %BCGUSERID% %BCGPASSWORD%
          cd %BCGOPTION1%
          mget *
          quit
```

The %BCGOPTION% in this case would be a directory name.

Schedule

Indicate whether you want interval-based scheduling or calendar-based scheduling.

- If you select **Interval Based Scheduling**, select the number of seconds that should elapse before the FTP server is polled (or accept the default value).
- If you select **Calendar Based Scheduling**, choose the type of scheduling (**Daily Schedule**, **Weekly Schedule**, or **Custom Schedule**).
  - If you select **Daily Schedule**, enter the time of day at which the FTP server should be polled.
  - If you select **Weekly Schedule**, select one or more days of the week in addition to the time of day.
  - If you select **Custom Schedule**, select the time of day and then choose **Range** or **Selective Days** for the week and the month. With **Range**, you indicate the start date and the end date. (For example, you can click **Mon** and **Fri** if you want the server polled at a certain time on weekdays only.) With **Selective Days**, you choose the specific days of the week and month.

Handlers

If you will be receiving files containing multiple EDI interchanges or XML or ROD documents that need to be split, configure the appropriate splitter handler in the Preprocess configuration point.

To modify the Preprocess configuration point, go to “Modifying configuration points” on page 43. Otherwise, click **Save**.

Setting up a target for a user-defined transport

If you are defining a target for a user-defined transport, the field names and other information are defined within the file that describes the transport.

Perform the following steps:

1. Click **Hub Admin > Hub Configuration > Targets**.
2. Click **Manage Transport Types**.
3. Enter the name of an XML file that defines the transport (or use **Browse** to navigate to the file).
4. Click **Upload**.

   Note: From the Target List, you can also delete a user-defined transport type. You cannot delete a transport provided by WebSphere Partner Gateway. Also, you cannot delete a user-defined transport after it has been used for creating a target.
5. Click **Create Target**.
6. Type a name for the target. This is a required field. The name you enter here will be displayed on the Targets list.
7. Optionally indicate the status of the target. **Enabled** is the default. A target that is enabled is ready to accept documents. A target that is disabled cannot accept documents.
8. Optionally enter a description of the target.
9. Select the user-defined transport from the list.
10. Fill in the fields (which will be unique for each user-defined transport).

11. If you want to modify configuration points for this target, go to “Modifying configuration points.” Otherwise, click **Save**.

Modifying configuration points

The number of configuration points available and the number of associated handlers for those configuration points vary, depending on the type of target you are setting up. For example, the SyncCheck configuration point is available only with HTTP/S and JMS targets.

For certain business protocols (RosettaNet, cXML, SOAP, and AS2) involved in synchronous exchanges, you must specify a handler for that protocol in the SyncCheck configuration point. You can also modify the way targets process documents by applying an uploaded user-defined handler (or a system-supplied process) to the Preprocess and Postprocess points of the target.

To apply a user-written handler for these configuration points, you must first upload the handler, as described in “Uploading user-defined handlers” on page 32. You can also use a system-supplied handler, which is already available and does not have to be uploaded.

Preprocess

The Preprocess configuration handler is available on all types of targets but is not applicable to SMTP targets.

Preprocess attributes

Table 3 describes the attributes you can set for a Preprocess handler and lists the splitter handlers to which the attributes apply.

The ROD attributes used as examples in this table correspond to those used in “ROD to EDI example” on page 209. In the example, the ROD attributes are contained in the map S_DT_ROD_TO_EDI.eif, which includes the following document flow definition:

- Package: None (version N/A)
- Protocol: ROD_TO_EDI_DICT (version ALL)
- Document Flow: DTROD-TO-EDI_ROD (version ALL)

The ROD metadictionary and metadocument associated with this flow are ROD_TO_EDI_DICT and DTROD-TO-EDI_ROD.

Table 3. Splitter handler attributes

Attribute	**Description**	**Splitter Handler**
Encoding	The character encoding of the document. The default is ASCII.	ROD Generic XML EDI
BATCHDOCS	When BCG_BATCHDOCS is on, the splitter adds batch IDs to the documents after the documents are split. If the documents are transformed into EDI transactions to be enveloped, the Enveloper uses the batch IDs to make sure that the transactions are put into the same EDI interchange (if possible) before being delivered. Note that the Enveloper must have the batching attribute set to **On** (the default value). See “Batch mode” on page 95.	ROD Generic XML

Table 3. Splitter handler attributes (continued)

Attribute	Description	Splitter Handler
From Packaging Name	The packaging associated with the document. This value must match the packaging specified in the document flow definition. For example, for a document that has a packaging of None, this value should be **None**.	ROD Generic
From Packaging Version	The version of the packaging specified in From Packaging Name. For example, if the document has a packaging of None, this value would be **N/A**.	ROD Generic
From Protocol Name	The protocol associated with the document. This value must match the protocol specified in the document flow definition. For example, for a ROD document, this value could be **ROD-TO-EDI_DICT**.	ROD Generic
From Protocol Version	The version of the protocol specified in From Protocol Name. For example, for the ROD-TO-EDI_DICT protocol, the value would be **ALL**.	ROD Generic
From Process Code	The process (document flow) associated with this document. This value must match the document flow in the document flow definition. For example, for a ROD document, this value could be DTROD-TO-EDI_ROD.	ROD Generic
From Process Version	The version of the process specified in From Process Code. For example, for DTROD-TO-EDI_ROD, this value would be **ALL**.	ROD Generic
Metadictionary	The metadictionary provides information that lets WebSphere Partner Gateway interpret the data. For example, for a ROD document, this value could be **ROD-TO-EDI_DICT**.	ROD Generic
Metadocument	The metadocument provides information that lets WebSphere Partner Gateway interpret the data. For example, for a ROD document, this value could be **DTROD-TO-EDI_ROD**.	ROD Generic
Metasyntax	The metasyntax describes the format of the document being split. The default value is **rod**.	ROD Generic

Notes:

1. Only one ROD document type per target instance is supported.
2. If a target has more than one splitter handler configured (for example, if it has ROD, XML, and EDI splitter handlers configured), the ROD splitter handler must be the last one in the **Configured List**.

Modifying the Preprocess configuration point

To modify the Preprocess configuration point, perform the following steps:

1. Select **Preprocess** from the **Configuration Point Handlers** list.

   Four preprocessing handlers are provided (by default) and are shown in the **Available List**.
   - com.ibm.bcg.edi.receiver.preprocesshandler.EDISplitterHandler
   - com.ibm.bcg.edi.receiver.preprocesshandler.XMLSplitterHandler
   - com.ibm.bcg.edi.receiver.preprocesshandler.RODSplitterHandler
   - com.ibm.bcg.edi.receiver.preprocesshandler.GenericDocumentFlowHandler

   Note: The preprocessing handlers do not apply to SMTP targets.

2. If you will be receiving multiple EDI interchanges or XML or ROD documents that need to be split, make sure you select the appropriate splitter handler. To configure the Preprocess step:
   a. Select a handler from the **Available List** and click **Add**. Note that the handler moves from the **Available List** to the **Configured List**, as illustrated in Figure 17:

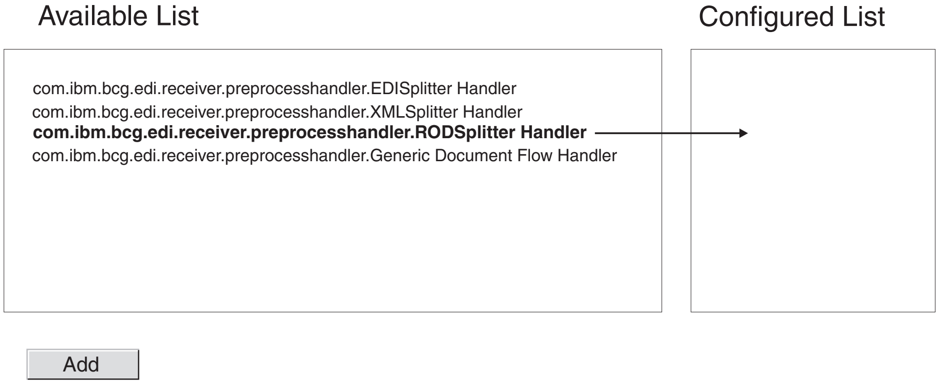

Available List
Configured List
com.ibm.bcg.edi.receiver.preprocesshandler.EDISplitter Handler
com.ibm.bcg.edi.receiver.preprocesshandler.XMLSplitter Handler
com.ibm.bcg.edi.receiver.preprocesshandler.RODSplitter Handler
com.ibm.bcg.edi.receiver.preprocesshandler.Generic Document Flow Handler
Add

Figure 17. Configuring the preprocessing step for a target

   b. Repeat this step for each handler you want to add to the configured list.

      Remember that for targets, the handlers are called in the order in which they appear on the **Configured List**. The first available handler processes the request, and subsequent handlers on the list are not called.
   c. Configure the handler by selecting it and clicking **Configure**:
      - If you have added the EDISplitterHandler, you can modify its attribute-Encoding. The default for encoding is ASCII.
      - If you have added the XMLSplitterHandler, you can modify its attribute--BCGBATCHDOCs. The default is **ON**. See "Preprocess attributes" on page 43 for information about this attribute.
      - If you have added the RODSplitterHandler, you can specify values for 11 attributes. Encoding, BATCHDOCS, and Metasyntax have default values. For the other attributes, you must type a value for From Packaging Name, From Packaging Version, From Protocol Name, From Protocol Version, From Process Code, From Process Version, Metadictionary, and Metadocument. See "Preprocess attributes" on page 43 for information about these attributes.
      - If you have added the GenericDocumentFlowHandler, you can specify values for 11 attributes. Encoding and BATCHDOCS have default values. For the other attributes, you must type a value for From Packaging Name, From Packaging Version, From Protocol Name, From Protocol Version, From Process Code, From Process Version, Metadictionary, Metadocument, and Metasyntax. See "Preprocess attributes" on page 43 for information about these attributes.

SyncCheck

The SyncCheck configuration point is available for HTTP/S and JMS targets only.

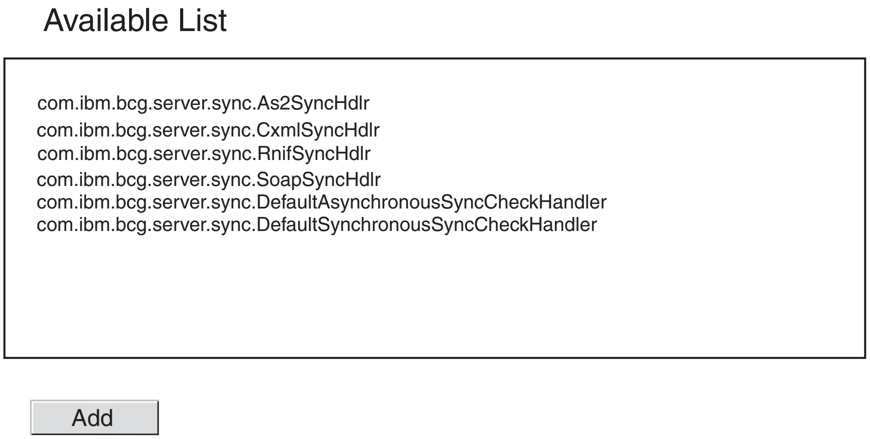
To specify a handler for a business protocol involved in a synchronous exchange, perform the following steps:

1. Select **SyncCheck** from the **Configuration Point Handlers** list.

Six SyncCheck handlers are provided (by default) for an HTTP/S target. These handlers are shown in the **Available List**:

- com.ibm.bcg.server.sync.As2SyncHdlr
- com.ibm.bcg.server.sync.CxmlSyncHdlr
- com.ibm.bcg.server.sync.RnifSyncHdlr
- com.ibm.bcg.server.sync.SoapSyncHdlr
- com.ibm.bcg.server.sync.DefaultAsynchronousSyncCheckHandler
- com.ibm.bcg.server.sync.DefaultSynchronousSyncCheckHandler

For example, if you are configuring an HTTP/S target, the Available List looks like this:



com.ibm.bcg.server.sync.As2SyncHdlr
com.ibm.bcg.server.sync.CxmlSyncHdlr
com.ibm.bcg.server.sync.RnifSyncHdlr
com.ibm.bcg.server.sync.SoapSyncHdlr
com.ibm.bcg.server.sync.DefaultAsynchronousSyncCheckHandler
com.ibm.bcg.server.sync.DefaultSynchronousSyncCheckHandler

Figure 18. List of available handlers for an HTTP/S SyncCheck configuration point

As you can see from the naming convention, the first four handlers are specific to the four document types that can be used for synchronous transactions. Any request that uses the DefaultAsynchronousSyncCheckHandler will be treated as an asynchronous request. Any request that uses the DefaultSynchronousSyncCheckHandler will be treated as a synchronous request.

The DefaultAsynchronousSyncCheckHandler and DefaultSynchronousSyncCheckHandler can be used with other targets (such as a JMS target).

2. If you will be receiving synchronous documents at this target, perform the following steps:
   a. Select one or more of the handlers from the **Available List** and click **Add**.
   b. Repeat this step if you want to add other handlers to the list. Remember that for targets, the handlers are called in the order in which they appear on the **Configured List**. The first available handler processes the request, and subsequent handlers on the list are not called.

   For HTTP and HTTPS targets, it is a good practice to list the specific SyncCheck handler (for example, com.ibm.bcg.server.sync.As2SyncHdlr for AS2 transactions) before listing the default SyncCheck handlers.

Postprocess

No handlers are provided by default for the Postprocess step, and, therefore, no handlers are listed by default in the **Available List**. You can, however, upload a handler for this configuration point for all types of targets that support synchronous communication. The available handler types for the postprocessing step are:

- RECEIVER.SYNCRESPONSEPROCESS.JMS
- RECEIVER.SYNCRESPONSEPROCESS.HttpS

You add a Postprocessing handler by uploading a handler that conforms to one of these handler types. You use the **Import** choice of the Handlers List page to upload a user-defined handler. When you upload a user-defined target handler, the handler is added to the Handlers List. It also appears on the Available List for the type of configuration point to which it pertains.

To modify the Postprocess configuration point, perform the following steps:

1. Select **Postprocess** from the **Configuration Point Handlers** list.
2. Select a user-defined handler from the **Available List** and click **Add**. Note that the handler moves from the **Available List** to the **Configured List**

Modifying the Configured List

If you need to change the order of the handlers, delete a handler, or configure attributes for the handler, perform the appropriate step:

- Remove a handler by selecting the handler from the **Configured List** and clicking **Remove**. The handler is moved to the **Available List**.
- Rearrange the order in which the handler is used by selecting the handler and clicking **Move Up** or **Move Down**.
- Configure the handler by selecting it from the **Configured List** and clicking **Configure**. The list of attributes that can be configured is displayed.

Chapter 6. Configuring fixed workflow steps and actions

This chapter describes optional tasks you can perform to configure fixed inbound and outbound workflows and actions. If you do not need to change the system-supplied behavior of workflows or actions, skip this chapter.

This chapter includes the following topics:

- "Uploading handlers"
- "Configuring fixed workflows" on page 50
- "Configuring actions" on page 51

Uploading handlers

If you are going to modify components, you first upload the handlers for those components before creating or configuring the components. You only need to upload the user-defined handlers for the components that require them. For example, if you are adding your own validation step, you need to upload that handler from the Actions page of **Handlers** (as described in steps 1 through 4).

Note: As mentioned in "Configuring document processing components with handlers" on page 9, you upload only user-defined handlers. The handlers supplied by WebSphere Partner Gateway are already available.

You can modify fixed workflows and actions and create new actions. You modify these components by the handlers you associate with them.

Note: You can list the valid handler types for actions and fixed workflows by clicking **Hub Admin > Hub Configuration > Handlers > Actions > Handler Types** or **Hub Admin > Hub Configuration > Handlers > Fixed Workflow > Handler Types**. Use this list to confirm that your handler is a valid type before uploading it. It must be one of the allowed types or it will not upload successfully.

To upload a handler, perform the following steps:

1. From the main menu, click **Hub Admin > Hub Configuration > Handlers**.
2. Select the type of handler (**Action** or **Fixed Workflow**).

   The list of handlers currently defined for that particular component is displayed. Notice that handlers provided by WebSphere Partner Gateway are listed. They have a Provider ID of **Product**.
3. From the Handler List page, click **Import**.
4. On the Import Handler page, specify the path to the XML file that describes the handler, or use **Browse** to search for that XML file.
5. Click **Upload**.

After a handler is uploaded, you can use it to create new actions and workflows.

Note: You can update user-defined handlers by uploading the modified XML file. For an action handler, for example, you would click **Hub Admin > Hub Configuration > Handlers > Action**, and then click **Import**.

You cannot modify or delete handlers provided by WebSphere Partner Gateway.

© Copyright IBM Corp. 2004, 2005

Configuring fixed workflows

Chapter 1, “Introduction” described the two fixed inbound workflow steps that you can configure--one for unpackaging a protocol and one for parsing the protocol. For outbound workflows, there is one step, for protocol packaging.

If you are going to use a user-defined handler to configure a workflow step, upload the handler, as described in “Uploading handlers” on page 49.

To configure a fixed workflow, perform the following steps:

1. Click **Hub Admin > Hub Configuration > Fixed Workflow**.
2. Click either **Inbound** or **Outbound**.
3. Click the **View Details** icon next to the name of the step you want to configure.

   The step, along with a list of handlers already configured for that step, is listed. See “Inbound workflows” and “Outbound workflow” on page 51 for a list of default handlers.
4. Click the **Edit** icon to edit the list of handlers.
5. Perform one or more of the following tasks for each step you want to modify.
   a. Add a handler by selecting the handler from the **Available List** and clicking **Add**. (A handler appears in the **Available List** if you uploaded a user-defined handler or if you previously removed a handler from the **Configured List**.) The handler is moved to the **Configured List**.
   b. Remove a handler by selecting the handler from the **Configured List** and clicking **Remove**. The handler is moved to the **Available List**.
   c. Rearrange the order in which the handlers are called by selecting the handler and clicking **Move Up** or **Move Down**.

      Handlers are called in the order in which they are listed in the **Configured List**. The first available handler that can process the request is the one that handles the request. If you anticipate receiving a large number of documents of a certain type (for example, ROD documents), you can move the handler associated with that type of document (in this example, com.ibm.bcg.edi.business.process.RODScannerHandler) to the top of the list.
6. Click **Save**.

Inbound workflows

This section lists the handlers configured for the inbound workflows.

Protocol unpackaging handlers

By default, the Protocol Unpackaging step has the following handlers configured:

- com.ibm.bcg.ediint.ASUnpackagingHandler
- com.ibm.bcg.server.pkg.NullUnpackagingHandler
- com.ibm.bcg.server.pkg.MIMEMultipartUnpackagingHandler
- com.ibm.bcg.eai.EAIUnpackagingHandler

Protocol processing handlers

By default, the Protocol Processing step has the following handlers configured:

- com.ibm.bcg.server.RNOChannelParseHandler
- com.ibm.bcg.server.RNSignalChannelParseHandler
- com.ibm.bcg.server.RNSCChannelParseHandler
- com.ibm.bcg.server.BinaryChannelParseHandler
- com.ibm.bcg.cxml.cXMLChannelParseHandler

- com.ibm.bcg.soap.SOAPChannelParseHandler
- com.ibm.bcg.server.XMLRouterBizProcessHandler
- com.ibm.bcg.edi.EDIRouterBizProcessHandler
- com.ibm.bcg.edi.business.process.RODScannerHandler
- com.ibm.bcg.edi.business.process.NetworkAckHandler

Outbound workflow

By default, the Protocol Packaging step has the following handlers configured:

- com.ibm.bcg.server.pkg.NullPackagingHandler
- com.ibm.bcg.ediint.ASPackagingHandler
- com.ibm.bcg.edi.server.EDITransactionHandler
- com.ibm.bcg.rosettanet.pkg.RNOPPackagingHandler
- com.ibm.bcg.server.pkg.RNPassThruPackagingHandler
- com.ibm.bcg.cxml.cXMLPackagingHandler
- com.ibm.bcg.soap.SOAPPackagingHandler
- com.ibm.bcg.eai.EAIPackagingHandler

Configuring actions

Chapter 1, “Introduction” described that actions can be made up of one or more steps. WebSphere Partner Gateway supplies a series of default actions. You can add to the list of actions by uploading one or more action handlers (which are steps in the action), which you can then use in an action. You can also create new actions, as described in “Creating actions” on page 52.

Note: You cannot modify the actions supplied by WebSphere Partner Gateway, although you can copy one of those actions and modify it, as described in “Copying an action” on page 52.

If you are going to use a user-defined handler to configure an action, upload the handler, as described in “Uploading handlers” on page 49.

Modifying a user-defined action

To configure a user-defined action, perform the following steps:

1. Click **Hub Admin > Hub Configuration > Actions**.
2. Click the **View details** icon next to the name of the user-defined action you want to configure.

   The action, along with a list of handlers (action steps) already configured for that action, is listed.
3. Perform one or more of the following steps for each action you want to modify.
   a. Add a step by selecting the associated handler from the **Available List** and clicking **Add**. The handler is moved to the **Configured List**.
   b. Remove a handler by selecting the handler from the **Configured List** and clicking **Remove**. The handler is moved to the **Available List**.
   c. Rearrange the order in which the handlers are called by selecting the handler and clicking **Move Up** or **Move Down**.
   d. Cause a handler to be processed more than once by selecting it and then clicking **Repeat**.

Remember that all handlers configured for an action are called and the steps that the handlers represent are performed in the order in which they appear in the **Configured List**.

e. Configure the handler by selecting it from the **Configured List** and clicking **Configure**. The list of attributes that can be configured is displayed.

4. Click **Save**.

Creating actions

You can create an action in one of the following ways:

- Create a new action and associate handlers with the action.
- Copy a product-supplied action and, if necessary, modify the handlers associated with it.

Creating a new action

To create a new action, perform the following steps:

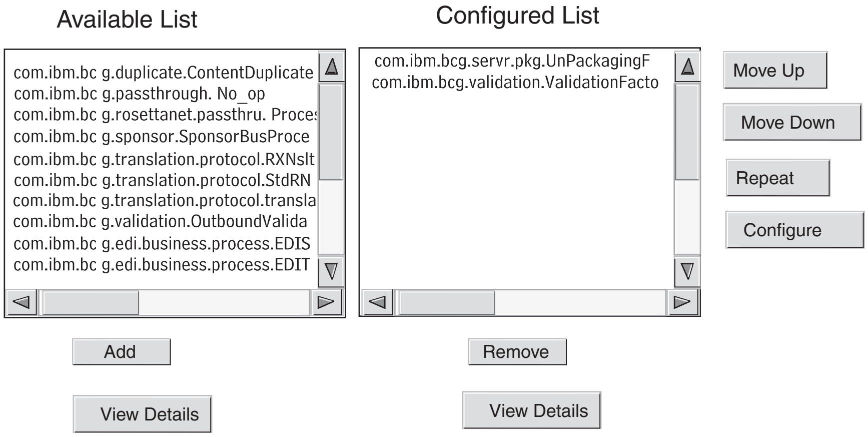
1. Click **Hub Admin > Hub Configuration > Actions**.
2. Click **Create**.
3. Enter a name for the action. This field is required.
4. Enter an optional description of the action.
5. Indicate whether the action is enabled for use.
6. For each step that will be invoked as part of the action, add the associated handler by selecting it from the **Available List** and clicking **Add**. The handler is moved to the **Configured List**.

   Remember that handlers are called by the action in the order in which they appear in the **Configured List**. Make sure you place the handlers in the correct order. You can use **Move Up** or **Move Down** to rearrange the order of the handlers or **Repeat** to cause a handler to be processed more than once.
7. Configure a handler by selecting it from the **Configured List** and clicking **Configure**. The list of attributes that can be configured is displayed.
8. Click **Save**.

Copying an action

To create an action by copying an existing action, perform the following steps:

1. Click **Hub Admin > Hub Configuration > Actions**.
2. From the Actions list, click the **Copy** icon next to the action you want to copy.
3. Enter a name for the action. This field is required.
4. Enter an optional description of the action.
5. Indicate whether the action is enabled for use.
6. Notice that one or more steps are already on the **Configured List**. These are the steps associated with the action you copied. For example, if you cloned the system-supplied Community Manager Cancellation of RosettaNet Process action, you would see the following list of available and configured handlers:



com.ibm.bc g.duplicate.ContentDuplicate
com.ibm.bc g.passthrough. No_op
com.ibm.bc g.rosettanet.passthru. Proces
com.ibm.bc g.sponsor.SponsorBusProce
com.ibm.bc g.translation.protocol.RXNslt
com.ibm.bc g.translation.protocol.StdRN
com.ibm.bc g.translation.protocol.transla
com.ibm.bc g.validation.OutboundValida
com.ibm.bc g.edi.business.process.EDIS
com.ibm.bc g.edi.business.process.EDIT

com.ibm.bcg.servr.pkg.UnPackagingF
com.ibm.bcg.validation.ValidationFacto

Figure 19. Cloning an action

To modify the **Configured List**, perform one or more of the following steps:

a. Add a step by selecting the associated handler from the **Available List** and clicking **Add**. The handler is moved to the **Configured List**.

b. Remove a step by selecting the associated handler from the **Configured List** and clicking **Remove**. The handler is moved to the **Available List**.

c. Rearrange the order in which the handlers are called by selecting the handler and clicking **Move Up** or **Move Down**.

   Remember that all handlers configured for an action are called and the steps associated with the handlers are performed in the order in which they appear in the **Configured List**.

d. Configure the step by selecting it from the **Configured List** and clicking **Configure**. The list of attributes that can be configured is displayed.

7. Click **Save.**

Chapter 7. Configuring document flows

This chapter describes how to configure the non-EDI documents you will be exchanging with your community participants and with your back-end applications. Configuring document flows and interactions for EDI documents (with the exception of EDI documents that are being passed through) is described in Chapter 8, “Configuring EDI document flows,” on page 81. Chapter 8 also describes how to configure document flows and interactions for XML and record-oriented-data (ROD) documents.

The chapter covers the following topics:

- “Overview”
- “Binary documents” on page 58
- “EDI documents with Pass Through action” on page 59
- “RosettaNet documents” on page 60
- “Web services” on page 68
- “cXML documents” on page 73
- “Custom XML documents” on page 77

Overview

A document flow definition is made up of, at minimum, a package, a protocol, and a document flow. For some protocols, an activity, action, and signal can be specified. The document flow definitions specify the types of document that will be processed by WebSphere Partner Gateway.

Packaging refers to the logic that is required to package a document according to a specification, such as AS2. A protocol flow is the logic that is required to process a document that adheres to a certain protocol, such as EDI-X12. A document flow describes what the document will look like.

The following sections briefly describe the overall steps for setting up a document flow between the Community Manager and a participant.

Step 1: Make sure the document flow definition is available

Check to see whether a document flow definition exists (from the ones that are predefined with the system). If the flow does not already exist, you create it by uploading the necessary files, or by manually creating a custom definition.

As part of establishing the document flow definition, you can modify certain attributes. Attributes are used to perform various document-processing and routing functions, such as validation, checking for encryption, and retry count. The attributes you set at the document flow definition level provide a global setting for the associated package, protocol, or document flow. The attributes that are available vary, depending on the document flow definition. Attributes for EDI document flow definitions, for example, have different attributes from RosettaNet document flow definitions.

For example, if you specify a value for **Time to Acknowledge** on the AS package, it applies to all documents packaged with AS. (**Time to Acknowledge** specifies the

© Copyright IBM Corp. 2004, 2005

amount of time to wait for an MDN (message disposition notification) acknowledgment before resending the original request.) If you later set the **Time to Acknowledge** attribute at the B2B capabilities level, that setting overrides the one set at the document flow definition level.

For attributes that can be set at all levels of the document flow definition, the values set at the document flow level take precedence over those set at the protocol level, and the attributes set at the protocol level take precedence over the package level.

You must have the document flow listed on the Manage Document Flow Definitions page before you can create interactions.

Step 2: Create interactions

Create interactions for the document flows that have been defined. The interaction tells WebSphere Partner Gateway which actions to perform on a document. For some exchanges, you need only two flows, one to describe the document that is received into the hub (from the participant or Community Manager) and one that describes the document that is sent from the hub (to the participant or Community Manager). However, if the hub is sending or receiving an EDI interchange that will be split into individual transactions or in which acknowledgments are required, you will actually create multiple interactions to perform the exchange.

Step 3: Create participant profiles, gateways, and B2B capabilities

Create participant profiles for the Community Manager and for community participants. Define gateways (which determine where documents will be sent) and B2B capabilities, which specify the documents the Community Manager and participants are capable of sending and receiving. The B2B capabilities page lists all the document flows that have been defined.

You can set attributes at the B2B capabilities level. Any attributes you set at this level override those set at the document flow definition level. For example, if you set **Time to Acknowledge** to 30 at the document flow definition level for AS package but then set it to 60 at the B2B capabilities level, the value of 60 is used. Setting an attribute at the B2B level lets you tailor the attribute to a specific participant.

You must have the profiles and B2B capabilities of the Community Manager and participants defined before you can create connections between them.

Step 4: Activate connections

Activate connections between the Community Manager and participants. The connections that are available are based on the B2B capabilities of the participants. The B2B capabilities are based on the interactions you created. The interactions depend on the document flow definitions being available.

For some exchanges, only one connection is required. For example, if a participant is sending a binary document to a Community Manager back-end application, only one connection is needed. For the exchange of EDI interchanges in which the interchange is de-enveloped and the individual transactions are transformed, however, multiple connections are set up.

Note: For EDI interchanges that are being passed through as is, only one connection is required.

You can set attributes at the connection level. Any attributes you set at this level override those set at the B2B attributes level. For example, if you set **Time to Acknowledge** to 60 for the AS2 package at the B2B capabilities level but then set it to 120, the value of 120 is used. Setting a value for an attribute at the connection level lets you further tailor the attribute, depending on the routing requirements of the participants and applications involved.

An example flow

By default, several packaging methods are enabled. To illustrate the overall procedure for establishing document flow definitions, consider the case in which you have an agreement with a community participant to receive an EDI interchange that adheres to the EDI-X12 standard. The participant will send the document in AS2 packaging. You will specify that the interchange be sent as is (without transformation) to a back-end application with no packaging.

1. At the Manage Document Flow Definitions page, verify that the document flow definition (which describes the type of document that will flow into the hub from the community participant) is enabled.
   a. Click **Hub Admin > Hub Configuration > Document Flow Definition**.
   b. Click the **Expand** icon next to **Package: AS**. Notice that **EDI-X12** is already listed.
   c. Click the **Expand** icon next to **Protocol: EDI-X12**. Notice that **Document Flow: ISA** is already listed.
2. With the Manage Document Flow Definition page still displayed, verify the second document flow definition (which describes the type of document that will flow to the back-end application) is enabled.
   a. Click the **Expand** icon next to **Package: None**. Notice that **EDI-X12** is already listed.
   b. Click the **Expand** icon next to **Protocol: EDI-X12**. Notice that **Document Flow: ISA** is already listed.
3. Create an interaction that describes whether the document flow will be a source flow or a target flow.
   a. With the Manage Document Flow Definition page still displayed, click **Manage Interactions**.
   b. Click **Create Interaction**.
   c. In the Source column, expand **Package: AS**, **Protocol: EDI-X12 (ALL)**, and then click **Document Flow: ISA**.
   d. In the Target column, expand **Package: None**, **Protocol: EDI-X12 (ALL)**, and then click **Document Flow: ISA**.
   e. In this example, no transformation is occurring. Therefore, do not select anything from the **Transformation Map** list.
   f. From the **Action list**, select **Pass Through**.
   g. Click **Save**.

At this point, you have specified that the hub is capable of accepting EDI-X12 interchanges (ISA standard) packaged as AS. You have also specified that the hub is capable of sending EDI-X12 interchanges (ISA standard) with no packaging. Further, you have specified that no transformation is to occur with the interchange; it is simply passed through to the back-end application (after the AS headers are removed).

You have not yet specified which community participant is capable of sending this type of interchange to the hub. You define that when you set up the participant profile and the participant's B2B capabilities. (You also define a profile and B2B capabilities for the Community Manager back-end system.) After you perform these tasks, you then create a connection between the community participant and the back-end application. Figure 20 shows the connection between the participant and the Community Manager back-end application for this example.

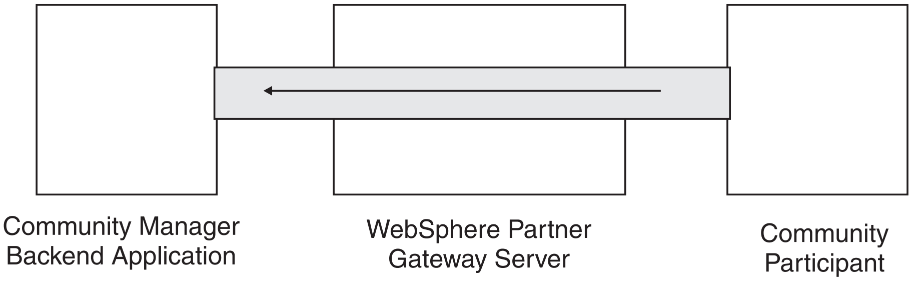

Community Manager Backend Application
WebSphere Partner Gateway Server
Community Participant

Figure 20. A one-way connection from a participant to the Community Manager

You verify that a connection exists using the Manage Connections page (**Account Admin > Participant Connections**). On the Manage Connections page, you select the participant from the **Source** list, Community Manager from the **Target** list, and click **Search**. The one available connection is listed. If necessary, you can modify attributes and actions, as will be described in subsequent sections.

There are three types of document flow definitions--ones supplied with the system that you can select from the console, ones that are already defined but not yet on the Community Console (you upload these definitions either from the WebSphere Partner Gateway installation medium or from another location), and those that you create yourself. For each type of document flow definition, you can (or sometimes must) specify attributes or upload maps that further define the document flow.

Binary documents

Binary document are passed through the hub as is, and, therefore, exchanging binary documents between a community participant and a Community Manager back-end application is a straightforward process. The binary protocol is already available for the AS, None, and Backend Integration packages; therefore, "Step 1: Make sure the document flow definition is available" on page 55 is already done.

Note: You can add attributes at any level (Package, Protocol, or Document Flow) to modify default processing by clicking the **Edit Attribute Values** icon. No attributes are associated by default with the binary protocol or document flow.

Similarly, four interactions involving binary documents are already provided by default, and for those interactions, it is not necessary for you to perform Step 2: Create interactions. Interactions are supplied for the following exchanges:

Table 4. System-supplied interactions

Source Package/Protocol/Document flow	Target Package/Protocol/Document flow
AS/Binary/Binary	Backend Integration/Binary/Binary
Backend Integration/Binary/Binary	AS/Binary/Binary
AS/Binary/Binary	None/Binary/Binary

Table 4. System-supplied interactions (continued)

Source Package/Protocol/Document flow	Target Package/Protocol/Document flow
None/Binary/Binary	AS/Binary/Binary

For the exchange of binary documents, you still have to perform:

- Step 3: Create participant profiles, gateways, and B2B capabilities, which is described in Chapter 9, "Creating the Community Manager profile and B2B capabilities," on page 119, Chapter 11, "Creating participants and their B2B capabilities," on page 139, and Chapter 10, "Creating gateways," on page 123.
- Step 4: Activate connections, which is described in Chapter 12, "Managing connections," on page 143.

EDI documents with Pass Through action

WebSphere Partner Gateway provides the capability to de-envelope and transform EDI interchanges, a process described in Chapter 8, "Configuring EDI document flows," on page 81.

Figure 21 shows the flow of an EDI interchange that is being passed through from a participant to the Community Manager.

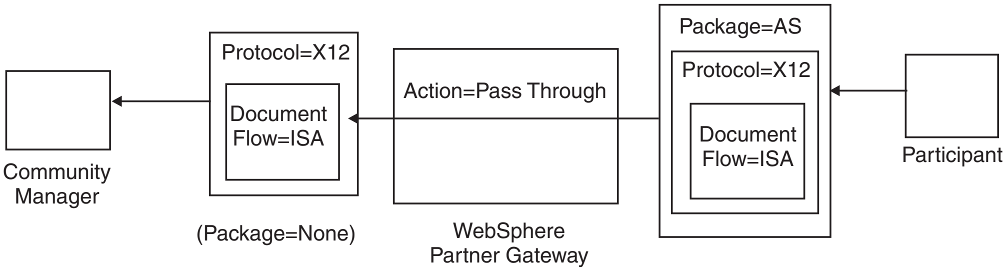


Figure 21. Incoming EDI interchange with Pass Through action

In this example, the AS2 headers are removed, but otherwise the interchange is left intact and flows through the system to the gateway of the Community Manager.

Creating document flow definitions

The document flow for EDI passthrough exchanges is already provided (by default) on the Manage Document Flow Definitions page, as described in "An example flow" on page 57. If you want to modify any of the attributes that have default values or set an attribute that has no assigned value, you can use the Manage Document Flow Definitions page to perform this task.

For example, suppose you want to change the **Time to Acknowledge** attribute for an EDI document packaged with AS. These are the steps you take:

1. Click **Hub Admin > Hub Configuration > Document Flow Definition**.
2. Click the **Edit Attribute Values** icon next to **Package: AS**.
3. Scroll down to the section of the page titled **Document Flow Context Attributes**.
4. In the **Time to Acknowledge** row, type a different value in the **Update** column.
5. Click **Save**.

Note that you changed a package attribute in this example. The attributes for protocol (for example, EDI-X12) and document flow (for example, ISA) are not relevant for a Pass Through action. This package attribute applies to all documents wrapped in AS packaging.

Creating interactions

To create the interaction for an EDI interchange with Pass Through action, perform the following steps:

1. Click **Hub Admin > Hub Configuration > Document Flow Definition**.
2. From the Manage Document Flow Definitions page, click **Manage Interactions**.
3. Click **Create Interaction**.
4. Under **Source**, expand **Package: AS** and **Protocol: EDI-X12** and then select **Document Flow: ISA**.
5. Under **Target**, expand **Package: None** and **Protocol: EDI-X12** and then select **Document Flow: ISA**.
6. From the **Action** list, select **Pass Through**.

Steps 1 through 6 have enabled WebSphere Partner Gateway to accept an EDI-X12 interchange packaged as AS from a source participant, to send an EDI-X12 interchange with no packaging to the target participant, and to have the interchange pass through from the source to the target.

If you want to set up an interaction that has the source document packaged as None/EDI-X12/ISA and the target document packaged as AS/EDI-X12/ISA, expand **Package: None** in step 4 (in the **Source** column) and expand **Package: AS** in step 5 (in the **Target** column).

RosettaNet documents

This section provides an overview of RosettaNet documents and shows you how to set up document flow definitions and interactions for those documents.

Overview

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

WebSphere Partner Gateway supports RosettaNet messaging using RNIF 1.1 and 2.0. When the hub receives a PIP message, it validates and transforms the message to send it to the appropriate back-end system. WebSphere Partner Gateway provides a protocol for packaging the transformed message into a RosettaNet Service Content (RNSC) message that the back-end system can handle. See the *Enterprise Integration Guide* for information about the packaging used on these messages to provide routing information.

The hub can also receive RNSC messages from back-end systems and create the appropriate PIP message and send the message to the appropriate trading partner (a participant). You provide the document flow definitions for the RNIF version and the PIPs you want to use.

In addition to providing routing capability for RosettaNet messages, WebSphere Partner Gateway maintains a state for each message it handles. This enables it to resend any messages that fail until the number of attempts reaches a specified threshold. The Event Notification mechanism alerts back-end systems if a PIP message cannot be delivered. Additionally, the hub can automatically generate 0A1 PIPs to send to appropriate participants if it receives certain Event Notification messages from back-end systems. See the *Enterprise Integration Guide* for more information about Event Notification.

RNIF and PIP document flow packages

To support RosettaNet messaging, WebSphere Partner Gateway provides two sets of zipped files called packages. The *RNIF packages* consist of document flow definitions required to support the RNIF protocol. These packages are in the B2BIntegrate directory.

For RNIF V1.1, the packages are:
- Package_RNIF_1.1.zip
- Package_RNSC_1.0_RNIF_1.1.zip

For RNIF V02.00, the packages are:
- Package_RNIF_V02.00.zip
- Package_RNSC_1.0_RNIF_V02.00.zip

The first package in each pair provides the document flow definitions required to support RosettaNet communications with participants, and the second package provides the document flow definitions required to support RosettaNet communications with back-end systems.

The second set of packages consists of PIP document flow packages. Each PIP document flow package has a Packages directory containing an XML file and a GuidelineMaps directory containing XSD files. The XML file specifies the document flow definitions that define how WebSphere Partner Gateway handles the PIP and define the exchanged messages and signals. The XSD files specify the format of the PIP messages and define acceptable values for XML elements in the messages. The zipped files for 0A1 PIPs also have an XML file that the hub uses as a template to create 0A1 documents.

The PIPs for which WebSphere Partner Gateway provides PIP document flow packages are:
- PIP 0A1 Notification of Failure v1.0
- PIP 0A1 Notification of Failure V02.00.00
- PIP 2A1 Distribute New Product Information V02.00.00
- PIP 2A12 Distribute Product Master V01.03.00
- PIP 3A1 Request Quote V02.00.00
- PIP 3A2 Request Price and Availability R02.01.00
- PIP 3A4 Request Purchase Order V02.02.00
- PIP 3A4 Request Purchase Order V02.00

- PIP 3A5 Query Order Status R02.00.00
- PIP 3A6 Distribute Order Status V02.02.00
- PIP 3A7 Notify of Purchase OrderUpdate V02.02.00
- PIP 3A8 Request Purchase Order Change V01.02.00
- PIP 3A8 Request Purchase Order Change V01.03.00
- PIP 3A9 Request Purchase Order Cancellation V01.01.00
- PIP 3B2 Notify of Advance Shipment V01.01.00
- PIP 3B3 Distribute Shipment Status R01.00.00
- PIP 3B11 Notify of Shipping Order R01.00.00A
- PIP 3B12 Request Shipping Order V01.01.00
- PIP 3B13 Notify of Shipping Order Confirmation V01.01.00
- PIP 3B14 Request Shipping Order Cancellation V01.00.00
- PIP 3B18 Notify of Shipping Documentation V01.00.00
- PIP 3C1 Return Product V01.00.00
- PIP 3C3 Notify of Invoice V01.01.00
- PIP 3C4 Notify of Invoice Reject V01.00.00
- PIP 3C6 Notify of Remittance Advice V01.00.00
- PIP 3C7 Notify of Self-Billing Invoice V01.00.00
- PIP 3D8 Distribute Work in Process V01.00.00
- PIP 4A1 Notify of Strategic Forecast V02.00.00
- PIP 4A3 Notify of Threshold Release Forecast V02.00.00
- PIP 4A4 Notify of Planning Release Forecast R02.00.00A
- PIP 4A5 Notify of Forecast Reply V02.00.00
- PIP 4B2 Notify of Shipment Receipt V01.00.00
- PIP 4B3 Notify of Consumption V01.00.00
- PIP 4C1 Distribute Inventory Report V02.03.00
- PIP 4C1 Distribute Inventory Report V02.01
- PIP 5C1 Distribute Product List V01.00.00
- PIP 5C2 Request Design Registration V01.00.00
- PIP 5C4 Distribute Registration Status V01.02.00
- PIP 5D1 Request Ship From Stock And Debit Authorization V01.00.00
- PIP 6C1 Query Service Entitlement V01.00.00
- PIP 6C2 Request Warranty Claim V01.00.00
- PIP 7B1 Distribute Work in Process V01.00.00
- PIP 7B5 Notify of Manufacturing Work Order V01.00.00
- PIP 7B6 Notify of Manufacturing Work Order Reply V01.00.00

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

- For RNIF 1.1 messaging with participants
- For RNIF 1.1 messaging with back-end systems
- For RNIF 2.0 messaging with participants
- For RNIF 2.0 messaging with back-end systems

Each PIP document flow package follows a specific naming convention you can use to identify whether the package is for messages between WebSphere Partner Gateway and participants or between WebSphere Partner Gateway and back-end systems. The naming convention also identifies the RNIF version, PIP, and PIP version that the package supports. For PIP document flow packages used for messaging between WebSphere Partner Gateway and participants, the format is:

```
BCG_Package_RNIF<RNIF_version>_<PIP><PIP_version>.zip
```

For PIP document flow packages used for messaging between WebSphere Partner Gateway and back-end systems, the format is:

```
BCG_Package_RNSC<Backend_Integration_version>_RNIF<RNIF_version>_
<PIP><PIP_version>.zip
```

For example, the BCG_Package_RNIF1.1_3A4V02.02.zip is for validating documents for version 02.02 of the 3A4 PIP sent between participants and WebSphere Partner Gateway using the RNIF 1.1 protocol. For PIP document flow packages for communicating with back-end systems, the name of the package must also identify the protocol used to send the RosettaNet contents to the back-end systems. See the *Enterprise Integration Guide* for information about the packaging used for these messages.

Creating document flow definitions

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

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

The first package supports RosettaNet messaging with participants and the second package supports RosettaNet messaging with back-end systems. The third and fourth packages enable WebSphere Partner Gateway to pass 3A4 messages between participants and back-end systems using RNIF 2.0.

To upload the RosettaNet packages:

1. Click **Hub Admin > Hub Configuration > Document Flow Definition**.
2. Click **Upload/Download Packages**.
3. Select **No** for **WSDL Package**.
4. Click **Browse** and select the RNIF package for communicating with participants.

   The RNIF packages are located, by default, in the B2BIntegrate/Rosettanet directory on the installation medium. For example, if you were uploading RNIF version 2.00 package, you would browse to the B2BIntegrate/Rosettanet directory and select: Package_RNIF_V0200.zip.
5. Make sure **Commit to Database** is set to **Yes**.
6. Click **Upload**.
7. Click **Browse** again and select the RNIF package for communicating with back-end applications.

   For example, if you were uploading the RNIF version 2.00 package, you would browse to the B2BIntegrate/Rosettanet directory and select Package_RNSC_1.0_RNIF_V02.00.zip.
8. Click **Upload**.

The packages needed to communicate with participants or with the back-end system are now installed in the system. If you check the Manage Document Definitions page, you see an entry for **Package: RNIF/Protocol: RosettaNet**, which represents the packaging for communicating with participants, and **Package: Backend Integration/Protocol: RNSC**, which represents the packaging for communicating with back-end applications.

9. For each PIP you want to support, upload the PIP document flow package for the PIP and for the RNIF version you are supporting. For example, to upload the 3A6 PIP (Notify of Remittance Advice) to be sent to a participant, perform the following steps:
   a. Click **Browse** and select BCG_Package_RNIFV02.00_3C6V02.02 from the B2BIntegrate/Rosettanet directory.
   b. Make sure **Commit to Database** is set to **Yes**.
   c. Click **Upload**.

   The 3C6V02.02 PIP now appears as the document flow underneath **Package: RNIF/Protocol: RosettaNet** on the Manage Document Definitions page. An activity, action, and two signals are also displayed. They are included in the upload of the PIP.

   To upload the 3A6 PIP to be sent to the back-end application, perform the following steps:
   a. Click **Browse** and select BCG_Package_RNSC1.0_RNIFV02.00_3C6V02.02.zip.
   b. Make sure **Commit to Database** is set to **Yes**.
   c. Click **Upload**.

   The 3C6V02.02 PIP now appears as the document flow underneath **Package: Backend Integration/Protocol: RNSC** on the Manage Document Flow Definitions page. If WebSphere Partner Gateway does not provide a package for the PIP or PIP version you want to use, you can create your own and upload it. See “Creating PIP document flow packages” on page 219 for more information.

Configuring attribute values

For PIP document flow definitions, most of the values of the attributes are already set and do not need to be configured. However, you do need to set the following attributes:

RNIF (1.0) package

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

RNIF (V02.00) package

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

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

Note: The behavior of the Sync Ack Required attribute differs between 1-way and 2-way PIPs. For a 2-way PIP, when Sync Ack Required is set to No, this setting takes precedence over a NonRep of Rec setting of Yes. For example, suppose you send a 3A7 with the following settings:

- SiqReq=Y
- NonRepofRec=Y
- SyncSupported=Y
- SyncAckReq=N

For a 2-way PIP, you receive an error message on the incoming document. On a 1-way PIP, however, you see the incoming document on the console, and a 0KB 200 is returned to the participant.

To set the attributes, perform the following steps:

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

Note: You can also update RosettaNet attributes at the connection level by clicking **Attributes** for the source or target and then entering or changing the values in the **Update** column. Refer to “Specifying or changing attributes” on page 144.

Creating interactions

The following process describes how to create an interaction between a back-end system and a participant. Note that you must create an interaction for each PIP that you want to send and one for each PIP that you want to receive.

Before you begin, make sure that the appropriate RNIF document flow definitions have been uploaded and that the packages for the PIP you want to use have been uploaded. If you want the ability to generate an 0A1 PIP (Notification of Failure), make sure you have uploaded that PIP, as described in step 9 on page 64.

To create an interaction for a particular PIP, perform the following steps:

1. Click **Hub Admin > Hub Configuration > Document Flow Definition**.
2. Click **Manage Interactions**.
3. Click **Create Interaction**.
4. Expand the **Source** tree to the **Action** level and expand the **Target** tree to the **Action** level.
5. In the trees, select the document flow definitions to use for the source context and the target context. For example, if the participant is the initiator of a 3C6 PIP (a one-action PIP), select the following document flow definitions:

Table 5. 3C6 PIP initiated by a participant

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

If the back-end system is the initiator of the 3C6 PIP, select the following document flow definitions:

Table 6. 3C6 PIP initiated by a back-end system

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

For a two-action PIP such as 3A4 initiated by a participant, select the following document flow definitions for the first action:

Table 7. 3A4 PIP initiated by a participant

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

If a back-end system initiates the two-action 3A4 PIP, select the following document flow definitions for the first action:

Table 8. 3A4 PIP initiated by a back-end system

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

6. In the Action field, select **Bi-Directional Translation of RosettaNet and RosettaNet Service Content with Validation**.
7. Click **Save**.
8. If you are setting up a two-action PIP, repeat the steps needed to create the interaction for the second action. For example, select the following document

flow definitions for the second action for a 3A4 PIP initiated by a participant. This is the action in which the back-end system sends the response.

Table 9. 3A4 PIP initiated by a participant (second action)

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

For the second action for a back-end system initiated 3A4 PIP, select the following document flow definitions:

Table 10. 3A4 PIP initiated by a back-end system (second action)

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

9. If you want to generate the 0A1 Notification of Failure, create an interaction for XMLEvent.
   a. Click **Hub Admin > Hub Configuration > Document Flow Definition**.
   b. Click **Manage Interactions**.
   c. Click **Create Interaction**.
   d. Expand the **Source** tree to the **Document Flow** level and expand the **Target** tree to the **Document Flow** level.
   e. Select the following document flow definitions:

Table 11. XML Event document flow definition

Source	**Target**
Package: Backend Integration (1.0)	Package: Backend Integration (1.0)
Protocol: XMLEvent (1.0)	Protocol: XMLEvent (1.0)
Document Flow: XMLEvent (1.0)	Document Flow: XMLEvent (1.0)

   f. In the Action field, select **Pass Through**.
   g. Click **Save**.
10. Create an interaction for XMLEvent to 0A1 RNSC.
   a. Click **Hub Admin > Hub Configuration > Document Flow Definition**.
   b. Click **Manage Interactions**.
   c. Click **Create Interaction**.
   d. Expand the **Source** tree to the **Document Flow** level and expand the **Target** tree to the **Activity** level.

e. Select the following document flow definitions:

Table 12. XML Event to 0A1 document flow definition

Source	Target
Package: Backend Integration (1.0)	Package: Backend Integration (1.0)
Protocol: XMLEvent (1.0)	Protocol: RNSC (1.0)
Document Flow: XMLEvent (1.0)	Document Flow: 0A1 (V02.00)
	Activity: Distribute Notification of Failure.

f. In the Action field, select **Bi-directional Translation of RosettaNet and XML with Validation**.

g. Click **Save**.

Web services

A participant can request a Web service provided by the Community Manager. Similarly, the Community Manager can request a Web service provided by a participant. The participant or Community Manager invokes the WebSphere Partner Gateway server to obtain the Web service. WebSphere Partner Gateway acts as a proxy, passing the Web service request to the Web service provider and returning the response synchronously from the provider to the requester.

This section contains the following information for setting up a Web service for use by a participant or a Community Manager:

- Identifying the participants for a Web service
- Setting up a document flow definition for a Web service
- Adding document flow definitions to participant B2B capabilities
- Restrictions and limitations of Web service support

Identifying the participants for a Web service

When a Web service is provided by the Community Manager for use by participants, WebSphere Partner Gateway requires that a participant identify itself. When posting the Web service request, set the identity in one of the following two ways:

1. Use HTTP Basic Authentication with User ID of the form *<participant's_business_ID>/<console_user_name>* (for example, 123456789/joesmith) and a password equal to the console user name's password.
2. Present an SSL client certificate that has been previously loaded into WebSphere Partner Gateway for the participant

When the Web service is provided by a participant, for use by the Community Manager, the public URL used by the Community Manager to invoke the Web service should contain the query string `?to=<participant's_business_ID>`. An example is:

```
http://<IP_address>/bcgreceiver/Receiver?to=123456789
```

This tells WebSphere Partner Gateway that the provider of the Web service is the participant with business ID 123456789.

Creating document flow definitions

To set up the document flow definition, you either upload the WSDL (Web Service Definition Language) files that define the Web service, or you enter the equivalent document flow definitions manually through the Community Console.

Uploading the WSDL files for a Web service

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

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

For example, suppose the primary WSDL file `helloworldRPC.wsdl` contains the following import element:

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

And suppose the imported WSDL file `bindingRPC.wsdl` contains the following import element:

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

The file should contain the following:

```
Name                Path

helloworldRPC.wsdl

bindingRPC.wsdl

porttypeRPC.wsdl            port\
```

When a WSDL file definition of a Web service is uploaded, the original WSDL is saved as a validation map. (Web service messages are not actually validated by WebSphere Partner Gateway. They are passed through directly, with the original service end-point URL.) This is called the *private* WSDL.

In addition, a public WSDL is saved with the private URL replaced by the target URL specified on the Upload/Download Packages page. The public WSDL will be provided to the users of the Web service, who will invoke the Web service at the target's URL (the public URL). WebSphere Partner Gateway will then route the Web service request to a gateway that is the original Web service provider's private URL. WebSphere Partner Gateway acts as a proxy, forwarding the Web service request to a private provider URL, which is hidden from the Web service user.

Both the private and public WSDLs (including any imported files) can be downloaded from the Community Console after the WSDL has been uploaded.

Uploading WSDL files using the Community Console: WebSphere Partner Gateway provides a way to import WSDL files. If a Web service is defined in a single WSDL file, you can upload the WSDL file directly. If the Web service is defined using multiple WSDL files (this happens when you have imported WSDL files within a primary WSDL file), they would be uploaded in a zipped archive.

Important: The WSDL files within the zipped archive must be within a directory specified in the WSDL import element. For example, suppose you have the following import element:

```
<import namespace="http://www.helloworld.com/wsdl/helloRPC.wsdl"
location="path1/bindingRPC.wsdl"/>
```

The directory structure within the zipped archive would be: `path1/bindingRPC.wsdl`.

Now consider this example:

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

The `bindingRPC.wsdl` file would be at the root level within the zipped archive.

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

1. Click **Hub Admin** > **Hub Configuration** > **Document Flow Definition**.
2. Click **Upload/Download Packages**.
3. For **WSDL Package**, click **Yes**.
4. For **Web Service Public URL**, perform one of the following steps:
   - For a Web service provided by the Community Manager (which will be invoked by a participant), type the public URL of the Web service. For example:

     `https://<`*`target_host:port`*`>/bcgreceiver/Receiver`

     The URL is typically the same as the production HTTP target defined in Targets.
   - For a Web service provided by a participant (which will be invoked by the Community Manager), type the public URL of the participant with a query string. For example:

     `https://<`*`target_host:port`*`>/bcgreceiver/Receiver?to=<`*`participant_business_ID`*`>`
5. Click **Browse** and select the WSDL file or zipped archive.
6. For **Commit to Database**, select **No** if you want to upload the file in test mode. When you select **No**, the file will not be installed into the system. Use the system-generated messages displayed in the Messages box to troubleshoot upload errors. Select **Yes** to upload the file into the system database.
7. For **Overwrite Data**, select **Yes** to replace a file currently in the database. Select **No** to add the file to the database.
8. Click **Upload**. The WSDL file is installed into the system.

Validating packages using schema files: A set of XML schemas that describe the XML files that can be uploaded through the console is provided on the WebSphere Partner Gateway installation medium. Uploaded files are validated against these schemas. The schema files are a useful reference for determining the cause of an error when a file cannot be uploaded because of non-conforming XML. The files are: `wsdl.xsd`, `wsdlhttp.xsd`, and `wsdlsoap.xsd`, which contain the schema describing valid Web Service Definition Language (WSDL) files.

The files are located in: `B2BIntegrate\packagingSchemas`

Creating the document flow definition manually

To enter the equivalent document flow definitions manually, follow the procedures in this section. You must also create the Document Flow, Activity, and Action entries individually under **Protocol: Web Service**, paying particular attention to the requirements for the Action and its relationship to the received SOAP messages.

In terms of the Package/Protocol/Document Flow/Activity/Action hierarchy of document flow definitions, a supported Web service is represented as:

- **Package: None**
- **Protocol: Web Service (1.0)**
- **Document Flow:** {<*Web_service_namespace*>:<*Web_service_name*>} (name and code), which is required to be unique among document flows for the Web Service protocol. This is typically the WSDL's namespace and name.
- **Activity:** One activity for each Web service operation, with name and code:

  {<*operation_namespace*>}:<*operation_name*>
- **Action**: One action for the input message of each operation, with name and code:

  {<*namespace_of_identifying_xml_element = first_child_of_soap:body*>}:
  <*name_of _identifying_xml_element = first_child_of_soap:body*>

The critical definitions are the Actions because WebSphere Partner Gateway will use an Action's namespace and name to recognize an incoming Web service request SOAP message and route it appropriately based on a defined participant connection. The namespace and name of the first child XML element of the received SOAP message's `soap:body` element must match a known Action's namespace and name in WebSphere Partner Gateway's document flow definitions.

For example, suppose a Web service request SOAP message for a document-literal SOAP binding is:

```
<?xml version="1.0" encoding="UTF-8"?>

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

WebSphere Partner Gateway would look for a defined Web Service Action with this code:

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

For an RPC binding style SOAP request message, for example:

```
<?xml version="1.0" encoding="UTF-8"?>

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

WebSphere Partner Gateway would look for a defined Web Service action with this code:

```
{http://www.helloworld.com/helloRPC}:helloWorldRPC
```

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

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

Creating interactions

To create an interaction for a Web service, you use the same Web service document flow action for both the Source and the Target.

To create interactions, use the following procedure.

1. Click **Hub Admin** > **Hub Configuration** > **Document Flow Definition**.
2. Click **Manage Interactions**.
3. Click **Create Interaction**.
4. Under **Source**, expand **Package: None > Protocol: Web Service > Document Flow: <** *document flow***> > Action:** <*action*>. Repeat this step in the **Target** column.
5. Select **Pass Through** from the **Action** list at the bottom of the page. (**Pass Through** is the only valid option supported in WebSphere Partner Gateway for a Web service.)

Restrictions and limitations of Web service support

WebSphere Partner Gateway supports the following standards:

- WSDL 1.1
- SOAP 1.1
- WS-I Basic Profile v. 1.0 (which contains important restrictions on the form of SOAP messages for document-literal binding)

Note:

- SOAP/HTTP binding are supported.
- Rebinding is not supported.
- RPC-encoded/RPC-literal and document-literal binding styles are supported (subject to the restrictions in the WS-I Basic Profile).
- Soap With Attachments is not supported.

cXML documents

This section contains an overview of cXML support and information about creating document flow definitions for cXML exchanges.

Overview

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

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

The Document Manager performs the DTD validation on cXML documents; however, WebSphere Partner Gateway does not provide cXML DTDs. You can download them from www.cxml.org and then upload them into WebSphere Partner Gateway through the Validation Map module in the Community Console. After you upload the DTD, associate it with the cXML document flow. Refer to "Associating maps with document flow definitions" on page 79 for more information about associating the DTD with the cXML document flow.

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

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

Note: Here and throughout this book, all DUNS numbers are meant to be examples only.

```
<Header>
<From>

            <Credential domain="AcmeUserId">
                <Identity>admin@acme.com</Identity>
            </Credential>
            <Credential domain="DUNS">
                <Identity>130313038</Identity>
            </Credential>
</From
<To>
            <Credential domain="DUNS">
                <Identity>987654321</Identity>
            </Credential>
            <Credential domain="IBMUserId">
                <Identity>test@ibm.com</Identity>
            </Credential>
</To>
```

If more than one credential element is used, the Document Manager uses the DUNS number as the Business Identifier for routing and authentication. In the case where there is no DUNS number given, the first Credential is used.

WebSphere Partner Gateway does not use the information in the Sender element.

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

cXML document types

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

Request: There are many types of cXML requests. The `Request` element within the cXML document corresponds to the Document Flow in WebSphere Partner Gateway. Typical request elements are:

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

The following table shows the relationship between the elements in a cXML request document and document flow definitions within WebSphere Partner Gateway:

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

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

- ProfileResponse
- PunchOutSetupResponse
- GetPendingResponse

The following table shows the relationship between the elements in a cXML response document and document flow definitions within WebSphere Partner Gateway:

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

Message: A cXML message contains the WebSphere Partner Gateway document flow information in the cXML `Message` element. It can contain an optional `Status` element identical to that found in a `Response` element. It would be used in messages that are responses to request messages.

The content of the message is custom defined by the business needs of the user. The element directly below the <Message> element corresponds to the document flow created in WebSphere Partner Gateway. In the following example, SubscriptionChangeMessage is the document flow:

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

The following table shows the relationship between the elements in a cXML message and the document flow definitions within WebSphere Partner Gateway:

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

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

A message can have the following attributes:

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

Content-type headers and attached documents

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

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

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

- Content-Type: multipart/related; boundary=<*something_unique*>
- Content-Type: multipart/mixed; boundary=<*something_unique*>

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

Valid cXML interactions

WebSphere Partner Gateway supports the following cXML document flow definition interactions:

- From participant to Community Manager: None/cXML to None/cXML with Pass Through and validation
- From Community Manager to participant:
  - None/cXML to None/cXML with Pass Through and validation
  - None/XML to None/cXML with Pass Through, validation, and transformation

Creating document flow definitions

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

Note: You must ensure that the correct version of cXML is defined before you create a cXML document flow definition. The default is version 1.2.009.

1. Click **Hub Admin** > **Hub Configuration** > **Document Flow Definition**.
2. Click **Create Document Flow Definition**. The Create Document Flow Definitions page is displayed.
3. Select **Document Flow** for Document flow type.
4. Perform one of the following tasks, depending on the type of document:
   - For requests, enter the request type (for example, `OrderRequest`) in the **Code** and **Name** fields.
   - For responses, if the Response does not have any child tags other than `<Status>`, enter `Response`. Otherwise, enter the next tag name following `<Status>`. In the example that follows, you would enter `Response` for the first Response element and `Profile Response` for the second.

     ```
     <cXML>
         <Response>
             <Status code="200" text="OK"/>
         </Response>
     </cXML>
     <cXML>
         <Response>
             <Status code="200" text="OK"/>
        <ProfileResponse>
         </Response>
     </cXML>
     ```
5. Enter **1.0** for **Version**.

   The version number is for reference only. The actual protocol version is derived from the DTD version within the cXML document.
6. Enter an optional **Description**.
7. Select **Yes** for **Document level**.
8. Select **Enabled** for **Status**.
9. Select **Yes** for all **Visibility** attributes.
10. Click on the **Package: None** folder to expand the package selection options.
11. Select **Protocol: cXML (1.2.009): cXML**.
12. Click **Save**.

Creating interactions

After you create the document flow definition, set up an interaction for the cXML document.

To create interactions, use the following procedure.

1. Click **Hub Admin** > **Hub Configuration** > **Document Flow Definition**.
2. Click **Manage Interactions**.
3. Click **Create Interaction**.
4. If the cXML document is the source, under **Source**, expand **Package: None** and **Protocol: cXML**, and select **Document Flow:**<*document _flow*>. If the cXML document is the target, expand **Package: None** and **Protocol: cXML**, and select **Document Flow:** <*document_flow*> in the **Target** column.
5. Expand the source or target column for the other half of the interaction (the document that will be converted to cXML or the document that will be transformed from cXML) and expand its package and protocol and select its document flow.
6. Select **Pass Through** from the **Action** list at the bottom of the page. (**Pass Through** is the only valid option supported for cXML documents.)

Custom XML documents

This section describe how to create custom XML documents.

Overview

XML (Extensible Markup Language) is the universal format for structured documents and data on the Web. Using the Manage XML Protocols page, you can create and manage custom XML formats that can be added to the list of available document flow definitions.

An XML format defines the paths within a set of XML documents. This enables the Document Manager to retrieve the values that uniquely identify an incoming document and access information within the document necessary for proper routing and processing.

Creating an XML format is a multi-step process. You must:

1. Create a protocol for the format and associate it with a package or packages
2. Create a document flow for the format and associate it with the newly created protocol
3. Create the format

You then create a valid interaction for the newly created format.

These steps are described in the sections that follow. You can also find an example of these steps in “Setting up the hub for custom XML documents” on page 181.

Creating a protocol definition format

The following steps describe how to create a custom XML protocol definition format:

1. Click **Hub Admin > Hub Configuration > Document Flow Definition > Create Document Flow Definition**.
2. For **Document flow type**, select **Protocol**.
3. For **Code**, enter the value for the type of object you selected in the previous step. For example, you might want to enter XML.
4. For **Name**, enter an identifier for the document flow definition. For example, for a custom XML protocol, you might enter Custom_XML. This field is required.

5. For **Version**, enter **1.0**.
6. Enter an optional description of the protocol.
7. Set **Document level** to **No**, because you are defining a protocol, rather than a document flow (which you will define in the next section).
8. Set **Status** to **Enabled**.
9. Set **Visibility** for this protocol. You will probably want it to be visible to all participants.
10. Select the packages in which this new protocol will be wrapped. For example, if you want this protocol to be associated with the AS, None, and Backend Integration packages, select **Package: AS**, **Package: None**, **Package: Backend Integration**.
11. Click **Save**.

Creating a document definition flow

Next, use the Create Document Flow Definition page again to create a document flow.

1. Click **Hub Admin > Hub Configuration > Document Flow Definition > Create Document Flow Definition**.
2. For **Document flow type**, select **Document Flow**.
3. For **Code**, enter the value for the type of object (document flow) you selected in the previous step.
4. For **Name**, enter an identifier for the document flow definition. For example, you might enter XML_Tester as a name for the document flow. This field is required.
5. For **Version**, enter **1.0**.
6. Enter an optional description of the protocol.
7. Set **Document level** to **Yes** (because you are defining a document level).
8. Set **Status** to **Enabled**.
9. Set **Visibility** for this flow. You will probably want it to be visible to all participants.
10. Click the **Expand** icon to expand each package you selected in step 10. Expand the folder and select the name of the protocol you created in the previous section (for example, Protocol: CustomXML.).
11. Click **Save**.

The Manage Document Flow Definitions page now contains a document flow of XML_Tester and a protocol of CustomXML under the AS, None, and Backend Integration packages.

Creating an XML format

After you create a custom XML protocol (and associate it with a package or set of packages) and create an associated document flow, you are ready to create the XML format.

To create an XML format, use the following procedure.

1. Click **Hub Admin > Hub Configuration > XML Formats**.
2. Click **Create XML Format**.
3. For **Routing Format**, select the document flow definition with which this format will be associated.
4. For **File Type**, select **XML**.

Note: XML is the only option available for file type.

5. For **Identifier Type**, select the element used to identify the incoming document type. The choices are **DTD**, **Name Space**, or **Root Tag**.
6. For each field for which a choice of types is offered, select either **Element Path**, which is the path to the value in the document, or **Constant**, which is the actual value in the document. Then provide a value.
   a. For **Source/Target Business ID**, enter the path of the business ID. This field is required.
   b. For **Source Document Flow & Version**, enter an expression that defines the path to the Document Flow and Version value within the XML document. This field is required.
   c. For **Document Identifier**, enter the path for the document ID number.
   d. For **Document Timestamp**, enter the path for the document creation time stamp.
   e. For **Duplicate Check Key 1-5**, enter paths used to identify the routing of a duplicate document.
7. Click **Save**.

Using validation maps

WebSphere Partner Gateway uses validation maps to validate the structure of certain documents. If you want to associate a validation map with a document, first make sure the validation map is available to WebSphere Partner Gateway, as described in "Adding validation maps."

Adding validation maps

An action can have an associated validation map to ensure that the destination participant or back-end system can parse the document. Note that a validation map only validates the *structure* of the document. It does not validate the contents of the message.

Note: Once you associate a validation map with a document flow definition, you cannot disassociate them.

To add a new validation map to the hub, use the following procedure.

1. Save the validation map file to the hub or to a location from which WebSphere Partner Gateway can read files.
2. Click **Hub Admin > Hub Configuration > Maps > Validation Maps**.
3. Click **Create**.
4. Type a description of the validation map.
5. Navigate to the schema file you want to use to validate documents and click **Open**.
6. Click **Save**.

Associating maps with document flow definitions

To associate a validation map with a document flow definition, use the following procedure.

1. Click **Hub Admin > Hub Configuration > Maps > Validation Maps**.
2. Click the **View details** icon next to the validation map you want to associate with the document flow definition.

3. Click the **Expand** icon next to a package to individually expand to the appropriate level (for example, **Action** for a RosettaNet document).
4. Select the document flow definition you want associated with the validation map.
5. Click **Save**.

Viewing documents

The Document Viewer displays information about the documents that make up a document flow. You can display raw documents and associated document processing details and events using specific search criteria. This information is useful if you are trying to determine whether a document was successfully delivered or to determine the cause of a problem.

To display the Document Viewer, click **Viewers > Document Viewer**. See the *Administrator Guide* for information on using the Document Viewer.

Chapter 8. Configuring EDI document flows

This chapter describes how to configure the document flow definitions and interactions for standard EDI interchanges. Also included in this chapter are descriptions of receiving and transforming XML and record-oriented-data (ROD) documents. This chapter covers the following topics.

- "Overview of EDI"
- "Overview of XML and ROD documents" on page 84
- "Overview of creating document flows and setting attributes" on page 85
- "Overview of possible flows" on page 87
- "How EDI interchanges are processed" on page 91
- "How XML or ROD documents are processed" on page 94
- "Setting up the EDI environment" on page 95
- "General steps for defining document exchanges" on page 106
- "Viewing EDI interchanges and transactions" on page 118

It is also possible to have an EDI interchange passed through with no de-enveloping or transformation. The steps for creating interactions for this type of exchange are presented in "EDI documents with Pass Through action" on page 59.

Overview of EDI

EDI is a method of transmitting business information over a network between business associates who agree to follow approved national or industry standards in translating and exchanging information. WebSphere Partner Gateway provides de-enveloping, transformation, and enveloping for the following EDI standards:

- X12, a common EDI standard approved by the American National Standards Institute
- UN/EDIFACT (United Nations Electronic Data Interchange for Administration Commerce and Support)
- UCS (Uniform Communication Standard)

The following sections provide a brief overview of EDI interchanges that conform to the X12, EDIFACT, and UCS standards and of the transactions and groups that are contained within the interchanges. Also described are how XML and ROD documents and EDI interchanges are transformed.

The EDI interchange structure

An EDI interchange contains one or more business transactions. In X12 and related standards, a business transaction is called a *transaction set*. In EDIFACT and related standards, a business transaction is called a *message*. This document generally uses the term *transaction* or *business transaction* to refer to an X12 or UCS transaction set or an EDIFACT message.

EDI interchanges are composed of *segments* which in turn contain *data elements*. Data elements represent things such as a name, quantity, date, or time. A segment is a group of related data elements. Segments are identified by a segment name or

© Copyright IBM Corp. 2004, 2005

segment tag, which appears at the beginning of the segment. (Data elements are not identified by name but are delimited by special separator characters reserved for this purpose.)

In some cases, it is useful to distinguish the detail or data segments in a transaction from other segments that are used for administrative purposes. The administrative segments are called *control segments* in X12 and *service segments* in EDIFACT. The *envelope* segments that delimit the boundaries of an EDI interchange are one example of these control or service segments.

EDI interchanges can contain three levels of segments. At each level, there is a header segment at the beginning and a trailer segment at the end.

An interchange always has an interchange header segment and an interchange trailer segment.

An interchange can contain one or more groups. A group in turn contains one or more related transactions. The group level is optional in EDIFACT but is required in X12 and related standards. When groups are present, there is a group header and a group trailer segment for each group.

A group (or an interchange, where groups are not present) contains one or more transactions. Each transaction has a transaction set header and a transaction set trailer.

A transaction represents a business document, such as a purchase order. The contents of the business document are represented by the detail segments between the transaction set header segment and the transaction set trailer segment.

Each EDI standard provides its own method for displaying the data within an interchange. The following table lists the segments for each of the three supported EDI standards.

Table 13. Segments for supported EDI standards

Standard segment	X12	UCS	EDIFACT
Interchange start	ISA	BG	UNB
Interchange end	IEA	EG	UNZ
Group start	GS	GS	UNG
Group end	GE	GE	UNE
Transaction start	ST	ST	UNH
Transaction end	SE	SE	UNT

Figure 22 on page 83 shows an example of an X12 interchange and the segments that make up the interchange.

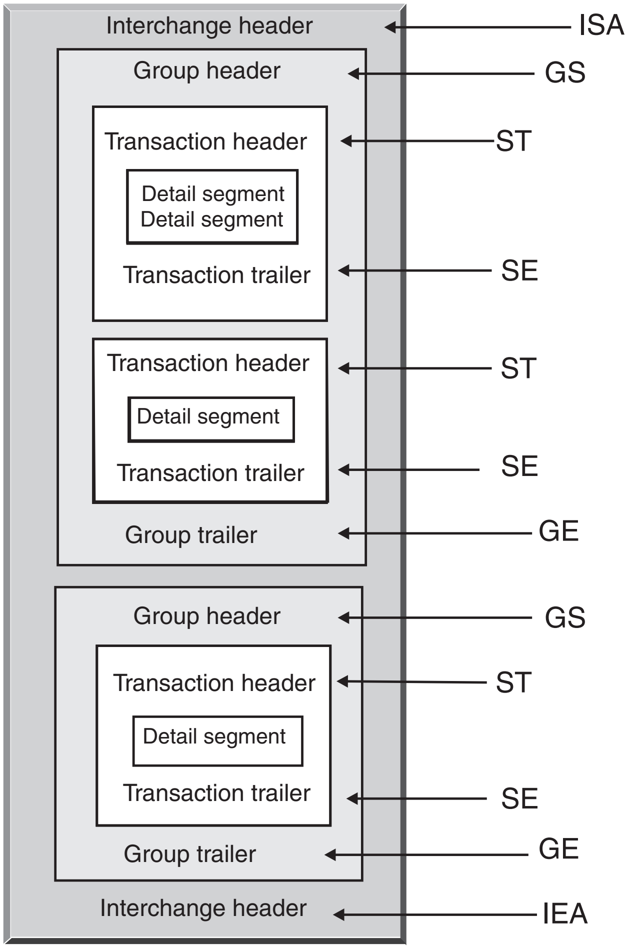


Figure 22. An interchange envelope

Maps

The Data Interchange Services client mapping specialist creates transformation maps that describe how to change a document in one format to a document in a different format. You can, for example, have a transformation map that changes an X12 transaction into an EDIFACT message. You can also transform an EDI transaction into an XML document or a record-oriented data document.

The transformation map can also create multiple documents from a single document. This type of map makes use of *map chaining*, which produces multiple outputs from a single translation. In map chaining, after a source document has been successfully translated into a target document, a subsequent map is used to translate the source document again to produce another target document. This can be repeated as many times as needed to produce as many documents as needed.

In addition to transformation maps, you can use functional acknowledgment maps and validation maps. Functional acknowledgment maps provide instructions on how to produce a functional acknowledgment, which notifies the sender of an EDI document that the document has arrived. Several EDI Standard functional acknowledgment maps are installed when WebSphere Partner Gateway is installed. See “Functional acknowledgments” on page 116 for a list of these maps. Additional functional acknowledgment maps can be created by the Data Interchange Services client mapping specialist. WebSphere Partner Gateway generates a functional acknowledgement when an EDI transaction is validated and the EDI transaction has a functional acknowledgement map associated with it. The source document must be an EDI document.

WebSphere Partner Gateway provides a standard level of validation on the EDI document. If a functional acknowledgment is going to be generated, results from validation of an EDI document are saved. Validation maps are created to provide additional validation on an EDI document. The generation of a functional acknowledgment uses the functional acknowledgment map and the results from the validation of the EDI document. The functional acknowledgment map contains mapping commands that indicate how to use the validation results to create a specific functional acknowledgment. If a document is accepted for translation by the validation process, the appropriate data transformation map is used to translate the source document.

Overview of XML and ROD documents

The Data Interchange Services client mapping specialist can create document definitions for XML and record-oriented data documents and then create transformation maps that change one type of document into another.

XML documents

XML documents are defined by either an XML DTD or an XML schema. The Data Interchange Services client mapping specialist creates a transformation map based on the DTD or schema that describes how to translate the XML document to another format. An XML document can be transformed into another XML document, a record-oriented data document, or an EDI transaction.

ROD documents

The term record-oriented data (ROD) refers to documents that conform to a proprietary format. The Data Interchange Services client mapping specialist defines a ROD document definition, which refers to the way a business application structures data in a document. After a document definition is defined, the mapping specialist can create a map to transform the ROD document into another ROD document, an XML document, or an EDI transaction.

Splitters and multiple documents

XML or ROD documents can enter the hub as individual documents or as a group of documents within the same file. Multiple documents might be put in the same file when, for example, a scheduled job at the participant or Community Manager periodically uploads documents to be sent. If multiple XML or ROD documents arrive in one file, the Receiver calls the associated splitter handler (XMLSplitterHander or RODSplitterHandler) to split the set of documents. (The splitter handlers are configured when you create a target. See “Preprocess” on page 43 for information.) The documents are then reintroduced into the Document Manager to be processed individually.

Note: The sender and receiver IDs must be part of the ROD document definition associated with the transformation map. The information necessary to determine the document type and dictionary values must also be present in the document definition. Make sure that the Data Interchange Services client mapping specialist is aware of these requirements when creating the transformation map.

Multiple EDI interchanges can also be sent in one file. If multiple EDI interchanges arrive in one file, the Receiver calls the EDISplitterHandler to split the set of interchanges. The interchanges are then reintroduced into the Document Manager to be processed individually.

Note: Splitting is performed on the interchange, not on the individual transactions within the interchange. Transactions within the interchange are de-enveloped.

Overview of creating document flows and setting attributes

A document flow definition is made up of, at minimum, a package, a protocol, and a document flow. The document flow definitions specify the types of documents that will be processed by WebSphere Partner Gateway.

Packaging refers to the logic that is required to package a document according to a specification, such as AS2. A protocol flow is the logic that is required to process a document that adheres to a certain protocol, such as EDI-X12. A document flow describes what the document will look like.

The following sections briefly describe the overall steps for setting up a document flow between the Community Manager and a participant. The sections also describe the points at which you can set attributes.

Step 1: Make sure the document flow definition is available

Before you can send or receive a document, a document flow definition must be defined for the document. WebSphere Partner Gateway provides several default document flow definitions, including ones that represent functional acknowledgments. When you import transformation maps for EDI transactions or XML or ROD documents, the associated document flow definitions appear on the Document Flow Definitions page. Similarly, if you import a functional acknowledgment map that is not already defined, the document flow definition for the acknowledgment appears on the Document Flow Definitions page. You can also create your own document flow definitions.

As part of establishing the document flow definition, you can modify certain attributes. Attributes are used to perform various document-processing and routing functions, such as validation, checking for encryption, and retry count. The attributes you set at the document flow definition level provide a global setting for the associated package, protocol, or document flow. The attributes that are available vary, depending on the document flow definition. Attributes for EDI document flow definitions have different attributes from RosettaNet document flow definitions.

For example, if you specify a value for **Allow a TA1 request** at the ISA document flow level, the setting applies to all ISA documents. If you later set the **Allow a TA1 attribute** at the B2B capabilities level for a participant or the Community Manager, that setting overrides the one set at the document flow definition level.

For attributes that can be set at multiple levels of the document flow definition, the values set at the document flow level take precedence over those set at the protocol level, and the attributes set at the protocol level take precedence over the package level. For example, if you specify an envelope profile at the &X44TA1 protocol level but specify a different envelope profile at the TA1 document flow level, the envelope profile you specify at the TA1 document flow level is used.

You must have the document flow listed on the Manage Document Flow Definitions page before you can create interactions.

Step 2: Create interactions

You next set up interactions, which are templates for creating participant connections. Interactions convey how the document comes in, what processing is performed on the document, and how the document is sent from the hub.

For some protocols, you need only two flows, one to describe the document that is received into the hub (from the participant or Community Manager) and one that describes the document that is sent from the hub (to the participant or Community Manager). However, if the hub is sending or receiving an EDI interchange that will be de-enveloped into individual transactions or in which acknowledgments are required, you will actually create multiple interactions. For example, if you are receiving an EDI interchange at the hub, you will have an interaction that describes how the interchange is sent to the hub and how it is processed at the hub. You will also have an interaction for each transaction within the hub that describes how the transaction is processed. For EDI interchanges leaving the hub, you will have an interaction that describes how the interchange envelope is sent to the recipient.

Step 3: Create participant profiles, gateways, and B2B capabilities

Next, you create participant profiles for the Community Manager and for community participants. You define gateways (which determine where documents will be sent) and B2B capabilities, which specify the documents the Community Manager or a participant is capable of sending and receiving. The B2B capabilities page lists all the document flows that have been defined.

You can set attributes at the B2B capabilities level. Any attributes you set at this level override those set at the document flow definition level. For example, if you set **Allow a TA1 request** to **No** at the document flow definition level for ISA documents but then set it to **Yes** at the B2B capabilities level, the value of **Yes** is used. Setting an attribute at the B2B level lets you tailor the attribute to a specific participant.

If you set the envelope profile at the protocol or document flow level (on the Manage Document Flow definitions page) and then set it to a different value on the B2B Capabilities page, the latter value is used.

You must have the profiles and B2B capabilities of the Community Manager and participants defined before you can create connections between them.

Step 4: Activate connections

Finally, you activate connections between the Community Manager and participants. The connections that are available are based on the B2B capabilities of the participants and the interactions you created. The interactions depend on the document flow definitions being available.

For some exchanges, only one connection is required. For example, if a participant is sending a binary document to a Community Manager back-end application, only one connection is needed. For the exchange of EDI interchanges in which the interchange is de-enveloped and the individual transactions are transformed, however, multiple connections are set up.

Note: For EDI interchanges that are being passed through as is, only one connection is required.

You can set attributes at the connection level. Any attributes you set at this level override those set at the B2B attributes level. For example, if you set **Allow a TA1 Request** to **Yes** at the B2B capabilities level but then set it to **No** at the connection level, the value of **No** is used. Setting a value for an attribute at the connection level lets you further tailor the attribute, depending on the routing requirements of the participants and applications involved.

Overview of possible flows

This section gives you a brief overview of the types of transformations WebSphere Partner Gateway can perform. Details of these transformations and what you need to do to set them up are described in "General steps for defining document exchanges" on page 106.

EDI to EDI flow

WebSphere Partner Gateway can accept an EDI interchange from a participant or the Community Manager, transform it into a different type of EDI interchange (for example, EDI-X12 to EDIFACT), and send the document to the Community Manager or participant. The following steps occur when an EDI interchange is transformed into another EDI interchange:

1. The EDI interchange received at the hub is de-enveloped.
2. The individual transactions within the EDI interchange are transformed to the recipient's EDI format.
3. The transformed EDI transactions are enveloped and sent to the recipient.

Figure 23 shows an X12 interchange consisting of three transactions being de-enveloped. The transactions are transformed into EDIFACT format and are then enveloped and sent to the participant.

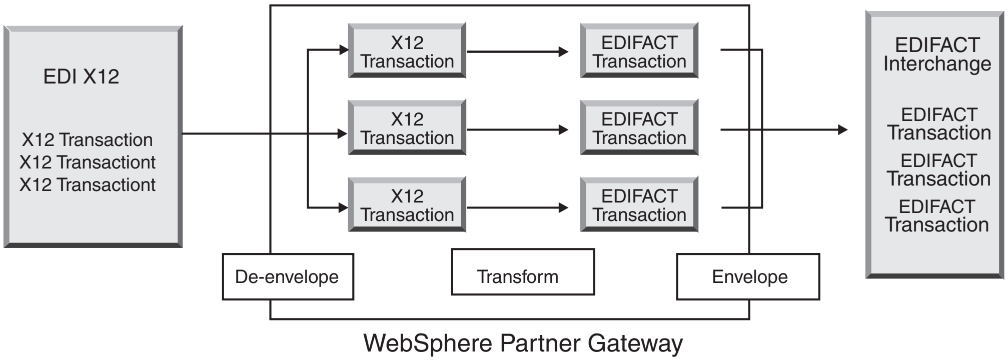


Figure 23. EDI interchange to EDI interchange flow

Each of the transactions has a transformation map associated with it, which specifies how the transaction is transformed. The transaction can be transformed into a single transaction or, if map chaining was used to create the map, multiple transactions. If Enveloper batching is turned on, transactions that enter the hub in one envelope will leave the hub in one envelope. However, if there are envelope breakpoints (for example, different values for EDI attributes or a different envelope profile) or if batching is turned off, the transactions will leave in different envelopes. See "Enveloper" on page 95 for a general description of the Enveloper (which is the component that gathers a set of transactions to be sent to a participant, wraps them in an envelope, and sends them). See "Batch mode" on page 95 for more information about batching.

The transaction might also have a validation map associated with it.

EDI to XML or ROD flow

WebSphere Partner Gateway can accept an EDI interchange from a participant or the Community Manager, de-envelope the interchange, and transform the resulting EDI transactions into XML or ROD documents.

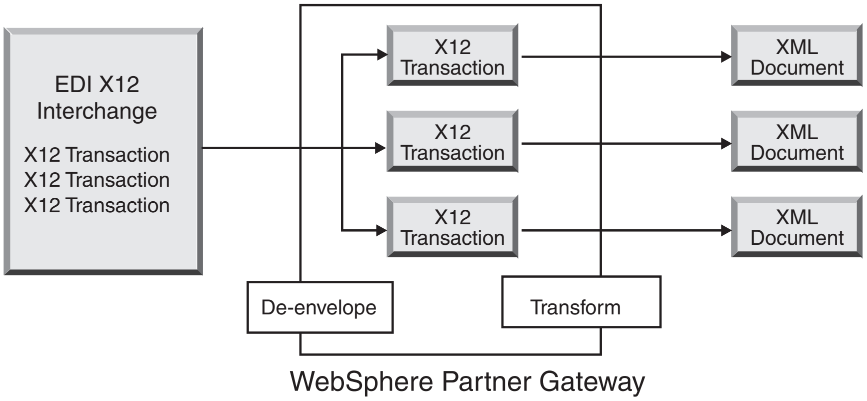


Figure 24. EDI interchange to XML documents flow

The transaction can be transformed into a single document or, if map chaining was used to create the map, multiple documents.

XML or ROD to EDI flow

WebSphere Partner Gateway can receive XML or ROD documents from a participant or the Community Manager, transform the documents into EDI transactions, envelope the transactions, and send them to the Community Manager or a participant.

Figure 25 on page 89 shows XML documents that are transformed into X12 transactions and then enveloped.

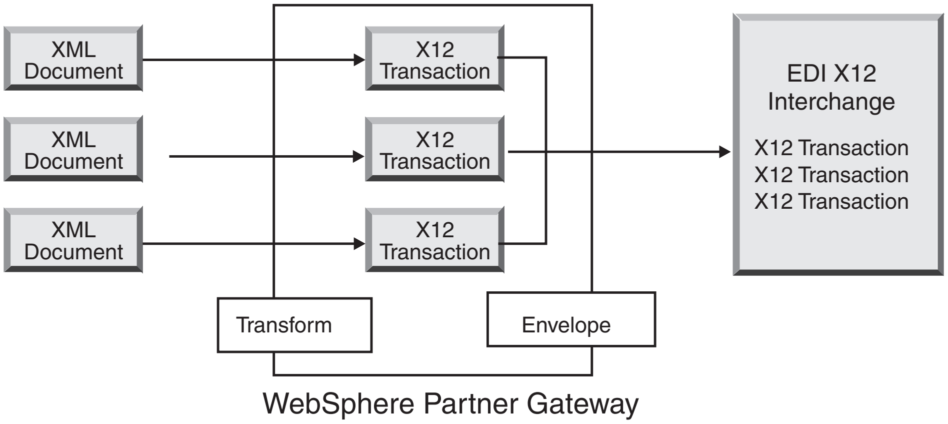


Figure 25. XML document to EDI interchange flow

One document can be transformed into multiple transactions (if map chaining was used to create the map), and the transactions can be enveloped into different interchanges. Figure 26 shows an XML document that is transformed into three X12 transactions. Two of the transactions are enveloped together. One is put in a separate envelope.

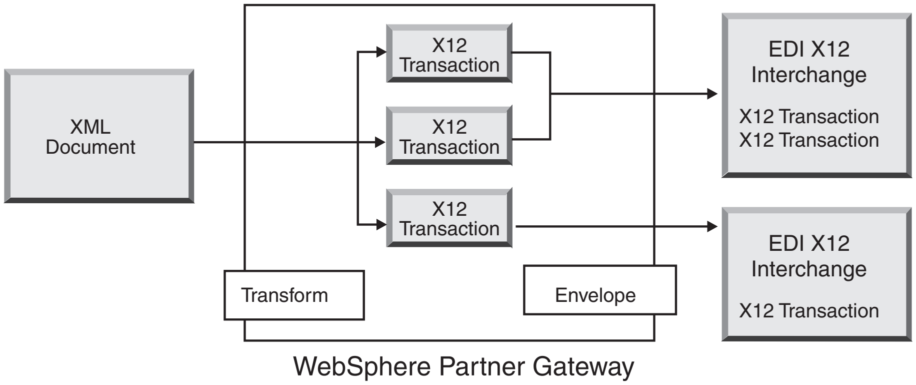


Figure 26. XML document to multiple EDI transactions flow

Multiple XML or ROD documents to EDI interchange flow

WebSphere Partner Gateway can receive a file consisting of one or more XML or ROD documents from a participant or the Community Manager, transform the document or documents into EDI transactions, envelope the EDI transactions into multiple envelopes, and send them to the Community Manager or participant.

Each document can be transformed into a single transaction or, if map chaining was used to create the map, multiple transactions.

Notes:

1. Documents sent in a file must be of the same type--either XML documents or ROD documents, but not both.
2. ROD documents must be of the same type.

Figure 27 on page 90 shows a set of XML documents being split, resulting in individual XML documents. The XML documents are transformed into X12 transactions, and the transactions are enveloped.

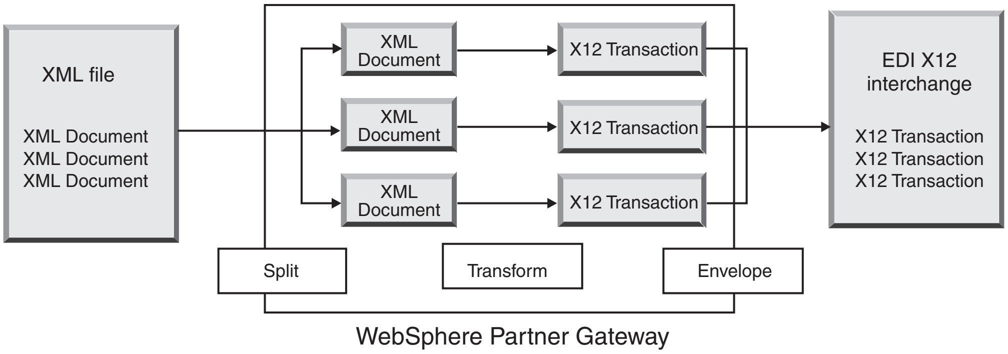


Figure 27. Multiple XML documents to EDI interchange flow

In Figure 27, the documents are split (by the XML Splitter Handler), and the transformed transactions are enveloped together. The XML Splitter Handler must have the BCG_BATCHDOCS option set to on (the default value) for this scenario to occur. If BCG_BATCHDOCS is set to on and the Enveloper batch mode is on, these transactions can be enveloped in the same EDI envelope. The Enveloper batch mode attribute is described in “Batch mode” on page 95.

XML to ROD or ROD to XML flow

WebSphere Partner Gateway can receive an XML or ROD document from a participant or the Community Manager, transform the document into the other type (XML to ROD or ROD to XML), and then send the document to the participant or Community Manager.

Figure 28 shows a series of XML documents being transformed into ROD documents.

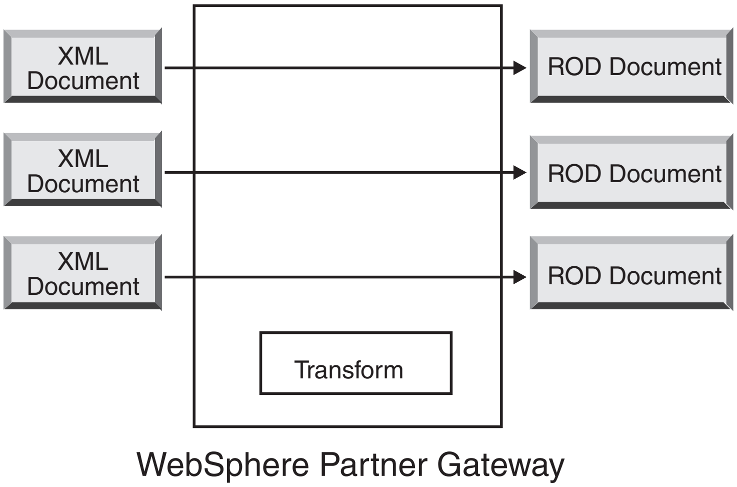


Figure 28. XML document to ROD document flow

The document can be transformed into a single document or, if map chaining was used to create the map, multiple documents.

XML to XML or ROD to ROD flow

WebSphere Partner Gateway can receive an XML or ROD document from a participant or Community Manager, transform it into a document of the same type (XML to XML or ROD to ROD), and then send the document to the participant or Community Manager.

Figure 29 shows XML documents that are transformed into XML documents of a different format.

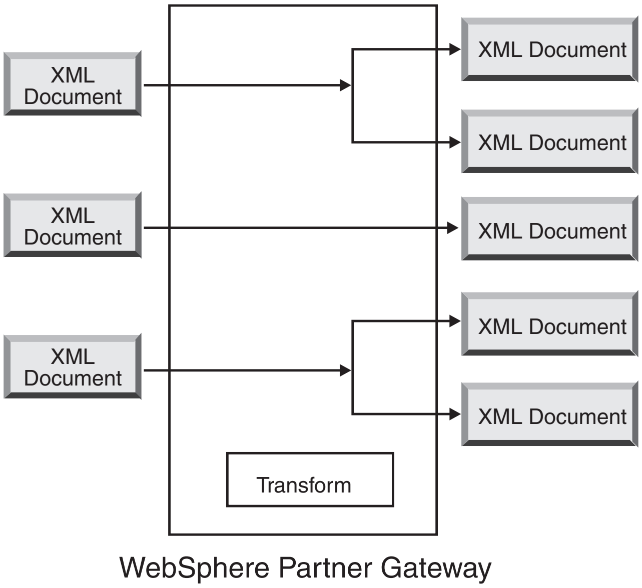


Figure 29. XML document to XML document flow

The document can be transformed into a single document or, if map chaining was used to create the map, multiple documents.

How EDI interchanges are processed

An EDI interchange received at the hub is typically de-enveloped, and the individual transactions are processed. Often, standard EDI transactions (such as the X12 850 or the EDIFACT ORDERS, which represents a purchase order) are transformed into a form that can be understood by a back-end application. In addition, a functional acknowledgment is often sent to the participant to indicate that the interchange was received. The exchange of EDI interchanges, therefore, requires multiple actions (such as EDI De-envelope and EDI Translate and EDI Validate). For example, if the interchange contains two transactions and no acknowledgments are required, WebSphere Partner Gateway performs the following actions:

1. De-envelopes the interchange

   WebSphere Partner Gateway extracts information about the interchange from the envelope header and trailer segments at the interchange, group, and transaction levels. This information can include:

   - At the interchange level, the business identifiers of the sending and receiving participants, the usage indicator, which specifies whether the interchange is meant for a production or test environment, and the date and time the interchange was prepared

- At the group level, the application identifiers of the sender and receiver and the date and time the group was prepared
- At the transaction level, the type of transaction (such as X12 850 or EDIFACT ORDERS)

2. Transforms the first transaction according to the map associated with it.
3. Transforms the second transaction according to the map associated with it.
4. Delivers the transformed documents to the back-end application.

Similarly, when the hub sends a document or documents that originated at the Community Manager back-end application, the documents are transformed into standard EDI transactions. The resulting EDI transactions are enveloped before being sent to the participant. As in the case of receiving an EDI interchange, multiple actions are required to create, envelope, and send an EDI interchange.

The individual transactions, groups, and interchanges are identified by control numbers. WebSphere Partner Gateway sets these numbers when an exchange takes place. You can customize the control numbers, however, as described in “Control numbers” on page 103.

The following illustration shows the overall picture of how an EDI interchange, packaged as AS, is sent from a participant, with the eventual goal of delivering two transformed XML documents to two different gateways on the Community Manager back-end system. In this example, the 850 transactions are transformed into purchase orders that a back-end application can process. The 890 transactions are transformed in warehouse shipping orders that the back-end application can process.

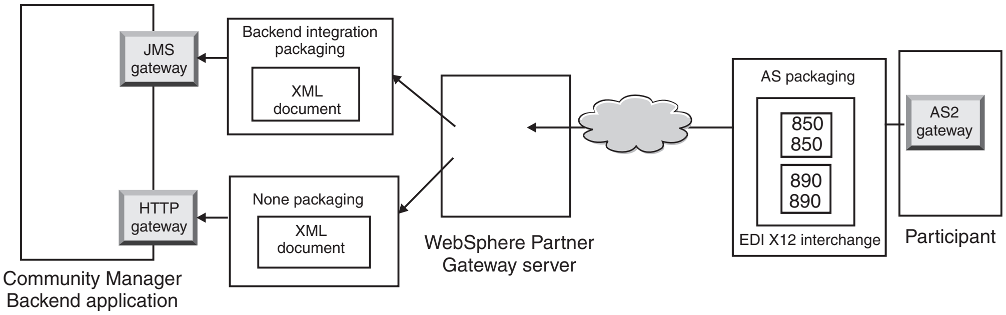


Figure 30. Overall flow from a participant to the Community Manager

Instead of requiring one connection from participant to Community Manager, this exchange requires three connections:

- One from the participant to the hub to de-envelope the interchange. Because this is an intermediate step (the interchange is de-enveloped but is not delivered to the participant), the target side of the participant connection is N/A (not applicable).

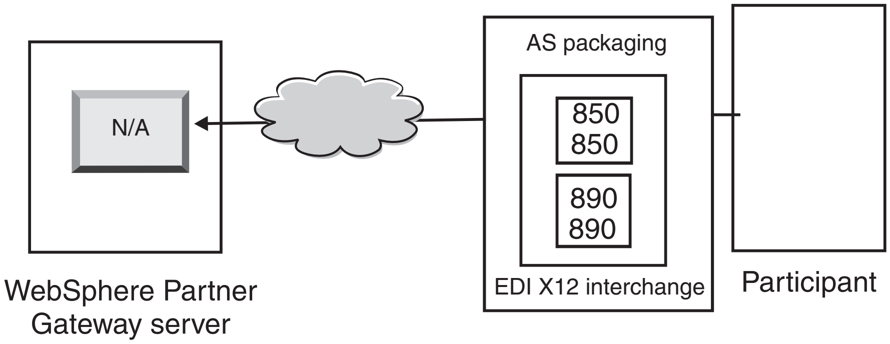
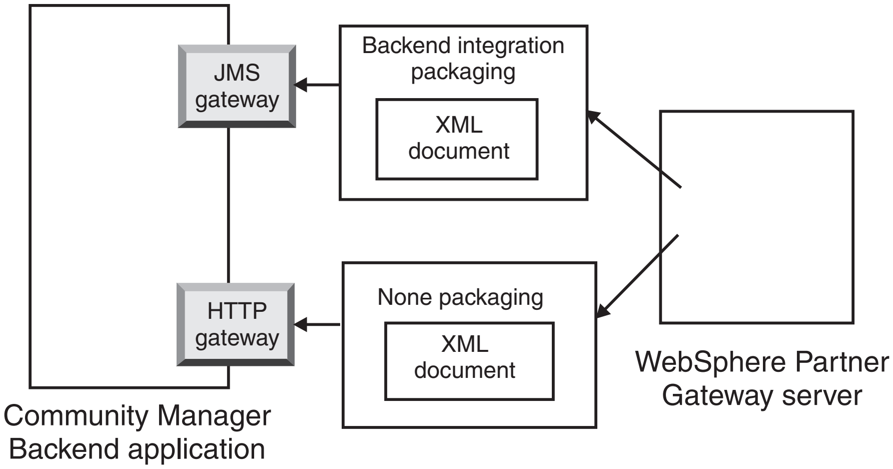


Figure 31. The de-enveloping connection

- One for the first transaction to be transformed and delivered to the JMS gateway of the Community Manager and one for the second transaction to be transformed and sent to the HTTP gateway of the Community Manager.

  For the transactions, the source packaging is not applicable because the transactions came in the original interchange that was de-enveloped by the system. Therefore, the source side of the transactions should have **Packaging: N/A** specified in the participant connection.

  For the transaction that is transformed into XML and that will flow to the back-end application over JMS, the target gateway on the participant connection of this transaction should be specified as the JMS gateway of the Community Manager. For the transaction that was transformed into XML and that will flow to the back-end application over HTTP, the target gateway on the participant connection of this transaction should be specified as the HTTP gateway.



JMS gateway
Backend integration packaging
XML document
HTTP gateway
None packaging
XML document
WebSphere Partner Gateway server
Community Manager Backend application

Figure 32. Connections for individual transactions

You can use the Document Viewer to view the interchange and the individual transactions, which, in the terms of the Document Viewer, are the *children* of the interchange. Using the Document Viewer, you can display the children associated with a source or target interchange, and you can display the events associated with them. The Document Viewer is described in the ″Viewing Events and Documents″ section of the *Administrator Guide*.

If the sender requests acknowledgments, you need additional connections:

- One for each of the acknowledgments sent back to the participant. The functional acknowledgments are generated by the system, and, therefore, the source side of the participant connection should have **Packaging: N/A** specified. Functional acknowledgments are enveloped before being delivered, and, therefore, the target side of the participant connection should also have **Packaging: N/A** specified. The Enveloper gathers these acknowledgments according to a schedule you set. See “Enveloper” on page 95 for information about setting the schedule.

- One to envelope the acknowledgments before they are sent back to the participant. The envelope is generated by the system, and, therefore, the source side of the participant connection should have **Packaging: NA** specified. The target side of the participant connection should have the target gateway set to the gateway of the participant and, in this case, with **Packaging: AS specified**. You can use a default envelope for the EDI standard, or you can customize envelopes. See “Envelope profiles” on page 96 for information about customizing envelopes.

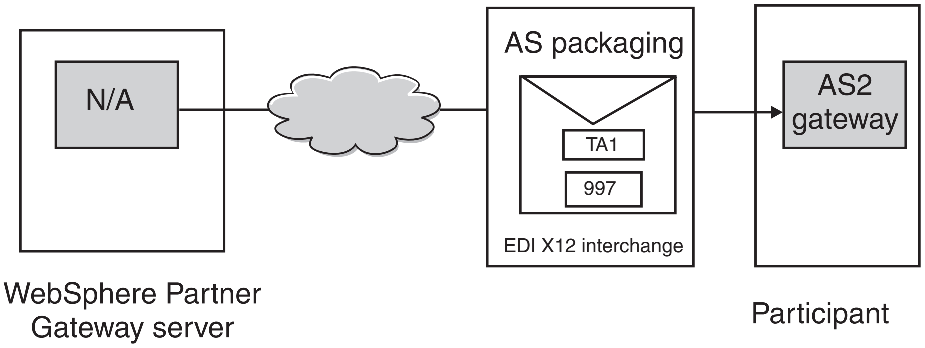


Figure 33. Enveloping and sending acknowledgments to the originator

How XML or ROD documents are processed

An XML or ROD document is received at the hub as an individual document or as a group of documents in the same file. When a group of documents in the same file is received at the hub, WebSphere Partner Gateway performs the following actions:

1. Splits the set of documents into individual documents.
2. Transforms each document according to the map associated with it.
3. If the documents are transformed into EDI transactions, it envelopes the transactions and delivers them to the back-end application. If the documents are transformed into XML or ROD documents, it delivers the transformed documents to the back-end application.

If the XML or ROD document arrives as a single document, WebSphere Partner Gateway performs the following actions:

1. Transforms the document according to the map associated with it.
2. If the document is transformed into an EDI transaction, envelopes the transaction and delivers it to the back-end application. If the document is transformed into another XML or ROD document, the document is delivered to the back-end application.

Similarly, when the hub sends a document or documents that originated at the Community Manager back-end application, the documents are transformed into XML or ROD documents, or they are transformed into EDI transactions. For EDI transactions, the transactions are enveloped before being sent to the participant. As in the case of receiving an EDI interchange, multiple actions are required to transform the document or documents, envelope the resulting transactions, and send the EDI interchange.

Setting up the EDI environment

As mentioned in the previous section, you can specify many attributes that pertain to the exchange of EDI interchanges. For example, you can change the system-supplied envelope profiles, you can define specific envelopes to be used for certain connections, 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.

Enveloper

The Enveloper is the component that gathers a set of transactions to be sent to a participant, wraps them in an envelope, and sends them. You schedule the Enveloper (or accept the default schedule) to indicate to WebSphere Partner Gateway when you want the Enveloper to look for transactions waiting to be sent. You can also update the default values for the lock time, queue age, and batch mode.

Note: Setting up the Enveloper is optional. If you do not change any of the values for the Enveloper, the system-supplied default values are used.

Locking

Each instance of the Document Manager has its own Enveloper. If you have two Document Managers installed on your system, you have two Envelopers. It is possible, therefore, for two (or more) instances of an Enveloper to attempt to poll transactions waiting to be enveloped. To ensure that a given transaction is polled by exactly one Enveloper, locks are used. Locks make sure that if multiple Envelopers are involved, only one Enveloper polls and processes a given transaction. Envelopers poll simultaneously but work on different transactions.

A time limit is set on the lock. The default value for an instance of the Enveloper to hold the lock is 240 seconds.

If the Enveloper has to wait for the lock, it is placed in a queue. The maximum queue age (the length of time the Enveloper should wait) is 740 seconds.

Typically, you will not need to change any of the default values for locking.

Batch mode

Multiple documents that arrive in one file are split, according to the splitter handler you have set up for that type of document. (Configuring splitter handlers, which is part of defining targets, is described in “Modifying configuration points” on page 43.) One of the attributes of the splitter handler is BCG_BATCHDOCS. When BCG_BATCHDOCS is set to on (the default value), the splitter adds batch IDs to the documents after the documents are split.

The Enveloper has an attribute for batch mode, which is related to the BCG_BATCHDOCS attribute. If batch IDs were assigned to the individual documents, and if you accept the default value (on) for batch mode, the Enveloper makes sure that all documents that arrive together in the same file are processed before it envelopes and sends them, to ensure that the transactions are enveloped together. For example, suppose five XML documents arrive in the same file. The

XML documents are to be transformed into EDI transactions and are intended to be delivered to the same recipient. After only three of the documents have been transformed, the Enveloper begins its scheduled polling for transactions. If batch mode is selected, the Enveloper does not process (envelope) the three transactions that are ready. Instead, it waits until all five transactions have finished processing before it envelopes and sends them. The transactions are placed in the same envelope, unless the applicable EDI standard prevents this.

Modifying the default values

To modify any of the default values for the Enveloper, perform the following steps:

1. Click **Hub Admin > Hub Configuration > EDI > Enveloper**.
2. Click the **Edit** icon.
3. Enter new values for **Maximum Lock Time (Seconds)** and **Maximum Queue Age (Seconds)** if you want more or less time assigned to these attributes.

   Note: Typically, you will not need to change any of the default values.
4. If you want to turn off batch mode, remove the check next to **Use Batch Mode**.
5. If you want to change how often the Enveloper checks for transactions waiting to be sent, perform one of the following sets of tasks:
   - To use interval-based scheduling (which is the default) but change the amount of time, enter a new time next to **Interval**. For example, if you change the value to 30 seconds, the Enveloper will check for documents every 30 seconds, envelope those documents, and send them to the recipient.
   - To use calendar-based scheduling, perform the following tasks:
     a. Click **Calendar Based Scheduling**.
     b. Choose the type of scheduling (**Daily Schedule**, **Weekly Schedule**, or **Custom Schedule**).
        - If you select **Daily Schedule**, select the time of day (the hours and minutes) when the Enveloper should check for documents.
        - If you select **Weekly Schedule**, select one or more days of the week in addition to the time of day.
        - If you select **Custom Schedule**, select the time of day and then choose **Range** or **Selective Days** for the week and the month. With **Range**, you indicate the start date and the end date. (For example, you can click **Mon** and **Fri** if you want the Enveloper to check for documents at a certain time on weekdays only.) With **Selective Days**, you choose the specific days of the week and month.
6. Click **Save**.

Envelope profiles

An envelope profile determines values that are placed in specific elements of the envelope. You assign the envelope profile to EDI transactions in the document flow definition **Envelope Profile** attribute. WebSphere Partner Gateway provides a predefined envelope profile for each supported standard (X12, EDIFACT, or UCS). You can use these predefined envelopes directly, you can modify them, or you can copy them into new envelope profiles. The steps for modifying an envelope profile or creating one are described in “Modifying the default values” on page 97.

The Envelope profiles have one field for each element in the envelope standard. The profiles provide literal or constant data for building header or trailer segments for transaction sets, messages, functional groups, and interchanges. You supply only the values that need to be populated and for which a value is not provided by another source.

The field names are designed to make cross-referencing easy. For example, the field UNB03 is the third data element in the UNB segment.

As described in "Envelope attributes," attributes set anywhere else take precedence over the values you set in the envelope profile. Some of the attributes can be overridden in document flow definition-related attributes or maps.

Envelope attributes

Envelope attributes can be set at several different points during the configuration process, and they can also be set in the transformation map associated with the documents. For example, the Data Interchange Services client mapping specialist can specify the CtlNumFlag property when defining a map. This property can also be set as part of the envelope profile (in the **Control Numbers by Transaction ID** field). Any attributes set in the transformation map override the related values set at the Community Console. For example, if CtlNumFlag is set in the transformation map as **N** (no) and you enter a value of **Y** (yes) in the **Control Numbers by Transaction ID** field, the value of **N** is the one that is used.

Other envelope profiles can be set at the protocol level (from the Manage Document Flow Definitions page or from the B2B capabilities page associated with a participant), or they can be set as part of the connection. The order of precedence is outlined in the following list:

1. Properties set in the transformation map take precedence over the associated attributes set in the Community Console.
2. Attributes set at the connection level take precedence over those set at the B2B capabilities level.
3. Attributes set at the B2B capabilities level take precedence over those set at the document flow definition level.
4. Attributes set anywhere (either in the transformation map or at the document flow definition, B2B capabilities, or connection level) take precedence over the values set in the envelope profile.

For a list of transformation map properties and their associated Community Console attributes, see "Data Interchange Services client properties" on page 281.

Modifying the default values

"Envelope profile attributes" on page 271 provides a table showing the default values used for each EDI standard envelope attribute if you do not enter a value in the profile or if you do not create a profile. Make sure the envelope profiles you are using supply any mandatory elements that are not provided by the system at runtime.

To set up an envelope profile, perform the following steps:

1. Click **Hub Admin > Hub Configuration > EDI > Envelope Profile**.
2. Perform one of the following sets of steps:
   - Create an envelope
     a. Click **Create**.
     b. Type a name for the profile. This is the name that will appear on the Envelope Profiles list.
     c. Optionally, type a description of the profile.

   d. Click the EDI standard to which the envelope pertains. For example, if you are exchanging documents that conform to the EDI-X12 standard, select **X12**.

- Modify an envelope
   a. Select one of the existing envelope profiles by clicking the **View details** icon next to the name of the profile.
   b. Click the **Edit** icon.

3. The **General** button is chosen by default. You can enter a value for any field except ENVTYPE, which is prefilled with the standard you chose in step 2d.

   You can add values for the following fields:

   - **Interchange Control Number Length**, to indicate how many characters should be used when a control number is assigned to an interchange within the envelope.
   - **Group Control Number Length**, to indicate how many characters should be used when a control number is assigned to a group within the envelope.
   - **Transaction Control Number Length**, to indicate how many characters should be used when a control number is assigned to a transaction within the envelope.
   - **Max Transactions Number**, to indicate the maximum number of transactions allowed in this envelope.
   - **Control Numbers by Transaction ID**, to indicate whether you want to use the transaction ID (as part of the key) when the set numbers are looked up in the database. If so, separate sets of control numbers are used per each transaction ID.

   The fields for the General envelope profile are the same across all three standards, except that EDIFACT has an additional field: **Create Groups for EDI**.

   If you have made any changes to the General page, click **Save**.

4. To specify values for the interchange, click **Interchange**. A new set of fields is displayed on the page. The fields vary, depending on the EDI standard. Note that some of the values are already filled in or will be filled in at run time.

   - For the EDI-X12 standard, you can change the following fields:
     - **ISA01: Authorization Information Qualifier**, which is a code for the type of information in ISA02.
     - **ISA02: Authorization Information**, which is information used to further identify or authorize the sender of the interchange data.
     - **ISA03: Security Information Qualifier**, which is a code for the type of information in ISA04. Valid values are:

       00 ISA04 is not meaningful

       01 ISA04 contains a password
     - **ISA04: Security Information**, which is security information about the sender or interchange data. The code in ISA03 defines the type of information.
     - **ISA11: Interchange Standards ID**, which is a code for the agency that controls the interchange. Valid values are: **U** (US EDI community of ASC X12), **TDCC**, and **UCS**.

       Note: This attribute is used for X12 versions through 4010. In X12 4020, the ISA11 element is used for the repetition separator.

- **ISA12: Interchange Version ID**, which is the version number of the syntax used in the interchange and functional group control segments.
- **ISA14: Acknowledge Requested**, which is the sender's code for requesting an acknowledgment. Valid values are:

  0 Request no acknowledgment

  1 Request an acknowledgment that ISA and IEA segments were received and recognized
- **ISA15: Test Indicator**, which is an indication that the interchange is for testing or production. Valid values are:

  T For test data

  P For production data

- For the UCS standard, you can change the following fields:
  - **BG01: Communications ID**, which is the identification of the transmitting company.
  - **BG02: Communications Password**, which is a password the receiver assigns, to be used as agreed upon by the participants.
- For the EDIFACT standard, you can change the following fields:
  - **UNB0101: Syntax Id**, which is the identification of the agency controlling the syntax being used. The controlling agency is UNO. The level is A or B.
  - **UNB0102: Syntax Version**, which is the version number of the syntax identified by the Syntax ID.
  - **UNB0601: Recipients Reference/Password**, which is a password assigned by the recipient, to be used as agreed upon by the participants.
  - **UNB0602: Recipients Reference/Password Qualifier**, which is a qualifier to the recipient's password, to be used as agreed upon by the participants.
  - **UNB07: Application Reference**, which is the sender's identification of the functional area to which the interchange messages relate.
  - **UNB08: Priority**, which is the sender's code for processing priority, as agreed upon with the participant. Code A is the highest priority.
  - **UNB09: Acknowledgement Request**, which is the sender's code for requesting an acknowledgment.
  - **UNB10: Communications Agreement Id**, which is the name or code for the type of agreement used for this interchange, as agreed to with the participant.
  - **UNB11: Test indicator (Usage Indicator)**, which is an indication that the interchange is for testing. 1 indicates a test interchange.

If you have made any changes to the Interchange page, click **Save**.

5. To specify values for the groups within the interchange, click **Group**. A new set of fields is displayed. The fields vary, depending on the EDI standard.

   The fields on this page generally define the sender and receiver of the group.
   - For the EDI-X12 and UCS standards, you can enter values in the following fields:
     - **GS01: Functional Group ID**, which is an identification of the type of transaction sets in the group.
     - **GS02: Application Sender**, which is the name or code for a specific department in the sender's company.
     - **GS03: Application Receiver**, which is the name or code for the specific department in the receiver's company that is to receive the group.

   - **GS07: Group Agency**, which is a code used with GS08 to identify the agency that has control of the standard.
   - **GS08: Group Version**, which is a code for the version, release, and industry of the standard.
   - For the EDIFACT standard, you can enter values in the following fields:
     - **UNG01: Function Group ID**, which is an identification of the type of messages in the group.
     - **UNG0201: Application Sender ID**, which is the name or code for a specific department in the sender's company.
     - **UNG0202: Application Sender Id Qualifier**, which is the qualifier for the sender ID code. Refer to the data element directory for a list of code qualifiers.
     - **UNG0301: Application Receiver Id**, which is the name or code for the specific department in the recipient's company that is to receive the group.
     - **UNG0302: Application Receiver Id Qualifier**, which is the qualifier for the recipient ID code. Refer to the data element directory for a list of code qualifiers.
     - **UNG06: Controlling Agency**, the code that identifies the agency that has control of the message type in the functional group.
     - **UNG0701: Message Version**, which is the version number for the message type.
     - **UNG0702: Message Release**, which is the release number within the version number for the message type.
     - **UNG0703: Association Assigned**, which is the code, assigned by the responsible association, that further identifies the message type.
     - **UNG08: Application Password**, which is the password assigned by the specific department in the recipient's company.

   If you have made any changes to the Group page, click **Save**.
6. To specify values for the transactions within a group, click **Transaction** or, in the case of EDIFACT, **Message**. A new set of fields is displayed. The fields vary, depending on the EDI standard.
   - For the EDI-X12 or USC standard, you can enter a value for **ST03: Implementation Convention ID String**.
   - For the EDIFACT standard, you can enter a value in the following fields:
     - **UNH0201: Message Type**, which is a code assigned by the controlling agency to identify the message type.
     - **UNH0202: Message Version**, which is the version number for the message type.
     - **UNH0203: Message Release**, which is the release number within the version number for the message type.
     - **UNH0204: Controlling Agency**, which is a code for the agency that has control of the message type.
     - **UNH0205: Association Assigned Code**, which is the code, assigned by the responsible association, that further identifies the message type.
     - **UNH03: Common Access Reference**, which is the key that relates all subsequent transfers of data to a common file. Participants can agree to using a key made up of components, but subelement separators cannot be used.

   If you have made any changes to the Transaction page, click **Save**.
7. Click **Save**.

8. Repeat steps 2 on page 97 through 7 on page 100 for any other envelope profiles you want to define or change.

After an envelope profile is defined, it is listed on the Envelope Profiles list. From the list, you can select the profile and then click the **Where Used** icon to determine the connections using the profile.

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.

The following table shows the connection profile attributes, their corresponding field names on the Connection Profile details page, and whether they apply to interchanges or to transactions:

Table 14. Connection profile attributes

Attribute	**Field name**	**EDI interchange**	**EDI transaction**
Connection Profile Qualifier1	Qualifier1	X	
Interchange usage indicator	EDI Usage Type		X
Group application sender identifier	Application Sender ID		X
Group application receiver identifier	Application Receiver ID		X
Group application password	Password		X

Transactions

When an EDI Interchange comes into WebSphere Partner Gateway, the first action is typically to de-envelope the interchange into the individual transactions. When the transactions are created, the De-envelope action sets the **Interchange usage indicator** and group information (**Group application sender identifier**, **Group application receiver identifier**, and **Group application password**) in the transaction metadata. Each transaction is then re-processed by WebSphere Partner Gateway in its own workflow.

Suppose you have two transactions of the same type (for example, 850) that need to be handled differently, depending on the group they were in or the values of their Interchange usage indicators. If the **Usage Indicator** is Production (**P**), for example, you might want one map (A) to be used, and if the **Usage Indicator** is Test (**T**), you want a second map (B) to be used. Two similar connections are required for this 850 transaction, with the only difference being that one connection uses map A and the other connection uses map B.

Because the transactions are otherwise the same (they have the same source and target participant, package, protocol, and document type), the Document Manager needs a way to determine which connection to use. It does this by matching the connection profile attribute you set to the transaction metadata. In this example, if you create two connection profiles -- one (CPProduction) with the **EDI Usage Type** set to **P** and the other (CPTest) with the **EDI Usage Type** set to **T**, the Document

Manager matches the transaction with the Usage Indicator of P with the CPProduction profile. It then knows to use map A to translate the transaction.

The example in this section used the **Interchange usage indicator** attribute, but you can also use the **Group sender application identifier**, **Group receiver application identifier**, and **Group application password attributes** as the distinguishing factor for a transaction.

Interchanges

For interchanges, you use the **Connection Profile Qualifier 1** attribute.

For example, suppose you are in the midst of migrating your company from using a VAN (None packaging) or the Internet (AS2 packaging). You want 840 (Request for Quote) transactions to use the VAN and 850 (Purchase Order) transactions to use the Internet. You set up two participant connections, both with the same source interchange but with different targets (one with None packaging and the other with AS2 packaging). The connection profiles help distinguish between the two connections.

Setting up the connection profile for interchanges involves several steps. These are the steps you would perform to create two connection profiles for the example:

1. Create two connections for the transactions. Set the **Connection Profile Qualifier 1** attribute on the ″To″ side of both connections. The value should be meaningful (for example, ConNone and ConAS2).
2. Define two connection profiles (for example, CPNone and CPAS2), each with the **Qualifier1** value set to match the **Connection Profile Qualifier1** attributes you set in step 1 (ConNone and ConAS2).
3. Create two connections for the interchange. Each connection has the same source packaging (N/A) but different target packaging (None and AS2). The participant connection with the connection profile CPNone will have the target gateway set to the FTP Scripting gateway that can connect to the VAN. The participant connection with the connection profile CPAS2 will have the target packaging set to AS.
4. Associate the appropriate connection profile with each one.

The Enveloper uses the **Connection Profile Qualifier 1** attribute on the ″To″ side of the participant connection as an envelope break point. Therefore, transactions having different values for the **Connection Profile Qualifier 1** attribute will be enveloped in different envelopes. When you set different values for the transactions, the Enveloper will never envelope the 840 and 850 transactions in the same interchange.

When the Document Manager looks up the connection, the two possible connections are found, but the one with the matching connection profile is used.

Setting connection profiles

Setting connection profiles is optional. If you have no need to have more than one connection for each type of document you will be exchanging for a participant, skip this section.

To set up a connection profile:

1. Click **Hub Admin > Hub Configuration > EDI > Connection Profiles**.
2. Click **Create Connection Profile**.

3. On the Connection Profile Details page, type a required name for this connection profile.
4. Type an optional description of the profile.

   The name and description (if you enter a description) will appear on the Connection Profile List page.
5. Optionally, enter a value for **Qualifier 1** to indicate the value that determines which connection to use for an EDI interchange. See "Interchanges" on page 102 for an example of using **Qualifier 1**.
6. Optionally, enter a value for **EDI Usage Type** to indicate whether this is a test, production, or information interchange. See "Transactions" on page 101 for an example of using **EDI Usage Type**.
7. Optionally, enter a value for **Application Sender ID** to indicate the application or company division associated with the sender of the group.
8. Optionally, enter a value for **Application Receiver ID** to indicate the application or company division associated with the recipient of the group.
9. Optionally, enter a value for **Password** if a password is required between the application sender and application receiver.
10. Click **Save**.

For those transactions that you want to put into certain interchange envelopes, you can specify the **Connection Profile Qualifier 1** attribute value that corresponds to the connection profile with the same value for attribute **Qualifier 1**. The **Connection Profile Qualifier 1** attribute can be set at the protocol level of a document flow definition (for example, you could edit the attributes of the X12V5R1 protocol on the Manage Document Flow Definitions screen to indicate which connection profile to use by clicking the corresponding **Connection Profile Qualifier 1** attribute value). Then when you activate the interchange connection, associate the connection profile by clicking the **Connection Profile** button and selecting the profile from the list.

Control numbers

The Enveloper uses control numbers to provide unique numbering for interchanges, groups, and transactions within an envelope. Control numbers are established for the Community Manager and for participants. When the exchange of documents takes place, control numbers are also generated for the *pair* of participants.

For each participant that has EDI B2B Capabilities, there is a set of seed initialization values for control numbers. These values are used the first time an EDI interchange is created and sent between a participant pair. The initialization values apply to the participant to whom the interchange is sent. After a document has been sent from one participant to another, the last numbers used can be viewed in the Current Control Numbers page. There can be several entries for a given participant pair if **Control Numbers by Transaction Id** is set to **Y**. After an entry exists, it is used to generate new control numbers.

As part of control number initialization, you can use masks to modify the normal control number creation by the Enveloper. Masks are used to base the control number on either the interchange or group control number. The mask descriptions follow. Replace the *n* in the edit mask with the number of bytes you wish to use to create the control number value. See Table 15 on page 104 for descriptions of the available codes:

Table 15. Control number masks

Code	Control Number	Description
G	Transaction	The transaction control number is the same as the group control number. Only one transaction for each group is allowed.
G*n*	Transaction	*n* bytes are taken from the group control number. The remainder of the transaction control number is padded with zeros to its maximum size. Only one transaction for each group is allowed.
C	Group, Transaction	The remaining bytes in the group or transaction control number field are used to maintain a control number for this participant.
V	Group, Transaction	An incrementing value is used so that the first group or transaction has a value of 1, the second a value of 2, and so on.
V*n*	Transaction	An incrementing value *n* bytes long is used so that the first transaction has a value of 1, the second a value of 2, and so on.
G*n*C	Transaction	*n* bytes are taken from the group control number and the remaining bytes in the transaction control number field are used to maintain a control number. The number of positions left determines the maximum value of the control number. For example, G5C leaves four positions; therefore the maximum value is 9999. The control number cycles from the maximum value to 1.
G*n*V	Transaction	*n* bytes are taken from the group control number. For the remaining bytes in the transaction control number field, an incrementing value is used so that the first transaction has a value of 1, the second a value of 2, and so on.
G*n*V*m*	Transaction	*n* bytes are taken from the group control number. For the remaining bytes, up to *m* bytes in the transaction control number field, an incrementing value is used so that the first transaction has a value of 1, the second a value of 2, and so on.
I	Group, Transaction	The group or transaction control number should be the same as the interchange control number. Only one group is allowed for the interchange, and only one transaction is allowed for the group or interchange.
I*n*	Group, Transaction	*n* bytes are taken from the interchange control number. The remainder of the group or transaction control number field is padded with zeros to its maximum size. Only one group is allowed for each interchange, and only one transaction is allowed for each group.
I*n*C	Group, Transaction	*n* bytes are taken from the interchange control number. The remaining bytes in the group or transaction control number field are used to maintain a control number. The number of positions left determines the maximum value of the control number. For example, I5C leaves four positions; therefore the maximum value is 9999. The control number cycles from the maximum value to 1.

Table 15. Control number masks (continued)

Code	Control Number	Description
I*n*V	Group, Transaction	*n* bytes are taken from the interchange control number. For the remaining bytes in the group or transaction control number field, an incrementing value is used so that the first group or transaction has a value of 1, the second a value of 2, and so on.
I*n*V*m*	Transaction	*n* bytes are taken from the interchange control number. For the remaining bytes, up to *m* bytes in the transaction control number field, an incrementing value is used so that the first transaction has a value of 1, the second a value of 2, and so on.
I*n*G*m*	Transaction	*n* bytes are taken from the interchange control number, and a maximum of *m* bytes are taken from the group control number. If *n* plus *m* is greater than 9, only 9 - *n* bytes are taken from the group control number. For example, using I4G6, 4 bytes are taken from the interchange
I*n*G*m*C	Transaction	*n* bytes are taken from the interchange control number, and *m* bytes are taken from the group control number. The remaining bytes in the transaction control number field are used to maintain a control number. The number of positions left determines the maximum value of the control number. For example, I2G4C leaves three positions; therefore the maximum value is 999. The control number cycles from the maximum value to 1.
I*n*G*m*V	Transaction	*n* bytes are taken from the interchange control number, and *m* bytes are taken from the group control number. For the remaining bytes in the transaction control number field, an incrementing value is used so that the first transaction has a value of 1, the second a value of 2, and so on.
I*n*G*m*V*o*	Transaction	*n* bytes are taken from the interchange control number, and *m* bytes are taken from the group control number. For the remaining bytes, up to *o* bytes in the transaction control number field, an incrementing value is used so that the first transaction has a value of 1, the second a value of 2, and so on.

Control number initialization

To configure control numbers that the Enveloper will use, perform the following steps:

1. Click **Hub Admin > Hub Configuration > EDI > Control Number Initialization**.
2. Type a participant's name and click **Search** or click **Search** without entering a name to display all participants. If you leave **EDI-capable** checked, you limit the search to those participants that have EDI document B2B capabilities. If you remove the check, you search all participants.
3. Click the **View details** icon next to the participant.
4. The participant's current control number assignments (if any) are listed on the Control Number Configuration Details page. Click the **Edit** icon to add or change the values.

5. Type (or change) the value next to **Interchange** to indicate the number you want to use to initialize control number generation for interchanges.
6. Type (or change) the value next to **Group** to indicate the number you want to use to initialize control number generation for groups. Alternatively, you can click **Mask** and type a mask to be used instead of a fixed value.
7. Type (or change) the value next to **Transaction** to indicate the number you want to use to initialize control number generation for transactions. Alternatively, you can click **Mask** and type a mask to be used instead of a fixed value.
8. Click **Save**.

Current control numbers

For a given participant-pair that already has data in the control table, you can change the control number generation. You can:

- Reset the control number generation for the pair to an initial state.
- Edit the interchange, group, or transaction number (or any combination of these numbers) and save it with a new value.

Note: Resetting control number generation or editing a group or mask should be done with caution so that numbers out of sequence or duplicate control number problems do not occur. You might want to perform either of these actions during test phase or if a partner specifically requests different control numbers.

To determine which participants have control numbers assigned (and to determine what those numbers are), you use the Current Control Numbers feature.

1. Click **Hub Admin > Hub Configuration > EDI > Current Control Numbers**.
2. Perform one of the following sets of steps:
   - If you want to see the current status of all participants, leave **Any Participant** selected in the participant lists, and click **View Current Status**.
   - If you want to view the status of selected participants, perform the following steps:
     a. Enter the name of the source and target participants and click **Search**. If you want to limit the search results to only those participants who are exchanging EDI documents, leave **Find EDI-Capable** checked.
     b. From the resulting lists, select one or more participants from each list, and click **View Current Status**.

General steps for defining document exchanges

This section provides a high-level overview of the tasks you need to perform to establish the exchange of documents for EDI interchanges entering the hub, documents or transactions transformed at the hub, and for EDI interchanges being sent from the hub. The steps shown in the following sections are general and apply only to the importing of maps and setting up of interactions. The general steps for enabling B2B capabilities for participants (for all types of document exchanges) are described in “Setting up B2B capabilities” on page 140. The general steps for managing connections (for all types of document exchanges) are described in Chapter 12, “Managing connections,” on page 143. If you want to see a comprehensive example of an EDI document exchange, from the importing of maps all the way through the management of connections, refer to Appendix B, “EDI examples,” on page 185. The appendix includes the following specific examples:

- "EDI to ROD example" on page 185
- "EDI to XML example" on page 197
- "ROD to EDI example" on page 209
- "XML to EDI example" on page 202

Importing maps

Transformation maps for EDI, XML, or record-oriented-data (ROD) documents can be created with the Data Interchange Services client program. The Data Interchange Services client is a program used to create and maintain XML schema document definitions, XML DTD document definitions, EDI standards, ROD document definitions, and maps.

The Data Interchange Services client is a separately installed program that is included on the WebSphere Partner Gateway media but that typically resides on another computer. The Data Interchange Services mapping specialist creates a map that specifies how the elements in one document are moved to the elements in another, different document. In addition to having instructions that explain how to convert a document from one format to another, Data Interchange Services must also know the layout, or format, of the source and target document. In Data Interchange Services the layout of a document is a *document definition*.

When the transformation map is imported into WebSphere Partner Gateway, the document definitions created in Data Interchange Services are displayed as document flow definitions (package, protocol, and document flow) on the Transformation Map and Manage Document Flow Definitions page.

For example, if you are converting an XML document to an X12 transaction, you import the map that defines the XML and X12 transaction document definitions and the transformation that is to take place.

There are two methods for receiving the map files from the Data Interchange Services. If the Data Interchange Services client has a direct connection to the WebSphere Partner Gateway database, the Data Interchange Services mapping specialist can export the file directly to the database. A more likely scenario is that you will receive the files in e-mail or as an FTP transfer. If the files are transferred to you through FTP, note that they must be in binary form.

If an error occurs during the export of a map from the Data Interchange Services client, you might still see the map name in the Community Console. The map cannot be used to translate documents. You will need to advise the Data Interchange Services client mapping specialist of the export problem and ask the mapping specialist to re-export the map before it can be used to translate documents.

To import a map, perform the following steps:

1. Open a command window.
2. Enter the following command or script:
   - On a UNIX system:
     ```
     <ProductDir>/bin/bcgDISImport.sh <database_user_ID>
     <password> <control_string_map>
     ```
   - On a Windows system:
     ```
     <ProductDir>\bin\bcgDISImport.bat <database_user_ID>
      <password> <control_string_map>
     ```

where <*database_user_ID*> and <*password*> are the values that you used when you installed the database as part of the WebSphere Partner Gateway installation. The <*control_string_map*> is the complete path of the map control string file exported from Data Interchange Services client.

3. For transformation maps, verify that the document flow definition was imported.
   a. Click **Hub Admin > Hub Configuration > Maps > Transformation Maps**.
   b. From the Transformation Maps page, click the **View details** icon next to the map from Data Interchange Services. You will notice that the document flow definitions for the source and target are displayed, indicating the format in which the document will be received at the hub and the format in which it will be delivered from the hub.
   c. Click **Hub Admin > Hub Configuration > Document Flow Definitions**.
   d. Expand the packages and protocols associated with the document definitions you saw on the Transformation Maps page to verify that the document flows are displayed on the Manage Document Flow Definitions page.

You can use validation maps in conjunction with transformation maps to add additional EDI Standards validation to any translation process involving EDI Standards. Validation maps give you complete control over the validation of an EDI document.

Note that transformation and validation maps exported from the Data Interchange Services client or imported with the bcgDISImport utility cannot be downloaded from the WebSphere Partner Gateway Community Console. The Data Interchange Services client mapping specialist administers these maps by connecting to the WebSphere Partner Gateway database through the Data Interchange Services client.

Setting up an EDI to EDI flow

This section describes interactions needed to receive an EDI interchange, de-envelope the interchange, transform a transaction from one EDI format to another, envelope the transaction, and deliver it.

1. Verify that a document flow definition exists for the EDI interchange that is received at the hub. Remember that after the interchange is de-enveloped, the original envelope does not continue to be processed. In other words, it has no delivery point. Therefore, you will use **N/A** for Package on the target interaction.
   a. Click **Hub Admin > Hub Configuration > Document Flow Definition**.
   b. Check to see whether a document flow definition already exists. For example, if a participant will be sending an EDI interchange in AS packaging, EDI-X12 protocol, and ISA document flow, the definition is already available. Similarly, an N/A/EDI-X12/ISA document flow definition already exists.
   c. Enter a value (or select the value from the list) for any attribute you want associated with the profile. For example, if you want to specify that the envelope should be discarded if errors are found with any of the transactions, click the **Edit attribute values** icon next to **Document Flow**. In the **Discard Envelope if Any Errors** row, select **Yes** from the list.
   d. If a document flow definition does not exist, create one by selecting the Package, Protocol, and Document Flow.
2. Create an interaction for the interchange.

   a. Click **Hub Admin > Hub Configuration > Document Flow Definitions > Manage Interactions**.
   b. Select **Create Interaction**.
   c. Select the source and target document flow definitions. Except for the packaging (which will be **N/A** for the target), the document flow definitions will be the same.
   d. Select **EDI De-envelope** from the Action list.
3. Import the transformation map that provides document definitions of the EDI transactions and that describes how the transaction is transformed from one EDI format to another. See "Importing maps" on page 107.

   If the interchange contains more than one transaction, repeat this step for each transaction.
4. If you want to edit attributes of the document definitions associated with the map, perform the following steps:
   a. Click **Hub Admin > Hub Configuration > Document Flow Definition**.
   b. Click the **Edit attribute values** icon next to the protocol. For EDI protocols, you see a long list of attributes that you can set.
   c. Enter a value (or select the value from the list) for any attribute you want associated with the protocol.
   d. Click the **Edit attribute values** icon next to the document flow. You generally see a smaller list of attributes than those associated with the protocol.
   e. Enter a value (or select the value from the list) for any attribute you want associated with the document flow. For example, you can change the **Validation Map** associated with the document flow.

      Make sure you select an envelope profile for the transaction.
5. Create an interaction for the map you just imported.
   a. Click **Hub Admin > Hub Configuration > Document Flow Definitions > Manage Interactions**
   b. Click **Create Interaction**.
   c. Under **Source**, select the document flow associated with the transaction. Expand the package and protocol and select the document flow. This will typically be **N/A** (because the transaction itself did not originate from a participant), the protocol defined in the map (for example, **X12V4R1**) and the actual EDI document defined in the map (for example, **850**).
   d. Under **Target**, select the document flow definition for the transformed document. Expand the package and protocol and select the document flow. Because the transaction will be enveloped (and will, therefore, not be directly delivered to a participant), the packaging will again be **N/A**.
   e. From the transformation map list, select the map that defines how to transform this document.
   f. From the Action list, select **EDI Validate and EDI Translate**.
6. Verify that a document flow definition exists for the EDI interchange that is being sent from the hub, and set any attributes that you want associated with the interchange.
   a. Click **Hub Admin > Hub Configuration > Document Flow Definition**.
   b. Check to see whether a document flow definition already exists. The source package will be N/A, with the protocol and document flow matching the

protocol and document flow used to deliver the interchange. For example, if the interchange will be delivered as AS/EDI-X12/ISA, the source will be N/A/EDI-X12/ISA.

   c. Edit any attributes that apply to the interchange that is being delivered.
   d. If a document flow definition does not exist, create one by selecting the Package, Protocol, and Document Flow.

7. Create an interaction for the EDI interchange that is sent from the hub after the transaction is transformed.
   a. Click **Hub Admin > Hub Configuration > Document Flow Definitions > Manage Interactions**.
   b. Click **Create Interaction**.
   c. Select the source and target documents. Except for the packaging (which will be **N/A** for the source document), the document flow definitions will be the same.
   d. Select **Pass Through** from the **Action** list.

To add an acknowledgment to the flow, see "Setting up acknowledgments" on page 115.

After setting up the interactions, create B2B capabilities for the participants.

- For the source participant, enable three document flow definitions (under **Set Source**)--one for the source document flow, one for the EDI transaction, and one for the envelope.
- For the target participant, enable three document flow definitions (under **Set Target**)--one for the de-enveloped document flow, one for the transformed EDI transaction, and one for the EDI envelope.

The detailed steps for creating B2B capabilities are described in "Setting up B2B capabilities" on page 140.

After setting up B2B capabilities for the participants, create connections. You need three connections:

- One for the envelope from the source participant to the hub.
- One for the source EDI transaction to the target EDI transaction.
- One for the envelope from the hub to the target participant.

The detailed steps for creating connections are described in Chapter 12, "Managing connections," on page 143.

Setting up an EDI to XML or ROD flow

This section describes interactions needed to receive an EDI interchange, de-envelope the interchange, transform a transaction from an EDI format to an XML or ROD document, and deliver it.

Note: For a comprehensive example of the EDI to XML flow, see "EDI to XML example" on page 197. For a comprehensive example of the EDI to ROD flow, see "EDI to ROD example" on page 185.

1. Verify that a document flow definition exists for the EDI interchange that is received at the hub. Remember that after the interchange is de-enveloped, the envelope does not continue to be processed. In other words, it has no delivery point. Therefore, you will use **N/A** for Package on the target interaction.
   a. Click **Hub Admin > Hub Configuration > Document Flow Definition**.

   b. Check to see whether a document flow definition already exists. For example, if a participant will be sending an EDI interchange in AS packaging, EDI-X12 protocol, and ISA document flow, the definition is already available. Similarly, an N/A/EDI-X12/ISA document flow definition already exists.
   c. If a document flow definition does not exist, create one.
2. Create an interaction for the EDI interchange that is received at the hub.
   a. Click **Hub Admin > Hub Configuration > Document Flow Definitions > Manage Interactions**.
   b. Select **Create Interaction**.
   c. Select the source and target documents. Except for the packaging (which will be **N/A** for the target), the document flow definitions will be the same.
   d. Select **EDI De-envelope** from the Action list.
3. Import the transformation map that provides document definitions of the EDI transaction and the XML or ROD document and describes how the transaction is transformed into the XML or ROD document. See "Importing maps" on page 107.

   If the interchange contains more than one transaction, repeat this step for each transaction.
4. Create an interaction for the map you just imported.
   a. Click **Hub Admin > Hub Configuration > Document Flow Definitions > Manage Interactions**.
   b. Click **Create Interaction**.
   c. Under **Source**, select the document flow associated with the transaction. Expand the package and protocol and select the document flow. This will typically be **N/A** (because the transaction itself did not originate from a participant), the protocol defined in the map (for example, **X12V4R1**) and the actual EDI document defined in the map (for example, **850**).
   d. Under **Target**, select the document flow definition for the transformed (XML or ROD) document. Expand the package and protocol and select the document flow.
   e. From the transformation map list, select the map that defines how to transform this document.
   f. From the Action list, select **EDI Validate and EDI Translate**.

To add an acknowledgment to the flow, see "Setting up acknowledgments" on page 115.

After setting up the interactions, create B2B capabilities for the participants.
- For the source participant, enable two document flow definitions (under **Set Source**)--one for the envelope and one for the EDI transaction.
- For the target participant, enable two document flow definitions (under **Set Target**)--one for the EDI envelope and one for the XML or ROD document.

The detailed steps for creating B2B capabilities are described in "Setting up B2B capabilities" on page 140.

After setting up B2B capabilities for the participants, create connections. You need two connections:
- One for the envelope from the source participant to the hub.
- One for the source EDI transaction to the XML or ROD document.

The detailed steps for creating connections are described in Chapter 12, “Managing connections,” on page 143.

Setting up an XML or ROD to EDI flow

This section describes interactions needed to receive an XML or ROD document, transform it into an EDI transaction, envelope the transaction, and deliver it.

Note: For a comprehensive example of the XML to EDI flow, see “XML to EDI example” on page 202. For a comprehensive example of the ROD to EDI flow, see “ROD to EDI example” on page 209.

1. Import the transformation map that provides document definitions of the XML or ROD document and EDI transaction and describes how the document is transformed to the EDI transaction. See “Importing maps” on page 107.
2. Create an interaction for the map you just imported.
   a. Click **Hub Admin > Hub Configuration > Document Flow Definitions > Manage Interactions**.
   b. Click **Create Interaction**.
   c. Under **Source**, select the document flow definition associated with the XML or ROD document. Expand the package and protocol and select the document flow.
   d. Under **Target**, select the document flow associated with the EDI transaction. Expand the package and protocol and select the document flow. Because the transaction will not be delivered directly (it will be put into an envelope before delivery), **N/A** will be listed for Package.
   e. From the transformation map list, select the map that defines how to transform this document.
   f. From the Action list, select **XML Translate and EDI Validate** or **ROD Translate and EDI Validate**.
3. Verify that a document flow definition exists for the EDI interchange that is being sent from the hub, and set any attributes that you want associated with the interchange.
   a. Click **Hub Admin > Hub Configuration > Document Flow Definition**.
   b. Check to see whether a document flow definition already exists. **N/A** should be used for Package for the source document (the interchange being sent from the hub).
   c. Edit any attributes that apply to the interchange that is being delivered.
   d. If a document flow definition does not exist, create one by selecting the Package, Protocol, and Document Flow.
4. Create an interaction for the EDI interchange that is sent from the hub after the document is transformed.
   a. Click **Hub Admin > Hub Configuration > Document Flow Definitions > Manage Interactions**
   b. Click **Create Interaction**.
   c. Select the source and target documents. The source and target documents have different packaging (the source document has a package of N/A), but the protocol (for example, EDI-X12) and the document flow (for example, ISA) should be the same.
   d. Select **Pass Through** from the Action list.

After setting up the interactions, create B2B capabilities for the participants.

- For the source participant, the number of document flow definitions you need to set (under **Set Source**) varies, depending on the type of document flow.
  - For example, for an XML document in which the document flow is ICGPO and the translated EDI transaction is MX12V3R1, enable three document flow definitions (under **Set Source**)--one for the XML (ICGPO) document, one for the EDI transaction (MX12V3R1), and one for the envelope being sent from the hub.
  - For other XML documents and for ROD documents, enable two document flow definitions (under **Set Source**)--one for the XML or ROD document and one for the envelope being sent from the hub.
- For the target participant, enable two document flow definitions (under **Set Target**)--one for the EDI transaction and one for the EDI envelope that is received. For the EDI transaction, click the **Edit attribute values** icon next to the protocol, and specify an envelope profile. You can specify other attributes as well.

The detailed steps for creating B2B capabilities are described in "Setting up B2B capabilities" on page 140.

After setting up B2B capabilities for the participants, create connections. You need two connections:

- One for the source XML or ROD document to EDI transaction.
- One for the envelope from the hub to the participant.

The detailed steps for creating connections are described in Chapter 12, "Managing connections," on page 143.

Setting up multiple XML or ROD documents in one file to EDI flow

This section describes interactions needed to receive multiple XML or ROD documents in one file, transform the documents into EDI transactions, envelope the transactions, and deliver the EDI interchange.

1. Import the transformation map that provides the document definitions of the XML or ROD documents and the EDI transactions and that describes the transformation. See "Importing maps" on page 107.
2. Create an interaction for the source and target documents.
   a. Click **Hub Admin > Hub Configuration > Document Flow Definitions > Manage Interactions**.
   b. Click **Create Interaction**.
   c. Select the source and target documents, and select **XML Translate and EDI Validate** or **ROD Translate and EDI Validate** from the Action list.
3. Repeat step 2 for the source document and each target document produced by the transformation map.
4. Verify that a document flow definition exists for the EDI interchange that is being sent from the hub, and set any attributes that you want associated with the interchange.
   a. Click **Hub Admin > Hub Configuration > Document Flow Definition**.
   b. Check to see whether a document flow definition already exists. The source will be N/A, with the protocol and document flow matching the protocol and document flow used to deliver the interchange. For example, if the interchange will be delivered as AS/EDI-X12/ISA, the source will be N/A/EDI-X12/ISA.

c. Edit any attributes that apply to the interchange that is being delivered.

d. If a document flow definition does not exist, create one by selecting the Package, Protocol, and Document Flow.

5. Create an interaction for the EDI interchange that is sent from the hub after the transaction is transformed.
   a. Click **Hub Admin > Hub Configuration > Document Flow Definitions > Manage Interactions**.
   b. Click **Create Interaction**.
   c. Select the source and target documents. The source and target documents have different packaging (the source document has a package of N/A), but the protocol (for example, EDI-X12) and the document flow (for example, ISA) should be the same.
   d. Select **Pass Through** from the Action list.

After setting up the interactions, create B2B capabilities for the participants.

- For the source participant, the number of document flow definitions you need to set (under **Set Source**) varies, depending on the type of document flow.
  - For example, for an XML document in which the document flow is ICGPO and the translated EDI transaction is MX12V3R1, enable three document flow definitions (under **Set Source**)--one for the XML (ICGPO) document, one for the EDI transaction (MX12V3R1), and one for the envelope being sent from the hub.
  - For other XML documents and for ROD documents, enable two document flow definitions (under **Set Source**)--one for the XML or ROD document and one for the envelope being sent from the hub.

The detailed steps for creating B2B capabilities are described in “Setting up B2B capabilities” on page 140.

After setting up B2B capabilities for the participants, create connections. You need several connections:

- One for each XML or ROD document that is transformed into an EDI transaction.
- One for the envelope from the hub to the participant.

The detailed steps for creating connections are described in Chapter 12, “Managing connections,” on page 143.

Setting up an XML to ROD or ROD to XML document flow

This section describes interactions needed to receive an XML or ROD document, transform it into the other document type (XML to ROD or ROD to XML) and deliver it.

1. Import the transformation map that provides document definitions of the XML and ROD documents and that describes how the documents are transformed. See “Importing maps” on page 107.
2. Click **Hub Admin > Hub Configuration > Maps > Transformation Maps** and click the **View details** icon next to the map you just imported.
3. Create an interaction for the map you just imported.
   a. Click **Hub Admin > Hub Configuration > Document Flow Definitions > Manage Interactions**
   b. Click **Create Interaction**.

4. Select the source and target documents, and select **XML Translate and EDI Validate** or **ROD Translate and EDI Validate** from the Action list.

After setting up the interactions, create B2B capabilities for the participants.

- For the source participant, enable document flow definitions (under **Set Source**) for the XML or ROD document.
- For the target participant, enable document flow definitions (under **Set Target**) for the XML or ROD document.

The detailed steps for creating B2B capabilities are described in "Setting up B2B capabilities" on page 140.

After setting up B2B capabilities for the participants, create connections. You need one connection--for the XML to ROD flow or for the ROD to XML flow. The detailed steps for creating connections are described in Chapter 12, "Managing connections," on page 143.

Setting up an XML to XML or ROD to ROD flow

This section describes interactions needed to receive an XML or ROD document, transform it into a document of the same type (XML to XML or ROD to ROD) and deliver it.

1. Import the transformation map that provides document definitions of the XML or ROD documents and that describes how the documents are transformed. See "Importing maps" on page 107.
2. Click **Hub Admin > Hub Configuration > Maps > Transformation Maps** and click the **View details** icon next to the map you just imported.
3. Create an interaction for the map you just imported.
   a. Click **Hub Admin > Hub Configuration > Document Flow Definitions > Manage Interactions**.
   b. Click **Create Interaction**.
   c. Select the source and target documents.
   d. Select **XML Translate and EDI Validate** or **ROD Translate and EDI Validate** from the Action list.

After setting up the interactions, create B2B capabilities for the participants.

- For the source participant, enable a document flow definition (under **Set Source**) for the XML or ROD document.
- For the target participant, enable a document flow definition (under **Set Target**) for the XML or ROD document.

The detailed steps for creating B2B capabilities are described in "Setting up B2B capabilities" on page 140.

After setting up B2B capabilities for the participants, create connections. You need one connection--for the XML to XML flow or for the ROD to ROD flow. The detailed steps for creating connections are described in Chapter 12, "Managing connections," on page 143.

Setting up acknowledgments

This section describes how to set up interactions to send acknowledgments of interchange or transaction receipt to the originator of the document.

Functional acknowledgments

Functional acknowledgment maps are used to provide generation of functional acknowledgments when responding to EDI documents received from a participant. WebSphere Partner Gateway provides a set of functional acknowledgment maps that produce the commonly used EDI functional acknowledgments. The mapping specialist can also create FA and validation maps, in which case these maps would be uploaded to WebSphere Partner Gateway.

Note: A functional acknowledgment map should be created only when a custom functional acknowledgment is required.

In addition to the functional acknowledgment maps provided with WebSphere Partner Gateway, the &FUNC_ACK_METADATA_DICTIONARY protocol and associated &FUNC_ACK_META are provided. They are listed under **Package: None** in the Document Flow Definitions page. &FUNC_ACK_META is the source document definition for all functional acknowledgment maps. This map provides the structure of the functional acknowledgment. A functional acknowledgment flows to participants, and the functional acknowledgment map tells the system how the acknowledgment should be generated. The name of the source document definition cannot be changed. The Data Interchange Services client mapping specialist cannot create a functional acknowledgment map without this document definition in your database.

The target document definition in a functional acknowledgment map describes the layout of the functional acknowledgment. It must be an EDI document definition with a name of 997, 999, or CONTRL.

The following functional acknowledgment maps are installed with WebSphere Partner Gateway and appear on the Manage Document Flow Definitions page under **Package: N/A**:

Table 16. System-supplied functional acknowledgment maps

Protocol	Document Flow	Description
&DTCTL21	CONTRL	Functional Acknowledgement CONTRL – UN/EDIFACT Version 2 Release 1 (D94B)
&DTCTL	CONTRL	Functional Acknowledgement CONTRL – UN/EDIFACT prior to D94B
&DT99933	999	Functional Acknowledgement 999 – UCS Version 3 Release 3
&DT99737	997	Functional Acknowledgement 997 – X12 Version 3 Release 7
&DT99735	997	Functional Acknowledgement 997 – X12 Version 3 Release 5
&DT99724	997	Functional Acknowledgement 997 – X12 Version 2 Release 4

In addition, the &X44TA1 protocol (with an associated TA1 document flow) are listed under **Package: N/A**. This map is used to generate a TA1. TA1 is a functional acknowledgment that is generated for incoming X12 interchanges.

The &WDIEVAL protocol (with an associated X12ENV) is also provided under **Package: N/A**.

Like EDI transactions, functional acknowledgments are always put into an EDI interchange before being delivered.

TA1 acknowledgments

TA1 is an EDI segment that provides X12 interchange acknowledgment. It acknowledges the receipt and syntactical correctness of an X12 interchange header and trailer (ISA and IEA) pair. The sender can request a TA1 from the receiver by setting element 14 of the ISA Interchange Control Header to **1**. The interchange control number of a TA1 is matched to a previously transmitted X12 interchange with the same control number to complete the acknowledgment process.

Like EDI transactions and functional acknowledgments, TA1s are always put into an EDI interchange before being delivered.

Adding an acknowledgment to the document flow

To add an acknowledgment to a flow, perform the following steps:

1. If the functional acknowlegment map is not supplied by WebSphere Partner Gateway, import the map from the Data Interchange Services client. See "Importing maps" on page 107.
2. Associate the FA map with a document flow definition:
   a. Click **Hub Admin > Hub Configuration > Maps > EDI FA Maps**.
   b. Click the **View details** icon next to the map.
   c. Click the **Expand** icon next to a package to individually expand to the appropriate level (for example, expand the **Package** and **Protocol** folders and select the transaction).
   d. Click **Save**.
3. Create an interaction for the map you just imported.
   a. Click **Hub Admin > Hub Configuration > Document Flow Definition > Manage Interactions**.
   b. Click **Create Interaction**.
   c. Under **Source**, select the document flow associated with the functional acknowledgment. Expand the package and protocol and select the document flow.
   d. Under **Target**, select the same values.
   e. From the Action list, select **Pass Through**.
4. Verify that a document flow definition exists for the EDI interchange that is being sent from the hub, and set any attributes that you want associated with the interchange.
   a. Click **Hub Admin > Hub Configuration > Document Flow Definition**.
   b. Check to see whether a document flow definition already exists. The source will be N/A, with the protocol and document flow matching the protocol and document flow used to deliver the interchange. For example, if the interchange will be delivered as AS/EDI-X12/ISA, the source will be N/A/EDI-X12/ISA.
   c. Edit any attributes that apply to the interchange that is being delivered.
   d. If a document flow definition does not exist, create one by selecting the Package, Protocol, and Document Flow.
5. Create an interaction for the EDI interchange that is sent from the hub after the document is transformed.
   a. Click **Hub Admin > Hub Configuration > Document Flow Definitions > Manage Interactions**.

b. Click **Create Interaction**.
c. Select the source and target documents.
d. Select **Pass Through** from the **Action** list.

After setting up the interactions, create B2B capabilities for the participants. Note that the target participant in a functional acknowledgment transmission is the source participant of the original EDI document.

- For the source participant, enable document flow definitions (under **Set Source**) for the functional acknowledgment. Also enable a document flow definition for the envelope that is being sent from the hub.
- For the target participant, enable a document flow definition (under **Set Target**) for the functional acknowledgment. Also enable a document flow definition for the EDI envelope that is received.

  For the functional acknowledgment, click the **Edit attribute values** icon next to the protocol, and specify an envelope profile.

The detailed steps for creating B2B capabilities are described in “Setting up B2B capabilities” on page 140.

After setting up B2B capabilities for the participants, create connections. You need two connections:

- One for the functional acknowledgment.
- One for the envelope from the hub to the participant.

The detailed steps for creating connections are described in Chapter 12, “Managing connections,” on page 143.

Viewing EDI interchanges and transactions

As mentioned earlier in this chapter, you use the Document Viewer to display information about the EDI interchanges and transactions that make up a document flow. You can display raw documents and associated document processing details and events using specific search criteria. This information is useful if you are trying to determine whether an EDI interchange was successfully delivered or to determine the cause of a problem.

To display the Document Viewer, click **Viewers > Document Viewer**. See the *Administrator Guide* for information on using the Document Viewer.

Chapter 9. Creating the Community Manager profile and B2B capabilities

After you have set up the hub, including establishing targets and setting up document flow definitions and interactions, you are ready to create the Community Manager for your hub community. You then establish the B2B capabilities of the Community Manager. After you create participants (as described in Chapter 11, "Creating participants and their B2B capabilities," on page 139), you activate the actual connections between the Community Manager and participants so that documents can be exchanged.

This chapter covers the following topics:

- "Creating the Community Manager profile"
- "Setting up B2B capabilities" on page 120

Creating the Community Manager profile

The Community Manager is typically the company that owns the WebSphere Partner Gateway server and that uses the server to communicate with participants. The Community Manager is also considered a participant of the hub, and, as such, has a profile, gateways, and B2B capabilities.

To create the Community Manager profile, perform the following steps:

1. Click **Account Admin > Profiles > Community Participant**.
2. Click **Create**.
3. For **Company Login Name**, enter the name the Community Manager will use in the Company field when logging in to the hub. For example, you might type Manager.
4. For **Participant Display Name**, enter the company name or some other descriptive name for the Community Manager. This is the name that appears on the **Participant Search** list.
5. From the Participant type list, select **Community Manager**.

   Note: WebSphere Partner Gateway supports only one Community Manager and one Community Operator. The Community Operator is created automatically when you install WebSphere Partner Gateway.
6. Select the status for the Community Manager. You will probably want to use the default value of **Enabled**.
7. Optionally enter the type of company in the **Vendor** field.
8. Optionally enter the Web site of the Community Manager.
9. Click **New** under **Business ID**.
10. Specify a type from the list, and enter the appropriate identifier. WebSphere Partner Gateway uses the number you enter here to route documents to and from the Community Manager.

    Observe the following guidelines when typing the identifier:

    a. DUNS numbers must equal nine digits.

    b. DUNS+4 must equal 13 digits.

    c. Freeform ID numbers accept up to 60 alphanumeric and special characters.

© Copyright IBM Corp. 2004, 2005

Note: You can assign more than one business ID to the Community Manager. In some cases, more than one business ID is required. For example, when the hub sends and receives EDI X12 and EDIFACT documents, it uses both the DUNS and Freeform IDs during the document exchange.

Both the Community Manager and the participants involved in these types of document flows should have both a DUNS and Freeform ID. The Freeform ID is used to represent EDI IDs that have both an identifier and a qualifier. For example, suppose the EDI qualifier is ″ZZ″ and the EDI identifier is ″810810810″. The Freeform ID could be specified as ZZ-810810810.

11. Optionally enter an IP address for the Community Manager by performing the following steps:
    a. Under **IP Address**, click **New**.
    b. Specify the gateway type.
    c. Enter the IP address of the Community Manager.
12. Click **Save**.
13. You will be presented with a password that the Community Manager will use to log on to the hub. Make a note of this password. You will provide it to the Community Manager Admin user.

    Note: When you create the Community Manager profile, you are actually creating the Admin user for the Community Manager. Admin users can then create individual users within their organizations, or, as Hub Admin, you can create the users for the participants.

After you create a profile for the Community Manager, establish the gateways that the hub will use to send documents to the Community Manager. Refer to the following sections for setting up gateways for the Community Manager:

- “Setting up an HTTP gateway” on page 125
- “Setting up an HTTPS gateway” on page 127
- “Setting up a JMS gateway” on page 130
- “Setting up a file-directory gateway” on page 132

After you set up the gateways for the Community Manager, you set up the B2B capabilities of the Community Manager.

Setting up B2B capabilities

The Community Manager has B2B capabilities that define the types of documents the Community Manager can send and receive.

You use the B2B Capabilities feature to associate the Community Manager’s B2B capabilities with a document flow definition.

Use the following procedure to set the B2B capabilities of the Community Manager.

1. Click **Account Admin > Profiles > Community Participant**.
2. Enter search criteria and click **Search**, or click **Search** without entering any search criteria to display a list of all participants.
3. Click the **View details** icon next to the Community Manager.

4. Click **B2B Capabilities**. The B2B capabilities page is displayed. The right side of the page shows the packages, protocols, and document flows supported by the system as document flow definitions.
5. Click the **Role is not active** icon under the **Set Source** column for the Packages on the right that contain documents the Community Manager will send to participants.
6. Select **Set Target** if you will receive those same documents from participants. The Community Console displays a check if the document flow definition is enabled.

   Note: The selection of Set Source will be the same for all actions in a 2-way PIP regardless of the fact that the request will originate from one participant and the corresponding confirmation from another. This also applies to Set Target.
7. Click the **Expand** icon at the **Package** level to expand an individual node to the appropriate document flow definition level, or select a number from **0-4** or **All** to expand all displayed document flow definitions to the selected level.
8. Again, select the **Set Source**, **Set Target**, or both roles for the lower **Protocol** and **Document Flow** levels for each document flow definition your system supports.

   If a definition is activated at the **Document Flow** level, the **Action** and **Activity** definitions (if any exist) will be activated automatically.
9. Optionally click **Enabled** under the **Enabled** column to place a document flow definition offline. (When you select **Set Source** or **Set Target**, the record is automatically enabled.) Click **Disabled** to place it online.

   If a package is disabled, all lower-level document flow definitions in that same node are also disabled, regardless of whether their individual status was enabled. If a lower-level document flow definition is disabled, all higher-level definitions within the same context remain enabled. When a document flow definition is disabled, all preexisting connections and attributes continue to function. The disabled document flow definition only restricts the creation of new connections.
10. Click the **Edit** icon to edit any of the attributes of a protocol, package, document flow, action, activity, or signal. You then see the settings for the attributes (if any attributes exist). You can modify the attributes by entering a value or selecting a value from the **Update** column and then clicking **Save**.

    As mentioned in step 10 on page 119, the Community Manager can (and in some cases must) have multiple business IDs assigned. If the participant has a requirement to receive only one form of the ID, you must select the appropriate value for the ID. To select the ID:
    a. Click the **Edit** icon next to **None**.

       You see the attribute (**AS Business ID**) associated with the None package.
    b. From the **Update** list, select the AS2 Business ID that is in the format acceptable by your participant.
    c. Click **Save**.

    Note: If you set the attribute on the B2B Capabilities screen, it applies to all exchanges that originate from the Community Manager with the None package. To make the selection more specific to a particular connection, you can set the value (or override the value you set here) at the connection level. Refer to "Activating participant connections" on page 143.

Chapter 10. Creating gateways

After you create the participants, you define gateways for the participants. Gateways define entry points into the participant's system.

This chapter covers the following topics:

- "Overview"
- "Setting up global transport values" on page 124
- "Configuring a forward proxy" on page 125
- "Setting up an HTTP gateway" on page 125
- "Setting up an HTTPS gateway" on page 127
- "Setting up an FTP gateway" on page 128
- "Setting up an SMTP gateway" on page 129
- "Setting up a JMS gateway" on page 130
- "Setting up a file-directory gateway" on page 132
- "Setting up an FTPS gateway" on page 133
- "Setting up an FTP Scripting gateway" on page 134
- "Configuring handlers" on page 137
- "Setting up a gateway for a user-defined transport" on page 138
- "Specifying a default gateway" on page 138

Overview

WebSphere Partner Gateway uses gateways to route documents to their proper destination. The recipient can be a community participant or the Community Manager.

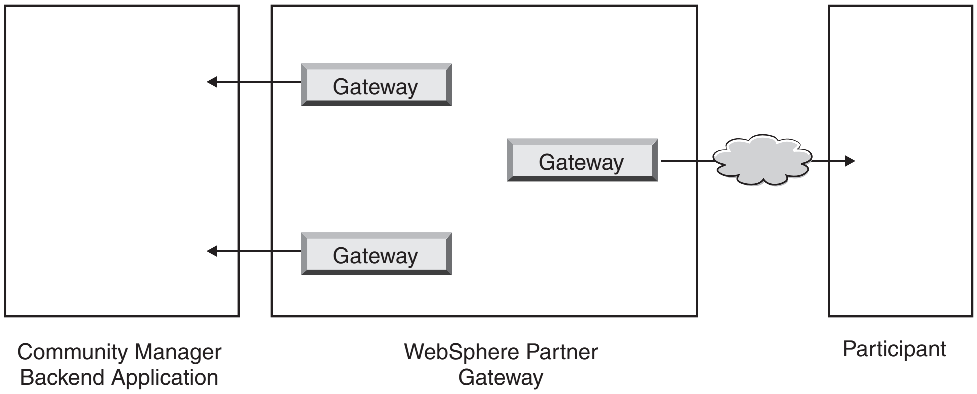

Gateway
Gateway
Gateway
Community Manager Backend Application
WebSphere Partner Gateway
Participant

Figure 34. Gateways to Community Manager and participants

The outbound transport protocol determines which information is used during gateway configuration.

The following transports are supported (by default) for participant gateways:

- HTTP/1.1
- HTTPS/1.0

© Copyright IBM Corp. 2004, 2005

- HTTPS/1.1
- FTP
- FTPS
- JMS
- SMTP

  Note: You can define an SMTP gateway for participants only (not for the Community Manager).
- File directory
- FTP Scripting

You can also specify a user-defined transport, which you upload during the creation of the gateway.

As the Hub Admin, you can set up the gateways for your participants, or the participants can perform this task themselves. In this chapter, you will see how to perform the task for the participants.

Setting up global transport values

You set global transport attributes that apply to all FTP Scripting gateways. If you are not defining any FTP Scripting gateways, this section does not apply to you.

The FTP Scripting transport uses a locking mechanism that prevents more than one FTP Scripting instance from accessing the same gateway at the same time. Default values are supplied for such things as how long a gateway instance waits to obtain the lock and how many times it attempts to retrieve it if the lock is in use. You can use these default values or change them.

1. Click **Account Admin > Profiles > Community Participant**.
2. Click **Gateways**.
3. Select **Global Transport Attributes** from the Gateway List.

   If you updated either **Maximum Lock Time (Seconds)** or **Maximum Queue Time (Seconds)** when you specified global transport values during the creation of targets, those updated values are reflected here.
4. If the default values are appropriate for your configuration, click **Cancel**. Otherwise, continue with the remaining steps in this section.
5. Click the **Edit** icon next to **FTP Scripting Transport**.
6. To change one or more of the values, type the new value or values. You can change:
   - **Lock Retry Count**, which indicates how many times the gateway will attempt to obtain a lock if the lock is currently in use. The default is 3.
   - **Lock Retry Interval (Seconds)**, which indicates the amount of time that will elapse between attempts to obtain the lock. The default is 260 seconds.
   - **Maximum Lock Time (Seconds)**, which indicates how long the gateway can hold the lock. The default is 240 seconds (unless you changed it when creating targets).
   - **Maximum Queue Age (Seconds)**, which indicates how long the target will wait in a queue to obtain the lock. The default is 740 seconds (unless you changed it when creating targets).
7. Click **Save**

Configuring a forward proxy

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 types of support:

- 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 gateway (for example, all HTTP gateways make use of the forward proxy).

To set up a forward proxy, perform the following steps:

1. Click **Account Admin > Profiles > Community Participant**.
2. Click **Gateways**.
3. Click **Forward Proxy Support**.
4. On the Forward Proxy List page, click **Create**.
5. Type a name for the proxy.
6. Optionally, type a description of the proxy.
7. Select the transport type from the list.

   Note: The available transports are HTTP and HTTPS.
8. Type the following information. Enter either Proxy Host and Proxy Port *or* Socks Proxy Host and Socks Proxy Port.
   - For **Proxy Host**, type the proxy server to use (for example: http://proxy.abc.com).
   - For **Proxy Port**, type the port number.
   - If the proxy server requires a user name and password, specify them in the **User Name** and **Password** fields.
   - For **Socks Proxy Host**, type the SOCKS proxy server to use.
   - For **Socks Proxy Port**, type the port number.
9. Select the check box if you want this proxy to be the default proxy (which can be used by any participant that has proxy support specified).
10. Click **Save**.

Setting up an HTTP gateway

You set up an HTTP gateway so that documents can be sent from the hub to your participant's IP address. When you set up an HTTP gateway, you can also specify that documents be sent through a configured proxy server.

To begin the process of creating an HTTP gateway, use the following procedure.

1. Click **Account Admin > Profiles > Community Participant**.
2. Enter search criteria and click **Search**, or click **Search** without entering any search criteria to display a list of all participants.
3. Click the **View details** icon to display the participant's profile.
4. Click **Gateways**.
5. Click **Create**.

Gateway Details

From the **Gateway List** page, perform the following steps:

1. Type a name to identify the gateway. This is a required field. This is the name that will appear on the list of gateways.
2. Optionally indicate the status of the gateway. **Enabled** is the default. A gateway that is enabled is ready to send documents. A gateway that is disabled cannot send documents.
3. Optionally indicate whether the gateway is Online or Offline. The default is **Online**.
4. Optionally enter a description of the gateway.

Gateway Configuration

In the **Gateway Configuration** section of the page, perform the following steps:

1. Select **HTTP/1.1** from the **Transport** list.
2. Optionally, select a proxy server to be used. The **Forward Proxy List** includes any proxy servers that you have created, including the default proxy server. The default value for this field is **Use default forward proxy**. If you want the selected participant to use a different proxy server, select that server from the list. If you do not want to use this feature with the selected participant, select **Use no forward proxy**.
3. In the **Address** field, enter the URI where the document will be delivered. This field is required.

   The format is: http://*<server_name>:<optional_port>/<path>*

   An example of this format is:

   ```
   http://anotherserver.ibm.com:57080/bcgreceiver/Receiver
   ```

   When you are setting up a gateway to be used for a Web service, specify the private URL supplied by the Web service provider. This is where WebSphere Partner Gateway will invoke the Web service when it acts as a proxy for the Web service provider.
4. Optionally enter a user name and password, if a user name and password are required to access the HTTP server.
5. In the **Retry Count** field, enter the number of times you want the gateway to attempt to send a document before it fails. The default is 3.
6. In the **Retry Interval** field, enter the amount of time the gateway should wait before attempting to send the document again. The default is 300 seconds.
7. In the **Number of Threads** field, enter the number of documents that can be processed simultaneously. The default is 3.
8. In the **Validate Client IP** field, select **Yes** if you want the IP address of the sender to be validated before the document is processed. Select **No** otherwise. The default is **No**.
9. In the **Auto Queue** field, select **Yes** if you want the gateway to be placed offline (automatically) if a delivery failure is about to occur because the number of retries has been exhausted. Select **No** otherwise. The default is **No**.

   When you select **Auto Queue**, all documents remain queued until the gateway is placed online manually.
10. In the **Connection Timeout** field, enter the number of seconds a socket will remain open with no traffic. The default is 120 seconds.
11. If you want to configure the Preprocess or Postprocess step for the gateway, go to “Configuring handlers” on page 137. Otherwise, click **Save**.

Setting up an HTTPS gateway

You set up an HTTPS gateway so that documents can be sent from the hub to your participant's IP address. When you set up an HTTPS gateway, you can also specify that documents be sent through a configured proxy server.

To create HTTPS gateways, use the following procedure.

1. Click **Account Admin > Profiles > Community Participant**.
2. Enter search criteria and click **Search**, or click **Search** without entering any search criteria to display a list of all participants.
3. Click the **View details** icon to display the participant's profile.
4. Click **Gateways**.
5. Click **Create**.

Gateway Details

From the Gateway List page, perform the following steps:

1. Type a name to identify the gateway. This is a required field.
2. Optionally indicate the status of the gateway. **Enabled** is the default. A gateway that is enabled is ready to send documents. A gateway that is disabled cannot send documents.
3. Optionally indicate whether the gateway is Online or Offline. The default is **Online**.
4. Optionally enter a description of the gateway.

Gateway Configuration

In the **Gateway Configuration** section of the page, perform the following steps:

1. Select **HTTPS/1.0** or **HTTPS/1.1** from the **Transport** list.
2. Optionally, select a proxy server to be used. The **Forward Proxy List** includes any proxy servers that you have created, including the default proxy server. The default value for this field is **Use default forward proxy**. If you want the selected participant to use a different proxy server, select that server from the list. If you do not want to use this feature with the selected participant, select **Use no forward proxy**.
3. In the **Address** field, enter the URI where the document will be delivered. This field is required.

   The format is: https://*<server_name>:<optional_port>/<path>*

   For example:

   ```
   https://anotherserver.ibm.com:57443/bcgreceiver/Receiver
   ```
4. Optionally enter a user name and password, if a user name and password are required to access the secure HTTP server.
5. In the **Retry Count** field, enter the number of times you want the gateway to attempt to send a document before it fails. The default is 3.
6. In the **Retry Interval** field, enter the amount of time the gateway should wait before attempting to send the document again. The default is 300 seconds.
7. In the **Number of Threads** field, enter the number of documents that can be processed simultaneously. The default is 3.
8. In the **Validate Client IP** field, select **Yes** if you want the IP address of the sender to be validated before the document is processed. Select **No** otherwise. The default is **No**.

9. In the **Validate Client SSL Cert** field, select **Yes** if you want the digital certificate of the sending partner to be validated against the business ID associated with the document. The default is **No**.
10. In the **Auto Queue** field, select **Yes** if you want the gateway to be placed offline (automatically) if a delivery failure is about to occur because the number of retries has been exhausted. Select **No** otherwise. The default is **No**.

    When you select **Auto Queue**, all documents remain queued until the gateway is placed online manually.
11. In the **Connection Timeout** field, enter the number of seconds a socket will remain open with no traffic. The default is 120 seconds.
12. If you want to configure the Preprocess or Postprocess step for the gateway, go to "Configuring handlers" on page 137. Otherwise, click **Save**.

Setting up an FTP gateway

To create an FTP gateway, use the following procedure.

1. Click **Account Admin > Profiles > Community Participant**.
2. Enter search criteria and click **Search**, or click **Search** without entering any search criteria to display a list of all participants.
3. Click the **View details** icon to display the participant's profile.
4. Click **Gateways**.
5. Click **Create**.

Gateway Details

From the Gateway Details page, perform the following steps:

1. Type a name to identify the gateway. This is a required field.
2. Optionally indicate the status of the gateway. **Enabled** is the default. A gateway that is enabled is ready to send documents. A gateway that is disabled cannot send documents.
3. Optionally indicate whether the gateway is Online or Offline. The default is **Online**.
4. Optionally enter a description of the gateway.

Gateway Configuration

In the **Gateway Configuration** section of the page, perform the following steps:

1. Select **FTP** from the **Transport** list.
2. In the **Address** field, enter the URI where the document will be delivered. This field is required.

   The format is: ftp://<*ftp_server_name*>:<*portno*>

   For example:

   ```
   ftp://ftpserver1.ibm.com:2115
   ```

   If you do not enter a port number, the standard FTP port is used.
3. Optionally enter a user name and password, if a user name and password are required to access the FTP server.
4. In the **Retry Count** field, enter the number of times you want the gateway to attempt to send a document before it fails. The default is 3.
5. In the **Retry Interval** field, enter the amount of time the gateway should wait before attempting to send the document again. The default is 300 seconds.

6. In the **Number of Threads** field, enter the number of documents that can be processed simultaneously. The default is 3.
7. In the **Validate Client IP** field, select **Yes** if you want the IP address of the sender to be validated before the document is processed. Select **No** otherwise. The default is **No**.
8. In the **Auto Queue** field, select **Yes** if you want the gateway to be placed offline (automatically) if a delivery failure is about to occur because the number of retries has been exhausted. Select **No** otherwise. The default is **No**.

   When you select **Auto Queue**, all documents remain queued until the gateway is placed online manually.
9. In the **Connection Timeout** field, enter the number of seconds a socket will remain open with no traffic. The default is 120 seconds.
10. In the **Use Unique File Name** field, leave the box checked if you want the document to have its original name when it is sent to its destination. Otherwise, click the box to remove the check, in which case WebSphere Partner Gateway will assign a name to the file.
11. If you want to configure the Preprocess or Postprocess step for the gateway, go to "Configuring handlers" on page 137. Otherwise, click **Save**.

Setting up an SMTP gateway

To create an SMTP gateway, use the following procedure.

1. Click **Account Admin > Profiles > Community Participant**.
2. Enter search criteria and click **Search**, or click **Search** without entering any search criteria to display a list of all participants.
3. Click the **View details** icon to display the participant's profile.
4. Click **Gateways**.
5. Click **Create**.

Gateway Details

From the Gateway List page, perform the following steps:

1. Type a name to identify the gateway. This is a required field.
2. Optionally indicate the status of the gateway. **Enabled** is the default. A gateway that is enabled is ready to send documents. A gateway that is disabled cannot send documents.
3. Optionally indicate whether the gateway is Online or Offline. The default is **Online**.
4. Optionally enter a description of the gateway.

Gateway Configuration

In the **Gateway Configuration** section of the page, perform the following steps:

1. Select **SMTP** from the **Transport** list.
2. In the **Address** field, enter the URI where the document will be delivered. This field is required.

   The format is: mailto:<*user@server_name*>

   For example:

   ```
   mailto:admin@anotherserver.ibm.com
   ```
3. Optionally enter a user name and password, if a user name and password are required to access the SMTP server.

4. In the **Retry Count** field, enter the number of times you want the gateway to attempt to send a document before it fails. The default is 3.
5. In the **Retry Interval** field, enter the amount of time the gateway should wait before attempting to send the document again. The default is 300 seconds.
6. In the **Number of Threads** field, enter the number of documents that can be processed simultaneously. The default is 3.
7. In the **Validate Client IP** field, select **Yes** if you want the IP address of the sender to be validated before the document is processed. Select **No** otherwise. The default is **No**.
8. In the **Auto Queue** field, select **Yes** if you want the gateway to be placed offline (automatically) if a delivery failure is about to occur because the number of retries has been exhausted. Select **No** otherwise. The default is **No**.

   When you select **Auto Queue**, all documents remain queued until the gateway is placed online manually.
9. In the **Authentication Required** field, indicate whether a user name and password are supplied with the document. The default is **No**.
10. If you want to configure the Preprocess or Postprocess step for the gateway, go to “Configuring handlers” on page 137. Otherwise, click **Save**.

Setting up a JMS gateway

To create JMS gateways, use the following procedure.

1. Click **Account Admin > Profiles > Community Participant**.
2. Enter search criteria and click **Search**, or click **Search** without entering any search criteria to display a list of all participants.
3. Click the **View details** icon to display the participant’s profile.
4. Click **Gateways**.
5. Click **Create**.

Gateway Details

From the Gateway List page, perform the following steps:

1. Type a name to identify the gateway. This is a required field.
2. Optionally indicate the status of the gateway. **Enabled** is the default. A gateway that is enabled is ready to send documents. A gateway that is disabled cannot send documents.
3. Optionally indicate whether the gateway is Online or Offline. The default is **Online**.
4. Optionally enter a description of the gateway.

Gateway Configuration

In the **Gateway Configuration** section of the page, perform the following steps:

1. Select **JMS** from the **Transport** list.
2. In the **Address** field, enter the URI where the document will be delivered. This field is required.

   For WebSphere MQ JMS, the format of the target URI is as follows:

   ```
   file:///<user_defined_MQ_JNDI_bindings_path>
   ```

   For example:

   ```
   file:///opt/JNDI-Directory
   ```

The directory contains the ".bindings" file for the file-based JNDI. This file indicates to WebSphere Partner Gateway how to route the document to its intended destination.

- For an internal JMS gateway (that is, the gateway to your back-end system), this should match the value you entered (the file system path to the bindings file) when you configured WebSphere Partner Gateway for JMS (step 5 on page 21). You can also specify the subfolder for the JMS context as part of the JMS provider URL.

  For example, without the JMS context, you would enter `c:/temp/JMS`. With the JMS context, you would enter `c:/temp/JMS/JMS`.
- For participant gateways, the participant will probably provide the ".bindings" file.

This field is required.

3. Optionally enter a user name and password, if a user name and password are required to access the JMS queue.
4. In the **Retry Count** field, enter the number of times you want the gateway to attempt to send a document before it fails. The default is 3.
5. In the **Retry Interval** field, enter the amount of time the gateway should wait before attempting to send the document again. The default is 300 seconds.
6. In the **Number of Threads** field, enter the number of documents that can be processed simultaneously. The default is 3.
7. In the **Validate Client IP** field, select **Yes** if you want the IP address of the sender to be validated before the document is processed. Select **No** otherwise. The default is **No**.
8. In the **Auto Queue** field, select **Yes** if you want the gateway to be placed offline (automatically) if a delivery failure is about to occur because the number of retries has been exhausted. Select **No** otherwise. The default is **No**.

   When you select **Auto Queue**, all documents remain queued until the gateway is placed online manually.
9. In the **Authentication Required** field, indicate whether a user name and password are supplied with the document. The default is **No**.
10. In the **JMS Factory Name** field, enter the name of the Java class the JMS provider uses to connect to the JMS queue. This field is required.

    For internal JMS gateways, this name should match the one you specified with the `define qcf` command when you created the bindings file (step 4 on page 22).

    If you entered the subfolder for the JMS context in step 2 on page 130, enter only the factory name here (for example, `Hub`). If you did not enter the subfolder for the JMS context in the **Address** field, specify the subfolder before the factory name (for example, `JMS/Hub`).
11. In the **JMS Message Class** field, enter the message class. The choices are any valid JMS Message class, such as TextMessage or BytesMessage. This field is required.
12. In the **JMS Message Type** field, enter the type of message. This is an optional field.
13. In the **Provider URL Packages** field, enter the name of the classes (or JAR file) that Java uses to understand the JMS context URL. This field is optional. If you do not specify a value, the file system path to the bindings file is used.
14. In the **JMS Queue Name** field, enter the name of the JMS queue where documents are to be sent. This field is required.

For internal JMS gateways, this name should match the one you specified with the `define q` command when you created the bindings file (step 4 on page 22).

If you entered the subfolder for the JMS context in step 2 on page 130, enter only the queue name here (for example, `outQ`). If you did not enter the subfolder for the JMS context in the JMS provider URL, specify the subfolder before the factory name (for example, `JMS/outQ`).

15. In the **JMS JNDI Factory Name** field, enter the factory name used to connect to the name service. This field is required. The value of com.sun.jndi.fscontext.RefFSContextFactory is the one you will probably use, if you set up your JMS configuration as described in "Configuring the hub for the JMS transport protocol" on page 20.
16. If you want to configure the Preprocess or Postprocess step for the gateway, go to "Configuring handlers" on page 137. Otherwise, click **Save**.

Setting up a file-directory gateway

To create file-directory gateways, use the following procedure.

1. Click **Account Admin > Profiles > Community Participant**.
2. Enter search criteria and click **Search**, or click **Search** without entering any search criteria to display a list of all participants.
3. Click the **View details** icon to display the participant's profile.
4. Click **Gateways**.
5. Click **Create**.

Gateway Details

From the Gateway List page, perform the following steps:

1. Type a name to identify the gateway. This is a required field.
2. Optionally indicate the status of the gateway. **Enabled** is the default. A gateway that is enabled is ready to send documents. A gateway that is disabled cannot send documents.
3. Optionally indicate whether the gateway is Online or Offline. The default is **Online**.
4. Optionally enter a description of the gateway.

Gateway Configuration

In the **Gateway Configuration** section of the page, perform the following steps:

1. Select **File Directory** from the **Transport** list.
2. In the **Address** field, enter the URI where the document will be delivered. This field is required.

   The format for UNIX systems and for Windows systems in which the file directory is on the same drive on which WebSphere Partner Gateway is installed is: file:///<*path_to_target_directory*>

   For example:

   ```
   file:///localfiledir
   ```

   where *localfiledir* is a directory off the root directory.

   For Windows systems in which the file directory is on a separate drive from WebSphere Partner Gateway, the format is: file:///<*drive_letter*>:/<*path*>
3. In the **Retry Count** field, enter the number of times you want the gateway to attempt to send a document before it fails. The default is 3.

4. In the **Retry Interval** field, enter the amount of time the gateway should wait before attempting to send the document again. The default is 300 seconds.
5. In the **Number of Threads** field, enter the number of documents that should be processed simultaneously. The default is 3.
6. In the **Validate Client IP** field, select **Yes** if you want the IP address of the sender to be validated before the document is processed. Select **No** otherwise. The default is **No**.
7. In the **Auto Queue** field, select **Yes** if you want the gateway to be placed offline (automatically) if a delivery failure is about to occur because the number of retries has been exhausted. Select **No** otherwise. The default is **No**.

   When you select **Auto Queue**, all documents remain queued until the gateway is placed online manually.
8. In the **Use Unique File Name** field, leave the box checked if you want the document to have its original name when it is sent to its destination. Otherwise, click the box to remove the check, in which case WebSphere Partner Gateway will assign a name to the file.
9. If you want to configure the Preprocess or Postprocess step for the gateway, go to “Configuring handlers” on page 137. Otherwise, click **Save**.

Setting up an FTPS gateway

To create FTPS gateways, use the following procedure.

1. Click **Account Admin > Profiles > Community Participant**.
2. Enter search criteria and click **Search**, or click **Search** without entering any search criteria to display a list of all participants.
3. Click the **View details** icon to display the participant’s profile.
4. Click **Gateways**.
5. Click **Create**.

Gateway Details

From the Gateway List page, perform the following steps:

1. Type a name to identify the gateway. This is a required field.
2. Optionally indicate the status of the gateway. **Enabled** is the default. A gateway that is enabled is ready to send documents. A gateway that is disabled cannot send documents.
3. Optionally indicate whether the gateway is Online or Offline. The default is **Online**.
4. Optionally enter a description of the gateway.

Gateway Configuration

In the **Gateway Configuration** section of the page, perform the following steps:

1. Select **FTPS** from the **Transport** list.
2. In the **Address** field, enter the URI where the document will be delivered. This field is required.

   The format is: ftp://<*ftp_server_name*>:<*portno*>

   For example:

   ```
   ftp://ftpserver1.ibm.com:2115
   ```

   If you do not enter a port number, the standard FTP port is used.

3. Optionally enter a user name and password, if a user name and password are required to access the secure FTP server.
4. In the **Retry Count** field, enter the number of times you want the gateway to attempt to send a document before it fails. The default is 3.
5. In the **Retry Interval** field, enter the amount of time the gateway should wait before attempting to send the document again. The default is 300 seconds.
6. In the **Number of Threads** field, enter the number of documents that should be processed simultaneously. The default is 3.
7. In the **Validate Client IP** field, select **Yes** if you want the IP address of the sender to be validated before the document is processed. Select **No** otherwise. The default is **No**.
8. In the **Auto Queue** field, select **Yes** if you want the gateway to be placed offline (automatically) if a delivery failure is about to occur because the number of retries has been exhausted. Select **No** otherwise. The default is **No**.

   When you select **Auto Queue**, all documents remain queued until the gateway is placed online manually.
9. In the **Connection Timeout** field, enter the number of seconds a socket will remain open with no traffic. The default is 120 seconds.
10. In the **Use Unique File Name** field, leave the box checked if you want the document to have its original name when it is sent to its destination. Otherwise, click the box to remove the check, in which case WebSphere Partner Gateway will assign a name to the file.
11. If you want to configure the Preprocess or Postprocess step for the gateway, go to “Configuring handlers” on page 137. Otherwise, click **Save**.

Setting up an FTP Scripting gateway

An FTP Scripting gateway runs according to the schedule you set. The behavior of an FTP Scripting gateway is governed by an FTP command script.

Creating the FTP script

To use an FTP Scripting gateway, you create a file that includes all the FTP commands required that can be accepted by your FTP server.

1. Create a script for the gateways, to indicate the actions you want performed. The following script is an example of connecting to the specified FTP server (with the name and password specified), changing to the specified directory on the FTP server, and sending all the files to the specified directory on the server.

   ```
   open %BCGSERVERIP% %BCGUSERID% %BCGPASSWORD% %BCGOPTIONx%
   cd %BCGOPTIONx%
   mput *
   quit
   ```

   The placeholders (for example, %BCGSERVERIP%) are replaced when the gateway is put in service by the values you enter when you create a specific instance of an FTP scripting gateway, as shown in the following table:

Table 17. How script parameters map to FTP Scripting gateway field entries

Script parameter	FTP Scripting gateway field entry
%BCGSERVERIP%	Server IP
%BCGUSERID%	User ID
%BCGPASSWORD%	Password
%BCGOPTIONx%	Option*x*, under **User Defined Attributes**

You can have up to 10 user-defined options.

2. Save the file.

FTP script commands

You can use the following commands when creating the script:

- ascii, binary, passive

  These commands are not sent to the FTP server. They modify the mode of transfer (ascii, binary, or passive) to the FTP server.
- cd

  This command changes to the specified directory.
- delete

  This command removes a file from the FTP server.
- mkdir

  This command creates a directory on the FTP server.
- mput

  This command takes a single argument, which specifies one or more files to be transferred to the remote system. This argument can contain the standard wildcard characters to identify multiple files (’*’ and ’?’).
- open

  This command takes three parameters--the FTP server IP address, the user name, and a password. These parameters map to the %BCGSERVERIP%, %BCGUSERID%, and %BCGPASSWORD% variables.

  The first line of your FTP Scripting gateway script, therefore, should be:

  ```
  open %BCGSERVERIP% %BCGUSERID% %BCGPASSWORD%
  ```
- quit, bye

  This command ends an existing connection to an FTP server.
- quote

  This command indicates that everything after the QUOTE should be sent to the remote system as a command. This allows you to send commands to a remote FTP server that might not be defined in the standard FTP protocol.
- rmdir

  This command removes a directory from the FTP server.
- site

  This command can be used to issue site-specific commands to the remote system. The remote system determines if the contents of this command are valid.

FTP Scripting gateways

If you will be using FTP Scripting gateways, perform the following tasks:

To create FTP Scripting gateways, use the following procedure.

1. Click **Account Admin > Profiles > Community Participant**.
2. Enter search criteria and click **Search**, or click **Search** without entering any search criteria to display a list of all participants.
3. Click the **View details** icon to display the participant’s profile.
4. Click **Gateways**.
5. Click **Create**.

Gateway Details

From the Gateway List page, perform the following steps:

1. Type a name to identify the gateway. This is a required field.
2. Optionally indicate the status of the gateway. **Enabled** is the default. A gateway that is enabled is ready to send documents. A gateway that is disabled cannot send documents.
3. Optionally indicate whether the gateway is Online or Offline. The default is **Online**.
4. Optionally enter a description of the gateway.

Gateway Configuration

In the **Gateway Configuration** section of the page, perform the following steps:

1. Select **FTP Scripting** from the **Transport** list.
2. Enter the IP address of the FTP server to which you are sending documents. The value you enter here will replace %BCGSERVERIP% when the FTP script is run.
3. Enter the user ID and password required to access the FTP server. The values you enter here will replace %BCGUSERID% and %BCGPASSWORD% when the FTP script is run.
4. If the target is in secure mode, use the default of **Yes** for **FTPS Mode**. Otherwise, click **No**.
5. Upload the script file by following these steps:
   a. Click **Upload Script File**.
   b. Type the name of the file that contains the script for processing documents, or use **Browse** to navigate to the file.
   c. Click **Load File** to load the script file into the **Currently loaded script file** text box.
   d. If the script file is the one you want to use, click **Save**.
   e. Click **Close Window**.
6. In the **Retry Count** field, enter the number of times you want the gateway to attempt to send a document before it fails. The default is 3.
7. In the **Retry Interval** field, enter the amount of time the gateway should wait before attempting to send the document again. The default is 300 seconds.
8. For **Connection Timeout**, enter the number of seconds a socket will remain open with no traffic. The default is 120 seconds.
9. In the **Lock User** field, indicate whether the gateway will request a lock, so that no other instances of an FTP Scripting gateway can gain access to the same FTP server directory at the same time.

Note: The **Global FTP Scripting Attributes** values are already filled in, and you cannot edit them from this page. To modify these values, you use the Global Transport Attributes page, as described in "Setting up global transport values" on page 124.

User-Defined Attributes

If you want to specify additional attributes, perform the following steps. The value you enter for the option will replace %BCGOPTION*x*% when the FTP script is run (where *x* corresponds to the number of the option.)

1. Click **New**.

2. Type a value next to **Option 1**.
3. If you have additional attributes to specify, click **New** again and type a value.
4. Repeat step 3 as often as necessary to define all the attributes.

For example, suppose your FTP script looked like this:

```
open %BCGSERVERIP% %BCGUSERID% %BCGPASSWORD%
          cd %BCGOPTION1%
          mput *
          quit
```

The %BCGOPTION% in this case would be a directory name.

Schedule

From the Schedule section of the page, perform the following steps:

1. Indicate whether you want interval-based scheduling or calendar-based scheduling.
   - If you select **Interval Based Scheduling**, select the number of seconds that should elapse before the gateway is polled (or accept the default value).
   - If you select **Calendar Based Scheduling**, choose the type of scheduling (**Daily Schedule**, **Weekly Schedule**, or **Custom Schedule**).
     - If you select **Daily Schedule**, enter the time of day when the gateway should be polled.
     - If you select **Weekly Schedule**, select one or more days of the week in addition to the time of day.
     - If you select **Custom Schedule**, select the time of day and then choose **Range** or **Selective Days** for the week and the month. With **Range**, you indicate the start date and the end date. (For example, click **Mon** and **Fri** if you want the server polled at a certain time on weekdays only.) With **Selective Days**, you choose the specific days of the week and month.
2. If you want to configure the Preprocess or Postprocess step for the gateway, go to "Configuring handlers." Otherwise, click **Save**.

Configuring handlers

As described in Chapter 1, "Introduction," you can modify two processing points for a gateway--Preprocess and Postprocess.

No handlers are provided by default for the Preprocess or Postprocess step, and, therefore, no handlers are listed by default in the **Available List**. If you have uploaded a handler, you can select it and move it to the **Configured List**.

To apply a user-written handler for these configuration points, you must first upload the handler, as described in "Uploading user-defined handlers" on page 32. (Select **Gateway** instead of **Target** for step 2 on page 32). Then perform the following steps:

1. Select **preprocess** or **postprocess** from the **Configuration Point Handlers** list.
2. Select the handler from the **Available List** and click **Add**.
3. If you want to change the attributes of the handler, select it from the **Configured List** and click **Configure**. You will see a list of attributes that can be changed. Make the necessary changes and click **Set Values**.
4. Click **Save**.

You can further modify the **Configured List** as follows:

- Remove a handler by selecting the handler from the **Configured List** and clicking **Remove**. The handler is moved to the **Available List**.
- Rearrange the order in which the handler is processed by selecting the handler and clicking **Move Up** or **Move Down**.

Setting up a gateway for a user-defined transport

If you want to upload a user-defined transport, perform the following steps.

1. Click **Account Admin > Profiles > Community Participant**.
2. Click **Gateways**.
3. Click **Manage Transport Types**.
4. Enter the name of an XML file that defines the transport (or use **Browse** to navigate to the file).
5. Use the default of **Yes** for **Commit to Database**. Select **No** if you are testing this transport before putting it into production.
6. Indicate whether this file should replace a file with the same name that is already in the database.
7. Click **Upload**.

   Note: From the Manage Transport Types page, you can also delete a user-defined transport type. You cannot delete a transport provided by WebSphere Partner Gateway. Also, you cannot delete a user-defined transport after it has been used for creating a gateway.
8. Click **Create**
9. Type a name to identify the gateway. This is a required field.
10. Optionally indicate the status of the gateway. **Enabled** is the default. A gateway that is enabled is ready to send documents. A gateway that is disabled cannot send documents.
11. Optionally indicate whether the gateway is Online or Offline. The default is **Online**.
12. Optionally enter a description of the gateway.
13. Fill in the fields (which will be unique for each user-defined transport) and click **Save**.

Specifying a default gateway

After you create gateways for the Community Manager or participant, select one of the gateways as the default gateway.

1. Click **Account Admin > Profiles > Community Participant**.
2. Enter search criteria and click **Search**, or click **Search** without entering any search criteria to display a list of all participants.
3. Click the **View details** icon to display the participant’s profile.
4. Click **Gateways**.
5. Click **View Default Gateways**.

   A list of gateways defined for the participant is displayed.
6. From the **Production** list, select the gateway that will be the default for this participant. You can also set default gateways for other types of gateways, such as **Test**.
7. Click **Save**.

Chapter 11. Creating participants and their B2B capabilities

For each participant with which you will be exchanging documents, you create a participant profile. You then set the B2B capabilities of the participants (or the participants can perform this step themselves).

This chapter covers the following topics:
- "Creating participant profiles"
- "Setting up B2B capabilities" on page 140

Creating participant profiles

To create a participant, you need to know, at minimum, the following information about the participant:
- The IP address of the participant
- The Business ID that the participant uses. This can be:
  - DUNS, which is the standard Dun & Bradstreet number associated with a company
  - DUNS+4, which is an extended version of the DUNS number
  - Freeform, which can be any number that the participant chooses to use to identify the company

For each participant you want to add to the hub community, follow this procedure:
1. Click **Account Admin > Profiles > Community Participant**.
2. Click **Create**.
3. For **Company Login Name**, enter the name the participant will use in the Company field when logging in to the hub.
4. For **Participant Display Name**, enter the company name or some other descriptive name for the participant. This is the name that appears on the **Participant Search** list.
5. Select the type of participant. Because WebSphere Partner Gateway can have only one Community Manager and one Community Operator, your choice is limited to **Community Participant**.
6. Select the status for the participant. When you are creating a participant, you will probably want to use the default value of **Enabled**.
7. Optionally enter the type of company in the **Vendor** field.
8. Optionally enter the Web site of the participant.
9. Click **New** under **Business ID**.
10. Specify a type from the list, and enter the appropriate identifier. WebSphere Partner Gateway uses the number you enter here to route the document to and from the participant.

    Observe the following guidelines when typing the identifier:

    a. DUNS numbers must equal nine digits.

    b. DUNS+4 must equal 13 digits.

    c. Freeform ID numbers accept up to 60 alphanumeric and special characters.

© Copyright IBM Corp. 2004, 2005

Note: You can assign more than one business ID to a participant. In some cases, more than one Business ID is required. For example, when the hub sends and receives EDI X12 and EDIFACT documents, it uses both the DUNS and Freeform IDs during the document exchange.

Both the Community Manager and the participants involved in these types of document flows should have both a DUNS and Freeform ID. The Freeform ID is used to represent EDI IDs that have both an identifier and a qualifier. For example, suppose the EDI qualifier is ″ZZ″ and the EDI identifier is ″810810810″. The Freeform ID could be specified as ZZ-810810810.

11. Optionally enter an IP address for the participant by performing the following steps:
    a. Under **IP Address**, click **New**.
    b. Specify the gateway type.
    c. Enter the IP address of the participant.
12. Click **Save**.
13. You will be presented with a password that the participant will use to log on to the hub. Make a note of this password. You will provide it to the participant Admin user.

When you create a participant, you are actually creating the Admin user for that participant. Admin users can then create individual users within their organizations, or, as Hub Admin, you can create the users for the participants.

After you create a profile for a participant, establish the gateways that the hub will use to send documents to the participant. Refer to the following sections for setting up gateways for participants:

- “Setting up global transport values” on page 124

  Note: These values pertain only to the FTP Scripting gateway.
- “Setting up an HTTP gateway” on page 125
- “Setting up an HTTPS gateway” on page 127
- “Setting up an FTP gateway” on page 128
- “Setting up an SMTP gateway” on page 129
- “Setting up a JMS gateway” on page 130
- “Setting up a file-directory gateway” on page 132
- “Setting up an FTPS gateway” on page 133
- “Setting up an FTP Scripting gateway” on page 134

Setting up B2B capabilities

Each participant has B2B capabilities that define the types of documents the participant can send and receive.

As the Hub Admin, you can set up the B2B capabilities of your participants, or the participants can perform this task themselves. In this chapter, you will see how to perform the task for the participants.

You use the B2B Capabilities feature to associate a participant’s B2B capabilities with a document flow definition.

Use the following procedure to set the B2B capabilities of each participant.

1. Click **Account Admin > Profiles > Community Participant**.
2. Enter search criteria and click **Search**, or click **Search** without entering any search criteria to display a list of all participants.
3. Click the **View details** icon to display the participant's profile.
4. Click **B2B Capabilities**. The B2B capabilities page is displayed. The right side of the page shows the packages, protocols, and documents supported by the system as document flow definitions.
5. Click the **Role is not active** icon under the **Set Source** column for the Packages on the right that contain documents the participants will send to the Community Manager.
6. Select both **Set Source** and **Set Target** if the participants will send and receive those same documents. The Console displays a check if the document flow definition is enabled.

   Note: The selection of Set Source will be the same for all actions in 2-way PIP regardless of the fact that the request will originate from one participant and the corresponding confirmation from another. This also applies to Set Target.
7. Click the **Expand** icon at the **Package** level to expand an individual node to the appropriate document flow definition level or select a number from **0-4** or **All** to expand all displayed document flow definitions to the selected level.
8. Again, select the **Set Source**, **Set Target**, or both roles for the lower **Protocol** and **Document Flow** levels for each Document Flow Definition your system supports.

   If a definition is activated at the **Document Flow** level, the **Action** and **Activity** definitions (if any exist) will be activated automatically.
9. Optionally click **Enabled** under the **Enabled** column to place a document flow definition offline. (When you select **Set Source** or **Set Target**, the record is automatically enabled.) Click **Disabled** to place it online.

   If a package is disabled, all lower-level document flow definitions in that same node are also disabled, regardless of whether their individual status was enabled. If a lower-level document flow definition is disabled, all higher-level definitions within the same context remain enabled. When a document flow definition is disabled, all preexisting connections and attributes continue to function. The disabled document flow definition only restricts the creation of new connections.
10. Optionally click the **Edit** icon if you want to edit any of the attributes of a protocol, package, document flow, action, activity, or signal. You then see the settings for the attributes (if any attributes exist). You can modify the attributes by entering a value or selecting a value from the **Update** column and then clicking **Save**.

Chapter 12. Managing connections

After you create the B2B capabilities of participants, you establish connections between the Community Manager and participants. This chapter covers the following topics:

- "Overview"
- "Activating participant connections"
- "Specifying or changing attributes" on page 144

Overview

You set up a connection between participants for each type of document that will be exchanged. For example, you might have multiple connections from the Community Manager to the same participant, because the packaging, protocol, document flow, action, or map might be different.

When you activate connections, you can specify attributes for the source or target participant. Any attributes you set at the connection level take precedence over attributes you set at the B2B capabilities level (for a particular participant) or at the document flow definition level.

For EDI, XML, and ROD documents, you have multiple connections for each exchange, if the exchange involves enveloping or transformation. You can further define connections for these types of documents by selecting from a set of profiles associated with the connection. See "Connection profiles" on page 101 for details.

Activating participant connections

Participant connections contain the information necessary for the proper exchange of each document flow. A document cannot be routed unless a connection exists between the Community Manager and one of its participants.

The system automatically creates connections between the Community Manager and participants based on their B2B capabilities.

You search for these connections and then activate them.

When selecting a Source and a Target, observe the following guidelines:

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

Use the following procedure to perform a basic search for connections and then activate the connections.

1. Click **Account Admin > Participant Connections**. The Manage Connections page is displayed.
2. Under **Source**, select a source. For example, if you are setting up an exchange that originates from the Community Manager, select the Community Manager.

© Copyright IBM Corp. 2004, 2005

3. Under **Target**, select a target. For example, if you are setting up an exchange that will be received by a participant, select that participant.

   Note: When you create a new connection, the Source and Target must be unique.
4. Click **Search** to find the connections that match your criteria.

   Note: You can also use the Advanced Search page if you want to enter more detailed search criteria.
5. To activate a connection, click **Activate**. The Manage Connections page is redisplayed, this time with the connection highlighted in green. This page shows the package, protocol, and document flow for the source and target. It also provides buttons you can click to view and change partner-connection status and parameters.
6. To specify attributes for the source or target or to select a connection profile, see "Specifying or changing attributes."

For a two-action PIP, activate the connection in both directions to support the second action of the PIP. To do this, the source and target of the second action are the opposite of the source and target of the first action.

For EDI, XML, or ROD documents for which you have defined more than one interaction, make sure you activate all the connections associated with the interactions.

Specifying or changing attributes

When you activate the connection, you can set attributes or modify attributes that were previously defined. To specify or change the attributes for this connection:

1. Click **Attributes** to view or change the attribute values.

   For example, suppose the Community Manager is sending a document packaged as None to a participant. The participant is going to receive the document packaged as AS. It is possible that the Community Manager has more than one Business ID assigned to it. To indicate to WebSphere Partner Gateway which ID to use:

   a. Click **Attributes** on the Source side of the connection.
   b. When the Connection Attributes page is displayed, expand the **None** folder.
   c. Select from the **Update** list the AS ID you want sent to the participant.
   d. Click **Save**.

   Note: If you previously specified an AS ID (in the B2B Capabilities page, for example), the value you enter here will override the earlier value.

   Another example of setting an attributes is to enter a value for the MDN address when you are receiving documents packaged as AS from a participant. The address specifies where the MDN is delivered.
2. Click **Actions** if you want to view or change an action or a transformation map associated with this connection. Any value you change here overrides any other values you have set for the action or map.
3. Click **Gateways** if you want to view or change the source or target gateway.
4. If the **Add Connection Profile** button and the **Active Profiles** list appears, you can associate this connection with a particular profile that you have previously defined.

The attributes that you set at the connection level take precedence over any attributes you set at the protocol or document flow level.

Chapter 13. Setting up security for inbound and outbound exchanges

With WebSphere Partner Gateway, you can install and use several types of certificates for inbound and outbound transactions. This chapter includes the following topics:

- "Security terms and concepts"
- "Creating and installing SSL certificates" on page 151
- "Creating and installing signature certificates" on page 157
- "Creating and installing encryption certificates" on page 159
- "Configuring inbound SSL for the Console and Receiver" on page 162
- "Certificate overview" on page 163

Security terms and concepts

This section provides a general overview of the types of security, the tools used to generate and upload certificates, and the types of data stores installed by WebSphere Partner Gateway.

Security mechanisms and protocols used in WebSphere Partner Gateway

This section provides information about SSL, digital signatures, and encryption.

SSL

WebSphere Partner Gateway can use SSL to secure inbound and outbound documents. An inbound document is one that is sent to the hub. An outbound document is one that is sent from the hub.

SSL is a commonly used protocol for managing security over the Internet. SSL provides secure connections by enabling two applications linked through a network connection to authenticate each other's identity and to ensure data confidentiality and data integrity.

A HTTP-based SSL connection is always initiated by the client using a URL starting with https:// instead of http://. An SSL connection begins with a handshake. During this stage, the applications exchange digital certificates, agree on the encryption algorithms to use, and generate encryption keys used for the remainder of the session.

Notes:

1. WebSphere Partner Gateway supports the RC2 and TripleDES algorithms. It does not support the RC5 algorithm. If you were using the RC5 algorithm in an earlier release, switch to one of the supported algorithms.
2. WebSphere Partner Gateway also supports the AES and DES algorithms. You can set these algorithms in the bcg.properties file or with the SecurityService API. Refer to the *Administrator Guide* for information about the bcg.properties file. Refer to the *Programmer Guide* for information about SecurityService.

The SSL protocol provides the following security features:

© Copyright IBM Corp. 2004, 2005

- Server authentication, which means that the server uses its digital certificate to authenticate itself to clients
- Client authentication, an optional step in which clients might be required to authenticate themselves to the server by providing their own digital certificates

Digital signature

Digital signing is the mechanism for ensuring non-repudiation. Non-repudiation means that a participant cannot deny having originated and sent a message. It also ensures that the participant cannot deny having received a message.

A digital signature allows an originator to sign a message so that the originator is verified as the person who actually sent the message. It also ensures that the message has not been modified since it was signed.

WebSphere Partner Gateway supports PKCS#7 SignedData detached digital signature formats as per the business protocols.

Encryption

WebSphere Partner Gateway uses a cryptographic system known as public key encryption to secure the communication between participants and the hub. Public key encryption uses a pair of mathematically related keys. A document encrypted with the first key must be decrypted with the second, and a document encrypted with the second key must be decrypted with the first.

Each participant in a public key system has a pair of keys. One of the keys is kept secret; this is the private key. The other key is distributed to anyone who wants it; this is the public key. WebSphere Partner Gateway uses a participant's public key to encrypt a document. The private key is used to decrypt a document.

The iKeyman utility

As described in the sections that follow, you use the IBM Key Management Tool (iKeyman) to create key databases, public and private key pairs, and certificate requests. You can also use iKeyman to create self-signed certificates. The iKeyman utility is included in the /*<ProductDir>*/was/bin directory, which WebSphere Partner Gateway creates during installation.

You can also use iKeyman to generate a request for a certificate to a Certifying Authority (CA).

Community Console

You use the Community Console to install all the required client, signature, and encryption certificates for WebSphere Partner Gateway storage. You can also use the Community Console to install Root and Intermediate CA (Certifying Authority) certificates.

Note: When a participant's certificate expires, it is the participant's responsibility to obtain a new certificate. The Community Console's Alert feature includes certificate expiration alerts for certificates stored in WebSphere Partner Gateway.

Key stores and trust stores

When you install WebSphere Partner Gateway, a key store and trust store for the Receiver and Console are installed.

- A key store is a file that contains your public and private keys.

- A trust store is a key database file that contains the public keys for your participants' self-signed and CA certificates. The public key is stored as a signer certificate. For commercial CA, the CA root certificate is added. The trust store file can be a more publicly accessible key database file that contains all the trusted certificates.

By default, the two key stores and two trust stores are created in the *<ProductDir>*`/common/security/keystore` directory. The names are:

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

Changing the default password

The default password for accessing all four stores is WebAS. The embedded WebSphere Application Server is configured to use these four stores. You can use the iKeyman utility to change the password. Alternatively, you can use the following UNIX command to change the password of the key store file:

```
/<ProductDir>/console/was/java/bin/keytool
 -storepasswd -new $NEW_PASSWORD$ -keystore $KEYSTORE_LOCATION$
 -storepass $CURRENT_PASSWORD$ -storetype JKS
```

If the key store passwords are changed, each WebSphere Application Server instance configuration must also be changed. This can be done using the `bcgChgPassword.jacl` script. For the Console instance, navigate to the following directory:

```
/<ProductDir>/bin
```

and issue the following command:

```
./bcgwsadmin.sh -f /<ProductDir>/scripts/
bcgChgPassword.jacl -conntype NONE
```

Repeat this command for the WebSphere Application Server instances of the Receiver and Document Manager.

Note: For Windows installations, use `bcgwsadmin.bat` instead of `./bcgwsadmin.sh`.

You will be prompted for the new password.

Replacing an expired certificate

If a certificate in a trust store has expired, you must add a new certificate to replace it by using the following procedure:

1. Start iKeyman, if it is not already running.
2. Open the trust store file.
3. Type the password and click **OK**.
4. Select **Signer Certificates** from the menu.
5. Click **Add**.
6. Click **Data type** and select a data type, such as Base64-encoded ASCII data.

   This data type must match the data type of the importing certificate.
7. Type a certificate file name and location for the CA root digital certificate or click **Browse** to select the name and location.
8. Click **OK**.
9. Type a label for the importing certificate.

10. Click **OK**.

Certificate chains

A certificate chain is made up of a participant's certificate and any certificates used to authenticate the participant's certificate. For example, if a CA was used to create the participant's certificate, that CA might itself have been certified by another CA. The chain of trust begins at the *root* CA (the trust anchor). The root CA's digital certificate is self-signed; that is, the certificate authority uses its own private key to sign the digital certificate. Any certificates between the trust anchor and the participant's certificate (the target certificate) are *intermediate* certificates.

For any CA-issued certificates, all certificates in the chain must be added. For example, in a certificate chain in which A (the trust anchor) is the issuer of B and B is the issuer of C (the target certificate), certificates A and B must be uploaded as CA certificates.

WebSphere Partner Gateway treats all self-signed certificates as trust anchors. The self-signed certificate can be of a certifying authority (CA), or it can be a self-signed certificate generated by the participant.

Primary and secondary certificates

You can create more than one certificate of a particular type and designate one as the primary certificate and one as the secondary certificate. If the primary certificate expires or is otherwise unable to be used, WebSphere Partner Gateway switches to the secondary certificate. You specify, on the Community Console, which certificate is primary and which is secondary.

The ability to provide primary and secondary certificates is available for the following certificates:

- Encryption certificate of a participant
- Signing certificate of the Hub Operator
- SSL Client certificate of the Hub Operator

Changing the encryption strength

Note the following important restrictions about the use of encryption certificates. The Java Runtime Environment (JRE) that ships with WebSphere Partner Gateway enforces restrictions regarding the cryptographic algorithms and maximum cryptographic strengths available for use. For example, restricted policy specifies limits on the allowable length, and, as a result, strength of encryption keys. These restrictions are specified in files called *jurisdiction policy files*. The maximum allowable length is 2048 bytes. If you want to support certificates with a key size greater than 2048 bytes, use the unrestricted or unlimited strength version of the jurisdiction policy files. You can specify that you want to use stronger, unrestricted policy by installing new policy files to a subdirectory of the installed JRE. There are also encryption restrictions on the symmetric key algorithms, such as DES3. If you need a strong symmetric key algorithm, replacing the jurisdiction policy files will also remove the restrictions for the symmetric keys.

To install unlimited jurisdiction policy files in WebSphere Partner Gateway, perform the following steps:

1. Download the unlimited jurisdiction strength policy files from the **IBM SDK Policy files** link at the following Web site: http://www.ibm.com/developerworks/java/jdk/security/142/.

2. Unzip the downloaded file to a temporary folder
3. Copy local_policy.jar and US_export_policy.jar from the temporary folder.
4. Change to the folder <*ProductDir*>\was\java\jre\lib\security.
5. Rename the existing local_policy.jar and US_export_policy.jar to local_policy.jar.bak and US_export_policy.jar.bak
6. Paste the jar files copied in step 3 to the folder <*ProductDir*>\was\java\jre\lib\security.
7. Restart the server.

These steps apply to all the WebSphere Application Server instances configured.

Creating and installing SSL certificates

The following sections describe how to create and install SSL certificates for use with WebSphere Partner Gateway. Also included is an overview of the SSL handshake process. If your community is not using SSL, neither you nor your participants need an inbound or outbound SSL certificate.

SSL handshake

Each SSL session begins with a handshake.

When a client (the participant or Community Manager) initiates a message exchange, the following steps occur:

1. The client sends a client ″hello″ message that lists the cryptographic capabilities of the client (sorted in client preference order), such as the version of SSL, the cipher suites supported by the client, and the data compression methods supported by the client. The message also contains a 28-byte random number.
2. The server responds with a server ″hello done″ message that contains the cryptographic method (cipher suite) and the data compression method selected by the server, the session ID, and another random number.

   Note: The client and the server must support at least one common cipher suite, or else the handshake fails. The server generally chooses the strongest common cipher suite.
3. The server sends its digital certificate.

   Server authentication happens at this step.
4. The server sends a ″digital certificate request″ message. In the ″digital certificate request″ message, the server sends a list of the types of digital certificates supported and the distinguished names of acceptable certificate authorities.
5. The server sends a server ″hello done″ message and waits for a client response.
6. Upon receipt of the server ″hello done″ message, the client verifies the validity of the server's digital certificate and checks that the server's ″hello″ parameters are acceptable.
7. If the server requested a client digital certificate, the client sends a digital certificate, or if no suitable digital certificate is available, the client sends a ″no digital certificate″ alert. This alert is only a warning, but the server application can fail the session if client authentication is mandatory.
8. The client sends a ″client key exchange″ message. This message contains the premaster secret, a 46-byte random number used in the generation of the

symmetric encryption keys and the message authentication code (MAC) keys, encrypted with the public key of the server.

9. If the client sent a digital certificate to the server, the client sends a ″digital certificate verify″ message signed with the client's private key. By verifying the signature of this message, the server can explicitly verify the ownership of the client digital certificate.

   Note: An additional process to verify the server digital certificate is not necessary. If the server does not have the private key that belongs to the digital certificate, it cannot decrypt the premaster secret and create the correct keys for the symmetric encryption algorithm, and the handshake fails.
10. The client uses a series of cryptographic operations to convert the premaster secret into a master secret, from which all key material required for encryption and message authentication is derived. Then the client sends a ″change cipher spec″ message to make the server switch to the newly negotiated cipher suite. The next message sent by the client (the ″finished″ message) is the first message encrypted with this cipher method and keys.
11. The server responds with a ″change cipher spec″ and a ″finished″ message of its own.

Client authentication requires steps 4 on page 151, 7 on page 151, and 9.

The SSL handshake ends, and encrypted application data can be sent.

Inbound SSL certificates

This section describes how to configure server authentication and client authentication for inbound connection requests from participants.

Server authentication

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

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

Using a self-signed certificate: If you are going to use self-signed server certificates, use the following procedure.

1. Start the iKeyman utility, which is located in /<*ProductDir*>/was/bin. If this is your first time using iKeyman, delete the "dummy" certificate that resides in the key store.
2. Use iKeyman to generate a self-signed certificate and a key pair for the Receiver or Console key store.
3. Use iKeyman to extract to a file the certificate that will contain your public key.

   Save the key store to a JKS, PKCS12, or JCEK file.
4. Install the file into the Receiver or Console key store for which it was created.

5. Distribute the certificate to your participants. The preferred method for distribution is to send the certificate in a zipped file that is password-protected, by e-mail. Your participants must call you and request the password for the zipped file.

Using a CA-generated certificate: If you are going to use a certificate signed by a CA, use the following procedure.

1. Start the iKeyman utility, which is located in the /*<ProductDir>*/was/bin directory.
2. Use iKeyman to generate a certificate request and a key pair for the Receiver.
3. Submit a Certificate Signing Request (CSR) to a CA.
4. When you receive the signed certificate from the CA, use iKeyman to place the signed certificate into the key store.
5. Distribute the CA certificate to all participants.

Client authentication

If you want to authenticate participants who send documents, perform the steps in this section.

Installing the client certificate: For client authentication, use the following procedure:

1. Obtain your participant's certificate.
2. Install the certificate or certificates into the trust store using iKeyman.
3. Place the related CA or CAs in the related key store.

Note: When you add more participants to your hub community, you can use iKeyman to add their certificates to the trust store. If a participant leaves the community, you can use iKeyman to remove the participant's certificates from the trust store.

Setting up client authentication: After installing the certificate or certificates, configure WebSphere Application Server to use client authentication by running the utility script bcgClientAuth.jacl.

1. Navigate to the following directory: /*<ProductDir>*/bin
2. To turn on client authentication, call the script as follows:

   ```
   ./bcgwsadmin.sh -f /<ProductDir>/scripts/bcgClientAuth.jacl
      -conntype NONE set
   ```

   Note: To turn off client authentication, call the script as follows:

   ```
   ./bcgwsadmin.sh -f /<ProductDir>/receiver/scripts/bcgClientAuth.jacl
     -conntype NONE clear
   ```

You must restart the bcgreceiver server for these changes to take effect.

Validating the client's certificate: There is an additional feature that can be used with SSL client authentication. This feature is enabled through the Community Console. For HTTPS, WebSphere Partner Gateway checks certificates against the Business IDs in the inbound documents. To use this feature, create the participant's profile, import the client certificate, and flag it as SSL.

1. Import the client certificate.
   a. Click **Account Admin > Profiles > Community Participant**, and search for the participant's profile.
   b. Click **Certificates**.

c. Click **Load Certificate**.
d. Select **SSL Client** as the type of certificate.
e. Type a description of the certificate (which is required).
f. Change the status to **Enabled**.
g. Click **Browse** and navigate to the directory in which you have saved the certificate.
h. Select the certificate and click **Open**.
i. If you want to select a gateway type other than **Production** (the default), select it from the list.
j. Click **Upload** and then click **Save**.

2. Update the client gateway.
   a. Click **Account Admin > Profiles > Community Participant**, and search for the participant's profile.
   b. Click **Gateways**.
   c. Select the HTTPS gateway you previously created. If you have not yet created the HTTPS gateway, see "Setting up an HTTPS gateway" on page 127.
   d. Click the **Edit** icon to edit the gateway.
   e. Select **Yes** for **Validate SSL Client Certificate**.
   f. Click **Save**.

Outbound SSL certificate

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

Server authentication

When SSL is being used to send outbound documents to your participants, WebSphere Partner Gateway requests a server-side certificate from the participants. The same CA certificate can be used for multiple participants. The certificate must be in X.509 DER format.

Note: You can convert the format with the iKeyman utility. Follow these steps to use iKeyman to convert the format:

1. Start iKeyman.
2. Create a new blank key store or open an existing key store.
3. In the Key Database Content, select **Signer Certificates**.
4. Add the ARM certificate using the **Add** option.
5. Extract the same certificate as a Binary DER data using the **Extract** option.
6. Close iKeyman.

Install the participant's self-signed certificate into the Hub Operator profile. If the certificate was signed by a CA and the CA root certificate and any other certificates that are part of the certificate chain are not already installed in the Hub Operator profile, install the certificates in the Hub Operator profile.

1. Click **Certificates**.
2. Click **Load Certificates**.
3. Select **Root and Intermediate** as the type of certificate.
4. Type a description of the certificate (which is required).
5. Change the status to **Enabled**.

6. Click **Browse** and navigate to the directory in which you have saved the certificate.
7. Select the certificate and click **Open**.
8. Click **Upload** and then click **Save**.

Note: You do not have to perform the previous steps if the CA certificate is already installed.

Client authentication

If SSL client authentication is required, the participant will, in turn, request a certificate from the hub. Use the Community Console to import your certificate into WebSphere Partner Gateway. You can generate the certificate using iKeyman. If the certificate is a self-signed certificate, it must be provided to the participant. If it is a CA-signed certificate, the CA root certificate must be given to the participants, so that they can add it to their trusted certificates.

You can have more than one SSL certificate. One is the primary certificate, which is the one used by default. The other is a secondary certificate, which is used if the primary certificate expires or is otherwise unable to be used.

Using a self-signed certificate: If you are going to use a self-signed certificate, use the following procedure.

1. Start the iKeyman utility.
2. Use iKeyman to generate a self-signed certificate and a key pair.
3. Use iKeyman to extract to a file the certificate that will contain your public key.
4. Distribute the certificate to your participants. The preferred method for distribution is to send the certificate in a zipped file that is password-protected, by e-mail. Your participants must call you and request the password for the zipped file.
5. Use iKeyman to export the self-signed certificate and private key pair in the form of a PKCS12 file.
6. Install the self-signed certificate and key through the Community Console.
   a. Click **Account Admin > Profiles > Certificates** to display the Certificate List page.

      Make sure you are logged in to the Community Console as the Hub Operator.
   b. Click **Load PKCS12**.

      Note: The PKCS12 file being uploaded should contain only one private key and the associated certificate.
   c. Select **SSL Client** as the type of certificate.
   d. Type a description of the certificate (which is required).
   e. Change the status to **Enabled**.
   f. Click **Browse** and navigate to the directory in which you have saved the certificate.
   g. Select the certificate and click **Open**.
   h. Enter the password.
   i. If you want to select a gateway type other than **Production** (the default), select it from the list.

j. If you have two SSL certificates, indicate whether this is the primary or secondary certificate by selecting **Primary** or **Secondary** from the **Certificate Usage** list.
k. Click **Upload** and then click **Save**.

If you are uploading primary and secondary certificates for both SSL client authentication and digital signature and you are uploading the primary certificates as two separate entries, make sure that the corresponding secondary certificates are uploaded as two different entries.

Using a CA-signed certificate: If you are going to use a certificate signed by a CA, use the following procedure:

1. Use iKeyman to generate a certificate request and a key pair for the Receiver.
2. Submit a Certificate Signing Request (CSR) to a CA.
3. When you receive the signed certificate from the CA, use iKeyman to place the signed certificate into the key store.
4. Distribute the signing CA certificate to all participants.

Adding a Certificate Revocation List (CRL)

WebSphere Partner Gateway includes a Certificate Revocation List (CRL) feature. The CRL, issued by a Certificate Authority (CA), identifies participants who have revoked certificates before their scheduled expiration date. Participants with revoked certificates will be denied access to WebSphere Partner Gateway.

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

CRLs are stored in the following location: /<*shared_data_directory*>/security/crl. WebSphere Partner Gateway uses the setting bcg.CRLDir in the bcg.properties file to identify the location of the CRL directory.

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

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

```
bcg.CRLDir=/<shared_data_directory>/security/crl
```

Enabling access to CRL distribution points

CAs maintain and update the CRLs. These CRLs are typically stored in a CRL distribution point. CRLs are used while doing revocation checks for the certificates to determine whether the certificate is revoked.

The bcgSetCRLDP.jacl script can be used to enable or disable CRL distribution point checking when the revocation check is performed. If you need the CRL distribution points to be accessed when revocation checking of a certificate is performed, enable the use of CRL distribution points. If the certificates you have installed contain a CRL DP extension, you can enable the use of CRL distribution points so that the distribution points are accessed when the revocation check is performed. If you have downloaded all the required CRLs in the directory set in bcg.properties for the property bcg.CRLDir, you might not want to enable the use of CRL distribution points. If the current CRLs are not likely to be available in the bcg.CRLDir directory, you should enable the use of CRL distribution points.

The CRL distribution points accessible via HTTP and LDAP are supported. You can also configure proxies to access the CRL distribution points.

Note: For Windows installations, use `bcgwsadmin.bat` instead of `./bcgwsadmin.sh` in the commands listed in this section.

To enable the use of CRL distribution points, run the following command from the <*ProductDir*>/bin directory:

```
./bcgwsadmin.sh -f <ProductDir>/scripts/bcgSetCRLDP.jacl install
 <nodename> <serverName> CRLDP
```

where:

<*server_root***>**
: The root directory of the server (for example, `/opt/ibm/receiver/was/profiles/bcgreceiver`)

<*serverName***>**
: Can be `bcgdocmgr`, `bcgreceiver`, or `bcgconsole`. The command needs to be run from the corresponding <*server_root*>.

To disable the use of CRL distribution points, run the following command from the <*ProductDir*>/bin directory:

```
./bcgwsadmin.sh -f <ProductDir>/scripts/bcgSetCRLDP.jacl uninstall
<nodename> <serverName> CRLDP
```

To enable the use of CRL distribution points with a proxy, run the following command from the <*ProductDir*>/bin directory:

```
./bcgwsadmin.sh -f <ProductDir>/scripts/bcgSetCRLDP.jacl install
 <nodename> <serverName> CRLDP <proxyHost> <proxyPort>
```

To specify that you do not want to use a proxy, run the following command from the <*ProductDir*>/bin directory:

```
./bcgwsadmin.sh -f <ProductDir>/scripts/bcgSetCRLDP.jacl
 uninstall <nodename> <serverName> PROXY
```

If you are using a Receiver user exit and if the user exit uses the SecurityService API, the above settings are applicable for the bcgreceiver server also. To run the above commands for the Receiver, replace `bcgdocmgr` with `bcgreceiver`.

Creating and installing signature certificates

This section describes signature certificates, which are used for non-repudiation and for verifying the signer.

Inbound signature certificate

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

To install the certificate, use the following procedure.

1. Receive the participant's X.509 signature certificate in DER format.
2. Install the certificate through the Community Console under the participant's profile.

a. Click **Account Admin > Profiles > Community Participant**, and search for the participant's profile.
b. Click **Certificates**.
c. Click **Load Certificates**.
d. Select **Digital Signature** as the type of certificate.
e. Type a description of the certificate (which is required).
f. Change the status to **Enabled**.
g. Click **Browse** and navigate to the directory in which you have saved the certificate.
h. Select the certificate and click **Open**.
i. Click **Upload** and then click **Save**.

3. If the certificate was signed by a CA and the CA root certificate and any other certificates that are part of the certificate chain are not already installed in the Hub Operator profile, install the certificates now.
   a. Click **Account Admin > Profiles > Certificates** to display the Certificate List page.

      Make sure you are logged in to the Community Console as the Hub Operator, and install the certificate in your own profile.
   b. Click **Load Certificate**.
   c. Select **Root and Intermediate**.
   d. Type a description of the certificate (which is required).
   e. Change the status to **Enabled**.
   f. Click **Browse** and navigate to the directory in which you have saved the certificate.
   g. Select the certificate and click **Open**.
   h. Click **Upload** and then click **Save**.

   Note: You do not have to perform the previous step if the CA certificate is already installed.
4. Enable signing at the package (highest level), participant, or connection level (lowest level). Your setting can override other settings at the connection level. The connection summary will inform you if any required attribute is missing.

   For example, to alter the attributes of a participant connection, click **Account Admin > Participant Connections** and then select the participants. Click **Attributes** and then edit the attribute (for example, **AS Signed**).

Outbound signature certificate

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

You can have more than one digital signature certificate. One is the primary certificate, which is the one used by default. The other is a secondary certificate, which is used if the primary certificate expires or is otherwise unable to be used.

Using a self-signed certificate

If you are going to use a self-signed certificate, use the following procedure.

1. Start the iKeyman utility.
2. Use iKeyman to generate a self-signed certificate and a key pair.
3. Use iKeyman to extract to a file the certificate that will contain your public key.

4. Distribute the certificate to your participants. The preferred method for distribution is to send the certificate in a zipped file that is password protected, by e-mail. Your participants must call you and request the password for the zipped file.
5. Use iKeyman to export the self-signed certificate and private key pair in the form of a PKCS12 file.
6. Install the self-signed certificate and private key pair in the form of a PKCS12 file through the Community Console.
   a. Click **Account Admin > Profiles > Certificates** to display the Certificate List page.

      Make sure you are logged in to the Community Console as the Hub Operator.
   b. Click **Load PKCS12**.

      Notes:
      1) The PKCS12 file being uploaded should contain only one private key and the associated certificate.
      2) You can also upload the certificate and private key as a DER-encoded certificate and PKCS#8-encoded private key.
   c. Select **Digital Signature** as the type of certificate.
   d. Type a description of the certificate (which is required).
   e. Change the status to **Enabled**.
   f. Click **Browse** and navigate to the directory in which you have saved the certificate.
   g. Select the certificate and click **Open**.
   h. Enter a password.
   i. If you have two digital signature certificates, indicate whether this is the primary or secondary certificate by selecting **Primary** or **Secondary** from the **Certificate Usage** list.
   j. Click **Upload** and then click **Save**.
7. Repeat step 6 if the participant has a second signature certificate.

If you are uploading primary and secondary certificates for both SSL client authentication and digital signature and you are uploading the primary certificates as two separate entries, make sure that the corresponding secondary certificates are uploaded as two different entries.

Using a CA-signed certificate

If you are going to use a certificate signed by a CA, use the following procedure:
1. Start the iKeyman utility.
2. Use iKeyman to generate a certificate request and a key pair for the Receiver.
3. Submit a Certificate Signing Request (CSR) to a CA.
4. When you receive the signed certificate from the CA, use iKeyman to place the signed certificate into the key store.
5. Distribute the signing CA certificate to all participants.

Creating and installing encryption certificates

This section describes encryption certificates.

Inbound encryption certificate

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

Note the following important restriction about receiving encrypted AS2 messages from participants. If a participant sends an encrypted AS2 message but uses the wrong certificate, the decryption fails. No MDN is returned to the participant to indicate the failure, however. In order for your participant to receive MDNs in this situation, create a connection to the participant with the following document flow definition:

- Package: **AS**
- Protocol: **Binary**
- Document Flow: **Binary**

Using a self-signed certificate

If you are going to use a self-signed certificate, use the following procedure.

1. Start the iKeyman utility.
2. Use iKeyman to generate a self-signed certificate and a key pair.
3. Use iKeyman to extract to a file the certificate that will contain your public key.
4. Distribute the certificate to your participants. They are required to import the file into their B2B product for use as an encryption certificate. Advise them to use it when they want to send encrypted files to the Community Manager. If your certificate is CA-signed, provide the CA certificate as well.
5. Use iKeyman to save the self-signed certificate and private key pair in the form of a PKCS12 file.
6. Install the self-signed certificate and private key pair in the form of a PKCS12 file through the Community Console.
   a. Click **Account Admin > Profiles > Certificates** to display the Certificate List page.

      Make sure you are logged in to the Community Console as the Hub Operator.

   b. Click **Load PKCS12**.

      Notes:

      1) The PKCS12 file being uploaded should contain only one private key and the associated certificate.
      2) You can also upload the certificate and private key as a DER-encoded certificate and PKCS#8-encoded private key.

   c. Select **Encryption** as the type of certificate.
   d. Type a description of the certificate (which is required).
   e. Change the status to **Enabled**.
   f. Click **Browse** and navigate to the directory in which you have saved the certificate.
   g. Select the certificate and click **Open**.
   h. Enter a password.
   i. Click **Upload** and then click **Save**.

7. Enable encryption at the package (highest level), participant, or connection level (lowest level). Your setting can override other settings at the connection level. The connection summary will inform you if any required attribute is missing.

   For example, to alter the attributes of a participant connection, click **Account Admin > Participant Connections** and then select the participants. Click **Attributes** and then edit the attribute (for example, **AS Encrypted**).

Using a CA-signed certificate

If you are going to use a certificate signed by a CA, use the following procedure:

1. Start the iKeyman utility.
2. Use iKeyman to generate a certificate request and a key pair for the Receiver.
3. Submit a Certificate Signing Request (CSR) to a CA.
4. When you receive the signed certificate from the CA, use iKeyman to place the signed certificate into the key store.
5. Distribute the signing CA certificate to all participants.

Outbound encryption certificate

The outbound encryption certificate is used when the hub sends encrypted documents to participants. WebSphere Partner Gateway encrypts documents with the public keys of the participants, and the participants decrypt the documents with their private keys.

The participant can have more than one encryption certificate. One is the primary certificate, which is the one used by default. The other is a secondary certificate, which is used if the primary certificate expires or is otherwise unable to be used.

1. Obtain the participant's encryption certificate. The certificate must be in X.509 DER format. Note that WebSphere Partner Gateway supports only X5.09 certificates.
2. Install the certificate through the Community Console under the participant's profile.
   a. Click **Account Admin > Profiles > Community Participant**, and search for the participant's profile.
   b. Click **Certificates**.
   c. Click **Load Certificate**.
   d. Select **Encryption** as the type of certificate.
   e. Type a description of the certificate (which is required).
   f. Change the status to **Enabled**.
   g. Click **Browse** and navigate to the directory in which you have saved the certificate.
   h. Select the certificate and click **Open**.
   i. If the participant has two encryption certificates, indicate whether this is the primary or secondary certificate by selecting **Primary** or **Secondary** from the **Certificate Usage** list.
   j. Click **Upload** and then click **Save**.
3. Repeat step 2 if the participant has a second encryption certificate.
4. If the certificate was signed by a CA and the CA root certificate and any other certificates that are part of the certificate chain are not already installed in the Hub Operator profile, install the certificates now.

a. Click **Account Admin > Profiles > Certificates** to display the Certificate List page.

   Make sure you are logged in to the Community Console as the Hub Operator, and install the certificate in your own profile.

b. Click **Load Certificate**.

c. Select **Root and Intermediate**.

d. Type a description of the certificate (which is required).

e. Change the status to **Enabled**.

f. Click **Browse** and navigate to the directory in which you have saved the certificate.

g. Select the certificate and click **Open**.

h. Click **Upload** and then click **Save**.

Note: You do not have to perform the previous step if the CA certificate is already installed.

5. Enable encryption at the package (highest level), participant, or connection level (lowest level). Your setting can override other settings at the connection level. The connection summary will inform you if any required attribute is missing.

   For example, to alter the attributes of a participant connection, click **Account Admin > Participant Connections** and then select the participants. Click **Attributes** and then edit the attribute (for example, **AS Encrypted**).

When the error message `No valid encryption certificate found` 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, the corresponding event (`Certificate revoked or expired`) in also visible in the Event Viewer. Note that these two events might be separated by other events. To display the Event Viewer, click **Viewers > Event Viewer**.

Configuring inbound SSL for the Console and Receiver

The WebSphere Partner Gateway key stores are preconfigured in WebSphere Application Server. This section applies only if you are using different key stores.

To configure SSL for the Console and Receiver in WebSphere Partner Gateway, use the following procedure.

1. Obtain the following information:
   - The full path names of the key file and the trust file; for example for the Receiver: <*ProductDir*>/common/security/keystore/receiver.jks and <*ProductDir*>/common/security/keystore/receiverTrust.jks

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

```
./bcgwsadmin.sh -f /<ProductDir>/
scripts/bcgssl.jacl -conntype NONE install
<keyFile_pathname>
<keyFile_password> <keyFile_format> <trustFile_pathname>
<trustFile_password> <trustFile_format>
```

4. Start the server. If the server fails to start, it might be because of an error when running bcgssl.jacl. If you make a mistake, you can rerun the script to correct it.
5. If you used bcgClientAuth.jacl to set the clientAuthentication SSL property, reset it after using bcgssl.jacl. This is because bcgssl.jacl overwrites any values that might have been set for client authentication with the value false.

Note: Repeat these steps for the Console, substituting **console** for **receiver** in the path name.

Certificate overview

Table 18 summarizes the way certificates are used in WebSphere Partner Gateway. Certificate locations are shown in parenthesis “( )”.

Table 18. Certificate summary information

Message delivery method (See note 1)	Hub operator certificate	Obtain certificate and CA from participant	CA (See note 2)	Give certificate to participant (See note 3)	Comments
Inbound SSL	Install on WebSphere Application server-side SSL. (Place in the WebSphere Application Server key store.)	N/A	Only needed if client authentication is used. (Place the CA or self-signed certificate in the WebSphere Application Server trust store.)	Hub operator certificate if self-signed or the CA root certificate if it is CA-authenticated.	
Outbound SSL	If client authentication is being used. (WebSphere Partner Gateway)	Participant server-side certificate or CA root certificate if it is CA-authenticated.	WebSphere Partner Gateway	Hub Operator certificate if self-signed or public key if signed by a third party.	
Inbound Encryption	Private key (WebSphere Partner Gateway)	N/A	N/A	Hub Operator certificate	For decrypting the message
Inbound Signature	N/A	Certificate for validating the certificate used for the digital signature. (WebSphere Partner Gateway)	WebSphere Partner Gateway	N/A	For verification and nonrepudiation
Outbound Encryption	N/A	Use the certificate obtained from the participant. (Certificate is installed in the participant’s profile)	CA for client certificate if not self-signed	N/A	For encryption of outbound messages

Table 18. Certificate summary information (continued)

Message delivery method (See note 1)	Hub operator certificate	Obtain certificate and CA from participant	CA (See note 2)	Give certificate to participant (See note 3)	Comments
Outbound Signature	Private key (WebSphere Partner Gateway)	N/A	N/A	Optional, depending on partner; give WebSphere Partner Gateway public key	
Certificate to DUNS validation	N/A	Load in participant profile	Load the same certificate (as the one in the column to the left) in the Hub Operator profile as the CA certificate		Validates that this certificate is for this DUNS ID when the SSL check is done

Notes:

1. An inbound message is one coming into WebSphere Partner Gateway from a participant. An outbound message is one going out of WebSphere Partner Gateway to a participant.
2. If the certificate is CA-issued, the issuing CA certificate must be obtained and stored. This applies to either the Hub Operator certificate or the participant's certificate.
3. If a private key is involved, this certificate corresponds to the private key.

Chapter 14. Finishing the configuration

This chapter describes additional tasks you can perform to configure the hub. It includes the following topics:

- "Enabling the use of APIs"
- "Specifying the queues used for events"
- "Specifying alertable events" on page 166
- "Updating a user-defined transport" on page 167

Enabling the use of APIs

WebSphere Partner Gateway supplies a set of APIs that can be used to access certain functions typically performed on the Community Console. These APIs are described in the *Programmer Guide*.

Use this procedure to enable the use of the XML-based APIs so that participants can make API calls to the WebSphere Partner Gateway server.

1. From the main menu, click **System Administration > Feature Administration > Administration API**.
2. Click the **Edit** icon next to **Enable the XML-Based API**.
3. Select the check box to enable the use of the XML-based API.
4. Click **Save**.

Specifying the queues used for events

You can configure the hub to deliver events to an external queue that is configured using JMS configuration.

The default JMS configuration is established when you install the hub. You can see some of these values on the Event Publishing Properties page. If you do not provide a value in the **Provider URL Packages** or the **JMS Provider URL** fields, the defaults that are in the MQ Properties section of the bcg.properties file are used. These defaults use the JMS bindings that were generated at installation time. If you took the defaults, the JMS bindings use port 9999 on the MQ Server that you named during installation.

To point to a different set of JMS bindings, change the **Provider URL Packages** to point to a directory containing a JMS bindings file that you have prepared yourself. Also change the **Queue Connection Factory** name and the **Queue name** to match the names you chose in your JMS bindings. You would do this if you want to publish the events to a queue on a different MQ server than the one you specified during installation.

To indicate where events should be delivered:

1. From the main menu, click **System Administration > Event Processing > Event Delivery Information**.
2. Click the **Edit** icon next to **Enable Event Delivery**.
3. Select the **Enable Event Delivery** check box to activate event publishing.

© Copyright IBM Corp. 2004, 2005

4. If the default values are correct for your installation, leave them as is. The default values support event delivery to the queue named DeliveryQ provided by the JMS Server that you configured at installation.

   If you want to change where events are delivered, update the fields, using the following information as reference:

   - Enter values for **User ID** and **Password**, if a user ID and password are required to access the queue
   - For **JMS Queue Factory Name**, enter the name of the JMS Queue Connection Factory from the JMS .bindings file that you are using.

     Note: On some Windows versions (prior to XP), you might need to change the default value of the **JMS Queue Factory Name** field if you want to use the default Event Delivery feature. You will need to change the value for **JMS Queue Factory Name** from: `WBIC/QCF` to `WBIC\\QCF`.
   - For **JMS Message Type**, enter the type of message that will be delivered. The choices are byte or text.
   - For **JMS Queue Name**, enter the name of the JMS queue to which the events will be published. This queue must already be defined in the JMS .bindings file that you are using in WebSphere MQ.

     Note: On some Windows versions (prior to XP), you might need to change the default value of the **JMS Queue Name** field if you want to use the default Event Delivery feature. You will need to change the value for **JMS Queue Name** from `WBIC/DeliveryQ` to `WBIC\\DeliveryQ. WBIC/QCF`.
   - For **JNDI Factory Name**, enter the name used to access the .bindings file. The default value provides access to the default binding in the file system.
   - For **Provider URL Packages**, enter a URL that provides access to the JMS bindings file. This URL must be consistent with the JNDI Factory Name. This field is optional and, when not filled in, it uses the default file system location for JMS bindings.
   - For **Message Char Set**, enter the character set to be used when creating the byte message on the JMS queue. The default value is UTF-8. This field is relevant only for byte messages.
   - For **JMS Provider URL**, enter the URL of the JMS provider. This field is optional and when not filled in, it uses the default JMS provider that was identified at installation.
5. Click **Save**.

Specifying alertable events

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

To indicate which events should be alertable:

1. Click **Hub Admin > Hub Configuration > Event Codes**.

   The Event Codes page is displayed.
2. For each event you want made alertable:
   a. Click the **View details** icon next to the event code. The Event Code Details page is displayed.
   b. Select **Alertable**.

c. Click **Save**.

Updating a user-defined transport

As described in Chapter 5, “Defining targets” and Chapter 10, “Creating gateways,” on page 123, you can upload an XML file that describes a user-defined transport. You use **Manage Transport Types** to upload the file. After you upload the XML file, the transport becomes available for use when defining a target or gateway.

The XML file that describes the user-defined transport includes the attributes for the transport. These attributes are displayed (in the section **Custom Transport Attributes**) on the target or gateway page when you specify a user-defined transport. For example, a user-defined transport for a gateway might include the attribute GatewayRetryCount.

The person who wrote the XML file describing the transport can update the attributes (by adding, deleting, or modifying the attributes).If the XML file is modified, you again use **Manage Transport Types** to upload the file. Any changes to the attributes are reflected in the gateway or target page.

Appendix A. Basic examples

This appendix provides examples of configuring the hub. It includes the following topics:

- "Basic Configuration – Exchanging passthrough EDI documents"
- "Basic configuration - Setting up security for inbound and outbound documents" on page 174
- "Extending the basic configuration" on page 180

A separate appendix is provided for examples of exchanging EDI interchanges that including de-enveloping, transformation, enveloping, and functional acknowledgment transmission. See Appendix B, "EDI examples," on page 185.

These examples are intended to provide you with a quick overview of the steps required to configure a system. If you are using these examples to set up your system, modify the specific information (for example, names and business IDs) to suit the needs of your business.

Basic Configuration – Exchanging passthrough EDI documents

In this example, the hub configuration is quite simple—two targets are defined (one for documents coming into the hub from a participant and one for documents coming into the hub from the Community Manager back-end system). The exchanges that are set up in this example use the document flow definitions provided by WebSphere Partner Gateway; therefore, you only have to create interactions based on those flows. No custom XML is used in this example.

This example shows an exchange between a back-end-application of the Community Manager and a community participant (Partner Two).

Configuring the hub

The first step in setting up the hub is creating the two targets.

- An HTTP Target (called "HttpTarget") to receive documents over HTTP (from Partner Two) that are to be sent to the back-end system of the Community Manager
- A File Directory Target (called "FileSystemTarget") to retrieve documents from the file system (from the Community Manager's back-end system) that are to be sent to Partner Two)

Defining the targets

To create a target for the receipt of documents over HTTP:

1. Click **Hub Admin > Hub Configuration > Targets**.
2. Click **Create Target**.
3. For Target Name, type: **HttpTarget**.
4. From the Transport list, select **HTTP/S**.
5. For the Gateway type, use the default of **Production**.
6. For the URI, type: **/bcgreceiver/submit**
7. Click **Save**.

© Copyright IBM Corp. 2004, 2005

Next, you create a target to poll a directory on the file system. Creating the target automatically creates a new directory on the file system.

To create the file-system target:

1. Click **Hub Admin > Hub Configuration > Targets**.
2. Click **Create Target**.
3. For Target Name, type: **FileSystemTarget**.
4. From the Transport list, select **File Directory**.
5. For Default Gateway Type, use the default of **Production**.
6. For the Document Root Path, type: **\temp\FileSystemTarget**

   Note: This will create a FileSystemTarget directory within the temp directory. Be sure a temp directory exists on the file system.
7. Click **Save**.

Defining document flows and interactions

In this example, you are setting up the exchange of documents that conform to the EDI-X12 standard. In this example, the documents are simply being passed through the hub. The EDI interchange is not being de-enveloped and no transformation occurs. See Appendix B, "EDI examples," on page 185 for examples of de-enveloping an interchange, transforming the transactions, and sending acknowledgments.

In this section, the following exchanges are described:

- Sending an EDI-X12 document, with no packaging, from the Community Manager to Partner Two
- Sending an EDI-X12 document, packaged in AS2, from Partner Two to the Community Manager

Because of the packaging and protocols involved, there is no need to create a new document flow definition. The packages, protocols, and document flows are ones that are predefined in the system.

However, you do need to define interactions based on these predefined document flows.

Create the first interaction, in which the source is an ISA-formatted document that conforms to the EDI-X12 standard and contains no packaging and the target is an ISA-formatted document that conforms to the EDI-X12 standard with AS packaging.

1. Click **Hub Admin > Hub Configuration > Document Flow Definition**.
2. Click **Manage Interactions** and then **Create Interaction**.
3. From the **Source** column, expand:
   a. **Package: None**
   b. **Protocol: EDI-X12**
4. Click **Document Flow: ISA**
5. From the **Target** column, expand:
   a. **Package: AS**
   b. **Protocol: EDI-X12**
6. Click **Document Flow: ISA**
7. From the **Action** list, select **Pass Through**.

8. Click **Save**.

Create a second interaction, in which the source format is an ISA-formatted document that conforms to the EDI-X12 standard with AS packaging, and the target format is an ISA-formatted document that conforms to the EDI-X12 standard and contains no packaging:

1. Click **Create Interaction**.
2. From the **Source** column, expand:
   a. **Package: AS**
   b. **Protocol: EDI-X12**
3. Click **Document Flow: ISA**
4. From the **Target** column, expand:
   a. **Package: None**
   b. **Protocol: EDI-X12**
5. Click **Document Flow: ISA**
6. From the **Action** list, select **Pass Through**.
7. Click **Save**.

Creating participants and participant connections

In this example, one external participant is created, in addition to the Community Manager. The gateways for the participants include standard transports, and no configuration points are defined for the gateways.

Creating the participants

Create two new participants. To define the Community Manager:

1. Click **Account Admin** from the main menu. The Participant Search page is the default view.
2. Click **Create**.
3. For **Company Login Name**, type: **CommMan**.
4. For **Participant Display Name**, type: **Comm Man**.
5. For **Participant Type**, select **Community Manager**.
6. Click **New** under **Business ID**.
7. Leave **Type** as **DUNS** and enter an Identifier value of **123456789**.

   Note: Here and throughout this book, all DUNS numbers are meant to be examples only.
8. Click **New** under **Business ID**.
9. Select **Freeform** and enter an Identifier value of **12-3456789**
10. Click **Save**.

To define Partner Two:

1. Click **Account Admin > Profiles > Community Participant**.
2. Click **Create**.
3. For **Company Login Name**, type: **partnerTwo**
4. For **Participant Display Name**, type: **Partner Two**
5. For **Participant Type**, select **Community Participant.**
6. Click **New** under **Business ID**.
7. Leave **Type** as **DUNS** and enter **987654321** as the Identifier.

8. Click **New** under **Business ID**.
9. Select **Freeform** and enter an Identifier value of **98-7654321**
10. Click **Save**.

You have now defined both the Community Manager and Partner Two to the hub.

The next steps are to configure gateways for both the Community Manager and Partner Two.

Creating the gateways

Before creating a file-directory gateway for the Community Manager, you must create the directory structure used by this gateway. Create a new FileSystemGateway directory on the root drive. This directory will be used by the Community Manager to store files received from participants.

In the case of the Community Manager, the gateway represents the entrance point into the back-end system.

To create a gateway for the Community Manager:

1. Click **Account Admin > Profiles > Community Participant**.
2. Click **Search**.
3. Select **Comm Man** by clicking the **View details** icon.
4. Click **Gateways** from the horizontal navigation bar.
5. Click **Create**.
6. For **Gateway Name**, type: **FileSystemGateway**
7. For **Transport**, select **File Directory**.
8. For **Address**, type: **file://C:\FileSystemGateway**
9. Click **Save**.

Next, set this newly created gateway as the default gateway for the Community Manager.

1. Click **List** to view all gateways configured for the Community Manager.
2. Click **View Default Gateways**.
3. From the **Production** list, select **FileSystemGateway**.
4. Click **Save**.

Create a gateway for Partner Two

1. Click **Account Admin > Profiles > Community Participant**.
2. Click **Search**, and then select **Partner Two** by clicking the **View details** icon.
3. Click **Gateways** from the horizontal navigation bar.
4. Click **Create**.
5. For **Gateway Name**, type: **HttpGateway**
6. For **Transport**, select **HTTP/1.1**.
7. For **Address**, type: **http://<*IP_address*>:80/input/AS2**, where <*IP_address*> represents Partner Two's computer.
8. For **User Name**, type: **Comm Man**.
9. For **Password**, type: **commMan**.
10. Click **Save**.

Note that this example assumes that Partner Two requires a user name and password for any participant logging in to its system.

Again, you need to define a default gateway for this participant.

1. Click **List** followed by **View Default Gateways**.
2. From the **Production** list, select **HttpGateway**.
3. Click **Save**.

Setting up B2B Capabilities

Next, define the B2B Capabilities for the Community Manager.

1. From the main menu, click **Account Admin > Profiles > Community Participant**.
2. Click **Search**.
3. Select **Comm Man** by clicking the **View details** icon.
4. Click **B2B Capabilities** from the horizontal navigation bar.
5. Set the Source and Target for Package: None, Protocol: EDI-X12, and Document Flow: ISA by performing the following steps:
   a. Click the **Role is not active** icon under **Set Source** for **Package: None**
   b. Click the **Role is not active** icon under **Set Target** for **Package: None**
   c. Click the **Expand** icon next to **Package: None**.
   d. Click the **Role is not active** icon for **Protocol: EDI-X12 (ALL)** for both source and target.
   e. Click the **Expand** icon next to **Protocol: EDI-X12 (ALL)**.
   f. Click the **Role is not active** icon for **Document Flow: ISA** for both source and target.

Then, set the B2B Capabilities for Partner Two.

1. From the main menu, click **Account Admin > Profiles > Community Participant**.
2. Click **Search**.
3. Select Partner Two by clicking the **View details** icon.
4. Click **B2B Capabilities** from the horizontal navigation bar.
5. Select Set Source and Set Target for Package: AS, Protocol: EDI-X12, and Document Flow: ISA by performing the following steps:
   a. Click the **Role is not active** icon under **Set Source** for **Package: AS**
   b. Click the **Role is not active** icon under **Set Target** for **Package: AS**
   c. Click the **Expand** icon next to **Package: AS**.
   d. Click the **Role is not active** icon for **Protocol: EDI-X12 (ALL)** for both source and target.
   e. Click the **Expand** icon next to **Protocol: EDI-X12 (ALL)**.
   f. Click the **Role is not active** icon for **Document Flow: ISA** for both source and target.

Defining participant connections

Define the participant connection for EDI documents with no packaging that come from the Community Manager to be delivered to Partner Two.

1. Click **Account Admin > Participant Connections**.
2. From the **Source** list, select **Comm Man**.
3. From the **Target** list, select **Partner Two**.

4. Click **Search**.
5. Click **Activate** for the connection with the following detail:
   a. **Source**
      1) Package: **None (N/A)**
      2) Protocol: **EDI-X12 (ALL)**
      3) Document Flow: **ISA(ALL)**
   b. **Target**
      1) Package: **AS (N/A)**
      2) Protocol: **EDI-X12 (ALL)**
      3) Document Flow: **ISA (ALL)**

Next, define the connection for EDI documents wrapped in AS2 packaging that come from Partner Two to be delivered to the Community Manager with no packaging. This is very similar to the connection you defined in the previous section, except that you will also configure AS2 attributes.

1. Click **Account Admin > Participant Connections**.
2. From the **Source** list, select **Partner Two**
3. From the **Target** list, select **Comm Man**.
4. Click **Search**.
5. Click **Activate** for the connection with the following detail:
   a. **Source**
      1) Package: **AS (N/A)**
      2) Protocol: **EDI-X12 (ALL)**
      3) Document Flow: **ISA (ALL)**
   b. **Target**
      1) Package: **None (N/A)**
      2) Protocol: **EDI-X12 (ALL)**
      3) Document Flow: **ISA (ALL)**

Next, select Attributes next to the **Package: AS (N/A)** box for Partner Two.

1. Edit the Package: AS (N\A) attributes by scrolling down the page and clicking the **Expand** icon next to **Package: AS (N/A)**.
2. Enter an AS MDN E-Mail Address (AS1) value. This can be any valid e-mail address.
3. Enter an AS MDN HTTP URL (AS2) value. This should be entered as follows: **http://<*IP_address*>:57080/bcgreceiver/submit,** where <*IP_Address*> represents the hub.
4. Click **Save**.

Basic configuration - Setting up security for inbound and outbound documents

In this section, you will see how to add the following types of security to the basic configuration:

- Secure Socket Layers (SSL) Server Authentication
- Encryption
- Digital Signatures

Setting up SSL authentication for incoming documents

In this section, you use iKeyman to set up server authentication so that Partner Two can send AS2 documents over HTTPS.

To set up server authentication, perform the following steps:

1. Initiate the iKeyman application, by opening the ikeyman.bat file from the /*<ProductDir>*/was/bin directory.
2. Open the Receiver's default key store, receiver.jks. From the menu bar, select **Key Database File Open**. On a default installation, receiver.jks resides in the directory: *<ProductDir>*/common/security/keystore
3. When prompted, enter the default password for receiver.jks. This password is WebAS.
4. If this is the first time you have opened receiver.jks, delete the "Dummy" certificate.

The next step is to create a new self-signed certificate. Creating a self-signed personal certificate creates a private key and public key within the server key store file.

To create a new self-signed certificate:

1. Click **New Self Signed**.
2. Give the certificate a key label that is used to uniquely identify the certificate within the key store. Use the label **selfSignedCert**.
3. Enter the server's Common Name. This is the primary, universal identity for the certificate. It should uniquely identify the principal that it represents.
4. Enter the name of your organization.
5. Accept all other defaults, and click **OK**.

Assume that Partner Two wants to send an EDI message over AS2 using secure HTTP. Partner Two will need to refer to the public certificate (which was created as part of the creation of the self-signed certificate) in order to do so.

To enable Partner Two to use the public certificate, export the public certificate from the server key store file as follows:

1. Select the newly created self-signed certificate from the IBM Key Management utility.
2. Click **Extract Certificate**.
3. Change the Data type to **Binary DER data**.
4. Provide the file name **commManPublic** and click **OK**.

Finally you use iKeyman to export the self-signed certificate and private key pair in the form of a PKCS12 file. This PCKS12 file will be used for encryption, which is described in a later section.

To export the self-signed certificate and private key pair:

1. Click **Export/Import**.
2. Change the Key file type to **PKCS12**.
3. Provide the File Name **commManPrivate** and click **OK**.
4. Enter a password to protect the target PKCS12 file. Confirm the password, and click **OK**.

Note: Stop and restart the Receiver for these changes to take effect.

The password entered will be used later when you import this private certificate into the hub.

Partner Two must also perform some configuration steps, including importing the certificate and changing the address to which it sends AS2 documents. For example, Partner Two would have to change the address to:

```
https://<IP_address>:57443/bcgreceiver/submit
```

where <*IP_address*> refers to the hub.

Now, the self-signed certificate that was placed in the Receiver's default key store is presented to Partner Two whenever Partner Two sends a document over secure HTTP.

To set up the reverse situation, Partner Two must provide the hub with an SSL key in the form of a .der file (in this case, partnerTwoSSL.der). If necessary, Partner Two must also change the configuration to permit the receipt of documents over the HTTPS transport.

Load Partner Two's file, partnerTwoSSL.der, into the Hub Operator's profile as a root certificate. A root certificate is a certificate issued from a Certifying Authority (CA) used when establishing a certificate chain. In this example, PartnerTwo generated the certificate, which is loaded as a root certificate to allow the hub to recognize and trust the sender.

Load partnerTwoSSL.der into the hub:

1. From the main menu, click **Account Admin > Profiles > Community Participant**.
2. Click **Search**.
3. Select **Hub Operator** by selecting the **View details** icon.
4. Click **Certificates** and then **Load Certificate**.
5. Set the **Certificate Type** as **Root and Intermediate Certificate**.
6. Change the Description to **Partner Two SSL Certificate**.
7. Set the **Status** as **Enabled**.
8. Click **Browse** and navigate to the directory in which you have saved partnerTwoSSL.der.
9. Select the certificate and click **Open**.
10. Click **Upload** and then click **Save**.

Change Partner Two's gateway to use secure HTTP.

1. Click **Account Admin > Profiles > Community Participant** from the horizontal navigation bar.
2. Click **Search** and select Partner Two by clicking the **View details** icon.
3. Click **Gateways** from the horizontal navigation bar. Next select HttpGateway by clicking the **View details** icon.
4. Edit it by clicking the **Edit** icon.
5. Change the transport value to **HTTPS/1.1**
6. Change the value of the address to read as follows: **https://<*IP_address*>:443/input/AS2**, where <*IP_address*> refers to Partner Two's machine.

7. All other values can remain unchanged. Click **Save**.

Setting up encryption

This section provides the steps for setting up encryption.

Partner Two must perform any necessary configuration steps (for example, importing the public certificate and the self-signed certificate) and set up encryption on documents sent to the hub.

WebSphere Partner Gateway will use its private key when decrypting documents. To allow the hub to do so, you first load the private key extracted from the self-signed certificate into the Community Console. Perform this task logged in to the Community Console as Hub Operator and install the certificate in your own profile.

To load the PKCS12 file:

1. Click **Account Admin > Profiles > Community Participant** from the horizontal navigation bar.
2. Click **Search**.
3. Select **Hub Operator** by clicking the **View details** icon.
4. Click **Certificates** and then click **Load PKCS12**.
5. Select the check box to the left of **Encryption**.
6. Change the Description to **CommManPrivate**.
7. Select **Enabled**.
8. Click **Browse** and navigate to the directory in which the PKCS12 file, commManPrivate.p12, is stored.
9. Select the file and click **Open**.
10. Enter the password provided for the PKCS12 file.
11. Leave the Gateway Type as **Production**.
12. Click **Upload**, and then click **Save**.

This completes the configuration required to allow a participant to send encrypted transactions over secure HTTP to the hub.

In the following section, the previous procedure is reversed—the hub sends an encrypted EDI transaction over secure HTTP.

Partner Two must generate a document decryption key pair (in this example, partnerTwoDecrypt.der) and should make the public certificate available to the hub.

As mentioned earlier, the public key will be used by the hub when encrypting transactions to be sent to the participant. In order to do so, you load the public certificate into the hub.

1. From the main menu, click **Account Admin > Profiles > Community Participant**.
2. Click **Search**.
3. Select Partner Two by clicking the **View details** icon.
4. Click **Certificates** from the horizontal navigation bar.
5. Click **Load Certificate**.
6. Select the check box next to **Encryption**.

7. Change the Description to read **Partner Two Decrypt**.
8. Set the status to **Enabled**.
9. Click **Browse**.
10. Navigate to the directory in which the decryption certificate, partnerTwoDecrypt.der, is stored.
11. Select the certificate and click **Open**.
12. Leave the Gateway Type as **Production**
13. Click **Upload** and then click **Save**.

The final step in configuring the hub to send encrypted messages over secure HTTP using AS2 is to modify the participant connection that exists between the Community Manager and Partner Two.

To modify the participant connection from the Community Console:
1. Click **Account Admin > Participant Connections** from the horizontal navigation bar.
2. From the **Source** list, select **Comm Man**.
3. From the **Target** list, select **Partner Two**.
4. Click **Search**.
5. Click the **Attributes** button for the Target.
6. From the Connection Summary, note that the **AS Encrypted** attribute has a current value of **No**. Edit this value by clicking the **Expand** icon next to **Package: AS (N/A)**.

   Note: You will need to scroll down the page for this option to appear.
7. From the list, update the **AS Encrypted** attribute to **Yes** and click **Save**.

Setting up document signing

When digitally signing a transaction or message, WebSphere Partner Gateway uses your private key to create the signature and sign. Your partner receiving that message uses your public key to validate the signature. WebSphere Partner Gateway uses digital signatures to this effect.

This section provides the steps required to configure both the hub and a participant for use with digital signatures.

Partner Two must perform any necessary configuration steps (for example, creating a self-signed document named, in this example, partnerTwoSigning.der) and configuring the signing of documents. Partner Two must make partnerTwoSigning.der available to the hub.

To load the digital certificate into the hub:
1. Click **Account Admin > Profiles > Community Participant** from the horizontal navigation bar.
2. Click **Search**.
3. Select Partner Two by clicking the **View details** icon.
4. Choose **Certificates** from the horizontal navigation bar.
5. Click **Load Certificate**.
6. Select the check box next to **Digital Signature**.
7. Change the Description to **CommMan Signing**.

8. Set the **Status** to **Enabled**.
9. Click **Browse**.
10. Navigate to the directory in which the digital certificate, partnerTwoSigning.der, is saved, select the certificate, and click **Open**.
11. Click **Upload** followed by **Save**.

This completes the initial configuration for digital signatures.

The participant uses the public certificate to authenticate signed transactions sent the hub.

The hub will use the private key to digitally sign outbound transactions sent to the participant. You first enable the private key for digital signature.

To enable the private key for digital signature:

1. Click **Account Admin > Profiles > Certificates** from the horizontal navigation bar.
2. Click the **View details** icon next to **Hub Operator**.
3. Click the **View details** icon next to **CommManPrivate**.

   Note: This was the private certificate loaded into the hub earlier.
4. Click the **Edit** icon.
5. Select the check box next to **Digital Signature**.

   Note: If there were more than one digital signature certificate, you would select which one was primary and which one was secondary by selecting **Primary** or **Secondary** from the **Certificate Usage** list.
6. Click **Save**.

Next you alter the attributes of the existing participant connection between the Community Manager and Partner Two to accommodate signed AS2.

To alter the attributes of the participant connection:

1. Click **Account Admin > Participant Connections** from the horizontal navigation bar.
2. Select **Comm Man** from the **Source** list.
3. Select **Partner Two** from the **Target** list.
4. Click **Search**.
5. Click the **Attributes** button for Partner Two.
6. Edit the **AS Signed** attribute by clicking the **Expand** icon next to **Package: AS (N/A)**.
7. Select **Yes** from the **AS Signed** list.
8. Click **Save**.

This completes the configuration required to send a signed AS2 transaction from WebSphere Partner Gateway to the participant.

Extending the basic configuration

This section shows you how to modify the basic configuration described in this appendix. Using the same partners and setup described earlier (a Community Manager named Comm Man, using a DUNS ID of 123456789 and a file-directory gateway, and a participant named PartnerTwo with a DUNS ID of 987654321 and an HTTP gateway), this section describes how to add support for:

- The FTP transport
- Custom XML documents
- Binary files (with no packaging)

Creating an FTP target

The FTP target receives files and passes them to the Document Manager for processing. As described in "Configuring the FTP server for receiving documents" on page 17, before you can create an FTP target, you must have an FTP server installed, and you must have created an FTP directory and configured your FTP server.

In this example, it is assumed that the FTP server has been configured for Partner Two and that the root directory is c:/ftproot.

1. Click **Hub Admin > Hub Configuration > Targets**.
2. Click **Create Target**.
3. Enter the following information:
   a. Target Name: **FTP_Receiver**
   b. Transport: **FTP Directory**
   c. FTP Root Directory: **C:/ftproot**
4. Click **Save**.

Setting up the hub to receive binary files

This section covers the steps required to configure the hub to receive binary documents that Partner Two wants to send to the Community Manager.

Creating an interaction for binary documents

By default, WebSphere Partner Gateway provides four interactions involving binary documents. It does not, however, provide an interaction for binary documents packaged as None going to a participant with the document also packaged as None. In this section, you will create the required interaction to allow binary documents to pass through the system.

1. Click **Hub Admin > Hub Configuration > Document Flow Definition**.
2. Click **Manage Interactions**.
3. Click **Create Interaction**.
4. From **Source** select: **Package: None Protocol: Binary (1.0) Document Flow: Binary (1.0)**.
5. From **Target** select: **Package: None Protocol: Binary (1.0) Document Flow: Binary (1.0)**.
6. From the **Action** list, select **Pass Through**.
7. Click **Save**.

Updating the B2B capabilities for the Community Manager

This section shows how to configure the Community Manager to be able to accept binary documents.

1. Click **Account Admin > Profiles > Community Participant**.
2. Click **Search**.
3. Click the **View details** icon next to **Comm Man**.
4. Click **B2B Capabilities**.
5. Click the **Role is not active** icon under **Set Target** for **Package: None** to enable it.
6. Click the **Expand** icon next to **Package: None**.
7. Click the **Role is not active** icon for **Protocol: Binary (1.0)** under **Set Target**.
8. Click the **Expand** icon next to **Protocol: Binary (1.0)**.
9. Finally, click the **Role is not active** icon for **Document Flow: Binary (1.0)** under **Set Target**.

Updating the B2B capabilities for Partner Two

This section shows how to configure Partner Two to be able to send binary documents.

1. Click **Account Admin > Profiles > Community Participant**.
2. Click **Search**.
3. Click the **View details** icon next to Partner Two.
4. Click **B2B Capabilities**.
5. Click the **Role is not active** icon under **Set Source** for **Package: None** to enable it.
6. Click the **Expand** icon next to **Package: None**.
7. Click the **Role is not active** icon for **Protocol: Binary (1.0)** under **Set Source**.
8. Click the **Expand** icon next to **Protocol: Binary (1.0)**.
9. Finally, click the **Role is not active** icon for **Document Flow: Binary (1.0)** under **Set Source**.

Creating a new participant connection

This section shows how to configure a new participant connection between the Community Manager and Partner Two for binary documents.

1. Click **Account Admin > Participant Connections**.
2. Select **Partner Two** from the **Source** list.
3. Select **Comm Man** from the **Target** list.
4. Click **Search**.
5. Locate the **None (N/A), Binary (1.0), Binary (1.0)** to **None (N/A), Binary (1.0), Binary (1.0)** connection and click **Activate** to activate it.

Setting up the hub for custom XML documents

As described in “Custom XML documents” on page 77, you must configure the hub to be able to route custom XML Files. This section covers the steps required to configure the Document Manager to be able to route the following XML document:

```
<?xml version="1.0" encoding="UTF-8"?>
       <!DOCTYPE Tester>
         <Tester>
        <From>987654321</From>
       <To>123456789</To>
   </Tester>
```

The Document Manager uses the RootTag to identify the type of XML document. It then extracts the values from the From and To fields to identify the From Participant Name and To Participant Name.

Creating the CustomXML protocol definition format

The first step is to create a new protocol for the Custom XML you are going to exchange.

1. Click **Hub Admin > Hub Configuration > Document Flow Definition**.
2. Click **Create Document Flow Definition**.
3. Select **Protocol** from the **Document flow type** list.
4. Enter the following information:
   a. Code: **CustomXML**
   b. Version: **1.0**
   c. Description: **CustomXML**
5. Set **Document Level** to **No**.
6. Set **Status** to **Enabled**.
7. Set **Visibility: Community Operator** to **Yes**.
8. Set **Visibility: Community Manager** to **Yes**.
9. Set **Visibility: Community Participant** to **Yes**.
10. Select:
    a. Package: **AS**
    b. Package: **None**
    c. Package: **Backend Integration**.
11. Click **Save**.

Creating the Tester_XML document definition

The second step is to create a document flow definition for the new protocol.

1. Click **Hub Admin > Hub Configuration > Document Flow Definition**.
2. Click **Create Document Flow Definition**.
3. Select **Document Flow** from the **Document flow type** list.
4. Enter the following information:
   a. Code: **XML_Tester**
   b. Version: **1.0**
   c. Description: **XML_Tester**
5. Set **Document Level** to **Yes**.
6. Set **Status** to **Enabled**.
7. Set **Visibility: Community Operator** to **Yes**.
8. Set **Visibility: Community Manager** to **Yes**.
9. Set **Visibility: Community Participant** to **Yes**.
10. Click the **Expand** icon next to **Package: AS** and select **Protocol: CustomXML**.
11. Click the **Expand** icon next to **Package: None** and select **Protocol: CustomXML**.
12. Click the **Expand** icon next to **Package: Backend Integration** and select **Protocol: CustomXML**.
13. Click **Save**.

Creating the Tester_XML XML Format

Finally, you create the XML format associated with the new protocol.

1. Click **Hub Admin > Hub Configuration > XML Formats**.
2. Click **Create XML Format**.
3. Select **CustomXML 1.0** from the **Routing Format** list.

4. Select **XML** from the **File Type** list.
5. Select **Root Tag** from the **Identifier Type** list, and type **Tester** for the value.
6. Select **Element Path** from the **Source Business Id** list, and type **/Tester/From** for the value.
7. Select **Element Path** from the **Target Business Id** list, and type **/Tester/To** for the value.
8. Select **Constant** from the **Source Document Flow** list, and type **XML_Tester** for the value.
9. Select **Constant** for the **Source Document Flow Version**, and type **1.0** for the value.
10. Click **Save**.

Creating an interaction for XML_Tester XML documents

You now have a new protocol and document flow with which to set up an interaction.

1. Click **Hub Admin > Hub Configuration > Document Flow Definition**.
2. Click **Manage Interactions**.
3. Click **Create Interaction**.
4. From **Source**, select:
   a. Package: **None**
   b. Protocol: **CustomXML (1.0)**
   c. Document Flow: **XML_Tester (1.0)**.
5. From **Target** select:
   a. Package: **None**
   b. Protocol: **CustomXML (1.0)**
   c. Document Flow: **XML_Tester (1.0)**.
6. From the **Action** list, select **Pass Through**.
7. Click **Save**.

Updating the B2B capabilities for the Community Manager

To enable the exchange of the custom XML document, you must update the B2B capabilities of the participants.

1. Click **Account Admin > Profiles > Community Participant**.
2. Click **Search**.
3. Click the **View details** icon next to **Comm Man**.
4. Click **B2B Capabilities**.
5. Click the **Role is not active** icon under **Set Target** for **Package: None** to enable it.
6. Click the **Expand** icon next to **Package: None**.
7. Click the **Role is not active** icon for **Protocol: CustomXML (1.0)** for **Set Target**.
8. Click the **Expand** icon next to **Protocol: CustomXML (1.0)**.
9. Finally, click the **Role is not active** icon for **Document Flow: XML_Tester (1.0)** for **Set Target**.

Updating the B2B capabilities for partnerTwo

You update the B2B capabilities of Partner Two to enable the exchange of the new custom XML format.

1. Click **Account Admin > Profiles> Community Participant**.
2. Click **Search**.

3. Click the **View details** icon next to Partner Two.
4. Click **B2B Capabilities**.
5. Click the **Role is not active** icon under **Set Source** for **Package: None** to enable it.
6. Click the **Expand** icon next to **Package: None**.
7. Click the **Role is not active** icon for **Protocol: CustomXML (1.0)** for **Set Source**.
8. Click the **Expand** icon next to **Protocol: CustomXML (1.0)**.
9. Finally, click the **Role is not active** icon for **Document Flow: XML_Tester (1.0)** for **Set Source**.

Creating a new participant connection

Finally, create a new participant connection.

1. Click **Account Admin > Participant Connections.**
2. Select **Partner Two** from the **Source** list.
3. Select **Comm Man** from the **Target** list.
4. Click **Search**.
5. Locate the **None (N/A), CustomXML (1.0), XML_Tester(1.0)** to **None (N/A), CustomXML(1.0), XML_Tester (1.0)** connection and click **Activate** to activate it.

Appendix B. EDI examples

This appendix provides examples of sending or receiving EDI interchanges and transforming them to and from XML and record-oriented data (ROD) documents.

The examples in this appendix are unrelated to those in Appendix A, "Basic examples," on page 169. New targets, gateways, and profiles are created for the examples in this appendix.

Note: An example of an EDI interchange that is passed through the hub (no de-enveloping or transformation) is included in Appendix A, "Basic examples."

Each of these four examples is self-contained. For example, if you follow the EDI to XML example, you will see all the steps (from creating targets through activating connections) for that example.

This appendix includes the following topics:

- "EDI to ROD example"
- "EDI to XML example" on page 197
- "XML to EDI example" on page 202
- "ROD to EDI example" on page 209

These examples are intended to provide you with a quick overview of the steps required to configure a system. If you are using these examples to set up your system, modify the specific information (for example, names and business IDs) to suit the needs of your business.

EDI to ROD example

This section provides an example of sending an EDI transaction (within an envelope) to the hub, where it is transformed into a record-oriented-data (ROD) document and sent to Community Manager.

De-enveloping and transforming an EDI interchange

In this example, it is assumed that the Data Interchange Services mapping specialist has created a transformation map that takes a standard EDI 850 transaction (defined with the X12V5R1 dictionary, corresponding to the version 5010 of X12) and transforms it into a record-oriented document (ROD) that will be processed by the back-end application of the Community Manager. In this example, the map is named S_DT_EDI_TO_ROD.eif.

The Data Interchange Services mapping specialist can export the transformation map directly to the WebSphere Partner Gateway database. Alternatively, the Data Interchange Services mapping specialist can send you the file, in which case you use the bcgDISImport utility to import it into WebSphere Partner Gateway. This appendix assumes the second scenario.

© Copyright IBM Corp. 2004, 2005

Importing the transformation map

This section describes the steps you take to import a transformation map that will take EDI input and transform it into record-oriented data (ROD) format. In the process of importing the transformation map, you also import the document definition associated with the map.

Before you can import the transformation map, the Data Interchange Services mapping specialist must send it to you. This set of steps assumes that the file, S_DT_EDI_TO_ROD.eif, is on your system.

1. Open a command window.
2. Enter the following command or script:
   - On a UNIX system:
     ```
     <ProductDir>/bin/bcgDISImport.sh <database_user_ID>
     <password> S_DT_EDI_TO_ROD.eif
     ```
   - On a Windows system:
     ```
     <ProductDir>\bin\bcgDISImport.bat <database_user_ID>
     <password> S_DT_EDI_TO_ROD.eif
     ```

     where <*database_user_ID*> and <*password*> are the values that you used when you installed the database as part of the WebSphere Partner Gateway installation.

Verifying the transformation map and document flow definitions

To verify that the transformation maps and document definitions you imported are available on the Community Console, perform the following steps:

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

   The S_DT_EDI_TO_ROD map is displayed.
2. Click the **View details** icon next to the map.

   You see the document flow definitions with which this map is associated:

Table 19. Document flow definition associated with the map

Source	Target
Package: N/A Protocol: X12V5R1 (ALL) Document Flow: 850 (ALL)	Package: None Protocol: DEMO850CL_DICTIONARY(ALL) Document Flow: DEMO850CLSUW (ALL)

The S_DT_EDI_TO_ROD map was defined to take an X12 850 transaction (which adheres to the X12V5R1 standard) and transform it to a custom protocol (DEMO850CL_DICTIONARY) and document flow (DEMO850CLSUW).

Configuring the target

In this section, you create a file-system directory target for the hub:

1. Click **Hub Admin > Hub Configuration > Targets** and click **Create Target**.
2. For Target Name, type: **EDIFileTarget**
3. From the Transport list, select **File Directory**.
4. For Root Path, type: **/Data/Manager/editarget**
5. Click **Save**.

The community participant sends the EDI interchange to this target.

Creating the interactions

You create two interactions--one for the EDI envelope and one for the transaction within the EDI envelope.

Create an interaction that represents the EDI envelope.

1. Click **HubAdmin > Hub Configuration > Document Flow Definition**.
2. Click **Manage Interactions** and then **Create Interaction**.
3. Under **Source**, expand **Package: None** and **Protocol: EDI-X12** and select **Document Flow: ISA**.
4. Under **Target**, expand **Package: N/A** and **Protocol: EDI-X12** and select **Document Flow: ISA.**
5. From the Action list, select **EDI De-envelope**.

   Note: No transformation is occurring in this interaction. The EDI interchange is being de-enveloped, resulting in the individual transaction (850). You do not, therefore, need a transformation map for this interaction.
6. Click **Save**.

Create an interaction that has a source that represents the 850 transaction and a target the represents the transformed document.

1. Click **HubAdmin > Hub Configuration > Document Flow Definition**.
2. Click **Manage Interactions** and click **Create Interaction**.
3. Under **Source**, expand **Package: N/A** and **Protocol: X12V5R1** and select **Document Flow: 850**.
4. Under **Target**, expand **Package: None** and **Protocol: DEMO850CL_DICTIONARY** and select **Document Flow: DEMO850CLSUW**.
5. From the Transformation Map list, select **S_DT_EDI_TO_ROD**.
6. From the Action list, select **EDI Validate and EDI Translate**.
7. Click **Save**.

This interaction represents the transformation of a standard EDI X12 850 transaction into a different format and, therefore, you must select a transformation map.

Creating the participants

For this example, you have two participants: the Community Manager (Manager) and a participant (TP1).

Create the Community Manager profile:

1. Click **Account Admin > Profiles > Community Participant** and click **Create**.
2. For Company Login Name, type: **ComManager**
3. For Participant Display Name: type **Manager**
4. For Participant Type, select **Community Manager**.
5. Click **New** for Business ID and type `000000000` as the Freeform ID.

   Note: Make sure you select Freeform and not DUNS.
6. Click **New** again for Business ID and type `01-000000000` as the Freeform ID.
7. Click **Save**.

Create the second participant:

1. Click **Account Admin > Profiles > Community Participant** and click **Create**.
2. For Company Login Name, type **TP1**
3. For Participant Display Name, type **TP1**
4. For Participant Type, select **Community Participant**.

5. Click **New** for Business ID and type `000000001` as the Freeform ID.

   Note: Make sure you select Freeform and not DUNS.
6. Click **New** again for Business ID and type `01-000000001` as the Freeform ID.
7. Click **Save**.

Creating the gateways

Create file-directory gateways for both participants in the example. First, create a gateway for the Manager:

1. Click **Account Admin > Profiles > Community Participant** and click **Search**.
2. Click the **View details** icon next to the Manager profile.
3. Click **Gateways** and then **Create**.
4. Enter the following values for the gateway. Remember that the file directory (the entire path) must already exist on your file system.
   a. For Name, type **ManagerFileGateway**.
   b. From the Transport List, select **File Directory**.
   c. For Address, type: **file:///Data/Manager/filegateway**
   d. Click **Save**.
5. Click **List** to list all the gateways for the Community Manager.
6. Click **View Default Gateways**.
7. From the **Production** list, select the gateway you created in step 4.
8. Click **Save**.

Next, create a gateway for the participant.

1. Click **Account Admin > Profiles > Community Participant** and click **Search**.
2. Select the other participant you created for this example by clicking on the **View details** icon next to **TP1**.
3. Click **Gateways** and then **Create**.
4. Enter the following values for the gateway. Remember that the file directory (the entire path) must already exist.
   a. For Name, type **TP1FileGateway**.
   b. From the Transport list, select **File Directory**.
   c. For Address, type: **file:///Data/TP1/filegateway**
   d. Click **Save**.
5. Click **List** to list all the gateways for the participant.
6. Click **View Default Gateways**.
7. From the **Production** list, select the gateway you created in step 4.
8. Click **Save**.

Setting up B2B capabilities

Enable the B2B capabilities of the two participants in this exchange. In this example, the EDI interchange is originating with the community participant (TP1) and will be delivered to the Community Manager.

1. Click **Account Admin > Profiles > Community Participant** and click **Search**.
2. Click the **View details** icon for the source participant for this example (**TP1**).
3. Click **B2B Capabilities**.
4. Enable two sets of capabilities for the source participant.
   a. First, enable the document flow definition representing the EDI envelope:

        1) Click the **Role is not active** icon under **Set Source** for **Package: None** to enable it.
        2) Expand **Package: None**.
        3) Click the **Role is not active** icon under **Set Source** for **Protocol EDI-X12 (ALL)**.
        4) Expand **Protocol EDI-X12 (ALL)**.
        5) Click the **Role is not active** icon under **Set Source** for **Document Flow: ISA (ALL)**.
    b. Next, enable the document flow definition representing the 850 transaction:
        1) Click the **Role is not active** icon under **Set Source** for **Package: N/A** to enable it.
        2) Expand **Package: N/A**.
        3) Click the **Role is not active** icon under **Set Source** for **Protocol: X12V5R1 (ALL)**.
        4) Expand **Protocol: X12V5R1 (ALL)**.
        5) Click the **Role is not active** icon under **Set Source** for **Document Flow: 850**.
5. Click on **Account Admin > Profiles > Community Participant** and click **Search**.
6. Click the **View details** icon for the target participant for this example (**Manager**).
7. Click **B2B Capabilities**.
8. Enable two sets of capabilities for the target participant.
    a. First, enable the document flow definition representing the envelope:
        1) Click the **Role is not active** icon under **Set Target** for **Package: N/A** to enable it.
        2) Expand **Package: N/A**.
        3) Click the **Role is not active** icon under **Set Target** for **Protocol: EDI-X12 (ALL)**.
        4) Expand **Protocol: EDI-X12 (ALL)**.
        5) Click the **Role is not active** icon under **Set Target** for **Document Flow: ISA (ALL)**.
    b. Next, enable the document flow definition representing the transformed document:
        1) Click the **Role is not active** icon under **Set Target** for **Package: None** to enable it.
        2) Expand **Package: None**.
        3) Click the **Role is not active** icon under **Set Target** for **Protocol: DEMO850CL_DICTIONARY (ALL)**.
        4) Expand **Protocol: DEMO850CL_DICTIONARY (ALL)**.
        5) Click the **Role is not active** icon under **Set Target** for **Document Flow: DEMO850CLSUW(ALL)**.

Activating the connections

To activate the connections:

1. Click **Account Admin > Participant Connections**.
2. Select **TP1** from the Source list.
3. Select **Manager** from the Target list.
4. Click **Search**.

5. Click **Activate** for the connection that represents the envelope:

Table 20. Envelope connection

Source	Target
Package: None (N/A) Protocol: EDI-X12 (ALL) Document Flow: ISA (ALL)	Package: N/A (N/A) Protocol: EDI-X12 (ALL) Document Flow: ISA(ALL)

6. Click **Activate** for the connection that represents the 850 transaction to the transformed document:

Table 21. EDI transaction to ROD document connection

Source	Target
Package: N/A (N/A) Protocol: X12V5R1 Document Flow: 850 (ALL)	Package: None (N/A) Protocol: DEMO850CL_DICTIONARY (ALL) Document Flow: DEMO850CLSUW (ALL)

Adding attributes

Set the attribute that allows documents with duplicate IDs:

1. Click **Hub Admin > Hub Configuration > Document Flow Definition**.
2. Click the **Expand** icon next to **Package: None**.
3. Click the **Edit Attribute Values** icon next to **Protocol: EDI-X12**.
4. Scroll down to the Document Flow Context Attributes section of the page. In the **Allow documents with duplicate document ids** row, select **Yes** from the list.
5. Click **Save**.

At this point, if TP1 sent an EDI interchange containing an 850 transaction to the Community Manager, the EDI interchange would be de-enveloped, resulting in an 850 transaction. The 850 transaction would then be transformed to the DEMO850CLSUW document type, and the transformed document would be sent to the gateway of the Community Manager.

Adding a TA1 to the exchange

In X12, the TA1 is an optional segment that can be used to acknowledge receipt of an interchange. The sender can request a TA1 from the receiver by setting element 14 of the ISA Interchange Control Header to **1**. The Allow a TA1 request attribute in WebSphere Partner Gateway can be used to control whether a TA1 is sent when the sender requests it.

The &WDI_TA1_ACK map is installed during the installation of WebSphere Partner Gateway, so you do not have to import it.

Creating the associations

To associate the map with a document flow definition, perform the following steps:

1. Click **Hub Admin > Hub Configuration > Maps > EDI FA Maps**.

   The &WDI_TA1_ACK map is displayed.
2. Click the **View details** icon next to the map.

   You see information about the map as well as a folder for each type of package available on the system.
3. Create the association to the document flow definition by performing these steps:

   a. Select the check box next to **Package: None** and expand the folder.
   b. Select the check box next to **Protocol: EDI-X12 (ALL)** and expand the folder.
   c. Select the check box next to **Document Flow: ISA (ALL)**.
   d. Click **Save**.

You have created an association between the &WDI_TA1_ACK1 map and the document flow definition for the envelope.

Creating interactions

Create an interaction that represents the TA1 transaction.

1. Click **HubAdmin > Hub Configuration > Document Flow Definition**.
2. Click **Manage Interactions** and then **Create Interaction**.
3. Under **Source**, expand **Package: N/A** and **Protocol: &X44TA1** and select **Document Flow: TA1**.
4. Under **Target**, expand **Package: N/A** and **Protocol: &X44TA1** and select **Document Flow: TA1**.
5. From the Action list, select **Pass Through**.
6. Click **Save**.

Create an interaction that has a source that represents the EDI envelope that will hold the TA1.

1. Click **HubAdmin > Hub Configuration > Document Flow Definition**.
2. Click **Manage Interactions** and then **Create Interaction**.
3. Under **Source**, expand **Package: N/A** and **Protocol: EDI-X12** and select **Document Flow: ISA**.
4. Under **Target**, expand **Package: None** and **Protocol: EDI-X12** and select **Document Flow: ISA.**
5. From the Action list, select **Pass Through**.
6. Click **Save**.

Enabling B2B capabilities

Next, you add the newly created interactions to the B2B capabilities of the participants.

1. Click on **Account Admin > Profiles > Community Participant** and click **Search**.
2. Click the **View details** icon for the source participant for this example (**Manager**).

   Note: Remember that the TA1 flows from the participant that receives the ROD document to the participant that sent it. In this example, the Manager is the source of the TA1 and participant TP1 is the target.
3. Click **B2B Capabilities**.
4. Enable two sets of capabilities for the source participant.
   a. First, enable the capability for the TA1.
      1) Click the **Role is not active** icon under **Set Source** for **Package: N/A** to enable it.
      2) Expand **Package: N/A**.
      3) Click the **Role is not active** icon under **Set Source** for **Protocol: &X44TA1**.
      4) Expand **Protocol: &X44TA1**.

5) Click the **Role is not active** icon under **Set Source** for **Document Flow: TA1 (ALL)**.

b. Next, enable the capability for the envelope:

1) Click the **Role is not active** icon under **Set Source** for **Package: N/A** to enable it.

2) Expand **Package: N/A**.

3) Click the **Role is not active** icon under **Set Source** for **Protocol: EDI-X12**.

4) Expand **Protocol: EDI-X12 (ALL)**.

5) Click the **Role is not active** icon under **Set Source** for **Document Flow: ISA (ALL)**.

5. Click on **Account Admin > Profiles > Community Participant** and click **Search**.
6. Click the **View details** icon for the target participant for this example (**TP1**).
7. Click **B2B Capabilities**.
8. Enable two sets of capabilities for the target participant.

a. First, enable the document flow definition representing the TA1:

1) Click the **Role is not active** icon under **Set Target** for **Package: N/A** to enable it.

2) Expand **Package: N/A**.

3) Click the **Role is not active** icon under **Set Target** for **Protocol: &X44TA1 (ALL)**.

4) Expand **Protocol: &X44TA1 (ALL)**.

5) Click the **Role is not active** icon under **Set Target** for **Document Flow: TA1 (ALL)**.

b. Next, enable the document flow definition representing the EDI envelope:

1) Click the **Role is not active** icon under **Set Target** for **Package: None** to enable it.

2) Expand **Package: None**.

3) Click the **Role is not active** icon under **Set Target** for **Protocol: EDI-X12 (ALL)**.

4) Expand **Protocol: EDI-X12 (ALL)**.

5) Click the **Role is not active** icon under **Set Target** for **Document Flow: ISA (ALL)**.

Creating the envelope profile

You next create the profile for the envelope that will contain the TA1:

1. Click **Hub Admin > Hub Configuration > EDI > Envelope Profile**.
2. Click **Create**.
3. Type the name of the profile: **EnvProf1**.
4. From the EDI Standard list, select **X12**.
5. The **General** button is selected by default. Type the following values for the general attributes of the envelope:
   - INTCTLLEN: **9**
   - GRPCTLLEN: **9**
   - TRXCTLLEN: **9**
   - MAXDOCS: **1000**

6. Click the **Interchange** button and type the following values for the interchange attributes:
   - ISA01: **01**
   - ISA02: **ISA0000002**
   - ISA03: **02**
   - ISA04: **ISA0000004**
   - ISA11: \
   - ISA12: **00501**
   - ISA15: **T**
7. Click **Save**.

Activating participant connections

To activate the connections:

1. Click **Account Admin > Participant Connections**.
2. Select **Manager** from the Source list.
3. Select **TP1** from the Target list.
4. Click **Search**.
5. Activate the connection that represents the TA1.

Table 22. TA1 connection

Source	Target
Package: N/A (N/A) Protocol: &X44TA1 (ALL) Document Flow: TA1 (ALL)	Package: N/A (N/A) Protocol: &X44TA1 (ALL) Document Flow: TA1 (ALL)

6. Activate the connection that represents the envelope:

Table 23. Envelope connection

Source	Target
Package: N/A (N/A) Protocol: EDI-X12 (ALL) Document Flow: ISA (ALL)	Package: None (N/A) Protocol: EDI-X12 (ALL) Document Flow: ISA (ALL)

Configuring the attributes

To specify attributes for the envelope profile:

1. Click **Account Admin > Profiles > Community Participant** and click **Search**.
2. Select **TP1** from the list.
3. Click **B2B Capabilities**.
4. Click the **Expand** icon next to **Package: None**.
5. Click the **Edit** icon next to **Protocol: EDI-X12 (ALL)**.
6. In the **Allow a TA1 Request** row, select **Yes**.
7. Click **Save**.
8. Click **B2B Capabilities** again.
9. Click the **Expand** icon next to **Package: N/A**.
10. Click the **Edit** icon next to **Protocol: &X44TA1 (ALL)**.
11. Specify the following attributes:
    a. In the Envelope Profile row, select **EnvProf1** from the list.
    b. In the Interchange qualifier row, type **01**.

   c. In the Interchange identifier row, type **000000001**.
   d. In the Interchange usage indicator row, type **T**.
12. Click **Save**.

In this series of tasks, you have added a TA1 acknowledgment to the exchange. When the interchange is received, WebSphere Partner Gateway sends a TA1 back to the sender (TP1). The TA1 is sent in an envelope that conforms to envelope profile EnvProf1.

Adding an FA map

This section describes how to add a standard functional acknowledgment (997) to the flow described in "EDI to ROD example" on page 185. The functional acknowledgment provides confirmation to the sender that the transaction was received.

Note: This example is similar to "Adding a TA1 to the exchange" on page 190. However, it is not directly related to that example. Instead, it builds on the tasks you performed in "EDI to ROD example" on page 185.

WebSphere Partner Gateway includes a set of preinstalled functional acknowledgment map names that begin with $DT_FA. This is followed by the name of the functional acknowledgment message and the version and release of the message. For example, Version 2 Release 4 of the 997 functional acknowledgment message is named $DT_997V2R4. See "Functional acknowledgments" on page 116 for the list of maps provided with WebSphere Partner Gateway.

Creating the associations

To associate the map with a document flow definition, perform the following steps:

1. Click **Hub Admin > Hub Configuration > Maps > EDI FA Maps**.

   The &DT_FA997V2R4 map is displayed.
2. Click the **View details** icon next to the map.

   You see information about the map as well as a folder for each type of package available on the system.
3. Create the association to the document flow definition by performing these steps:
   a. Select the check box next to **Package: N/A** and expand the folder
   b. Select the check box next to **Protocol: X12V5R1** and expand the folder.
   c. Select the check box next to **Document Flow: 850**.
   d. Click **Save**.

You have associated this functional acknowledgment 997 map with the X12 protocol.

Creating interactions

Create an interaction that represents the 997 acknowledgment.

1. Click **HubAdmin > Hub Configuration > Document Flow Definition**.
2. Click **Manage Interactions** and then **Create Interaction**.
3. Under **Source**, expand **Package: N/A** and **Protocol: &DT99724** and select **Document Flow: 997**.
4. Under **Target**, expand **Package: N/A** and **Protocol: &DT99724** and select **Document Flow: 997**.

5. From the Action list, select **Pass Through**.
6. Click **Save**.

Create an interaction that represents the envelope.

1. Click **HubAdmin > Hub Configuration > Document Flow Definition**.
2. Click **Manage Interactions** and then **Create Interaction**.
3. Expand **Package: N/A** and **Protocol: EDI-X12** and select **Document Flow: ISA**.
4. Expand **Package: None** and **Protocol: EDI-X12** and select **Document Flow: ISA**.
5. From the Action list, select **Pass Through**.
6. Click **Save**.

Enabling B2B capabilities

Next, you add the newly created interactions to the B2B capabilities of the participants.

1. Click on **Account Admin > Profiles > Community Participant** and click **Search**.
2. Click the **View details** icon for the source participant for this example (**Manager**).

   Note: Remember that the functional acknowledgment flows from the participant that receives the ROD document to the participant that sent it. In this example, the Manager is the source of the functional acknowledgment, and participant TP1 is the target.
3. Click **B2B Capabilities**.
4. Enable two sets of capabilities for the source participant.
   a. First, enable the capability for the FA.
      1) Click the **Role is not active** icon under **Set Source** for **Package: N/A** to enable it.
      2) Expand **Package: N/A**.
      3) Click the **Role is not active** icon under **Set Source** for **Protocol: &DT99724**.
      4) Expand **Protocol: &DT99724**.
      5) Click the **Role is not active** icon under **Set Source** for **Document Flow: 997 (ALL)**.
   b. Next, enable the capability for the envelope:
      1) Click the **Role is not active** icon under **Set Source** for **Package: N/A** to enable it.
      2) Expand **Package: N/A**.
      3) Click the **Role is not active** icon under **Set Source** for **Protocol: EDI-X12**.
      4) Expand **Protocol: EDI-X12 (ALL)**.
      5) Click the **Role is not active** icon under **Set Source** for **Document Flow: ISA (ALL)**.
5. Click on **Account Admin > Profiles > Community Participant** and click **Search**.
6. Click the **View details** icon for the target participant for this example (**TP1**).
7. Click **B2B Capabilities**.
8. Enable two sets of capabilities for the target participant.

a. First, enable the document flow definition representing the 997:
    1) Click the **Role is not active** icon under **Set Target** for **Package: N/A** to enable it.
    2) Expand **Package: N/A**.
    3) Click the **Role is not active** icon under **Set Target** for **Protocol: &DT99724 (ALL)**.
    4) Expand **Protocol: &DT99724 (ALL)**.
    5) Click the **Role is not active** icon under **Set Target** for **Document Flow: 997 (ALL)**.

b. Next, enable the document flow definition representing the EDI envelope:
    1) Click the **Role is not active** icon under **Set Target** for **Package: None** to enable it.
    2) Expand **Package: None**.
    3) Click the **Role is not active** icon under **Set Target** for **Protocol: EDI-X12 (ALL)**.
    4) Expand **Protocol: EDI-X12 (ALL)**.
    5) Click the **Role is not active** icon under **Set Target** for **Document Flow: ISA(ALL)**.

Creating the envelope profile

You next create the profile for the envelope that will contain the 997 functional acknowledgment. A functional acknowledgment, like a transaction, must be enveloped before it can be sent.

1. Click **Hub Admin > Hub Configuration > EDI > Envelope Profile**.
2. Click **Create**.
3. Type the name of the profile: **EnvProf1**.
4. From the EDI Standard list, select **X12**.
5. The **General** button is selected by default. Type the following values for the general attributes of the envelope:
    - INTCTLLEN: **9**
    - GRPCTLLEN: **9**
    - TRXCTLLEN: **9**
    - MAXDOCS: **1000**
6. Click the **Interchange** button and type the following values for the interchange attributes:
    - ISA01: **01**
    - ISA02: **ISA0000002**
    - ISA03: **02**
    - ISA04: **ISA0000004**
    - ISA11: ****
    - ISA12: **00501**
    - ISA15: **T**
7. Click **Save**.

Activating participant connections

To activate the connections:

1. Click **Account Admin > Participant Connections**.
2. Select **Manager** from the Source list.

3. Select **TP1** from the Target list.
4. Click **Search**.
5. Click **Activate** for the connection that represents the 997 functional acknowledgment:

Table 24. Functional acknowledgment connection

Source	Target
Package: N/A (N/A) Protocol: &DT99724 (ALL) Document Flow: 997 (ALL)	Package: N/A (N/A) Protocol: &DT99724 (ALL) Document Flow: 997 (ALL)

6. Click **Activate** for the connection that represents the EDI envelope being sent back to the originator of the exchange.

Table 25. Envelope connection

Source	Target
Package: N/A (N/A) Protocol: EDI-X12 (ALL) Document Flow: ISA (ALL)	Package: None (N/A) Protocol: EDI-X12 (ALL) Document Flow: ISA (ALL)

Configuring attributes

First, you specify which FA map to use:

1. Click **Account Admin > Profiles > Community Participant** and click **Search**.
2. Select **TP1** from the list.
3. Click **B2B Capabilities**.
4. Click the **Expand** icon next to **Package: N/A**.
5. Click the **Edit** icon next to **Protocol: X12V5R1 (ALL)**.
6. In the FA Map row, select **&DT_FA997V2R4**.
7. Click **B2B Capabilities** again.
8. Click the **Expand** icon next to **Package: N/A**.
9. Click the **Edit** icon next to **Protocol: &DT99724 (ALL)**.
10. Specify the following attributes:
    a. In the Envelope Profile row, select **EnvProf1** from the list.
    b. In the Interchange qualifier row, type **01**.
    c. In the Interchange identifier row, type **000000001**.
    d. In the Interchange usage indicator row, type **T**.
11. Click **Save**.

In this series of tasks, you have added an EDI-X12 997 functional acknowledgment to the exchange, so that when the Community Manager receives the document, it sends the 997 back to the sender (TP1). The 997 acknowledgment is sent in an envelope that conforms to envelope profile EnvProf1.

EDI to XML example

This section provides an example of sending an EDI transaction (within an envelope) to the hub, where it is transformed into an XML document and sent to the Community Manager.

In this example, it is assumed that the Data Interchange Services mapping specialist has created a transformation map that takes a standard EDI 879 transaction (defined with the X12V5R1 dictionary, corresponding to the version 5010 of X12) and transforms it into an XML document that will be processed by the back-end application of the Community Manager. In this example, the map is named S_DT_EDI_TO_XML.eif.

The Data Interchange Services mapping specialist can export the transformation map directly to the WebSphere Partner Gateway database. Alternatively, the Data Interchange Services mapping specialist can send you the file, in which case you use the bcgDISImport utility to import it into WebSphere Partner Gateway. This appendix assumes the second scenario.

Importing the transformation map

This section describes the steps you take to import a transformation map that will take EDI input and transform it into XML format. In the process of importing the transformation map, you also import the document definition associated with the map.

Before you can import the transformation map, the Data Interchange Services mapping specialist must send it to you. This set of steps assumes that the file, S_DT_EDI_TO_XML.eif, is on your system.

1. Open a command window.
2. Enter the following command or script:
   - On a UNIX system:

     ```
     <ProductDir>/bin/bcgDISImport.sh <database_user_ID>
      <password> S_DT_EDI_TO_XML.eif
     ```
   - On a Windows system:

     ```
     <ProductDir>\bin\bcgDISImport.bat <database_user_ID>
      <password> S_DT_EDI_TO_XML.eif
     ```

     where <*database_user_ID*> and <*password*> are the values that you used when you installed the database as part of the WebSphere Partner Gateway installation.

Verifying the transformation map and document flow definitions

To verify that the transformation maps and document definitions you imported are available on the Community Console, perform the following steps:

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

   The S_DT_EDI_TO_XML map is displayed.
2. Click the **View details** icon next to the map.

   You see the document flow definitions with which this map is associated:

Table 26. Document flow definition associated with the map

Source	Target
Package: N/A Protocol: X12V5R1 Document Flow: 879 (ALL)	Package: None Protocol: FVT-XML-TEST (ALL) Document Flow: WWRE_ITEMCREATIONINTERNAL (ALL)

The S_DT_EDI_TO_XML map was defined to take an X12 879 transaction (which adheres to the X12V5R1 standard) and transform it to a custom protocol.

Configuring the target

In this section, you create a file-system directory target for the hub:

1. Click **Hub Admin > Hub Configuration > Targets** and click **Create Target**.
2. For Target Name, type: **EDIFileTarget**
3. From the Transport list, select **File Directory**.
4. For Root Path, type: **/Data/Manager/editarget**
5. Click **Save**.

The community participant sends the EDI interchange to this target.

Creating the interactions

You create two interactions--one for the EDI envelope and one for the transaction within the EDI envelope.

Create an interaction that represents the EDI envelope.

1. Click **HubAdmin > Hub Configuration > Document Flow Definition**.
2. Click **Manage Interactions** and then **Create Interaction**.
3. Expand **Package: None** and **Protocol: EDI-X12** and select **Document Flow: ISA**.
4. Expand **Package: N/A** and **Protocol: EDI-X12** and select **Document Flow: ISA.**
5. From the Action list, select **EDI De-envelope**.

   Note: No transformation is occurring in this interaction. The EDI interchange is being de-enveloped, resulting in the individual transaction (879). You do not, therefore, need a transformation map for this interaction.
6. Click **Save**.

Create an interaction that has a source that represents the 879 transaction and a target the represents the transformed document.

1. Click **HubAdmin > Hub Configuration > Document Flow Definition**.
2. Click **Manage Interactions** and then **Create Interaction**.
3. Expand **Package: N/A** and **Protocol: X12V5R1** and select **Document Flow: 879**.
4. Expand **Package: None** and **Protocol: FVT-XML-TEST** and select **Document Flow: WWRE_ITEMCREATIONINTERNAL**.
5. From the Transformation Map list, select **S_DT_EDI_TO_XML**.
6. From the Action list, select **EDI Validate and EDI Translate**.
7. Click **Save**.

This interaction represents the transformation of a standard EDI X12 879 transaction into a different format and, therefore, you must select a transformation map.

Creating the participants

For this example, you have two participants: the Community Manager (Manager) and a participant (TP1).

Create the Community Manager profile:

1. Click **Account Admin > Profiles > Community Participant** and click **Create**.
2. For Company Login Name, type: **ComManager**

3. For Participant Display Name: type **Manager**
4. For Participant Type, select **Community Manager**.
5. Click **New** for Business ID and type `000000000` as the Freeform ID.

   Note: Make sure you select Freeform and not DUNS.
6. Click **New again** for Business ID and type `01-000000000` as the Freeform ID.
7. Click **Save**.

Create the second participant:
1. Click **Account Admin > Profiles > Community Participant** and click **Create**.
2. For Company Login Name, type **TP1**
3. For Participant Display Name, type **TP1**
4. For Participant Type, select **Community Participant**.
5. Click **New** for Business ID and type `000000001` as the Freeform ID.

   Note: Make sure you select Freeform and not DUNS.
6. Click **New** again for Business ID and type `01-000000001` as the Freeform ID.
7. Click **Save**.

Creating the gateways

Create file-directory gateways for both participants in the example. First, create a gateway for the Manager:
1. Click **Account Admin > Profiles > Community Participant** and click **Search**.
2. Click the **View details** icon next to the Manager profile.
3. Click **Gateways** and then **Create**.
4. Enter the following values for the gateway. Remember that the file directory (the entire path) must already exist on your file system.
   a. For Name, type **ManagerFileGateway**.
   b. From the Transport List, select **File Directory**.
   c. For Address, type: **file:///Data/Manager/filegateway**
   d. Click **Save**.
5. Click **List** to list all the gateways for the Community Manager.
6. Click **View Default Gateways**.
7. From the **Production** list, select the gateway you created in step 4.
8. Click **Save**.

Next, create a gateway for the participant.
1. Click **Account Admin > Profiles > Community Participant** and click **Search**.
2. Select the other participant you created for this example by clicking on the **View details** icon next to **TP1**.
3. Click on **Gateways** and then **Create**.
4. Enter the following values for the gateway. Remember that the file directory (the entire path) must already exist.
   a. For Name, type **TP1FileGateway**.
   b. From the Transport list, select **File Directory**.
   c. For Address, type: **file:///Data/TP1/filegateway**
   d. Click **Save**.

5. Click **List** to list all the gateways for the participant.
6. Click **View Default Gateways**.
7. From the **Production** list, select the gateway you created in step 4 on page 200.
8. Click **Save**.

Setting up B2B capabilities

Enable the B2B capabilities of the two participants in this exchange. In this example, the EDI interchange is originating with the community participant (TP1) and will be delivered to the Community Manager.

1. Click on **Account Admin > Profiles > Community Participant** and click **Search**.
2. Click the **View details** icon for the source participant for this example (**TP1**).
3. Click **B2B Capabilities**.
4. Enable two sets of capabilities for the source participant.
   a. First, enable the document flow definition representing the EDI envelope:
      1) Click the **Role is not active** icon under **Set Source** for **Package: None** to enable it.
      2) Expand **Package: None**.
      3) Click the **Role is not active** icon under **Set Source** for **Protocol EDI-X12 (ALL)**.
      4) Expand **Protocol EDI-X12 (ALL)**.
      5) Click the **Role is not active** icon under **Set Source** for **Document Flow: ISA (ALL)**.
   b. Next, enable the document flow definition representing the transaction:
      1) Click the **Role is not active** icon under **Set Source** for **Package: N/A** to enable it.
      2) Expand **Package: N/A**.
      3) Click the **Role is not active** icon under **Set Source** for **Protocol: X12V5R1 (ALL)**.
      4) Expand **Protocol: X12V5R1 (ALL)**.
      5) Click the **Role is not active** icon under **Set Source** for **Document Flow: 879**.
5. Click on **Account Admin > Profiles > Community Participant** and click **Search**.
6. Click the **View details** icon for the target participant for this example (**Manager**).
7. Click **B2B Capabilities**.
8. Enable two sets of capabilities for the target participant.
   a. First, enable the document flow definition:
      1) Click the **Role is not active** icon under **Set Target** for **Package: N/A** to enable it.
      2) Expand **Package: N/A**.
      3) Click the **Role is not active** icon under **Set Target** for **Protocol: EDI-X12 (ALL)**.
      4) Expand **Protocol: EDI-X12 (ALL)**.
      5) Click the **Role is not active** icon under **Set Target** for **Document Flow: ISA (ALL)**.

b. Next, enable the document flow definition representing the transformed document:

   1) Click the **Role is not active** icon under **Set Target** for **Package: None** to enable it.
   2) Expand **Package: None**.
   3) Click the **Role is not active** icon under **Set Target** for **Protocol: FVT-XML-TEST (ALL)**.
   4) Expand **Protocol: FVT-XML-TEST (ALL)**.
   5) Click the **Role is not active** icon under **Set Target** for **Document Flow: WWRE_ITEMCREATIONINTERNAL(ALL)**.

Activating the connections

To activate the connections:

1. Click **Account Admin > Participant Connections**.
2. Select **TP1** from the Source list.
3. Select **Manager** from the Target list.
4. Click **Search**.
5. Click **Activate** for the connection that represents the envelope:

Table 27. Envelope connection

Source	Target
Package: None (N/A) Protocol: EDI-X12 (ALL) Document Flow: ISA (ALL)	Package: N/A (N/A) Protocol: EDI-X12 (ALL) Document Flow: ISA (ALL)

6. Click **Activate** for the connection that represents the 879 transaction to the transformed document:

Table 28. EDI transaction to XML document connection

Source	Target
Package: N/A (N/A) Protocol: X12V5R1 (ALL) Document Flow: 879 (ALL)	Package: None (N/A) Protocol: FVT-XML-TEST (ALL) Document Flow: WWRE_ITEMCREATIONINTERNAL (ALL)

At this point, if TP1 sent an EDI interchange containing an 879 transaction to the Community Manager, the EDI interchange would be de-enveloped, resulting in an 879 transaction. The 879 transaction would then be transformed and the transformed document would be sent to the gateway of the Community Manager.

XML to EDI example

This section provides an example of the Community Manager sending an XML document to the hub, where it is transformed into an EDI transaction, enveloped within an EDI interchange, and sent to a participant.

In this example, it is assumed that the Data Interchange Services mapping specialist has created a transformation map that takes an XML document and transforms it into a standard EDI 850 transaction (defined with the MX12V3R1 dictionary) that will be processed by the participant. In this example, the map is named S_DT_XML_TO_EDI.eif.

The Data Interchange Services mapping specialist can export the transformation map directly to the WebSphere Partner Gateway database. Alternatively, the Data Interchange Services mapping specialist can send you the file, in which case you use the bcgDISImport utility to import it into WebSphere Partner Gateway. This appendix assumes the second scenario.

Importing the transformation map

This section describes the steps you take to import a transformation map that will take XML input and transform it into an EDI transaction. In the process of importing the transformation map, you also import the document definition associated with the map.

Before you can import the transformation map, the Data Interchange Services mapping specialist must send it to you. This set of steps assumes that the file, S_DT_XML_TO_EDI.eif, is on your system.

1. Open a command window.
2. Enter the following command or script:
   - On a UNIX system:
     ```
     <ProductDir>/bin/bcgDISImport.sh <database_user_ID>
      <password> S_DT_XML_TO_EDI.eif
     ```
   - On a Windows system:
     ```
     <ProductDir>\bin\bcgDISImport.bat <database_user_ID>
      <password> S_DT_XML_TO_EDI.eif
     ```
     where *<database_user_ID>* and *<password>* are the values that you used when you installed the database as part of the WebSphere Partner Gateway installation.

Verifying the transformation map and document flow definitions

To verify that the transformation maps and document definitions you imported are available on the Community Console, perform the following steps:

1. Click **Hub Admin > Hub Configuration > Maps > Transformation Maps**.
   The S_DT_XML_TO_EDI map is displayed.
2. Click the **View details** icon next to the map.
   You see the document flow definitions with which this map is associated:

Table 29. Document flow definitions associated with the map

Source	Target
Package: None Protocol: FVT-XML-TEST (ALL) Document Flow: ICGCPO (ALL)	Package: N/A Protocol: MX12V3R1 (ALL) Document Flow: 850 (ALL)

The S_DT_XML_TO_EDI map was defined to take an XML document and transform it to an EDI transaction.

Configuring the target

In this section, you create a file-system directory target for the hub:

1. Click **Hub Admin > Hub Configuration > Targets** and click **Create Target**.
2. For Target Name, type: **XMLFileTarget**
3. From the Transport list, select **File Directory**.

4. For Root Path, type: **/Data/Manager/xmltarget**
5. From the Configuration Point list, select **Preprocess**.
6. Select **com.ibm.bcg.edi.receiver.preprocesshandler.XMLSplitterHandler** from the Available List and click **Add** to move it to the Configured List.
7. Click **Save**.

The Community Manager sends the XML document to this target.

Creating the interactions

You create two interactions--one for the XML-to-EDI transformation and one for the EDI envelope.

Create an interaction that has a source that represents the XML document and a target that represents the transformed 850 transaction.

1. Click **Hub Admin > Hub Configuration > Document Flow Definition**.
2. Click **Manage Interactions** and then **Create Interaction**.
3. Expand **Package: None** and **Protocol: FVT-XML-TEST** and select **Document Flow: ICGCPO**.
4. Expand **Package: N/A** and **Protocol: MX12V3R1** and select **Document Flow: 850**.
5. From the Transformation Map list, select **S_DT_XML_TO_EDI**.
6. From the Action list, select **XML Translate and EDI Validate**.
7. Click **Save**.

This interaction represents the transformation of an XML document into an EDI transaction and, therefore, you must select a transformation map.

Create an interaction that represents the EDI envelope.

1. Click **Hub Admin > Hub Configuration > Document Flow Definition**.
2. Click **Manage Interactions** and then **Create Interaction**.
3. Expand **Package: N/A** and **Protocol: EDI-X12** and select **Document Flow: ISA**.
4. Expand **Package: None** and **Protocol: EDI-X12** and select **Document Flow: ISA.**
5. From the Action list, select **Pass Through**.

   Note: No transformation is occurring in this interaction.
6. Click **Save**.

Creating the participants

For this example, you have two participants: the Community Manager (Manager) and a participant (TP1).

Create the Community Manager profile:

1. Click **Account Admin > Profiles > Community Participant** and click **Create**.
2. For Company Login Name, type: **ComManager**
3. For Participant Display Name, type: **Manager**.
4. For Participant Type, select **Community Manager**.
5. Click **New** for Business ID and type `000000000` as the Freeform ID.

   Note: Make sure you select Freeform and not DUNS.

6. Click **New** for Business ID again and type `01-000000000` as the FreeForm ID.
7. Click **Save**.

Create the second participant:

1. Click **Account Admin > Profiles > Community Participant** and click **Create**.
2. For Company Login Name, type **TP1**
3. For Participant Display Name, type **TP1**
4. For Participant Type, select **Participant**.
5. Click **New** for Business ID and type `000000001` as the Freeform ID.

   Note: Make sure you select Freeform and not DUNS.
6. Click **New** for Business ID again and type `01-000000001` as the Freeform ID.
7. Click **Save**.

Creating the gateways

Create file-directory gateways for both participants in the example. First, create a gateway for the Manager:

1. Click **Account Admin > Profiles > Community Participant** and click **Search**.
2. Click the **View details** icon next to the Manager profile.
3. Click **Gateways** and then **Create**.
4. Enter the following values for the gateway. Remember that the file directory (the entire path) must already exist on your file system.
   a. For Name, type **ManagerFileGateway**.
   b. From the Transport List, select **File Directory**.
   c. For Address, type: **file:///Data/Manager/filegateway**
   d. Click **Save**.
5. Click **List** to list all the gateways for the Community Manager.
6. Click **View Default Gateways**.
7. From the **Production** list, select the gateway you created in step 4.
8. Click **Save**.

Next, create a gateway for the participant.

1. Click **Account Admin > Profiles > Community Participant** and click **Search**.
2. Select the other participant you created for this example by clicking on the **View details** icon next to **TP1**.
3. Click on **Gateways** and then **Create**.
4. Enter the following values for the gateway. Remember that the file directory (the entire path) must already exist.
   a. For Name, type **TP1FileGateway**.
   b. From the Transport list, select **File Directory**.
   c. For Address, type: **file:///Data/TP1/filegateway**
   d. Click **Save**.
5. Click **List** to list all the gateways for the participant.
6. Click **View Default Gateways**.
7. From the **Production** list, select the gateway you created in step 4.
8. Click **Save**.

Setting up B2B capabilities

Enable the B2B capabilities of the two participants in this exchange. In this example, the XML document is originating from the Community Manager and will be delivered to the participant.

1. Click **Account Admin > Profiles > Community Participant** and click **Search**.
2. Click the **View details** icon for the source participant for this example (**ComMan**).
3. Click **B2B Capabilities**.
4. Enable three sets of capabilities for the source participant.
   a. Enable the document flow definition representing the XML document:
      1) Click the **Role is not active** icon under **Set Source** for **Package: None** to enable it.
      2) Expand **Package: None**.
      3) Click the **Role is not active** icon under **Set Source** for **Protocol: FVT-XML-TEST (ALL)**.
      4) Expand **Protocol: FVT-XML-TEST (ALL)**.
      5) Click the **Role is not active** icon under **Set Source** for **Document Flow: ICGCPO (ALL)**.

   b. Next, enable the document flow definition representing the transformed document:
      1) Click the **Role is not active** icon under **Set Source** for **Package: N/A** to enable it.
      2) Expand **Package: N/A**.
      3) Click the **Role is not active** icon under **Set Source** for **Protocol: MX12V3R1(ALL)**.
      4) Expand **Protocol: MX12V3R1 (ALL)**.
      5) Click the **Role is not active** icon under **Set Source** for **Document Flow: 850**.

   c. Then, enable the document flow definition representing the EDI envelope:
      1) Click the **Role is not active** icon under **Set Source** for **Package: N/A** to enable it.
      2) Expand **Package: N/A**.
      3) Click the **Role is not active** icon under **Set Source** for **Protocol EDI-X12 (ALL)**.
      4) Expand **Protocol EDI-X12 (ALL)**.
      5) Click the **Role is not active** icon under **Set Source** for **Document Flow: ISA (ALL)**.
5. Click on **Account Admin > Profiles > Community Participant** and click **Search**.
6. Click the **View details** icon for the target participant for this example (**TP1**).
7. Click **B2B Capabilities**.
8. Enable two sets of capabilities for the target participant.
   a. First, enable the document flow definition representing the EDI 850 transaction:
      1) Click the **Role is not active** icon under **Set Target** for **Package: N/A** to enable it.
      2) Expand **Package: N/A**.

3) Click the **Role is not active** icon under **Set Target** for **Protocol: MX12V3R1 (ALL)**.
4) Expand **Protocol: MX12V3R1 (ALL)**.
5) Click the **Role is not active** icon under **Set Target** for **Document Flow: 850 (ALL)**.

b. Next, enable the document flow definition:
   1) Click the **Role is not active** icon under **Set Target** for **Package: None** to enable it.
   2) Expand **Package: None**.
   3) Click the **Role is not active** icon under **Set Target** for **Protocol: EDI-X12 (ALL)**.
   4) Expand **Protocol: EDI-X12 (ALL)**.
   5) Click the **Role is not active** icon under **Set Target** for **Document Flow: ISA(ALL)**.

Creating the envelope profile

You next create the profile for the envelope that will contain the transformed 850 transaction.

1. Click **Hub Admin > Hub Configuration > EDI > Envelope Profile**.
2. Click **Create**.
3. Type the name of the profile: **EnvProf1**.
4. From the EDI Standard list, select **X12**.
5. The **General** button is selected by default. Type the following values for the general attributes of the envelope:
   - INTCTLLEN: **9**
   - GRPCTLLEN: **9**
   - TRXCTLLEN: **9**
   - MAXDOCS: **1000**
6. Click the **Interchange** button and type the following values for the interchange attributes:
   - ISA01: **01**
   - ISA02: **ISA0000002**
   - ISA03: **02**
   - ISA04: **ISA0000004**
   - ISA11: **U**
   - ISA12: **00301**
   - ISA15: **T**
7. Click **Save**.

Creating the XML format

In this section, you create the custom XML format.

1. Click **Hub Admin > Hub Configuration > XML Formats**.
2. Click **Create XML Format**.
3. For Routing Format, select **FVT-XML-TEST ALL**.
4. For File Type, select **XML**.
5. For Identifier Type, select **Root Tag** and type **MMDoc**.
6. For Source Business Id, select **Constant** and type **000000000**.

7. For Target BusinessId, select **Constant** and type **000000001**.
8. For Source Document Flow, select **Constant** and type **ICGCPO**.
9. For Source Document Flow Version, select **Constant** and type **ALL**.
10. Click **Save**.

Activating the connections

Activate the participant connections:

1. Click **Account Admin > Participant Connections**.
2. Select **Manager** from the Source list.
3. Select **TP1** from the Target list.
4. Click **Search**.
5. Click **Activate** for the following connection:

Table 30. XML document to EDI transaction connection

Source	Target
Package: None (N/A) Protocol: FVT-XML-TEST (ALL) Document Flow: ICGCPO (ALL)	Package: N/A (N/A) Protocol: MX12V3R1 (ALL) Document Flow: 850 (ALL)

6. Click **Activate** for the connection that represents the EDI envelope:

Table 31. EDI envelope connection

Source	Target
Package: N/A (N/A) Protocol: EDI-X12 (ALL) Document Flow: ISA (ALL)	Package: None (N/A) Protocol: EDI-X12 (ALL) Document Flow: ISA (ALL)

Configuring attributes

Configure the B2B Capabilities attributes of the target participant (TP1) and the source participant (Manager):

1. Click **Account Admin > Profiles > Community Participant** and click on **Search**.
2. Click the **View details** icon next to **TPI** to select it.
3. Click **B2B Capabilities**.
4. Click the **Expand** icon next to **Package: N/A**.
5. Click the **Edit** icon next to **Protocol: MX12V3R1**.
6. Specify the following attributes:
   a. In the Envelope Profile row, select **EnvProf1** from the list.
   b. In the Interchange qualifier row, type **01**.
   c. In the Interchange identifier row, type **000000001**.
   d. In the Interchange usage indicator row, type **T**.
7. Click **Save**.
8. Click **Account Admin > Profiles > Community Participant** and click on **Search**.
9. Click the View details next to **Manager** to select it.
10. Click **B2B Capabilities**.
11. Click the **Expand** icon next to **Package: N/A**.
12. Click the **Edit** icon next to **Protocol: MX12V3R1 (ALL)**.

13. Specify the following attributes:
    a. In the Interchange qualifier row, type **01**.
    b. In the Interchange identifier row, type **000000000**.
    c. In the Interchange usage indicator row, type **T**.
14. Click **Save**.

At this point, if the source participant (the Community Manager) sent an XML document to the participant, it would be translated (at the hub) to an EDI transaction, enveloped, and then sent to the participant's gateway.

ROD to EDI example

This section provides an example of the Community Manager sending a ROD document to the hub, where it is transformed into an EDI transaction, enveloped within an EDI interchange, and sent to a participant.

In this example, it is assumed that the Data Interchange Services mapping specialist has created a transformation map that takes a a record-oriented document (ROD) and transforms it into a standard EDI 850 transaction (defined with the X12V5R1 dictionary, corresponding to the version 5010 of X12) that will be processed by the participant. In this example, the map is named S_DT_ROD_TO_EDI.eif.

The Data Interchange Services mapping specialist can export the transformation map directly to the WebSphere Partner Gateway database. Alternatively, the Data Interchange Services mapping specialist can send you the file, in which case you use the bcgDISImport utility to import it into WebSphere Partner Gateway. This appendix assumes the second scenario.

Importing the transformation map

This section describes the steps you take to import a transformation map that will take ROD input and transform it into an X12 transaction. In the process of importing the transformation map, you also import the document definition associated with the map.

Before you can import the transformation map, the Data Interchange Services mapping specialist must send it to you. This set of steps assumes that the file, S_DT_ROD_TO_EDI.eif, is on your system.

1. Open a command window.
2. Enter the following command or script:
    - On a UNIX system:

      ```
      <ProductDir>/bin/bcgDISImport.sh <database_user_ID>
       <password> S_DT_ROD_TO_EDI.eif
      ```
    - On a Windows system:

      ```
      <ProductDir>\bin\bcgDISImport.bat <database_user_ID>
       <password> S_DT_ROD_TO_EDI.eif
      ```

      where *<database_user_ID>* and *<password>* are the values that you used when you installed the database as part of the WebSphere Partner Gateway installation.

Verifying the transformation map and document flow definitions

To verify that the transformation maps and document definitions you imported are available on the Community Console, perform the following steps:

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

   The S_DT_ROD_TO_EDI map is displayed.
2. Click the **View details** icon next to the map.

   You see the document flow definitions with which this map is associated:

Table 32. Document flow definitions associated with the map

Source	Target
Package: None Protocol: ROD-TO-EDI_DICT (ALL) Document Flow: DTROD-TO-EDI_ROD (ALL)	Package: N/A Protocol: X12V5R1(ALL) Document Flow: 850 (ALL)

The S_DT_ROD_TO_EDI map was defined to take a ROD document associated with the ROD-TO-EDI_DICT dictionary and transform it to an X12 850 transaction that conforms to the X12V5R1 standard.

Configuring the target

In this section, you create a file-system directory target for the hub:

1. Click **Hub Admin > Hub Configuration > Targets** and click **Create Target**.
2. For Target Name, type: **RODFileTarget**
3. From the Transport list, select **File Directory**.
4. For Root Path, type: **/Data/Manager/rodtarget**
5. From the Configuration Point list, select **Preprocess**.
6. Select **com.ibm.bcg.edi.receiver.preprocesshandler.RODSplitterHandler** from the Available List and click **Add** to move it to the Configured List.
7. Select **com.ibm.bcg.edi.receiver.preprocesshandler.RODSplitterHandler** from the Configured List and click **Configure**.
8. Add the values shown in table:

Table 33. ROD Splitter Handler attributes

Field	Value
From Packaging Name	None
From Packaging Version	N/A
From Protocol Name	ROD-TO-EDI_DICT
From Protocol Version	ALL
From Process Code	DTROD-TO-EDI_ROD
From Process Version	ALL
METADICTIONARY	ROD-TO-EDI_DICT
METADOCUMENT	DTROD-TO-EDI_ROD
METASYNTAX	rod
ENCODING	ascii
BCG_BATCHDOCS	ON

9. Click **Set Values**.
10. Click **Save**.

The Community Manager sends the ROD document to this target.

Creating the interactions

You create two interactions--one for the EDI envelope that will be sent from the hub and one for the transformation of the ROD document to EDI.

Create an interaction that has a source that represents the ROD document and a target the represents the X12 document.

1. Click **HubAdmin > Hub Configuration > Document Flow Definition**.
2. Click **Manage Interactions** and then **Create Interaction**.
3. Expand **Package: None** and **Protocol: ROD-TO-EDI_DICT** and select **DTROD-TO-EDI_ROD**.
4. Expand **Package: N/A** and **Protocol: X12V5R1** and select **Document Flow: 850**.
5. From the Transformation Map list, select **S_DT_ROD_TO_EDI**.
6. From the Action list, select **ROD Translate and EDI Validate**.
7. Click **Save**.

This interaction represents the transformation of a ROD document into a standard X12 transaction and, therefore, you must select a transformation map.

Create an interaction that represents the EDI envelope.

1. Click **HubAdmin > Hub Configuration > Document Flow Definition**.
2. Click **Manage Interactions** and then **Create Interaction**.
3. Expand **Package: N/A** and **Protocol: EDI-X12** and select **Document Flow: ISA**.
4. Expand **Package: None** and **Protocol: EDI-X12** and select **Document Flow: ISA.**
5. From the Action list, select **Pass Through**.

   Note: No transformation is occurring in this interaction. This interaction is to envelope the EDI interchange.
6. Click **Save**.

Creating the participants

For this example, you have two participants: the Community Manager (Manager) and a participant (TP1).

Create the Community Manager profile:

1. Click **Account Admin > Profiles > Community Participant** and click **Create**.
2. For Company Login Name, type: **ComManager**
3. For Participant Display Name: type **Manager**
4. For Participant Type, select **Community Manager**.
5. Click **New** for Business ID and type `000000000` as the Freeform ID.

   Note: Make sure you select Freeform and not DUNS.
6. Click **New** again for Business ID and type `01-000000000` as the Freeform ID.
7. Click **Save**.

Create the second participant:

1. Click **Account Admin > Profiles > Community Participant** and click **Create**.
2. For Company Login Name, type **TP1**
3. For Participant Display Name, type **TP1**
4. For Participant Type, select **Community Participant**.
5. Click **New** for Business ID and type `000000001` as the Freeform ID.

   Note: Make sure you select Freeform and not DUNS.
6. Click **New** again for Business ID and type `01-000000001` as the Freeform ID.
7. Click **Save**.

Creating the gateways

Create file-directory gateways for both participants in the example. First, create a gateway for the Manager:

1. Click **Account Admin > Profiles > Community Participant** and click **Search**.
2. Click the **View details** icon next to the Manager profile.
3. Click **Gateways** and then **Create**.
4. Enter the following values for the gateway. Remember that the file directory (the entire path) must already exist on your file system.
   a. For Name, type **ManagerFileGateway**.
   b. From the Transport List, select **File Directory**.
   c. For Address, type: **file:///Data/Manager/filegateway**
   d. Click **Save**.
5. Click **List** to list all the gateways for the Community Manager.
6. Click **View Default Gateways**.
7. From the **Production** list, select the gateway you created in step 4
8. Click **Save**.

Next, create a gateway for the participant.

1. Click **Account Admin> Profiles > Community Participant** and click **Search**.
2. Select the other participant you created for this example by clicking on the **View details** icon next to **TP1**.
3. Click on **Gateways** and then **Create**.
4. Enter the following values for the gateway. Remember that the file directory (the entire path) must already exist.
   a. For Name, type **TP1FileGateway**.
   b. From the Transport list, select **File Directory**.
   c. For Address, type: **file:///Data/TP1/filegateway**
   d. Click **Save**.
5. Click **List** to list all the gateways for the participant.
6. Click **View Default Gateways**.
7. From the **Production** list, select the gateway you created in step 4.
8. Click **Save**.

Setting up B2B capabilities

Enable the B2B capabilities of the two participants in this exchange. In this example, the ROD document is originating from the Community Manager and will be delivered to the participant (TP1).

1. Click on **Account Admin > Profiles > Community Participant** and click **Search**.
2. Click the **View details** icon for the source participant for this example (**Manager**).
3. Click **B2B Capabilities**.
4. Enable two sets of capabilities for the source participant.
   a. First, enable the document flow definition representing the ROD document:
      1) Click the **Role is not active** icon under **Set Source** for **Package: None** to enable it.
      2) Expand **Package: None**.
      3) Click the **Role is not active** icon under **Set Source** for **Protocol: ROD-TO-EDI_DICT (ALL)**.
      4) Expand **Protocol: ROD-TO-EDI_DICT (ALL)**.
      5) Click the **Role is not active** icon under **Set Source** for **Document Flow: DTROD-TO-EDI_ROD (ALL)**.
   b. Next, enable the document flow definition representing the EDI envelope:
      1) Click the **Role is not active** icon under **Set Source** for **Package: N/A** to enable it.
      2) Expand **Package: N/A**.
      3) Click the **Role is not active** icon under **Set Source** for **Protocol EDI-X12 (ALL)**.
      4) Expand **Protocol EDI-X12 (ALL)**.
      5) Click the **Role is not active** icon under **Set Source** for **Document Flow: ISA (ALL)**.
5. Click on **Account Admin > Profiles > Community Participant** and click **Search**.
6. Click the **View details** icon for the target participant for this example (**TP1**).
7. Click **B2B Capabilities**.
8. Enable two sets of capabilities for the target participant.
   a. First, enable the document flow definition representing the EDI 850 transaction:
      1) Click the **Role is not active** icon under **Set Target** for **Package: N/A** to enable it.
      2) Expand **Package: N/A**.
      3) Click the **Role is not active** icon under **Set Target** for **Protocol: X12V5R1 (ALL)**.
      4) Expand **Protocol: X12V5R1 (ALL)**.
      5) Click the **Role is not active** icon under **Set Target** for **Document Flow: 850 (ALL)**.
   b. Next, enable the document flow definition representing the envelope:
      1) Click the **Role is not active** icon under **Set Target** for **Package: None** to enable it.
      2) Expand **Package: None**.

3) Click the **Role is not active** icon under **Set Target** for **Protocol: EDI-X12 (ALL)**.
4) Expand **Protocol: EDI-X12 (ALL)**.
5) Click the **Role is not active** icon under **Set Target** for **Document Flow: ISA (ALL)**.

Creating the envelope profile

You next create the profile for the envelope that will contain the transformed 850 transaction.

1. Click **Hub Admin > Hub Configuration > EDI > Envelope Profile**.
2. Click **Create**.
3. Type the name of the profile: **EnvProf1**.
4. From the EDI Standard list, select **X12**.
5. The **General** button is selected by default. Type the following values for the general attributes of the envelope:
   - INTCTLLEN: **9**
   - GRPCTLLEN: **9**
   - TRXCTLLEN: **9**
   - MAXDOCS: **1000**
6. Click the **Interchange** button and type the following values for the interchange attributes:
   - ISA01: **01**
   - ISA02: **ISA0000002**
   - ISA03: **02**
   - ISA04: **ISA0000004**
   - ISA11: \
   - ISA12: **00501**
   - ISA15: **T**
7. Click **Save**.

Activating the connections

To activate the connections:

1. Click **Account Admin > Participant Connections**.
2. Select **Manager** from the Source list.
3. Select **TP1** from the Target list.
4. Click **Search**.
5. Click **Activate** for the connection that represents the ROD document to EDI transaction:

Table 34. ROD to EDI connection

Source	**Target**
Package: N/A (N/A) Protocol: ROD-TO-EDI_DICT (ALL) Document Flow: DTROD-TO-EDI_ROD (ALL)	Package: None (N/A) Protocol: X12V5R1 (ALL) Document Flow: 850

6. Click **Activate** for the connection that represents the envelope:

Table 35. Envelope connection

Source	Target
Package: None (N/A) Protocol: EDI-X12 (ALL) Document Flow: ISA (ALL)	Package: N/A (N/A) Protocol: EDI-X12 (ALL) Document Flow: ISA(ALL)

Configuring attributes

To specify attributes for the envelope profile:

1. Click **Account Admin > Profiles > Community Participant** and click **Search**.
2. Select **TP1** from the list.
3. Click **B2B Capabilities**.
4. Click the **Expand** icon next to **Package: N/A**.
5. Click the **Edit** icon next to **Protocol: X12V5R1**.
6. Specify the following attributes:
   a. In the Envelope Profile row, select **EnvProf1** from the list.
   b. In the Interchange qualifier row, type **01**.
   c. In the Interchange identifier row, type **000000001**.
   d. In the Interchange usage indicator row, type **T**.
7. Click **Save**.

At this point, if the Community Manager sent a ROD document to the hub, the document would be transformed to an 850 transaction, which would then be enveloped and sent to the gateway of the participant.

Appendix C. Additional RosettaNet information

This appendix gives you additional information about RosettaNet support. It includes the following topics:

- "Deactivating PIPs"
- "Providing failure notification"
- "Creating PIP document flow packages" on page 219
- "PIP document flow package contents" on page 230

Deactivating PIPs

After a PIP package has been uploaded into WebSphere Partner Gateway, it cannot be removed. However, you can deactivate the PIP so that it cannot be used.

To deactivate a PIP for all communications with participants, perform the following steps:

1. Click **Hub Admin > Hub Configuration > Document Flow Definition**.
2. Expand the document flow definitions to reveal the Document Flow of the PIP you want to disable.
3. In the Status column of the package, click **Enabled**. The Status column now displays **Disabled**, and WebSphere Partner Gateway cannot use the document flow definition for the PIP.

To deactivate a PIP communication with a specific participant, deactivate the connection to the participant defined for the PIP.

Providing failure notification

This section describes failure notification.

0A1 PIP

If a failure occurs during the processing of a PIP message, WebSphere Partner Gateway uses the 0A1 PIP as the mechanism to broadcast the failure to the participant or back-end system that sent the message. For example, say a back-end system initiates a 3A4 PIP. WebSphere Partner Gateway processes the RNSC message and sends a RosettaNet message to a participant. WebSphere Partner Gateway waits for the response to the RosettaNet message until the waiting time reaches the timeout limit. After this occurs, WebSphere Partner Gateway creates a 0A1 PIP and sends it to the participant. The 0A1 PIP identifies the exception condition so that the participant can then compensate for the failure of the 3A4 PIP.

To provide failure notification, upload a 0A1 package and create a PIP connection to the participant using this package.

Updating contact information

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

© Copyright IBM Corp. 2004, 2005

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

- **bcg.0A1.fromContactName**
- **bcg.0A1.fromEMailAddr**
- **bcg.0A1.fromPhoneNbr**
- **bcg.0A1.fromFaxNbr**

The telephone numbers are limited to 30 bytes in length. The other fields are unlimited in length. When the values are changed, the Document Manager must be restarted.

Editing RosettaNet attribute values

For RosettaNet support, an action type document flow definition has a specific set of attributes. These attributes provide information used to validate the PIP message, to define the roles and services used in the PIP, and to define the response to the action. The PIP packages provided by WebSphere Partner Gateway automatically define values for these attributes and you typically do not need to change them.

To edit the RosettaNet attributes of an action document flow definition, perform the following steps:

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

Table 36. RosettaNet attributes

RosettaNet attribute	Description
DTD Name	Identifies the name of the action of the PIP in the DTD provided by RosettaNet
From Service	Contains the network component service name of the participant or back-end system that is sending the message
To Service	Contains the network component service name of the participant or back-end system that is receiving the message
From Role	Contains the role name of the participant or back-end system that is sending the message
To Role	Contains the role name of the participant or back-end system that is receiving the message
Root Tag	Contains the name of the root element in the XML document associated with the PIP
Response From Action Name	Identifies the next Action to perform in the PIP

Note: If the Console displays the `No attributes were found` message, the attributes have not been defined.

5. If the Console displays this message for a lower-level definition, the definition might still work, because it inherits the attributes of the higher-level definition. Adding attributes and their values overrides the inherited attributes and changes the function of the document flow definition.
6. Click **Save**.

Creating PIP document flow packages

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

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

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

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

- Creating the XSD files
- Creating the XML file
- Creating the packages

Creating the XSD files

A PIP document flow package contains XML schema files that define message formats and acceptable values for elements. The following procedure describes how to create these files based on the contents of the PIP specification file.

You create at least one XSD file for each DTD file in the PIP specification file. For the example of upgrading to PIP 5C4 V01.03.00, because the message format changed, the procedure describes how to create the BCG_5C4RegistrationStatusNotification_V01.03.xsd file as an example. For information about the XSD files, see “About validation” on page 229.

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

1. Import or load the DTD file into an XML editor such as WebSphere Studio Application Developer. For example, load the 5C4_MS_V01_03_RegistrationStatusNotification.dtd file.
2. Using the XML editor, convert the DTD into an XML schema. The following steps describe how to do this using Application Developer:
   a. In the Navigation pane of the XML perspective, open the project containing the imported DTD file.
   b. Right click the DTD file and select **Generate > XML Schema**.
   c. In the Generate panel, type or select where you want to save the new XSD file. In the File name field, type the name of the new XSD file. In the case of the example, you would type a name such as BCG_5C4RegistrationStatusNotification_V01.03.xsd.
   d. Click **Finish**.
3. Compensate for elements that have multiple cardinality values in the RosettaNet XML guidelines by adding specifications to the new XSD file. The guidelines show the elements in the message using a tree and displaying the cardinality of each element to the left of the element.

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

   1 contactName

   0..1 EmailAddress

   0..1 facsimileNumber

   0..1 PhysicalLocation

   0..1 telephoneNumber

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

   1 contactName

   1 EmailAddress

   0..1 facsimileNumber

   1 telephoneNumber

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

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

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

a. Delete the definition of the element. For example, delete the ContactInformation element.

b. Open the PIP document flow package of the version being replaced. For example, open the BCG_Package_RNIFV02.00_5C4V01.02.zip file.

c. Find the definition you want to reuse. For example, the ContactInformation_type7 definition in the BCG_ContactInformation_Types.xsd file matches the definition you need for line 15 of the guidelines.

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

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

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

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

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

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

a. Delete the definition of the element. For example, delete the ContactInformation element.

b. Create the replacement definition. For example, create the ContactInformation_localType1 definition to match the definition in line 15 of the guidelines.

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

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

name="ContactInformation"
type="ContactInformation_localType1"

Figure 35 shows the productProviderFieldApplicationEngineer element before it is modified.

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

Figure 35. Element productProviderFieldApplicationEngineer before modification

Figure 36 shows the productProviderFieldApplicationEngineer element after it is modified.

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

Figure 36. Element productProviderFieldApplicationEngineer after modification

4. Specify the enumeration values for elements that can only have specific values. The guidelines define the enumeration values in the tables in the Guideline Information section.

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

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

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

      ```
      <xsd:simpleType name="_GlobalRegistrationComplexityLevelCode">
        <xsd:restriction base="xsd:string">
          <xsd:enumeration value="Above average"/>
          <xsd:enumeration value="Average"/>
          <xsd:enumeration value="Maximum"/>
          <xsd:enumeration value="Minimum"/>
      ```

```
      <xsd:enumeration value="None"/>
      <xsd:enumeration value="Some"/>
    </xsd:restriction>
  </xsd:simpleType>
```

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

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

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

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

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

a. Delete the definition of the element. For example, delete the GlobalRegistrationComplexityLevelCode element.

b. Create the replacement definition. For example, create the GlobalRegistrationComplexityLevelCode_localType definition and include the enumeration value definitions as described by the table.

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

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

```
name="GlobalRegistrationComplexityLevelCode"
type="GlobalRegistrationComplexityLevelCode_localType"
```

Figure 37 on page 224 shows the Element DesignAssemblyInformation element before it is modified.

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

Figure 37. Element DesignAssemblyInformation before modification

Figure 38 shows the Element DesignAssemblyInformation after it was modified.

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

      <xsd:element maxOccurs="1" minOccurs="0"
         ref="GlobalRegistrationInvolvementLevelCode"/>
      <xsd:element maxOccurs="1" minOccurs="0"
         ref="RegistrationStatus"/>
    </xsd:sequence>
  </xsd:complexType>
</xsd:element>
```

Figure 38. Element DesignAssemblyInformation after modification

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

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

   a. Delete the definition for the data entity element. For example, delete the DateStamp element.

b. Open the PIP document flow package of the version you are replacing. For example, open the BCG_Package_RNIFV02.00_5C4V01.02.zip file.

c. Find the definition you want to reuse. For example, the _common_DateStamp_R definition in the BCG_common.xsd file contains the following definition, which complies with the information given in the guidelines.

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

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

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

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

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

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

a. Delete the definition of the element. For example, delete the DateStamp element.

b. Create the replacement definition. For example, use the data type, minimum length, maximum length, and representation information to create the DateStamp_localType definition.

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

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

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

Figure 39 shows the Element beginDate before it is modified.

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

Figure 39. Element beginDate before modification

Figure 40 on page 226 shows the Element beginDate after it is modified.

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

Figure 40. Element beginDate after modification

Creating the XML file

After you have created the XSD files for your PIP document flow package, you are ready to create the XML file for the RNIF package and the XML file for the Backend Integration package. For example, these packages are called BCG_Package_RNIFV02.00_5C4V01.03.zip and BCG_Package_RNSC1.0_RNIFV02.00_5C4V01.03.zip. The following procedure describes how to create the XML file for the RNIF package:

1. Extract the XML file from an RNIF PIP document flow package file. If you are upgrading, extract the file from the previous version of the package (for example, BCG_Package_RNIFV02.00_5C4V01.02.zip). If you are creating a new package, extract the file from a PIP document flow package that is similar to the one you are creating. For example, if you are creating a package to support a two-action PIP, copy the XML file from another two-action PIP package.
2. Copy the file and rename it appropriately (for example, BCG_RNIFV02.00_5C4V01.03.xml).
3. In the new file, update the elements that contain information about the PIP. For example, the following table lists the information you need to update in the 5C4 PIP example. Note that the information might appear more than once in the file. Make sure that you update all instances.

Table 37. 5C4 PIP update information

Information to change	Old value	New value
PIP ID	5C4	5C4
Version of the PIP	V01.02	V01.03
The name of the request message DTD file without the file extension	5C4_MS_V01_02_ RegistrationStatusNotification	5C4_MS_V01_03_ RegistrationStatusNotification
The name of the confirmation message DTD file without the file extension (for two-action PIPs only)	N/A	N/A
The name of the request message XSD file without the file extension	BCG_5C4RegistrationStatus Notification_V01.02	BCG_5C4RegistrationStatus Notification_V01.03
The name of the confirmation message XSD file without the file extension (for two-action PIPs only)	N/A	N/A

Table 37. 5C4 PIP update information (continued)

Information to change	Old value	New value
Root element name in the XSD file for the request message	Pip5C4RegistrationStatus Notification	Pip5C4RegistrationStatus Notification
Root element name in the XSD file for the confirmation message (for two-action PIPs only)	N/A	N/A

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

Table 38. 5C4 PIP update information from the PIP specification

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

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

   Note: If you are creating the Backend Integration package, skip this step and go to step 6 on page 228.

Table 39. 5C4 PIP attribute updates

Information to update	Description	Value in the 5C4 package	Element path in the XML file
NonRepudiation Required	Specified in Table 3-3	N	ns1:Package ns1:Protocol ns1:Process ns1:Attribute (Its ATTRIBUTEKEY is NonRepudiationRequired) ns1:AttributeValue AttributePickListItem ATTRVALUEKEY
NonRepudiationOf Receipt	Specified in Table 3-3	N	ns1:Package ns1:Protocol ns1:Process ns1:Attribute (Its ATTRIBUTEKEY is NonRepudiationOfReceipt) ns1:AttributeValue AttributePickListItem ATTRVALUEKEY

Table 39. 5C4 PIP attribute updates (continued)

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

6. Update the ns1:Package/ns1:Protocol/GuidelineMap elements to remove unused XSD files and to add any XSD files you created or referenced.

To create the Backend Integration package, repeat step 1 through 6 except for the following differences:

- In step 1 on page 226, extract the XML file from the Backend Integration package (for example, BCG_Package_RNSC1.0_RNIFV02.00_5C4V01.02.zip).
- Do not do step 5 on page 227.

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

Creating the package

To create the RNIF package, perform the following steps:

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

To create the Backend Integration package, perform steps 1 through 3 but use the Backend Integration XML file instead of the RNIF file.

After you have created the PIP package, you can upload it using the procedure in “RNIF and PIP document flow packages” on page 61.

About validation

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

Because RosettaNet specifies the format of a PIP message, typically you will not need to customize the validation maps. However, if you do, see “Creating PIP document flow packages” on page 219 for information about the steps needed to upgrade the XSD files used to validate the messages and how to create a custom PIP document flow package.

Cardinality

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

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

If WebSphere Partner Gateway does not need to check the cardinality of an element, the values of the element’s minOccurs and maxOccurs attributes in the validation map are ″0″ and ″unbounded″, as shown in the following example:

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

Format

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

Example 1

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

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

Example 2

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

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

Example 3

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

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

Enumeration

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

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

All _local_GlobalDesignRegistrationNotificationCode type elements in a message must have only ″Initial″ or ″Update″ for their values.

PIP document flow package contents

The following sections show the PIP document flow packages provided by WebSphere Partner Gateway for each PIP. Within each package is an XML file contained in a Packages directory and several XSD files contained in a GuidelineMaps directory, which are common to all PIP document flow packages for the PIP.

0A1 Notification of Failure V1.0

The following section describes the contents for the 0A1 Notification of Failure V1.0 PIP.

Package file contents

The following table shows the ZIP files and corresponding XML files for the 0A1 Notification of Failure V1.0 PIP. The guideline maps, which are common to all versions, are shown in the section that follows.

Table 40. 0A1 Notification of Failure V1.0 PIP ZIP and XML files

ZIP file name	XML file name
BCG_Package_RNIF1.1_0A11.0.zip	BCG_RNIF1.1_0A11.0.xml
BCG_Package_RNSC1.0_RNIF1.1_0A11.0.zip	BCG_RNSC1.0_RNIF1.1_0A11.0.xml

Guideline map contents

This section lists the guideline maps contents for 0A1 Notification of Failure V1.0:

- 0A1FailureNotification_1.0.xml
- BCG_0A1FailureNotification_1.0.xsd
- BCG_common.xsd
- BCG_GlobalPartnerClassificationCode.xsd
- BCG_GlobalPartnerRoleClassificationCode.xsd
- BCG_string_len_0.xsd
- BCG_xml.xsd

0A1 Notification of Failure V02.00

The following section describes the contents for the 0A1 Notification of Failure V02.00 PIP.

Package file contents

The following table shows the ZIP files and corresponding XML files for the 0A1 Notification of Failure V02.00 PIP. The guideline maps, which are common to all versions, are shown in the section that follows.

Table 41. 0A1 Notification of Failure V02.00 PIP ZIP and XML files

ZIP file name	XML file name
BCG_Package_RNIFV02.00_0A1V02.00.zip	BCG_RNIFV02.00_0A1V02.00.xml
BCG_Package_RNSC1.0_RNIFV02.00_0A1V02.00.zip	BCG_RNSC1.0_RNIFV02.00_0A1V02.00.xml

Guideline map contents

This section lists the guideline maps contents for 0A1 Notification of Failure V02.00:

- 0A1FailureNotification_V02.00.xml
- BCG_0A1FailureNotification_V02.00.xsd
- BCG_common.xsd
- BCG_GlobalPartnerClassificationCode.xsd
- BCG_GlobalPartnerRoleClassificationCode.xsd
- BCG_string_len_0.xsd
- BCG_xml.xsd

2A1 Distribute New Product Information

The following section describes the contents for the 2A1 Distribute New Product Information PIP.

Package file contents

The following table shows the ZIP files and corresponding XML files for the 2A1 Distribute New Product Information PIP. The guideline maps, which are common to all versions, are shown in the section that follows.

Table 42. 2A1 Distribute New Product Information ZIP and XML files

ZIP file name	XML file name
BCG_Package_RNIF1.1_2A1V02.00.zip	BCG_RNIF1.1_2A1V02.00.xml
BCG_Package_RNIFV02.00_2A1V02.00.zip	BCG_RNIFV02.00_2A1V02.00.xml
BCG_Package_RNSC1.0_RNIF1.1_2A1V02.00.zip	BCG_RNSC1.0_RNIF1.1_2A1V02.00.xml
BCG_Package_RNSC1.0_RNIFV02.00_2A1V02.00.zip	BCG_RNSC1.0_RNIFV02.00_2A1V02.00.xml

Guideline map contents

This section lists the guideline maps contents for 2A1 Distribute New Product Information:

- BCG_2A1ProductCatalogInformationNotification_V02.00.xsd
- BCG_BusinessDescription_Types.xsd
- BCG_BusinessDescription_Types_V422.xsd
- BCG_BusinessDescription_Types_V43.xsd
- BCG_BusinessTaxIdentifier_Types.xsd
- BCG_common.xsd
- BCG_common_V422.xsd
- BCG_common_V43.xsd
- BCG_ContactInformation_Types.xsd
- BCG_ContactInformation_Types_V422.xsd
- BCG_ContactInformation_Types_V43.xsd
- BCG_GlobalCountryCode.xsd
- BCG_GlobalCurrencyCode.xsd
- BCG_GlobalDocumentReferenceTypeCode.xsd
- BCG_GlobalIntervalCode.xsd
- BCG_GlobalLeadTimeClassificationCode_V43.xsd
- BCG_GlobalMonetaryAmountTypeCode.xsd
- BCG_GlobalPackageTypeCode_V422.xsd
- BCG_GlobalPartnerClassificationCode_V43.xsd
- BCG_GlobalPartnerRoleClassificationCode_V422.xsd
- BCG_GlobalPriceTypeCode_V43.xsd
- BCG_GlobalProductAssociationCode_V43.xsd
- BCG_GlobalProductLifeCycleStatusCode.xsd
- BCG_GlobalProductProcurementTypeCode_V43.xsd
- BCG_GlobalProductTypeCode_V43.xsd
- BCG_GlobalProductUnitofMeasureCode_V43.xsd
- BCG_GlobalProprietaryProductIdentificationTypeCode_V43.xsd
- BCG_GlobalStandardClassificationSchemeCode_V43.xsd
- BCG_GlobalWarrantyTypeCode_V43.xsd
- BCG_InvoiceChargeTypeCode_V422.xsd
- BCG_NationalExportControlClassificationCode.xsd
- BCG_PartnerDescription_Types_V43.xsd
- BCG_PhysicalAddress_Types.xsd
- BCG_PhysicalAddress_Types_V422.xsd
- BCG_string_len_0.xsd

- BCG_xml.xsd

2A12 Distribute Product Master

The following section describes the contents for the 2A12 Distribute Product Master PIP.

Package file contents

The following table shows the ZIP files and corresponding XML files for the 2A12 Distribute Product Master PIP. The guideline maps, which are common to all versions, are shown in the section that follows.

Table 43. 2A12 Distribute Product Master ZIP and XML files

ZIP file name	XML file name
BCG_Package_RNIF1.1_2A12V01.03.zip	BCG_RNIF1.1_2A12V01.03.xml
BCG_Package_RNIFV02.00_2A12V01.03.zip	BCG_RNIFV02.00_2A12V01.03.xml
BCG_Package_RNSC1.0_RNIF1.1_2A12V01.03.zip	BCG_RNSC1.0_RNIF1.1_2A12V01.03.xml
BCG_Package_RNSC1.0_RNIFV02.00_2A12V01.03.zip	BCG_RNSC1.0_RNIFV02.00_2A12V01.03.xml

Guideline map contents

This section lists the guideline maps contents for 2A12 Distribute Product Master:

- BCG_2A12ProductMasterNotification_V01.03.xsd
- BCG_BusinessDescription_Types.xsd
- BCG_BusinessTaxIdentifier_Types.xsd
- BCG_common.xsd
- BCG_ContactInformation_Types.xsd
- BCG_GlobalAssemblyLevelCode.xsd
- BCG_GlobalCountryCode.xsd
- BCG_GlobalIntervalCode.xsd
- BCG_GlobalLeadTimeClassificationCode.xsd
- BCG_GlobalPartnerClassificationCode.xsd
- BCG_GlobalPartnerRoleClassificationCode.xsd
- BCG_GlobalProductLifeCycleStatusCode.xsd
- BCG_GlobalProductProcurementTypeCode.xsd
- BCG_GlobalProductUnitOfMeasureCode.xsd
- BCG_PartnerDescription_Types.xsd
- BCG_PhysicalAddress_Types.xsd
- BCG_string_len_0.xsd
- BCG_xml.xsd

3A1 Request Quote

The following section describes the contents for the 3A1 Request Quote PIP.

Package file contents

The following table shows the ZIP files and corresponding XML files for the 3A1 Request Quote PIP. The guideline maps, which are common to all versions, are shown in the section that follows.

Table 44. 3A1 Request Quote PIP ZIP and XML files

ZIP file name	XML file name
BCG_Package_RNIF1.1_3A1V02.00.zip	BCG_RNIF1.1_3A1V02.00.xml
BCG_Package_RNIFV02.00_3A1V02.00.zip	BCG_RNIFV02.00_3A1V02.00.xml
BCG_Package_RNSC1.0_RNIF1.1_3A1V02.00.zip	BCG_RNSC1.0_RNIF1.1_3A1V02.00.xml
BCG_Package_RNSC1.0_RNIFV02.00_3A1V02.00.zip	BCG_RNSC1.0_RNIFV02.00_3A1V02.00.xml

Guideline map contents

This section lists the guideline maps contents for 3A1 Request Quote:

- BCG_3A1QuoteConfirmation_V02.00.xsd
- BCG_3A1QuoteRequest_V02.00.xsd
- BCG_BusinessDescription_Types.xsd
- BCG_BusinessTaxIdentifier_Types.xsd
- BCG_common.xsd
- BCG_ContactInformation_Types.xsd
- BCG_GlobalCountryCode.xsd
- BCG_GlobalCurrencyCode.xsd
- BCG_GlobalGovernmentPriorityRatingCode.xsd
- BCG_GlobalMonetaryAmountTypeCode.xsd
- BCG_GlobalPartnerClassificationCode.xsd
- BCG_GlobalPartnerRoleClassificationCode.xsd
- BCG_GlobalProductSubstitutionReasonCode.xsd
- BCG_GlobalProductTermsCode.xsd
- BCG_GlobalProductUnitOfMeasureCode.xsd
- BCG_GlobalQuoteLineItemStatusCode.xsd
- BCG_GlobalQuoteTypeCode.xsd
- BCG_GlobalStockIndicatorCode.xsd
- BCG_GlobalTaxExemptionCode.xsd
- BCG_PartnerDescription_Types.xsd
- BCG_PhysicalAddress_Types.xsd
- BCG_string_len_0.xsd
- BCG_xml.xsd

3A2 Request Price and Availability

The following section describes the contents for the 3A2 Request Price and Availability PIP.

Package file contents

The following table shows the ZIP files and corresponding XML files for the 3A2 Request Price and Availability PIP. The guideline maps, which are common to all versions, are shown in the section that follows.

Table 45. 3A2 Request Price and Availability ZIP and XML files

ZIP file name	XML file name
BCG_Package_RNIF1.1_3A2R02.01.zip	BCG_RNIF1.1_3A2R02.01.xml
BCG_Package_RNIFV02.00_3A2R02.01.zip	BCG_RNIFV02.00_3A2R02.01.xml

Table 45. 3A2 Request Price and Availability ZIP and XML files (continued)

ZIP file name	XML file name
BCG_Package_RNSC1.0_RNIF1.1_3A2R02.01.zip	BCG_RNSC1.0_RNIF1.1_3A2R02.01.xml
BCG_Package_RNSC1.0_RNIFV02.00_3A2R02.01.zip	BCG_RNSC1.0_RNIFV02.00_3A2R02.01.xml

Guideline map contents

This section lists the guideline maps contents for 3A2 Request Price and Availability:

- BCG_3A2PriceAndAvailabilityRequest_R02.01.xsd
- BCG_3A2PriceAndAvailabilityResponse_R02.01.xsd
- BCG_BusinessDescription_Types.xsd
- BCG_BusinessTaxIdentifier_Types.xsd
- BCG_common.xsd
- BCG_ContactInformation_Types.xsd
- BCG_GlobalCountryCode.xsd
- BCG_GlobalCurrencyCode.xsd
- BCG_GlobalCustomerAuthorizationCode.xsd
- BCG_GlobalPartnerClassificationCode.xsd
- BCG_GlobalPricingTypeCode.xsd
- BCG_GlobalProductAvailabilityCode.xsd
- BCG_GlobalProductStatusCode.xsd
- BCG_GlobalProductSubstitutionReasonCode.xsd
- BCG_GlobalProductUnitOfMeasureCode.xsd
- BCG_PartnerDescription_Types.xsd
- BCG_PhysicalAddress_Types.xsd
- BCG_string_len_0.xsd
- BCG_xml.xsd

3A4 Request Purchase Order V02.00

The following section describes the contents for the 3A4 Request Purchase OrderV02.00 PIP.

Package file contents

The following table shows the ZIP files and corresponding XML files for the 3A4 Request Purchase Order PIP. The guideline maps, which are common to all versions, are shown in the section that follows.

Table 46. 3A4 Request Purchase Order ZIP and XML files

ZIP file name	XML file name
BCG_Package_RNIF1.1_3A4V02.00.zip	BCG_RNIF1.1_3A4V02.00.xml
BCG_Package_RNIFV02.00_3A4V02.00.zip	BCG_RNIFV02.00_3A4V02.00.xml
BCG_Package_RNSC1.0_RNIF1.1_3A4V02.00.zip	BCG_RNSC1.0_RNIF1.1_3A4V02.00.xml
BCG_Package_RNSC1.0_RNIFV02.00_3A4V02.00.zip	BCG_RNSC1.0_RNIFV02.00_3A4V02.00.xml

Guideline map contents

This section lists the guideline maps contents for 3A4 Request Purchase Order:

- BCG_3A4PurchaseOrderConfirmation_V02.00.xsd

- BCG_3A4PurchaseOrderRequest_V02.00.xsd
- BCG_BusinessDescription_Types.xsd
- BCG_BusinessDescription_Types_V422.xsd
- BCG_BusinessTaxIdentifier_Types.xsd
- BCG_common.xsd
- BCG_common_V422.xsd
- BCG_ContactInformation_Types.xsd
- BCG_GlobalAccountClassificationCode.xsd
- BCG_GlobalConfirmationTypeCode.xsd
- BCG_GlobalCountryCode.xsd
- BCG_GlobalCreditCardClassificationCode.xsd
- BCG_GlobalCurrencyCode.xsd
- BCG_GlobalDocumentReferenceTypeCode.xsd
- BCG_GlobalDocumentReferenceTypeCode_V422.xsd
- BCG_GlobalFinanceTermsCode.xsd
- BCG_GlobalGovernmentPriorityRatingCode.xsd
- BCG_GlobalMonetaryAmountTypeCode.xsd
- BCG_GlobalPartnerClassificationCode.xsd
- BCG_GlobalPartnerRoleClassificationCode_V422.xsd
- BCG_GlobalPaymentConditionCode.xsd
- BCG_GlobalPriceUnitOfMeasureCode.xsd
- BCG_GlobalProductSubstitutionReasonCode.xsd
- BCG_GlobalProductUnitOfMeasureCode.xsd
- BCG_GlobalPurchaseOrderAcknowledgmentReasonCode.xsd
- BCG_GlobalPurchaseOrderFillPriorityCode.xsd
- BCG_GlobalPurchaseOrderStatusCode.xsd
- BCG_GlobalPurchaseOrderTypeCode.xsd
- BCG_GlobalShipmentTermsCode.xsd
- BCG_GlobalShipmentTermsCode_V422.xsd
- BCG_GlobalShippingServiceLevelCode.xsd
- BCG_GlobalSpecialFulfillmentRequestCode.xsd
- BCG_GlobalSpecialHandlingCode_V422.xsd
- BCG_GlobalTaxExemptionCode.xsd
- BCG_GlobalTaxExemptionCode_V422.xsd
- BCG_InvoiceChargeTypeCode.xsd
- BCG_PartnerDescription_Types.xsd
- BCG_PhysicalAddress_Types.xsd
- BCG_PhysicalAddress_Types_V422.xsd
- BCG_string_len_0.xsd
- BCG_xml.xsd

3A4 Request Purchase Order V02.02

The following section describes the contents for the 3A4 Request Purchase OrderV02.02 PIP.

Package file contents

The following table shows the ZIP files and corresponding XML files for the 3A4 Request Purchase Order PIP. The guideline maps, which are common to all versions, are shown in the section that follows.

Table 47. 3A4 Request Purchase Order ZIP and XML files

ZIP file name	XML file name
BCG_Package_RNIF1.1_3A4V02.02.zip	BCG_RNIF1.1_3A4V02.02.xml
BCG_Package_RNIFV02.00_3A4V02.02.zip	BCG_RNIFV02.00_3A4V02.02.xml
BCG_Package_RNSC1.0_RNIF1.1_3A4V02.02.zip	BCG_RNSC1.0_RNIF1.1_3A4V02.02.xml
BCG_Package_RNSC1.0_RNIFV02.00_3A4V02.02.zip	BCG_RNSC1.0_RNIFV02.00_3A4V02.02.xml

Guideline map contents

This section lists the guideline maps contents for 3A4 Request Purchase Order:

- BCG_3A4PurchaseOrderConfirmation_V02.02.xsd
- BCG_3A4PurchaseOrderRequest_V02.02.xsd
- BCG_BusinessDescription_Types.xsd
- BCG_BusinessTaxIdentifier_Types.xsd
- BCG_common.xsd
- BCG_ContactInformation_Types.xsd
- BCG_GlobalAccountClassificationCode.xsd
- BCG_GlobalConfirmationTypeCode.xsd
- BCG_GlobalCountryCode.xsd
- BCG_GlobalCreditCardClassificationCode.xsd
- BCG_GlobalCurrencyCode.xsd
- BCG_GlobalDocumentReferenceTypeCode.xsd
- BCG_GlobalFinanceTermsCode.xsd
- BCG_GlobalGovernmentPriorityRatingCode.xsd
- BCG_GlobalMonetaryAmountTypeCode.xsd
- BCG_GlobalPartnerClassificationCode.xsd
- BCG_GlobalPartnerRoleClassificationCode.xsd
- BCG_GlobalPaymentConditionCode.xsd
- BCG_GlobalPriceUnitOfMeasureCode.xsd
- BCG_GlobalProductSubstitutionReasonCode.xsd
- BCG_GlobalProductUnitOfMeasureCode.xsd
- BCG_GlobalPurchaseOrderAcknowledgmentReasonCode.xsd
- BCG_GlobalPurchaseOrderFillPriorityCode.xsd
- BCG_GlobalPurchaseOrderStatusCode.xsd
- BCG_GlobalPurchaseOrderTypeCode.xsd
- BCG_GlobalShipmentTermsCode.xsd
- BCG_GlobalShippingServiceLevelCode.xsd
- BCG_GlobalSpecialFulfillmentRequestCode.xsd
- BCG_GlobalSpecialHandlingCode.xsd
- BCG_GlobalTaxExemptionCode.xsd
- BCG_InvoiceChargeTypeCode.xsd
- BCG_PartnerDescription_Types.xsd

- BCG_PhysicalAddress_Types.xsd
- BCG_string_len_0.xsd
- BCG_xml.xsd

3A5 Query Order Status

The following section describes the contents for the 3A5 Query Order Status PIP.

Package file contents

The following table shows the ZIP files and corresponding XML files for the 3A5 Query Order Status PIP. The guideline maps, which are common to all versions, are shown in the section that follows.

Table 48. 3A5 Query Order Status ZIP and XML files

ZIP file name	XML file name
BCG_Package_RNIF1.1_3A5R02.00.zip	BCG_RNIF1.1_3A5R02.00.xml
BCG_Package_RNIFV02.00_3A5R02.00.zip	BCG_RNIFV02.00_3A5R02.00.xml
BCG_Package_RNSC1.0_RNIF1.1_3A5R02.00.zip	BCG_RNSC1.0_RNIF1.1_3A5R02.00.xml
BCG_Package_RNSC1.0_RNIFV02.00_3A5R02.00.zip	BCG_RNSC1.0_RNIFV02.00_3A5R02.00.xml

Guideline map contents

This section lists the guideline maps contents for 3A5 Query Order Status:

- BCG_3A5PurchaseOrderStatusQuery_R02.00.xsd
- BCG_3A5PurchaseOrderStatusResponse_R02.00.xsd
- BCG_BusinessDescription_Types.xsd
- BCG_BusinessTaxIdentifier_Types.xsd
- BCG_common.xsd
- BCG_ContactInformation_Types.xsd
- BCG_GlobalAccountClassificationCode.xsd
- BCG_GlobalCountryCode.xsd
- BCG_GlobalCreditCardClassificationCode.xsd
- BCG_GlobalCurrencyCode.xsd
- BCG_GlobalCustomerTypeCode.xsd
- BCG_GlobalDocumentReferenceTypeCode.xsd
- BCG_GlobalFinanceTermsCode.xsd
- BCG_GlobalFreeOnBoardCode.xsd
- BCG_GlobalGovernmentPriorityRatingCode.xsd
- BCG_GlobalLineItemStatusCode.xsd
- BCG_GlobalOrderQuantityTypeCode.xsd
- BCG_GlobalPartnerClassificationCode.xsd
- BCG_GlobalPartnerRoleClassificationCode.xsd
- BCG_GlobalProductSubstitutionReasonCode.xsd
- BCG_GlobalProductUnitOfMeasureCode.xsd
- BCG_GlobalPurchaseOrderAcknowledgmentReasonCode.xsd
- BCG_GlobalPurchaseOrderFillPriority
- BCG_GlobalPurchaseOrderStatusCode.xsd
- BCG_GlobalPurchaseOrderTypeCode.xsd

- BCG_GlobalShipmentTermsCode.xsd
- BCG_GlobalShippingServiceLevelCode.xsd
- BCG_GlobalSpecialFulfillmentRequestCode.xsd
- BCG_GlobalSpecialHandlingCode.xsd
- BCG_GlobalTaxExemptionCode.xsd
- BCG_GlobalTransportEventCode.xsd
- BCG_PartnerDescription_Types.xsd
- BCG_PhysicalAddress_Types.xsd
- BCG_string_len_0.xsd
- BCG_xml.xsd

3A6 Distribute Order Status

The following section describes the contents for the 3A6 Distribute Order Status PIP.

Package file contents

The following table shows the ZIP files and corresponding XML files for the 3A6 Distribute Order Status PIP. The guideline maps, which are common to all versions, are shown in the section that follows.

Table 49. 3A6 Distribute Order Status ZIP and XML files

ZIP file name	XML file name
BCG_Package_RNIF1.1_3A6V02.02.zip	BCG_RNIF1.1_3A6V02.02.xml
BCG_Package_RNIFV02.00_3A6V02.02.zip	BCG_RNIFV02.00_3A6V02.02.xml
BCG_Package_RNSC1.0_RNIF1.1_3A6V02.02.zip	BCG_RNSC1.0_RNIF1.1_3A6V02.02.xml
BCG_Package_RNSC1.0_RNIFV02.00_3A6V02.02.zip	BCG_RNSC1.0_RNIFV02.00_3A6V02.02.xml

Guideline map contents

This section lists the guideline maps contents for 3A6 Distribute Order Status:

- BCG_3A6PurchaseOrderStatusNotification_V02.02.xsd
- BCG_BusinessDescription_Types.xsd
- BCG_BusinessTaxIdentifier_Types.xsd
- BCG_common.xsd
- BCG_ContactInformation_Types.xsd
- BCG_GlobalAccountClassificationCode.xsd
- BCG_GlobalCountryCode.xsd
- BCG_GlobalCreditCardClassificationCode.xsd
- BCG_GlobalCurrencyCode.xsd
- BCG_GlobalDocumentReferenceTypeCode.xsd
- BCG_GlobalFinanceTermsCode.xsd
- BCG_GlobalGovernmentPriorityRatingCode.xsd
- BCG_GlobalLineItemStatusCode.xsd
- BCG_GlobalMonetaryAmountTypeCode.xsd
- BCG_GlobalNotificationReasonCode.xsd
- BCG_GlobalOrderQuantityTypeCode.xsd
- BCG_GlobalPartnerClassificationCode.xsd
- BCG_GlobalPartnerRoleClassificationCode.xsd

- BCG_GlobalPaymentConditionCode.xsd
- BCG_GlobalPriceUnitOfMeasureCode.xsd
- BCG_GlobalProductSubstitutionReasonCode.xsd
- BCG_GlobalProductUnitOfMeasureCode.xsd
- BCG_GlobalPurchaseOrderAcknowledgmentReasonCode.xsd
- BCG_GlobalPurchaseOrderFillPriorityCode.xsd
- BCG_GlobalPurchaseOrderStatusCode.xsd
- BCG_GlobalPurchaseOrderTypeCode.xsd
- BCG_GlobalShipmentTermsCode.xsd
- BCG_GlobalShippingServiceLevelCode.xsd
- BCG_GlobalSpecialFulfillmentRequestCode.xsd
- BCG_GlobalSpecialHandlingCode.xsd
- BCG_GlobalTaxExemptionCode.xsd
- BCG_GlobalTrackingReferenceTypeCode.xsd
- BCG_InvoiceChargeTypeCode.xsd
- BCG_PartnerDescription_Types.xsd
- BCG_PhysicalAddress_Types.xsd
- BCG_string_len_0.xsd
- BCG_xml.xsd

3A7 Notify of Purchase Order Update

The following section describes the contents for the 3A7 Notify of Purchase Order Update PIP.

Package file contents

The following table shows the ZIP files and corresponding XML files for the 3A7 Notify of Purchase Order Update PIP. The guideline maps, which are common to all versions, are shown in the section that follows.

Table 50. 3A7 Notify of Purchase Order Update ZIP and XML files

ZIP file name	XML file name
BCG_Package_RNIF1.1_3A7V02.02.zip	BCG_RNIF1.1_3A7V02.02.xml
BCG_Package_RNIFV02.00_3A7V02.02.zip	BCG_RNIFV02.00_3A7V02.02.xml
BCG_Package_RNSC1.0_RNIF1.1_3A7V02.02.zip	BCG_RNSC1.0_RNIF1.1_3A7V02.02.xml
BCG_Package_RNSC1.0_RNIFV02.00_3A7V02.02.zip	BCG_RNSC1.0_RNIFV02.00_3A7V02.02.xml

Guideline map contents

This section lists the guideline maps contents for 3A7 Notify of Purchase Order Update:

- BCG_3A7PurchaseOrderUpdateNotification_V02.02.xsd
- BCG_BusinessDescription_Types.xsd
- BCG_BusinessTaxIdentifier_Types.xsd
- BCG_common.xsd
- BCG_ContactInformation_Types.xsd
- BCG_GlobalAccountClassificationCode.xsd
- BCG_GlobalActionCode.xsd
- BCG_GlobalConfirmationTypeCode.xsd

- BCG_GlobalCountryCode.xsd
- BCG_GlobalCreditCardClassificationCode.xsd
- BCG_GlobalCurrencyCode.xsd
- BCG_GlobalDocumentReferenceTypeCode.xsd
- BCG_GlobalFinanceTermsCode.xsd
- BCG_GlobalGovernmentPriorityRatingCode.xsd
- BCG_GlobalMonetaryAmountTypeCode.xsd
- BCG_GlobalPartnerClassificationCode.xsd
- BCG_GlobalPartnerRoleClassificationCode.xsd
- BCG_GlobalPaymentConditionCode.xsd
- BCG_GlobalPriceUnitOfMeasureCode.xsd
- BCG_GlobalProductSubstitutionReasonCode.xsd
- BCG_GlobalProductUnitOfMeasureCode.xsd
- BCG_GlobalPurchaseOrderAcknowledgmentReasonCode.xsd
- BCG_GlobalPurchaseOrderFillPriorityCode.xsd
- BCG_GlobalPurchaseOrderStatusCode.xsd
- BCG_GlobalPurchaseOrderTypeCode.xsd
- BCG_GlobalShipmentTermsCode.xsd
- BCG_GlobalShippingServiceLevelCode.xsd
- BCG_GlobalSpecialFulfillmentRequestCode.xsd
- BCG_GlobalSpecialHandlingCode.xsd
- BCG_GlobalTaxExemptionCode.xsd
- BCG_InvoiceChargeTypeCode.xsd
- BCG_PartnerDescription_Types.xsd
- BCG_PhysicalAddress_Types.xsd
- BCG_string_len_0.xsd
- BCG_xml.xsd

3A8 Request Purchase Order Change V01.02

The following section describes the contents for the 3A8 Request Purchase Order Change V01.02 PIP.

Package file contents

The following table shows the ZIP files and corresponding XML files for the 3A8 Request Purchase Order Change PIP. The guideline maps, which are common to all versions, are shown in the section that follows.

Table 51. 3A8 Request Purchase Order Change ZIP and XML files

ZIP file name	XML file name
BCG_Package_RNIF1.1_3A8V01.02.zip	BCG_RNIF1.1_3A8V01.02.xml
BCG_Package_RNIFV02.00_3A8V01.02.zip	BCG_RNIFV02.00_3A8V01.02.xml
BCG_Package_RNSC1.0_RNIF1.1_3A8V01.02.zip	BCG_RNSC1.0_RNIF1.1_3A8V01.02.xml
BCG_Package_RNSC1.0_RNIFV02.00_3A8V01.02.zip	BCG_RNSC1.0_RNIFV02.00_3A8V01.02.xml

Guideline map contents

This section lists the guideline maps contents for 3A8 Request Purchase Order Change:

- BCG_3A8PurchaseOrderChangeConfirmation_V01.02.xsd
- BCG_3A8PurchaseOrderChangeRequest_V01.02.xsd
- BCG_BusinessDescription_Types.xsd
- BCG_BusinessTaxIdentifier_Types.xsd
- BCG_common.xsd
- BCG_ContactInformation_Types.xsd
- BCG_GlobalAccountClassificationCode.xsd
- BCG_GlobalActionCode.xsd
- BCG_GlobalConfirmationTypeCode.xsd
- BCG_GlobalCountryCode.xsd
- BCG_GlobalCreditCardClassificationCode.xsd
- BCG_GlobalCurrencyCode.xsd
- BCG_GlobalDocumentReferenceTypeCode.xsd
- BCG_GlobalFinanceTermsCode.xsd
- BCG_GlobalGovernmentPriorityRatingCode.xsd
- BCG_GlobalMonetaryAmountTypeCode.xsd
- BCG_GlobalPartnerClassificationCode.xsd
- BCG_GlobalPartnerRoleClassificationCode.xsd
- BCG_GlobalPaymentConditionCode.xsd
- BCG_GlobalPriceUnitOfMeasureCode.xsd
- BCG_GlobalProductSubstitutionReasonCode.xsd
- BCG_GlobalProductUnitOfMeasureCode.xsd
- BCG_GlobalPurchaseOrderAcknowledgmentReasonCode.xsd
- BCG_GlobalPurchaseOrderFillPriorityCode.xsd
- BCG_GlobalPurchaseOrderStatusCode.xsd
- BCG_GlobalPurchaseOrderTypeCode.xsd
- BCG_GlobalShipmentTermsCode.xsd
- BCG_GlobalShippingServiceLevelCode.xsd
- BCG_GlobalSpecialFulfillmentRequestCode.xsd
- BCG_GlobalSpecialHandlingCode.xsd
- BCG_GlobalTaxExemptionCode.xsd
- BCG_InvoiceChargeTypeCode.xsd
- BCG_PartnerDescription_Types.xsd
- BCG_PhysicalAddress_Types.xsd
- BCG_string_len_0.xsd
- BCG_xml.xsd

3A8 Request Purchase Order Change V01.03

The following section describes the contents for the 3A8 Request Purchase Order Change V01.03 PIP.

Package file contents

The following table shows the ZIP files and corresponding XML files for the 3A8 Request Purchase Order Change PIP. The guideline maps, which are common to all versions, are shown in the section that follows.

Table 52. 3A8 Request Purchase Order Change ZIP and XML files

ZIP file name	XML file name
BCG_Package_RNIF1.1_3A8V01.03.zip	BCG_RNIF1.1_3A8V01.03.xml
BCG_Package_RNIFV02.00_3A8V01.03.zip	BCG_RNIFV02.00_3A8V01.03.xml
BCG_Package_RNSC1.0_RNIF1.1_3A8V01.03.zip	BCG_RNSC1.0_RNIF1.1_3A8V01.03.xml
BCG_Package_RNSC1.0_RNIFV02.00_3A8V01.03.zip	BCG_RNSC1.0_RNIFV02.00_3A8V01.03.xml

Guideline map contents

This section lists the guideline maps contents for 3A8 Request Purchase Order Change:

- BCG_3A8PurchaseOrderChangeConfirmation_V01.03.xsd
- BCG_3A8PurchaseOrderChangeRequest_V01.03.xsd
- BCG_BusinessDescription_Types.xsd
- BCG_BusinessDescription_Types_V43.xsd
- BCG_BusinessTaxIdentifier_Types.xsd
- BCG_common.xsd
- BCG_common_V422.xsd
- BCG_common_V43.xsd
- BCG_ContactInformation_Types.xsd
- BCG_GlobalAccountClassificationCode.xsd
- BCG_GlobalActionCode.xsd
- BCG_GlobalConfirmationTypeCode.xsd
- BCG_GlobalCountryCode.xsd
- BCG_GlobalCreditCardClassificationCode.xsd
- BCG_GlobalCurrencyCode.xsd
- BCG_GlobalDocumentReferenceTypeCode.xsd
- BCG_GlobalFinanceTermsCode.xsd
- BCG_GlobalFreeOnBoardCode_V422.xsd
- BCG_GlobalGovernmentPriorityRatingCode.xsd
- BCG_GlobalMonetaryAmountTypeCode.xsd
- BCG_GlobalPartnerClassificationCode_V43.xsd
- BCG_GlobalPartnerRoleClassificationCode_V43.xsd
- BCG_GlobalPaymentConditionCode.xsd
- BCG_GlobalProductSubstitutionReasonCode.xsd
- BCG_GlobalProductUnitOfMeasureCode_V43.xsd
- BCG_GlobalPurchaseOrderAcknowledgmentReasonCode.xsd
- BCG_GlobalPurchaseOrderFillPriorityCode.xsd
- BCG_GlobalPurchaseOrderStatusCode.xsd
- BCG_GlobalPurchaseOrderTypeCode.xsd
- BCG_GlobalShipmentTermsCode.xsd
- BCG_GlobalShippingServiceLevelCode.xsd
- BCG_GlobalSpecialFulfillmentRequestCode.xsd
- BCG_GlobalSpecialHandlingCode_V43.xsd
- BCG_GlobalTaxExemptionCode.xsd
- BCG_GlobalTransportEventCode.xsd

- BCG_InvoiceChargeTypeCode_V422.xsd
- BCG_PartnerDescription_Types.xsd
- BCG_PartnerDescription_Types_V43.xsd
- BCG_PhysicalAddress_Types.xsd
- BCG_string_len_0.xsd
- BCG_xml.xsd

3A9 Request Purchase Order Cancellation

The following section describes the contents for the 3A9 Request Purchase Order Cancellation PIP.

Package file contents

The following table shows the ZIP files and corresponding XML files for the 3A9 Request Purchase Order Cancellation PIP. The guideline maps, which are common to all versions, are shown in the section that follows.

Table 53. 3A9 Request Purchase Order Cancellation ZIP and XML files

ZIP file name	XML file name
BCG_Package_RNIF1.1_3A9V01.01.zip	BCG_RNIF1.1_3A9V01.01.xml
BCG_Package_RNIFV02.00_3A9V01.01.zip	BCG_RNIFV02.00_3A9V01.01.xml
BCG_Package_RNSC1.0_RNIF1.1_3A9V01.01.zip	BCG_RNSC1.0_RNIF1.1_3A9V01.01.xml
BCG_Package_RNSC1.0_RNIFV02.00_3A9V01.01.zip	BCG_RNSC1.0_RNIFV02.00_3A9V01.01.xml

Guideline map contents

This section lists the guideline maps contents for 3A9 Request Purchase Order Cancellation:

- BCG_3A9PurchaseOrderCancellationConfirmation_V01.01.xsd
- BCG_3A9PurchaseOrderCancellationRequest_V01.01.xsd
- BCG_BusinessDescription_Types.xsd
- BCG_BusinessTaxIdentifier_Types.xsd
- BCG_common.xsd
- BCG_ContactInformation_Types.xsd
- BCG_GlobalCountryCode.xsd
- BCG_GlobalPartnerClassificationCode.xsd
- BCG_GlobalPurchaseOrderCancellationCode.xsd
- BCG_GlobalPurchaseOrderCancellationResponseCode.xsd
- BCG_PartnerDescription_Types.xsd
- BCG_PhysicalAddress_Types.xsd
- BCG_string_len_0.xsd
- BCG_xml.xsd

3B2 Notify of Advance Shipment

The following section describes the contents for the 3B2 Notify of Advance Shipment PIP.

Package file contents

The following table shows the ZIP files and corresponding XML files for the 3B2 Notify of Advance Shipment PIP. The guideline maps, which are common to all versions, are shown in the section that follows.

Table 54. 3B2 Notify of Advance Shipment ZIP and XML files

ZIP file name	XML file name
BCG_Package_RNIF1.1_3B2V01.01.zip	BCG_RNIF1.1_3B2V01.01.xml
BCG_Package_RNIFV02.00_3B2V01.01.zip	BCG_RNIFV02.00_3B2V01.01.xml
BCG_Package_RNSC1.0_RNIF1.1_3B2V01.01.zip	BCG_RNSC1.0_RNIF1.1_3B2V01.01.xml
BCG_Package_RNSC1.0_RNIFV02.00_3B2V01.01.zip	BCG_RNSC1.0_RNIFV02.00_3B2V01.01.xml

Guideline map contents

This section lists the guideline maps contents for 3B2 Notify of Advance Shipment:

- BCG_3B2AdvanceShipmentNotification_V01.01.xsd
- BCG_BusinessDescription_Types.xsd
- BCG_BusinessTaxIdentifier_Types.xsd
- BCG_common.xsd
- BCG_ContactInformation_Types.xsd
- BCG_GlobalCountryCode.xsd
- BCG_GlobalDocumentReferenceTypeCode.xsd
- BCG_GlobalIncotermsCode.xsd
- BCG_GlobalLotQuantityClassificationCode.xsd
- BCG_GlobalPackageTypeCode.xsd
- BCG_GlobalPartnerClassificationCode.xsd
- BCG_GlobalPhysicalUnitOfMeasureCode.xsd
- BCG_GlobalProductUnitOfMeasureCode.xsd
- BCG_GlobalShipDateCode.xsd
- BCG_GlobalShipmentChangeDispositionCode.xsd
- BCG_GlobalShipmentModeCode.xsd
- BCG_GlobalShippingServiceLevelCode.xsd
- BCG_GlobalTrackingReferenceTypeCode.xsd
- BCG_NationalExportControlClassificationCode.xsd
- BCG_PartnerDescription_Types.xsd
- BCG_PhysicalAddress_Types.xsd
- BCG_string_len_0.xsd
- BCG_xml.xsd

3B3 Distribute Shipment Status

The following section describes the contents for the 3B3 Distribute Shipment Status PIP.

Package file contents

The following table shows the ZIP files and corresponding XML files for the 3B3 Distribute Shipment Status PIP. The guideline maps, which are common to all versions, are shown in the section that follows.

Table 55. 3B3 Distribute Shipment Status ZIP and XML files

ZIP file name	XML file name
BCG_Package_RNIF1.1_3B3R01.00.zip	BCG_RNIF1.1_3B3R01.00.xml
BCG_Package_RNIFV02.00_3B3R01.00.zip	BCG_RNIFV02.00_3B3R01.00.xml
BCG_Package_RNSC1.0_RNIF1.1_3B3R01.00.zip	BCG_RNSC1.0_RNIF1.1_3B3R01.00.xml
BCG_Package_RNSC1.0_RNIFV02.00_3B3R01.00.zip	BCG_RNSC1.0_RNIFV02.00_3B3R01.00.xml

Guideline map contents

This section lists the guideline maps contents for 3B3 Distribute Shipment Status:

- 3B3 Distribute Shipment Status_R01.00.xsd
- BCG_BusinessDescription_Types.xsd
- BCG_BusinessDescription_Types_V422.xsd
- BCG_BusinessDescription_Types_V43.xsd
- BCG_BusinessTaxIdentifier_Types.xsd
- BCG_common_V422.xsd
- BCG_common_V43.xsd
- BCG_ContactInformation_Types.xsd
- BCG_ContactInformation_Types_V422.xsd
- BCG_ContactInformation_Types_V43.xsd
- BCG_GlobalCountryCode.xsd
- BCG_GlobalDocumentReferenceTypeCode_V43.xsd
- BCG_GlobalPartnerClassificationCode_V43.xsd
- BCG_GlobalShipmentDispositionCode.xsd
- BCG_GlobalShipmentModeCode.xsd
- BCG_GlobalShipmentStatusCode_V43.xsd
- BCG_GlobalShipmentStatusReportingLevelCode_V43.xsd
- BCG_GlobalTrackingReferenceTypeCode.xsd
- BCG_PartnerDescription_Types_V43.xsd
- BCG_PhysicalAddress_Types.xsd
- BCG_PhysicalAddress_Types_V422.xsd
- BCG_PhysicalAddress_Types_V423.xsd
- BCG_string_len_0.xsd
- BCG_xml.xsd

3B11 Notify of Shipping Order

The following section describes the contents for the 3B11 Notify of Shipping Order PIP.

Package file contents

The following table shows the ZIP files and corresponding XML files for the 3B11 Notify of Shipping Order PIP. The guideline maps, which are common to all versions, are shown in the section that follows.

Table 56. 3B11 Notify of Shipping Order ZIP and XML files

ZIP file name	XML file name
BCG_Package_RNIF1.1_3B11R01.00A.zip	BCG_RNIF1.1_3B11R01.00A.xml

Table 56. 3B11 Notify of Shipping Order ZIP and XML files (continued)

ZIP file name	XML file name
BCG_Package_RNIFV02.00_3B11R01.00A.zip	BCG_RNIFV02.00_3B11R01.00A.xml
BCG_Package_RNSC1.0_RNIF1.1_3B11R01.00A.zip	BCG_RNSC1.0_RNIF1.1_3B11R01.00A.xml
BCG_Package_RNSC1.0_RNIFV02.00_3B11R01.00A.zip	BCG_RNSC1.0_RNIFV02.00_3B11R01.00A.xml

Guideline map contents

This section lists the guideline maps contents for 3B11 Notify of Shipping Order:

- 3B11 ShippingOrderNotification_R01.00A.xsd
- BCG_BusinessDescription_Types.xsd
- BCG_BusinessDescription_Types_V422.xsd
- BCG_BusinessTaxIdentifier_Types.xsd
- BCG_common.xsd
- BCG_ContactInformation_Types.xsd
- BCG_ContactInformation_Types_V422.xsd
- BCG_GlobalCountryCode.xsd
- BCG_GlobalCurrencyCode.xsd
- BCG_GlobalDocumentReferenceTypeCode_V422.xsd
- BCG_GlobalFreightPaymentTermsCode_V422.xsd
- BCG_GlobalIncotermsCode.xsd
- BCG_GlobalOrderAdminCode_V422.xsd
- BCG_GlobalPartnerClassificationCode.xsd
- BCG_GlobalPartnerRoleClassificationCode.xsd
- BCG_GlobalProductUnitOfMeasureCode.xsd
- BCG_GlobalShipDateCode.xsd
- BCG_GlobalShipmentModeCode.xsd
- BCG_GlobalShippingServiceLevelCode.xsd
- BCG_GlobalSpecialHandlingCode.xsd
- BCG_GlobalWarrantyTypeCode_V43.xsd
- BCG_PartnerDescription_Types.xsd
- BCG_PartnerDescription_Types_V422.xsd
- BCG_PhysicalAddress_Types.xsd
- BCG_string_len_0.xsd
- BCG_xml.xsd

3B12 Request Shipping Order

The following section describes the contents for the 3B12 Request Shipping Order PIP.

Package file contents

The following table shows the ZIP files and corresponding XML files for the 3B12 Request Shipping Order PIP. The guideline maps, which are common to all versions, are shown in the section that follows.

Table 57. 3B12 Request Shipping Order ZIP and XML files

ZIP file name	XML file name
BCG_Package_RNIF1.1_3B12V01.01.zip	BCG_RNIF1.1_3B12V01.01.xml
BCG_Package_RNIFV02.00_3B12V01.01.zip	BCG_RNIFV02.00_3B12V01.01.xml
BCG_Package_RNSC1.0_RNIF1.1_3B12V01.01.zip	BCG_RNSC1.0_RNIF1.1_3B12V01.01.xml
BCG_Package_RNSC1.0_RNIFV02.00_3B12V01.01.zip	BCG_RNSC1.0_RNIFV02.00_3B12V01.01.xml

Guideline map contents

This section lists the guideline maps contents for 3B12 Request Shipping Order:

- BCG_3B12ShippingOrderConfirmation_V01.01.xsd
- BCG_3B12ShippingOrderRequest_V01.01.xsd
- BCG_BusinessTaxIdentifier_Types.xsd
- BCG_common.xsd
- BCG_common_V422.xsd
- BCG_ContactInformation_Types.xsd
- BCG_ContactInformation_Types_V422.xsd
- BCG_GlobalCountryCode.xsd
- BCG_GlobalCurrencyCode.xsd
- BCG_GlobalDocumentReferenceTypeCode.xsd
- BCG_GlobalIncotermsCode.xsd
- BCG_GlobalPackageTypeCode.xsd
- BCG_GlobalPartnerClassificationCode.xsd
- BCG_GlobalPartnerRoleClassificationCode.xsd
- BCG_GlobalPhysicalUnitOfMeasureCode.xsd
- BCG_GlobalProductUnitOfMeasureCode.xsd
- BCG_GlobalShipDateCode.xsd
- BCG_GlobalShippingServiceLevelCode.xsd
- BCG_GlobalSpecialHandlingCode.xsd
- BCG_PartnerDescription_Types.xsd
- BCG_PartnerDescription_Types_V422.xsd
- BCG_PhysicalAddress_Types.xsd
- BCG_string_len_0.xsd
- BCG_xml.xsd

3B13 Notify of Shipping Order Confirmation

The following section describes the contents for the 3B13 Notify of Shipping Order Confirmation PIP.

Package file contents

The following table shows the ZIP files and corresponding XML files for the 3B13 Notify of Shipping Order Confirmation PIP. The guideline maps, which are common to all versions, are shown in the section that follows.

Table 58. 3B13 Notify of Shipping Order Confirmation ZIP and XML files

ZIP file name	XML file name
BCG_Package_RNIF1.1_3B13V01.01.zip	BCG_RNIF1.1_3B13V01.01.xml

Table 58. 3B13 Notify of Shipping Order Confirmation ZIP and XML files (continued)

ZIP file name	XML file name
BCG_Package_RNIFV02.00_3B13V01.01.zip	BCG_RNIFV02.00_3B13V01.01.xml
BCG_Package_RNSC1.0_RNIF1.1_3B13V01.01.zip	BCG_RNSC1.0_RNIF1.1_3B13V01.01.xml
BCG_Package_RNSC1.0_RNIFV02.00_3B13V01.01.zip	BCG_RNSC1.0_RNIFV02.00_3B13V01.01.xml

Guideline map contents

This section lists the guideline maps contents for 3B13 Notify of Shipping Order Confirmation:

- BCG_3B13ShippingOrderConfirmationNotification_V01.01.xsd
- BCG_BusinessDescription_Types.xsd
- BCG_BusinessTaxIdentifier_Types.xsd
- BCG_common.xsd
- BCG_common_V422.xsd
- BCG_ContactInformation_Types.xsd
- BCG_GlobalCountryCode.xsd
- BCG_GlobalCurrencyCode.xsd
- BCG_GlobalDocumentReferenceTypeCode.xsd
- BCG_GlobalPartnerClassificationCode.xsd
- BCG_GlobalPartnerRoleClassificationCode.xsd
- BCG_GlobalPhysicalUnitOfMeasureCode.xsd
- BCG_GlobalProductUnitOfMeasureCode.xsd
- BCG_GlobalShipDateCode.xsd
- BCG_GlobalShippingServiceLevelCode.xsd
- BCG_GlobalSpecialHandlingCode.xsd
- BCG_GlobalTrackingReferenceTypeCode.xsd
- BCG_PartnerDescription_Types.xsd
- BCG_PhysicalAddress_Types.xsd
- BCG_string_len_0.xsd
- BCG_xml.xsd

3B14 Request Shipping Order Cancellation

The following section describes the contents for the 3B14 Request Shipping Order Cancellation PIP.

Package file contents

The following table shows the ZIP files and corresponding XML files for the 3B14 Request Shipping Order Cancellation PIP. The guideline maps, which are common to all versions, are shown in the section that follows.

Table 59. 3B14 Request Shipping Order Cancellation ZIP and XML files

ZIP file name	XML file name
BCG_Package_RNIF1.1_3B14V01.00.zip	BCG_RNIF1.1_3B14V01.00.xml
BCG_Package_RNIFV02.00_3B14V01.00.zip	BCG_RNIFV02.00_3B14V01.00.xml
BCG_Package_RNSC1.0_RNIF1.1_3B14V01.00.zip	BCG_RNSC1.0_RNIF1.1_3B14V01.00.xml
BCG_Package_RNSC1.0_RNIFV02.00_3B14V01.00.zip	BCG_RNSC1.0_RNIFV02.00_3B14V01.00.xml

Guideline map contents

This section lists the guideline maps contents for 3B14 Request Shipping Order Cancellation:

- 3B14_ShippingOrderCancellationConfirmation_V01.00.xsd
- 3B14_ShippingOrderCancellationRequest_V01.00.xsd
- BCG_common.xsd
- BCG_common_V422.xsd
- BCG_ContactInformation_Types.xsd
- BCG_GlobalDocumentReferenceTypeCode.xsd
- BCG_GlobalOrderAdminCode_V22.xsd
- BCG_GlobalPartnerRoleClassificationCode.xsd
- BCG_GlobalPartnerRoleClassificationCode_V43.xsd
- BCG_GlobalShippingOrderCancellationStatusReasonCode_V43.xsd
- BCG_PartnerDescription_Types.xsd
- BCG_PartnerDescription_Types_V43.xsd
- BCG_string_len_0.xsd
- BCG_xml.xsd

3B18 Notify of Shipping Documentation

The following section describes the contents for the 3B18 Notify of Shipping Documentation PIP.

Package file contents

The following table shows the ZIP files and corresponding XML files for the 3B18 Notify of Shipping Documentation PIP. The guideline maps, which are common to all versions, are shown in the section that follows.

Table 60. 3B18 Notify of Shipping Documentation ZIP and XML files

ZIP file name	XML file name
BCG_Package_RNIF1.1_3B18V01.00.zip	BCG_RNIF1.1_3B18V01.00.xml
BCG_Package_RNIFV02.00_3B18V01.00.zip	BCG_RNIFV02.00_3B18V01.00.xml
BCG_Package_RNSC1.0_RNIF1.1_3B18V01.00.zip	BCG_RNSC1.0_RNIF1.1_3B18V01.00.xml
BCG_Package_RNSC1.0_RNIFV02.00_3B18V01.00.zip	BCG_RNSC1.0_RNIFV02.00_3B18V01.00.xml

Guideline map contents

This section lists the guideline maps contents for 3B18 Notify of Shipping Documentation:

- BCG_3B18ShippingDocumentationNotification_V01.00.xsd
- BCG_BusinessDescription_Types.xsd
- BCG_BusinessDescription_Types_V422.xsd
- BCG_common_V422.xsd
- BCG_ContactInformation_Types.xsd
- BCG_GlobalCountryCode.xsd
- BCG_GlobalCurrencyCode.xsd
- BCG_GlobalDocumentReferenceTypeCode.xsd
- BCG_GlobalFreeOnBoardCode_V422.xsd
- BCG_GlobalFreightPaymentTermsCode_V422.xsd

- BCG_GlobalIncotermsCode.xsd
- BCG_GlobalMonetaryAmountTypeCode.xsd
- BCG_GlobalOrderAdminCode_V422.xsd
- BCG_GlobalPackageTypeCode_V422.xsd
- BCG_GlobalPartnerClassificationCode_V422.xsd
- BCG_GlobalPartnerRoleClassificationCode_V422.xsd
- BCG_GlobalPaymentTermsCode.xsd
- BCG_GlobalPhysicalUnitOfMeasureCode_V422.xsd
- BCG_GlobalPortIdentifierAuthorityCode_V422.xsd
- BCG_GlobalPortTypeCode_V422.xsd
- BCG_GlobalProductUnitOfMeasureCode.xsd
- BCG_GlobalShipDateCode.xsd
- BCG_GlobalShipmentModeCode.xsd
- BCG_GlobalShippingDocumentCode_V422.xsd
- BCG_GlobalShippingServiceLevelCode.xsd
- BCG_GlobalSpecialHandlingCode_V422.xsd
- BCG_GlobalTrackingReferenceTypeCode.xsd
- BCG_InvoiceChargeTypeCode_V422.xsd
- BCG_NationalExportControlClassificationCode.xsd
- BCG_PhysicalAddress_Types.xsd
- BCG_string_len_0.xsd
- BCG_xml.xsd

3C1 Return Product

The following section describes the contents for the 3C1 Return Product PIP.

Package file contents

The following table shows the ZIP files and corresponding XML files for the 3C1 Return Product PIP. The guideline maps, which are common to all versions, are shown in the section that follows.

Table 61. 3C1 Return Product ZIP and XML files

ZIP file name	XML file name
BCG_Package_RNIF1.1_3C1V01.00.zip	BCG_RNIF1.1_3C1V01.00.xml
BCG_Package_RNIFV02.00_3C1V01.00.zip	BCG_RNIFV02.00_3C1V01.00.xml
BCG_Package_RNSC1.0_RNIF1.1_3C1V01.00.zip	BCG_RNSC1.0_RNIF1.1_3C1V01.00.xml
BCG_Package_RNSC1.0_RNIFV02.00_3C1V01.00.zip	BCG_RNSC1.0_RNIFV02.00_3C1V01.00.xml

Guideline map contents

This section lists the guideline maps contents for 3C1 Return Product:

- BCG_3C1ReturnProductConfirmation_V01.00.xsd
- BCG_3C1ReturnProductRequest_V01.00.xsd
- BCG_BusinessDescription_Types.xsd
- BCG_BusinessDescription_Types_V43.xsd
- BCG_common.xsd
- BCG_common_V422.xsd

- BCG_common_V43.xsd
- BCG_ContactInformation_Types.xsd
- BCG_GlobalCurrencyCode.xsd
- BCG_GlobalDocumentReferenceTypeCode.xsd
- BCG_GlobalFailureTypeCode_V43.xsd
- BCG_GlobalPartnerClassificationCode_V43.xsd
- BCG_GlobalPartnerRoleClassificationCode_V43.xsd
- BCG_GlobalProductUnitOfMeasureCode_V43.xsd
- BCG_GlobalShippingServiceLevelCode.xsd
- BCG_PartnerDescription_Types.xsd
- BCG_PartnerDescription_Types_V43.xsd
- BCG_PhysicalAddress_Types.xsd
- BCG_string_len_0.xsd
- BCG_xml.xsd

3C3 Notify of Invoice

The following section describes the contents for the 3C3 Notify of Invoice PIP.

Package file contents

The following table shows the ZIP files and corresponding XML files for the 3C3 Notify of Invoice PIP. The guideline maps, which are common to all versions, are shown in the section that follows.

Table 62. 3C3 Notify of Invoice ZIP and XML files

ZIP file name	XML file name
BCG_Package_RNIF1.1_3C3V01.01.zip	BCG_RNIF1.1_3C3V01.01.xml
BCG_Package_RNIFV02.00_3C3V01.01.zip	BCG_RNIFV02.00_3C3V01.01.xml
BCG_Package_RNSC1.0_RNIF1.1_3C3V01.01.zip	BCG_RNSC1.0_RNIF1.1_3C3V01.01.xml
BCG_Package_RNSC1.0_RNIFV02.00_3C3V01.01.zip	BCG_RNSC1.0_RNIFV02.00_3C3V01.01.xml

Guideline map contents

This section lists the guideline maps contents for 3C3 Notify of Invoice:

- BCG_3C3InvoiceNotification_V01.01.xsd
- BCG_BusinessDescription_Types.xsd
- BCG_BusinessTaxIdentifier_Types.xsd
- BCG_common.xsd
- BCG_ContactInformation_Types.xsd
- BCG_GlobalCountryCode.xsd
- BCG_GlobalCurrencyCode.xsd
- BCG_GlobalDocumentTypeCode.xsd
- BCG_GlobalMonetaryAmountTypeCode.xsd
- BCG_GlobalPartnerClassificationCode.xsd
- BCG_GlobalPartnerRoleClassificationCode.xsd
- BCG_GlobalPaymentTermsCode.xsd
- BCG_GlobalProductUnitOfMeasureCode.xsd
- BCG_GlobalSaleTypeCode.xsd

- BCG_GlobalShipmentTermsCode.xsd
- BCG_GlobalShippingServiceLevelCode.xsd
- BCG_GlobalSpecialHandlingCode.xsd
- BCG_InvoiceChargeTypeCode.xsd
- BCG_NationalExportControlClassificationCode.xsd
- BCG_PartnerDescription_Types.xsd
- BCG_PhysicalAddress_Types.xsd
- BCG_string_len_0.xsd
- BCG_xml.xsd

3C4 Notify of Invoice Reject

The following section describes the contents for the 3C4 Notify of Invoice Reject PIP.

Package file contents

The following table shows the ZIP files and corresponding XML files for the 3C4 Notify of Invoice Reject PIP. The guideline maps, which are common to all versions, are shown in the section that follows.

Table 63. 3C4 Notify of Invoice Reject ZIP and XML files

ZIP file name	XML file name
BCG_Package_RNIF1.1_3C4V01.00.zip	BCG_RNIF1.1_3C4V01.00.xml
BCG_Package_RNIFV02.00_3C4V01.00.zip	BCG_RNIFV02.00_3C4V01.00.xml
BCG_Package_RNSC1.0_RNIF1.1_3C4V01.00.zip	BCG_RNSC1.0_RNIF1.1_3C4V01.00.xml
BCG_Package_RNSC1.0_RNIFV02.00_3C4V01.00.zip	BCG_RNSC1.0_RNIFV02.00_3C4V01.00.xml

Guideline map contents

This section lists the guideline maps contents for 3C4 Notify of Invoice Reject:

- BCG_3C4InvoiceRejectNotification_V01.00.xsd
- BCG_BusinessDescription_Types.xsd
- BCG_BusinessTaxIdentifier_Types.xsd
- BCG_common.xsd
- BCG_ContactInformation_Types.xsd
- BCG_GlobalCountryCode.xsd
- BCG_GlobalInvoiceRejectionCode.xsd
- BCG_GlobalMonetaryAmountTypeCode.xsd
- BCG_GlobalPartnerClassificationCode.xsd
- BCG_PartnerDescription_Types.xsd
- BCG_PhysicalAddress_Types.xsd
- BCG_string_len_0.xsd
- BCG_xml.xsd

3C6 Notify of Remittance Advice

The following section describes the contents for the 3C6 Notify of Remittance Advice PIP.

Package file contents

The following table shows the ZIP files and corresponding XML files for the 3C6 Notify of Remittance Advice PIP. The guideline maps, which are common to all versions, are shown in the section that follows.

Table 64. 3C6 Notify of Remittance Advice ZIP and XML files

ZIP file name	XML file name
BCG_Package_RNIF1.1_3C6V01.00.zip	BCG_RNIF1.1_3C6V01.00.xml
BCG_Package_RNIFV02.00_3C6V01.00.zip	BCG_RNIFV02.00_3C6V01.00.xml
BCG_Package_RNSC1.0_RNIF1.1_3C6V01.00.zip	BCG_RNSC1.0_RNIF1.1_3C6V01.00.xml
BCG_Package_RNSC1.0_RNIFV02.00_3C6V01.00.zip	BCG_RNSC1.0_RNIFV02.00_3C6V01.00.xml

Guideline map contents

This section lists the guideline maps contents for 3C6 Notify of Remittance Advice:

- BCG_3C6RemittanceAdviceNotification_V01.00.xsd
- BCG_BusinessDescription_Types.xsd
- BCG_BusinessTaxIdentifier_Types.xsd
- BCG_common.xsd
- BCG_ContactInformation_Types.xsd
- BCG_GlobalCountryCode.xsd
- BCG_GlobalCurrencyCode.xsd
- BCG_GlobalDocumentTypeCode.xsd
- BCG_GlobalFinancialAdjustmentReasonCode.xsd
- BCG_GlobalInvoiceRejectionCode.xsd
- BCG_GlobalMonetaryAmountTypeCode.xsd
- BCG_GlobalPartnerClassificationCode.xsd
- BCG_GlobalPaymentMethodCode.xsd
- BCG_PartnerDescription_Types.xsd
- BCG_PhysicalAddress_Types.xsd
- BCG_string_len_0.xsd
- BCG_xml.xsd

3C7 Notify of Self-Billing Invoice

The following section describes the contents for the 3C7 Notify of Self-Billing Invoice PIP.

Package file contents

The following table shows the ZIP files and corresponding XML files for the 3C7 Notify of Self-Billing Invoice PIP. The guideline maps, which are common to all versions, are shown in the section that follows.

Table 65. 3C7 Notify of Self-Billing Invoice ZIP and XML files

ZIP file name	XML file name
BCG_Package_RNIF1.1_3C7V01.00.zip	BCG_RNIF1.1_3C7V01.00.xml
BCG_Package_RNIFV02.00_3C7V01.00.zip	BCG_RNIFV02.00_3C7V01.00.xml
BCG_Package_RNSC1.0_RNIF1.1_3C7V01.00.zip	BCG_RNSC1.0_RNIF1.1_3C7V01.00.xml
BCG_Package_RNSC1.0_RNIFV02.00_3C7V01.00.zip	BCG_RNSC1.0_RNIFV02.00_3C7V01.00.xml

Guideline map contents

This section lists the guideline maps contents for 3C7 Notify of Self-Billing Invoice:

- BCG_3C7SelfBillingInvoiceNotification_V01.00.xsd
- BCG_BusinessDescription_Types.xsd
- BCG_BusinessDescription_Types_V422.xsd
- BCG_BusinessTaxIdentifier_Types.xsd
- BCG_common.xsd
- BCG_common_V422.xsd
- BCG_ContactInformation_Types.xsd
- BCG_GlobalCountryCode.xsd
- BCG_GlobalCurrencyCode.xsd
- BCG_GlobalDocumentReferenceTypeCode.xsd
- BCG_GlobalDocumentTypeCode.xsd
- BCG_GlobalDocumentTypeCode_V422.xsd
- BCG_GlobalMonetaryAmountTypeCode.xsd
- BCG_GlobalPartnerClassificationCode.xsd
- BCG_GlobalPartnerRoleClassificationCode.xsd
- BCG_GlobalPaymentTermsCode.xsd
- BCG_GlobalProductUnitOfMeasureCode.xsd
- BCG_GlobalSaleTypeCode.xsd
- BCG_GlobalShipmentTermsCode.xsd
- BCG_GlobalShippingServiceLevelCode.xsd
- BCG_InvoiceChargeTypeCode.xsd
- BCG_NationalExportControlClassificationCode.xsd
- BCG_PartnerDescription_Types.xsd
- BCG_PhysicalAddress_Types.xsd
- BCG_string_len_0.xsd
- BCG_xml.xsd

3D8 Distribute Work in Process

The following section describes the contents for the 3D8 Distribute Work in Process PIP.

Package file contents

The following table shows the ZIP files and corresponding XML files for the 3D8 Distribute Work in Process PIP. The guideline maps, which are common to all versions, are shown in the section that follows.

Table 66. 3D8 Distribute Work in Process ZIP and XML files

ZIP file name	XML file name
BCG_Package_RNIF1.1_3D8V01.00.zip	BCG_RNIF1.1_3D8V01.00.xml
BCG_Package_RNIFV02.00_3D8V01.00.zip	BCG_RNIFV02.00_3D8V01.00.xml
BCG_Package_RNSC1.0_RNIF1.1_3D8V01.00.zip	BCG_RNSC1.0_RNIF1.1_3D8V01.00.xml
BCG_Package_RNSC1.0_RNIFV02.00_3D8V01.00.zip	BCG_RNSC1.0_RNIFV02.00_3D8V01.00.xml

Guideline map contents

This section lists the guideline maps contents for 3D8 Distribute Work in Process:

- BCG_3D8WorkInProcessNotification_V01.00.xsd
- BCG_BusinessDescription_Types.xsd
- BCG_BusinessTaxIdentifier_Types.xsd
- BCG_common.xsd
- BCG_ContactInformation_Types.xsd
- BCG_GlobalCountryCode.xsd
- BCG_GlobalDocumentReferenceTypeCode.xsd
- BCG_GlobalLotCode.xsd
- BCG_GlobalLotQuantityClassificationCode.xsd
- BCG_GlobalLotStatusCode.xsd
- BCG_GlobalPartnerClassificationCode.xsd
- BCG_GlobalPriorityCode.xsd
- BCG_GlobalProductUnitOfMeasureCode.xsd
- BCG_GlobalWorkInProcessLocationCode.xsd
- BCG_GlobalWorkInProcessPartTypeCode.xsd
- BCG_PartnerDescription_Types.xsd
- BCG_PhysicalAddress_Types.xsd
- BCG_string_len_0.xsd
- BCG_xml.xsd

4A1 Notify of Strategic Forecast

The following section describes the contents for the 4A1 Notify of Strategic Forecast PIP.

Package file contents

The following table shows the ZIP files and corresponding XML files for the 4A1 Notify of Strategic Forecast PIP. The guideline maps, which are common to all versions, are shown in the section that follows.

Table 67. 4A1 Notify of Strategic Forecast ZIP and XML files

ZIP file name	XML file name
BCG_Package_RNIF1.1_4A1V02.00.zip	BCG_RNIF1.1_4A1V02.00.xml
BCG_Package_RNIFV02.00_4A1V02.00.zip	BCG_RNIFV02.00_4A1V02.00.xml
BCG_Package_RNSC1.0_RNIF1.1_4A1V02.00.zip	BCG_RNSC1.0_RNIF1.1_4A1V02.00.xml
BCG_Package_RNSC1.0_RNIFV02.00_4A1V02.00.zip	BCG_RNSC1.0_RNIFV02.00_4A1V02.00.xml

Guideline map contents

This section lists the guideline maps contents for 4A1 Notify of Strategic Forecast:

- BCG_4A1StrategicForecastNotification_V02.00.xsd
- BCG_BusinessDescription_Types.xsd
- BCG_BusinessTaxIdentifier_Types.xsd
- BCG_common.xsd
- BCG_ContactInformation_Types.xsd
- BCG_GlobalCountryCode.xsd
- BCG_GlobalCurrencyCode.xsd

- BCG_GlobalForecastEventCode.xsd
- BCG_GlobalForecastIntervalCode.xsd
- BCG_GlobalForecastTypeCode.xsd
- BCG_GlobalPartnerClassificationCode.xsd
- BCG_GlobalPartnerReferenceTypeCode.xsd
- BCG_GlobalProductUnitOfMeasureCode.xsd
- BCG_PartnerDescription_Types.xsd
- BCG_PhysicalAddress_Types.xsd
- BCG_StrategicForecastQuantityTypeCode.xsd
- BCG_string_len_0.xsd
- BCG_xml.xsd

4A3 Notify of Threshold Release Forecast

The following section describes the contents for the 4A3 Notify of Threshold Release Forecast PIP.

Package file contents

The following table shows the ZIP files and corresponding XML files for the 4A3 Notify of Threshold Release Forecast PIP. The guideline maps, which are common to all versions, are shown in the section that follows.

Table 68. 4A3 Notify of Threshold Release Forecast ZIP and XML files

ZIP file name	XML file name
BCG_Package_RNIF1.1_4A3V02.00.zip	BCG_RNIF1.1_4A3V02.00.xml
BCG_Package_RNIFV02.00_4A3V02.00.zip	BCG_RNIFV02.00_4A3V02.00.xml
BCG_Package_RNSC1.0_RNIF1.1_4A3V02.00.zip	BCG_RNSC1.0_RNIF1.1_4A3V02.00.xml
BCG_Package_RNSC1.0_RNIFV02.00_4A3V02.00.zip	BCG_RNSC1.0_RNIFV02.00_4A3V02.00.xml

Guideline map contents

This section lists the guideline maps contents for 4A3 Notify of Threshold Release Forecast:

- BCG_4A3ThresholdReleaseForecastNotification_V02.00.xsd
- BCG_BusinessDescription_Types.xsd
- BCG_BusinessTaxIdentifier_Types.xsd
- BCG_common.xsd
- BCG_ContactInformation_Types.xsd
- BCG_GlobalCountryCode.xsd
- BCG_GlobalCurrencyCode.xsd
- BCG_GlobalForecastEventCode.xsd
- BCG_GlobalForecastIntervalCode.xsd
- BCG_GlobalForecastInventoryTypeCode.xsd
- BCG_GlobalForecastReferenceTypeCode.xsd
- BCG_GlobalPartnerClassificationCode.xsd
- BCG_GlobalPartnerReferenceTypeCode.xsd
- BCG_GlobalProductUnitOfMeasureCode.xsd
- BCG_OrderForecastQuantityTypeCode.xsd
- BCG_PartnerDescription_Types.xsd

- BCG_PhysicalAddress_Types.xsd
- BCG_string_len_0.xsd
- BCG_xml.xsd

4A4 Notify of Planning Release Forecast

The following section describes the contents for the 4A4 Notify of Planning Release Forecast PIP.

Package file contents

The following table shows the ZIP files and corresponding XML files for the 4A4 Notify of Planning Release Forecast. PIP. The guideline maps, which are common to all versions, are shown in the section that follows.

Table 69. 4A4 Notify of Planning Release Forecast ZIP and XML files

ZIP file name	XML file name
BCG_Package_RNIF1.1_4A4R02.00A.zip	BCG_RNIF1.1_4A4R02.00A.xml
BCG_Package_RNIFV02.00_4A4R02.00A.zip	BCG_RNIFV02.00_4A4R02.00A.xml
BCG_Package_RNSC1.0_RNIF1.1_4A4R02.00A.zip	BCG_RNSC1.0_RNIF1.1_4A4R02.00A.xml
BCG_Package_RNSC1.0_RNIFV02.00_4A4R02.00A.zip	BCG_RNSC1.0_RNIFV02.00_4A4R02.00A.xml

Guideline map contents

This section lists the guideline maps contents for 4A4 Notify of Planning Release Forecast:

- BCG_4A4PlanningReleaseForecastNotification_R02.00A.xsd
- BCG_BusinessDescription_Types.xsd
- BCG_BusinessTaxIdentifier_Types.xsd
- BCG_common.xsd
- BCG_ContactInformation_Types.xsd
- BCG_GlobalCountryCode.xsd
- BCG_GlobalCurrencyCode.xsd
- BCG_GlobalForecastInventoryTypeCode.xsd
- BCG_GlobalForecastQuantityTypeCode_V422.xsd
- BCG_GlobalForecastReferenceTypeCode.xsd
- BCG_GlobalIntervalCode.xsd
- BCG_GlobalPartnerClassificationCode.xsd
- BCG_GlobalPartnerReferenceTypeCode.xsd
- BCG_GlobalProductUnitOfMeasureCode.xsd
- BCG_GlobalTransportEventCode.xsd
- BCG_PartnerDescription_Types.xsd
- BCG_PhysicalAddress_Types.xsd
- BCG_PhysicalAddress_Types_V422.xsd
- BCG_string_len_0.xsd
- BCG_xml.xsd

4A5 Notify of Forecast Reply

The following section describes the contents for the 4A5 Notify of Forecast Reply PIP.

Package file contents

The following table shows the ZIP files and corresponding XML files for the 4A5 Notify of Forecast Reply PIP. The guideline maps, which are common to all versions, are shown in the section that follows.

Table 70. 4A5 Notify of Forecast Reply ZIP and XML files

ZIP file name	XML file name
BCG_Package_RNIF1.1_4A5V02.00.zip	BCG_RNIF1.1_4A5V02.00.xml
BCG_Package_RNIFV02.00_4A5V02.00.zip	BCG_RNIFV02.00_4A5V02.00.xml
BCG_Package_RNSC1.0_RNIF1.1_34A5V02.00.zip	BCG_RNSC1.0_RNIF1.1_34A5V02.00.xml
BCG_Package_RNSC1.0_RNIFV02.00_4A5V02.00.zip	BCG_RNSC1.0_RNIFV02.00_4A5V02.00.xml

Guideline map contents

This section lists the guideline maps contents for 4A5 Notify of Forecast Reply:

- BCG_4A5ForecastReplyNotification_V02.00.xsd
- BCG_BusinessDescription_Types.xsd
- BCG_BusinessTaxIdentifier_Types.xsd
- BCG_common.xsd
- BCG_ContactInformation_Types.xsd
- BCG_ForecastReplyQuantityTypeCode.xsd
- BCG_GlobalCountryCode.xsd
- BCG_GlobalCurrencyCode.xsd
- BCG_GlobalForecastEventCode.xsd
- BCG_GlobalForecastIntervalCode.xsd
- BCG_GlobalForecastInventoryTypeCode.xsd
- BCG_GlobalForecastReferenceTypeCode.xsd
- BCG_GlobalForecastResponseCode.xsd
- BCG_GlobalForecastRevisionReasonCode.xsd
- BCG_GlobalPartnerClassificationCode.xsd
- BCG_GlobalPartnerReferenceTypeCode.xsd
- BCG_GlobalProductUnitOfMeasureCode.xsd
- BCG_PartnerDescription_Types.xsd
- BCG_PhysicalAddress_Types.xsd
- BCG_string_len_0.xsd
- BCG_xml.xsd

4B2 Notify of Shipment Receipt

The following section describes the contents for the 4B2 Notify of Shipment Receipt PIP.

Package file contents

The following table shows the ZIP files and corresponding XML files for the 4B2 Notify of Shipment Receipt PIP. The guideline maps, which are common to all versions, are shown in the section that follows.

Table 71. 4B2 Notify of Shipment Receipt ZIP and XML files

ZIP file name	XML file name
BCG_Package_RNIF1.1_4B2V01.00.zip	BCG_RNIF1.1_4B2V01.00.xml
BCG_Package_RNIFV02.00_4B2V01.00.zip	BCG_RNIFV02.00_4B2V01.00.xml
BCG_Package_RNSC1.0_RNIF1.1_4B2V01.00.zip	BCG_RNSC1.0_RNIF1.1_4B2V01.00.xml
BCG_Package_RNSC1.0_RNIFV02.00_4B2V01.00.zip	BCG_RNSC1.0_RNIFV02.00_4B2V01.00.xml

Guideline map contents

This section lists the guideline maps contents for 4B2 Notify of Shipment Receipt:

- BCG_4B2ShipmentReceiptNotification_V01.00.xsd
- BCG_BusinessDescription_Types.xsd
- BCG_BusinessTaxIdentifier_Types.xsd
- BCG_common.xsd
- BCG_ContactInformation_Types.xsd
- BCG_GlobalCountryCode.xsd
- BCG_GlobalDocumentReferenceTypeCode.xsd
- BCG_GlobalLotDiscrepancyReasonCode.xsd
- BCG_GlobalPartnerClassificationCode.xsd
- BCG_GlobalPartnerRoleClassificationCode.xsd
- BCG_GlobalProductUnitOfMeasureCode.xsd
- BCG_GlobalReceivingDiscrepancyCode.xsd
- BCG_GlobalReceivingDiscrepancyReasonCode.xsd
- BCG_GlobalSpecialFulfillmentRequestCode.xsd
- BCG_GlobalSpecialHandlingCode.xsd
- BCG_GlobalTrackingReferenceTypeCode.xsd
- BCG_PartnerDescription_Types.xsd
- BCG_PhysicalAddress_Types.xsd
- BCG_string_len_0.xsd
- BCG_xml.xsd

4B3 Notify of Consumption

The following section describes the contents for the 4B3 Notify of Consumption PIP.

Package file contents

The following table shows the ZIP files and corresponding XML files for the 4B3 Notify of Consumption PIP. The guideline maps, which are common to all versions, are shown in the section that follows.

Table 72. 4B3 Notify of Consumption ZIP and XML files

ZIP file name	XML file name
BCG_Package_RNIF1.1_4B3V01.00.zip	BCG_RNIF1.1_4B3V01.00.xml
BCG_Package_RNIFV02.00_4B3V01.00.zip	BCG_RNIFV02.00_4B3V01.00.xml
BCG_Package_RNSC1.0_RNIF1.1_4B3V01.00.zip	BCG_RNSC1.0_RNIF1.1_4B3V01.00.xml
BCG_Package_RNSC1.0_RNIFV02.00_4B3V01.00.zip	BCG_RNSC1.0_RNIFV02.00_4B3V01.00.xml

Guideline map contents

This section lists the guideline maps contents for 4B3 Notify of Consumption:

- BCG_4B3ConsumptionNotification_V01.00.xsd
- BCG_BusinessDescription_Types.xsd
- BCG_BusinessDescription_Types_V422.xsd
- BCG_BusinessDescription_Types_V43.xsd
- BCG_BusinessTaxIdentifier_Types.xsd
- BCG_common.xsd
- BCG_common_V43.xsd
- BCG_ContactInformation_Types.xsd
- BCG_ContactInformation_Types_V422.xsd
- BCG_ContactInformation_Types_V43.xsd
- BCG_GlobalCountryCode.xsd
- BCG_GlobalCurrencyCode.xsd
- BCG_GlobalDocumentReferenceTypeCode_V43.xsd
- BCG_GlobalInventoryCode_V43.xsd
- BCG_GlobalPartnerClassificationCode_V422.xsd
- BCG_GlobalPartnerClassificationCode_V43.xsd
- BCG_GlobalProductUnitOfMeasureCode.xsd
- BCG_PartnerDescription_Types_V43.xsd
- BCG_PhysicalAddress_Types.xsd
- BCG_string_len_0.xsd
- BCG_xml.xsd

4C1 Distribute Inventory Report V02.01

The following section describes the contents for the 4C1 Distribute Inventory Report V02.01PIP.

Package file contents

The following table shows the ZIP files and corresponding XML files for the 4C1 Distribute Inventory Report PIP. The guideline maps, which are common to all versions, are shown in the section that follows.

Table 73. 4C1 Distribute Inventory Report ZIP and XML files

ZIP file name	XML file name
BCG_Package_RNIF1.1_4C1V02.01.zip	BCG_RNIF1.1_4C1V02.01.xml
BCG_Package_RNIFV02.00_4C1V02.01.zip	BCG_RNIFV02.00_4C1V02.01.xml
BCG_Package_RNSC1.0_RNIF1.1_4C1V02.01.zip	BCG_RNSC1.0_RNIF1.1_4C1V02.01.xml
BCG_Package_RNSC1.0_RNIFV02.00_4C1V02.01.zip	BCG_RNSC1.0_RNIFV02.00_4C1V02.01.xml

Guideline map contents

This section lists the guideline maps contents for 4C1 Distribute Inventory Report:

- BCG_4C1InventoryReportNotification_V02.01.xsd
- BCG_BusinessDescription_Types.xsd
- BCG_BusinessTaxIdentifier_Types.xsd
- BCG_common.xsd
- BCG_common_V422.xsd

- BCG_ContactInformation_Types.xsd
- BCG_ContactInformation_Types_V422.xsd
- BCG_GlobalCountryCode.xsd
- BCG_GlobalDocumentReferenceTypeCode.xsd
- BCG_GlobalInventoryCode.xsd
- BCG_GlobalPartnerClassificationCode.xsd
- BCG_GlobalPartnerRoleClassificationCode.xsd
- BCG_GlobalProductUnitOfMeasureCode.xsd
- BCG_PhysicalAddress_Types.xsd
- BCG_PhysicalAddress_Types_V422.xsd
- BCG_string_len_0.xsd
- BCG_xml.xsd

4C1 Distribute Inventory Report V02.03

The following section describes the contents for the 4C1 Distribute Inventory Report V02.03 PIP.

Package file contents

The following table shows the ZIP files and corresponding XML files for the 4C1 Distribute Inventory Report PIP. The guideline maps, which are common to all versions, are shown in the section that follows.

Table 74. 4C1 Distribute Inventory Report ZIP and XML files

ZIP file name	XML file name
BCG_Package_RNIF1.1_4C1V02.03.zip	BCG_RNIF1.1_4C1V02.03.xml
BCG_Package_RNIFV02.00_4C1V02.03.zip	BCG_RNIFV02.00_4C1V02.03.xml
BCG_Package_RNSC1.0_RNIF1.1_4C1V02.03.zip	BCG_RNSC1.0_RNIF1.1_4C1V02.03.xml
BCG_Package_RNSC1.0_RNIFV02.00_4C1V02.03.zip	BCG_RNSC1.0_RNIFV02.00_4C1V02.03.xml

Guideline map contents

This section lists the guideline maps contents for 4C1 Distribute Inventory Report:

- BCG_4C1InventoryReportNotification_V02.03.xsd
- BCG_BusinessDescription_Types.xsd
- BCG_BusinessTaxIdentifier_Types.xsd
- BCG_common.xsd
- BCG_ContactInformation_Types.xsd
- BCG_GlobalCountryCode.xsd
- BCG_GlobalDocumentReferenceTypeCode.xsd
- BCG_GlobalInventoryCode.xsd
- BCG_GlobalPartnerClassificationCode.xsd
- BCG_GlobalPartnerRoleClassificationCode.xsd
- BCG_GlobalProductUnitOfMeasureCode.xsd
- BCG_PhysicalAddress_Types.xsd
- BCG_string_len_0.xsd
- BCG_xml.xsd

5C1 Distribute Product List

The following section describes the contents for the 5C1 Distribute Product List PIP.

Package file contents

The following table shows the ZIP files and corresponding XML files for the 5C1 Distribute Product List PIP. The guideline maps, which are common to all versions, are shown in the section that follows.

Table 75. 5C1 Distribute Product List ZIP and XML files

ZIP file name	XML file name
BCG_Package_RNIF1.1_5C1V01.00.zip	BCG_RNIF1.1_5C1V01.00.xml
BCG_Package_RNIFV02.00_5C1V01.00.zip	BCG_RNIFV02.00_5C1V01.00.xml
BCG_Package_RNSC1.0_RNIF1.1_5C1V01.00.zip	BCG_RNSC1.0_RNIF1.1_5C1V01.00.xml
BCG_Package_RNSC1.0_RNIFV02.00_5C1V01.00.zip	BCG_RNSC1.0_RNIFV02.00_5C1V01.00.xml

Guideline map contents

This section lists the guideline maps contents for 5C1 Distribute Product List:

- BCG_5C1ProductListNotification_V01.00.xsd
- BCG_BusinessDescription_Types.xsd
- BCG_BusinessTaxIdentifier_Types.xsd
- BCG_common.xsd
- BCG_ContactInformation_Types.xsd
- BCG_GlobalCountryCode.xsd
- BCG_GlobalCurrencyCode.xsd
- BCG_GlobalPartnerClassificationCode.xsd
- BCG_GlobalPartnerRoleClassificationCode.xsd
- BCG_GlobalPriceTypeCode.xsd
- BCG_PartnerDescription_Types.xsd
- BCG_PhysicalAddress_Types.xsd
- BCG_string_len_0.xsd
- BCG_xml.xsd

5C2 Request Design Registration

The following section describes the contents for the 5C2 Request Design Registration PIP.

Package file contents

The following table shows the ZIP files and corresponding XML files for the 5C2 Request Design Registration PIP. The guideline maps, which are common to all versions, are shown in the section that follows.

Table 76. 5C2 Request Design Registration ZIP and XML files

ZIP file name	XML file name
BCG_Package_RNIF1.1_5C2V01.00.zip	BCG_RNIF1.1_5C2V01.00.xml
BCG_Package_RNIFV02.00_5C2V01.00.zip	BCG_RNIFV02.00_5C2V01.00.xml
BCG_Package_RNSC1.0_RNIF1.1_5C2V01.00.zip	BCG_RNSC1.0_RNIF1.1_5C2V01.00.xml
BCG_Package_RNSC1.0_RNIFV02.00_5C2V01.00.zip	BCG_RNSC1.0_RNIFV02.00_5C2V01.00.xml

Guideline map contents

This section lists the guideline maps contents for 5C2 Request Design Registration:

- BCG_5C2DesignRegistrationConfirmation_V01.00.xsd
- BCG_5C2DesignRegistrationRequest_V01.00.xsd
- BCG_BusinessDescription_Types.xsd
- BCG_common.xsd
- BCG_common_V422.xsd
- BCG_common_V43.xsd
- BCG_ContactInformation_Types.xsd
- BCG_DesignWinStatusReasonCode_V43.xsd
- BCG_GlobalAttachmentDescriptionCode_V422.xsd
- BCG_GlobalCountryCode.xsd
- BCG_GlobalCurrencyCode.xsd
- BCG_GlobalDocumentReferenceTypeCode.xsd
- BCG_GlobalMimeTypeQualifierCode_V43.xsd
- BCG_GlobalMonetaryAmountTypeCode.xsd
- BCG_GlobalPartnerClassificationCode_V43.xsd
- BCG_GlobalPartnerRoleClassificationCode_V43.xsd
- BCG_GlobalPriceTypeCode_V43.xsd
- BCG_GlobalRegistrationComplexityLevelCode.xsd
- BCG_GlobalRegistrationInvolvementLevelCode.xsd
- BCG_InvoiceChargeTypeCode_V422.xsd
- BCG_PartnerDescription_Types.xsd
- BCG_PartnerDescription_Types_V43.xsd
- BCG_PhysicalAddress_Types.xsd
- BCG_string_len_0.xsd
- BCG_xml.xsd

5C4 Distribute Registration Status

The following section describes the contents for the 5C4 Distribute Registration Status PIP.

Package file contents

The following table shows the ZIP files and corresponding XML files for the 5C4 Distribute Registration Status PIP. The guideline maps, which are common to all versions, are shown in the section that follows.

Table 77. 5C4 Distribute Registration Status ZIP and XML files

ZIP file name	XML file name
BCG_Package_RNIF1.1_5C4V01.02.zip	BCG_RNIF1.1_5C4V01.02.xml
BCG_Package_RNIFV02.00_5C4V01.02.zip	BCG_RNIFV02.00_5C4V01.02.xml
BCG_Package_RNSC1.0_RNIF1.1_5C4V01.023.zip	BCG_RNSC1.0_RNIF1.1_5C4V01.023.xml
BCG_Package_RNSC1.0_RNIFV02.00_5C4V01.02.zip	BCG_RNSC1.0_RNIFV02.00_5C4V01.02.xml

Guideline map contents

This section lists the guideline maps contents for 5C4 Distribute Registration Status:

- BCG_5C4RegistrationStatusNotification_V01.02.xsd
- BCG_BusinessDescription_Types.xsd
- BCG_BusinessTaxIdentifier_Types.xsd
- BCG_common.xsd
- BCG_ContactInformation_Types.xsd
- BCG_GlobalCountryCode.xsd
- BCG_GlobalPartnerClassificationCode.xsd
- BCG_GlobalPartnerRoleClassificationCode.xsd
- BCG_GlobalRegistrationComplexityLevelCode.xsd
- BCG_GlobalRegistrationInvolvementLevelCode.xsd
- BCG_PartnerDescription_Types.xsd
- BCG_PhysicalAddress_Types.xsd
- BCG_string_len_0.xsd
- BCG_xml.xsd

5D1 Request Ship From Stock And Debit Authorization

The following section describes the contents for the 5D1 Request Ship From Stock And Debit Authorization PIP.

Package file contents

The following table shows the ZIP files and corresponding XML files for the 5D1 Request Ship From Stock And Debit Authorization PIP. The guideline maps, which are common to all versions, are shown in the section that follows.

Table 78. 5D1 Request Ship from Stock and Debit Authorization ZIP and XML files

ZIP file name	XML file name
BCG_Package_RNIF1.1_5D1V01.00.zip	BCG_RNIF1.1_5D1V01.00.xml
BCG_Package_RNIFV02.00_5D1V01.00.zip	BCG_RNIFV02.00_5D1V01.00.xml
BCG_Package_RNSC1.0_RNIF1.1_5D1V01.00.zip	BCG_RNSC1.0_RNIF1.1_5D1V01.00.xml
BCG_Package_RNSC1.0_RNIFV02.00_5D1V01.00.zip	BCG_RNSC1.0_RNIFV02.00_5D1V01.00.xml

Guideline map contents

This section lists the guideline maps contents for 5D1 Request Ship From Stock And Debit Authorization:

- BCG_5D1ShipFromStockAndDebitAuthorizationConfirmation_V01.00.xsd
- BCG_5D1ShipFromStockAndDebitAuthorizationRequest_V01.00.xsd
- BCG_BusinessDescription_Types.xsd
- BCG_BusinessTaxIdentifier_Types.xsd
- BCG_common.xsd
- BCG_ContactInformation_Types.xsd
- BCG_GlobalCountryCode.xsd
- BCG_GlobalCurrencyCode.xsd
- BCG_GlobalDocumentReferenceTypeCode.xsd
- BCG_GlobalPartnerClassificationCode.xsd

- BCG_GlobalPartnerRoleClassificationCode.xsd
- BCG_GlobalPriceTypeCode.xsd
- BCG_GlobalProductUnitOfMeasureCode.xsd
- BCG_GlobalShipFromStockAndDebitAuthorizationRejectionCode.xsd
- BCG_PartnerDescription_Types.xsd
- BCG_PhysicalAddress_Types.xsd
- BCG_string_len_0.xsd
- BCG_xml.xsd

6C1 Query Service Entitlement

The following section describes the contents for the 6C1 Query Service Entitlement PIP.

Package file contents

The following table shows the ZIP files and corresponding XML files for the 6C1 Query Service Entitlement PIP. The guideline maps, which are common to all versions, are shown in the section that follows.

Table 79. 6C1 Query Service Entitlement ZIP and XML files

ZIP file name	XML file name
BCG_Package_RNIF1.1_6C1V01.00.zip	BCG_RNIF1.1_6C1V01.00.xml
BCG_Package_RNIFV02.00_6C1V01.00.zip	BCG_RNIFV02.00_6C1V01.00.xml
BCG_Package_RNSC1.0_RNIF1.1_6C1V01.00.zip	BCG_RNSC1.0_RNIF1.1_6C1V01.00.xml
BCG_Package_RNSC1.0_RNIFV02.00_6C1V01.00.zip	BCG_RNSC1.0_RNIFV02.00_6C1V01.00.xml

Guideline map contents

This section lists the guideline maps contents for 6C1 Query Service Entitlement:

- BCG_6C1ServiceEntitlementQuery_V01.00.xsd
- BCG_6C1ServiceEntitlementStatusResponse_V01.00.xsd
- BCG_common_V43.xsd
- BCG_ContactInformation_Types.xsd
- BCG_ContactInformation_Types_V43.xsd
- BCG_GlobalCurrencyCode.xsd
- BCG_GlobalNotificationCode_V43.xsd
- BCG_GlobalPartnerClassificationCode_V43.xsd
- BCG_GlobalPaymentTypeCode_V43.xsd
- BCG_GlobalServiceDeliveryMethodCode_V43.xsd
- BCG_GlobalShippingServiceLevelCode.xsd
- BCG_GlobalWarrantyMethodCode_V43.xsd
- BCG_GlobalWarrantyProgramCode_V43.xsd
- BCG_GlobalWarrantyTypeCode_V43.xsd
- BCG_PartnerDescription_Types_V43.xsd
- BCG_string_len_0.xsd
- BCG_xml.xsd

6C2 Request Warranty Claim

The following section describes the contents for the 6C2 Request Warranty Claim PIP.

Package file contents

The following table shows the ZIP files and corresponding XML files for the 6C2 Request Warranty Claim PIP. The guideline maps, which are common to all versions, are shown in the section that follows.

Table 80. 6C2 Request Warranty Claim ZIP and XML files

ZIP file name	XML file name
BCG_Package_RNIF1.1_6C2V01.00.zip	BCG_RNIF1.1_6C2V01.00.xml
BCG_Package_RNIFV02.00_6C2V01.00.zip	BCG_RNIFV02.00_6C2V01.00.xml
BCG_Package_RNSC1.0_RNIF1.1_6C2V01.00.zip	BCG_RNSC1.0_RNIF1.1_6C2V01.00.xml
BCG_Package_RNSC1.0_RNIFV02.00_6C2V01.00.zip	BCG_RNSC1.0_RNIFV02.00_6C2V01.00.xml

Guideline map contents

This section lists the guideline maps contents for 6C2 Request Warranty Claim:

- BCG_6C2WarrantyClaimConfirmation_V01.00.xsd
- BCG_6CWarrantyClaimRequest_V01.00.xsd
- BCG_common.xsd
- BCG_ContactInformation_Types.xsd
- BCG_GlobalCurrencyCode.xsd
- BCG_GlobalDocumentReferenceTypeCode.xsd
- BCG_GlobalFailureTypeCode_V43.xsd
- BCG_GlobalOperatingSystemCode_V43.xsd
- BCG_GlobalPartnerClassificationCode_V43.xsd
- BCG_GlobalPartnerRoleClassificationCode_V43.xsd
- BCG_GlobalPaymentTypeCode_V43.xsd
- BCG_GlobalServiceDeliveryMethodCode_V43.xsd
- BCG_GlobalWarrantyTypeCode_V43.xsd
- BCG_PartnerDescription_Types_V43.xsd
- BCG_string_len_0.xsd
- BCG_xml.xsd

7B1 Distribute Work in Process

The following section describes the contents for the 7B1 Distribute Work in Process PIP.

Package file contents

The following table shows the ZIP files and corresponding XML files for the 7B1 Distribute Work in Process PIP. The guideline maps, which are common to all versions, are shown in the section that follows.

Table 81. 7B1 Distribute Work in Process ZIP and XML files

ZIP file name	XML file name
BCG_Package_RNIF1.1_7B1V01.00.zip	BCG_RNIF1.1_7B1V01.00.xml
BCG_Package_RNIFV02.00_37B1V01.00.zip	BCG_RNIFV02.00_37B1V01.00.xml

Table 81. 7B1 Distribute Work in Process ZIP and XML files (continued)

ZIP file name	XML file name
BCG_Package_RNSC1.0_RNIF1.1_7B1V01.00.zip	BCG_RNSC1.0_RNIF1.1_7B1V01.00.xml
BCG_Package_RNSC1.0_RNIFV02.00_7B1V01.00.zip	BCG_RNSC1.0_RNIFV02.00_7B1V01.00.xml

Guideline map contents

This section lists the guideline maps contents for 7B1 Distribute Work in Process:

- BCG_7B1WorkInProcessNotification_V01.00.xsd
- BCG_BusinessDescription_Types.xsd
- BCG_BusinessTaxIdentifier_Types.xsd
- BCG_common.xsd
- BCG_ContactInformation_Types.xsd
- BCG_GlobalChangeReasonCode.xsd
- BCG_GlobalCountryCode.xsd
- BCG_GlobalDocumentReferenceTypeCode.xsd
- BCG_GlobalEquipmentTypeCode.xsd
- BCG_GlobalLotCode.xsd
- BCG_GlobalLotQuantityClassificationCode.xsd
- BCG_GlobalLotStatusCode.xsd
- BCG_GlobalPartnerClassificationCode.xsd
- BCG_GlobalPartnerRoleClassificationCode.xsd
- BCG_GlobalPriorityCode.xsd
- BCG_GlobalProductUnitOfMeasureCode.xsd
- BCG_GlobalWorkInProcessLocationCode.xsd
- BCG_GlobalWorkInProcessPartTypeCode.xsd
- BCG_GlobalWorkInProcessQuantityChangeCode.xsd
- BCG_GlobalWorkInProcessTypeCode.xsd
- BCG_PartnerDescription_Types.xsd
- BCG_PhysicalAddress_Types.xsd
- BCG_string_len_0.xsd
- BCG_xml.xsd

7B5 Notify Of Manufacturing Work Order

The following section describes the contents for the 7B5 Notify Of Manufacturing Work Order PIP.

Package file contents

The following table shows the ZIP files and corresponding XML files for the 7B5 Notify Of Manufacturing Work Order PIP. The guideline maps, which are common to all versions, are shown in the section that follows.

Table 82. 7B5 Notify of Manufacturing Work Order ZIP and XML files

ZIP file name	XML file name
BCG_Package_RNIF1.1_7B5V01.00.zip	BCG_RNIF1.1_7B5V01.00.xml
BCG_Package_RNIFV02.00_7B5V01.00.zip	BCG_RNIFV02.00_7B5V01.00.xml
BCG_Package_RNSC1.0_RNIF1.1_7B5V01.00.zip	BCG_RNSC1.0_RNIF1.1_7B5V01.00.xml

Table 82. 7B5 Notify of Manufacturing Work Order ZIP and XML files (continued)

ZIP file name	XML file name
BCG_Package_RNSC1.0_RNIFV02.00_7B5V01.00.zip	BCG_RNSC1.0_RNIFV02.00_7B5V01.00.xml

Guideline map contents

This section lists the guideline maps contents for 7B5 Notify Of Manufacturing Work Order:

- BCG_7B5NotifyOfManufacturingWorkOrder_V01.00.xsd
- BCG_BusinessDescription_Types.xsd
- BCG_BusinessTaxIdentifier_Types.xsd
- BCG_common.xsd
- BCG_ContactInformation_Types.xsd
- BCG_GlobalAttachmentDescriptionCode_V422.xsd
- BCG_GlobalBusinessActionCode_V422.xsd
- BCG_GlobalChangeReasonCode.xsd
- BCG_GlobalCountryCode.xsd
- BCG_GlobalDevicePackageTypeCode_V422.xsd
- BCG_GlobalDocumentReferenceTypeCode.xsd
- BCG_GlobalLineItemStatusCode.xsd
- BCG_GlobalLotCode.xsd
- BCG_GlobalMimeTypeQualifierCode_V422.xsd
- BCG_GlobalPackageTypeCode.xsd
- BCG_GlobalPartnerClassificationCode.xsd
- BCG_GlobalPartnerRoleClassificationCode.xsd
- BCG_GlobalPhysicalUnitOfMeasureCode.xsd
- BCG_GlobalPriorityCode.xsd
- BCG_GlobalProductUnitOfMeasureCode.xsd
- BCG_GlobalWorkInProcessLocationCode.xsd
- BCG_PartnerDescription_Types.xsd
- BCG_PhysicalAddress_Types.xsd
- BCG_string_len_0.xsd
- BCG_xml.xsd

7B6 Notify Of Manufacturing Work Order Reply

The following section describes the contents for the 7B6 Notify Of Manufacturing Work Order Reply PIP.

Package file contents

The following table shows the ZIP files and corresponding XML files for the 7B6 Notify Of Manufacturing Work Order Reply PIP. The guideline maps, which are common to all versions, are shown in the section that follows.

Table 83. 7B6 Notify of Manufacturing Work Order Reply ZIP and XML files

ZIP file name	XML file name
BCG_Package_RNIF1.1_7B6V01.00.zip	BCG_RNIF1.1_7B6V01.00.xml
BCG_Package_RNIFV02.00_7B6V01.00.zip	BCG_RNIFV02.00_7B6V01.00.xml

Table 83. 7B6 Notify of Manufacturing Work Order Reply ZIP and XML files (continued)

ZIP file name	XML file name
BCG_Package_RNSC1.0_RNIF1.1_7B6V01.00.zip	BCG_RNSC1.0_RNIF1.1_7B6V01.00.xml
BCG_Package_RNSC1.0_RNIFV02.00_7B6V01.00.zip	BCG_RNSC1.0_RNIFV02.00_7B6V01.00.xml

Guideline map contents

This section lists the guideline maps contents for 7B6 Notify Of Manufacturing Work Order Reply:

- BCG_7B6NotifyOfManufacturingWorkOrderReply_V01.00.xsd
- BCG_BusinessDescription_Types.xsd
- BCG_BusinessTaxIdentifier_Types.xsd
- BCG_common.xsd
- BCG_ContactInformation_Types.xsd
- BCG_GlobalChangeReasonCode.xsd
- BCG_GlobalCountryCode.xsd
- BCG_GlobalDocumentReferenceTypeCode.xsd
- BCG_GlobalLineItemStatusCode.xsd
- BCG_GlobalPartnerClassificationCode.xsd
- BCG_GlobalPartnerRoleClassificationCode.xsd
- BCG_GlobalProductUnitOfMeasureCode.xsd
- BCG_PartnerDescription_Types.xsd
- BCG_PhysicalAddress_Types.xsd
- BCG_string_len_0.xsd
- BCG_xml.xsd

Appendix D. Attributes

This appendix describes attributes you can set from the Community Console. The following attributes are described:

- "EDI attributes"
- "AS attributes" on page 283
- "RosettaNet attributes" on page 285
- "Backend Integration attribute" on page 287

EDI attributes

This section provides a description of the EDI attributes that you can use while setting up your EDI exchanges. Some of these attributes are predefined in the control string representing the transformation map associated with the EDI document. The values set in the control string (at the Data Interchange Services client) override any values you enter at the Community Console.

Envelope profile attributes

You can set various attributes for an EDI envelope profile. The attributes that are available depend on the EDI Type. In general, the attributes correspond to an EDI standard, and the allowable values depend on the EDI standard the envelope profile represents.

None of the attributes requires a value. For some of the attributes, a default value is used if you do not enter a value. The tables in this section list the attributes that have associated defaults and their default values.

Note: The envelope profile properties not listed do not have default values. The text value you specify is used if it is not overridden by generic or specific envelope properties set in the map or in a connection.

X12 attributes

The tables in this section list the X12 attributes for which default values are supplied.

General attributes: Table 84 lists the General attributes for which default values are provided.

Table 84. General attributes

Field name	Required?	Description	Default
INTCTLLEN (Interchange Control Number Length)	No	Defines a specific length for the interchange control number. If you enter a value, it must be an integer. If no value is entered, the default length is used.	9
GRPCTLLEN (Group Control Number Length)	No	Defines a specific length for the group control number. If you enter a value, it must be an integer. If no value is entered, the default length is used.	9

© Copyright IBM Corp. 2004, 2005

Table 84. General attributes (continued)

Field name	Required?	Description	Default
TRXCTLLEN (Transaction Control Number Length)	No	Defines a specific length for the transaction control number. If you enter a value, it must be an integer. If no value is entered, the default length is used.	9
ENVTYPE (Envelope Type)	No	This attribute is not set by the Hub Admin but is derived from the envelope profile type being created.	X12
MAXDOCS (Max Transactions Number)	No	Maximum number of transactions in an envelope. If you enter a value, it must be an integer.	No maximum
CTLNUMFLAG (Control Numbers by Transaction ID)	No	Yes indicates that separate sets of control numbers are kept based on the EDI transaction type. No indicates that a common set of control numbers for any EDI transaction type should be used.	No

Interchange attributes: No X12 interchange attributes are required, and the attributes do not have default values.

Group attributes: Table 85 lists the group attributes for which default values are provided.

Table 85. Group attributes

Field name	Required?	Description	Default
GS01 (Functional group ID)	No	The group identifier.	The default value comes from the control-string header. You can view this value in the Data Interchange Services client by looking at the Functional Group column of the EDI Document Definitions page.
GS08 (Group version)	No	The group version.	The default value is per the standard.

Transaction attributes: No transaction attributes are required. The attributes do not have default values.

UCS attributes

This section lists whether default values apply to a UCS interchange, group, and transaction.

General attributes: Table 86 lists the General attributes for which default values are provided.

Table 86. General attributes

Field name	Required?	Description	Default
INTCTLLEN (Interchange Control Number Length)	No	Defines a specific length for the interchange control number. If you enter a value, it must be an integer. If no value is entered, the default length is used.	5
GRPCTLLEN (Group Control Number Length)	No	Defines a specific length for the group control number. If you enter a value, it must be an integer. If no value is entered, the default length is used.	9

Table 86. General attributes (continued)

Field name	Required?	Description	Default
TRXCTLLEN (Transaction Control Number Length)	No	Defines a specific length for the transaction control number. If you enter a value, it must be an integer. If no value is entered, the default length is used.	9
ENVTYPE (Envelope Type)	No	This attribute is not set by the Hub Admin but is derived from the envelope profile type being created.	UCS
MAXDOCS (Max Transactions Number)	No	Maximum number of transactions in an envelope. If you enter a value, it must be an integer.	No maximum
CTLNUMFLAG (Control Numbers by Transaction ID)	No	Yes indicates that separate sets of control numbers are kept based on the EDI transaction type. No indicates that a common set of control numbers for any EDI transaction type should be used.	No

Interchange attributes: No interchange attributes are required. The attributes do not have default values.

Group attributes: Table 87 lists the group attributes for which default values are provided.

Table 87. Group attributes

Field name	Required?	Description	Default
GS01 (Functional group ID)	No	The group identifier.	The default value comes from the control-string header. You can view this value in the Data Interchange Services client by looking at the Functional Group column of the EDI Document Definitions page.
GS08 (Group version)	No	The group version.	The default value is per the standard.

Transaction attributes: No transaction attributes are required. The attributes do not have default values.

EDIFACT attributes

This section lists whether default values apply to an EDIFACT interchange, group, and message.

General attributes: Table 88 lists the General attributes for which default values are provided.

Table 88. General attributes

Field name	Required?	Description	Default
INTCTLLEN (Interchange Control Number Length)	No	Defines a specific length for the interchange control number. If you enter a value, it must be an integer. If no value is entered, the default length is used.	9
GRPCTLLEN (Group Control Number Length)	No	Defines a specific length for the group control number. If you enter a value, it must be an integer. If no value is entered, the default length is used.	9

Table 88. General attributes (continued)

Field name	Required?	Description	Default
TRXCTLLEN (Transaction Control Number Length)	No	Defines a specific length for the transaction control number. If you enter a value, it must be an integer. If no value is entered, the default length is used.	9
ENVTYPE (Envelope Type)	No	This attribute is not set by the Hub Admin but is derived from the envelope profile type being created.	EDIFACT
EDIFACTGRP (Create Groups for EDI)	No	This value is only for EDIFACT envelope types. (The group level has been deprecated in EDIFACT.) Yes indicates that functional groups (UNG/UNE segments) should be created for EDIFACT DATA. No indicates that they should not.	No
MAXDOCS (Max Transactions Number)	No	Maximum number of transactions in an envelope. If you enter a value, it must be an integer.	No maximum
CTLNUMFLAG (Control Numbers by Transaction ID)	No	Yes indicates that separate sets of control numbers are kept based on the EDI transaction type. No indicates that a common set of control numbers for any EDI transaction type should be used.	No

Interchange attributes: No interchange attributes are required. The attributes do not have default values.

Group attributes: Table 89 lists the group attributes for which default values are provided.

Table 89. Group attributes

Field name	Required?	Description	Default
UNG01 (Functional group ID)	No	The group identifier.	The default value comes from the control-string header. You can view this value in the Data Interchange Services client by looking at the Functional Group column of the EDI Document Definitions page.

Message attributes: Table 90 lists the message attributes for which default values are provided.

Table 90. Message attributes

Field name	Required?	Description	Default
UNH0201 (Message Type)	No	The type of message.	The default value comes from the control-string header. You can view this value in the Data Interchange Services client by looking at the EDI Document Definitions page.
UNH0202 (Message Version)	No	The version of the message.	D
UNH0203 (Message Release)	No	The release of the message.	Per the standard

Table 90. Message attributes (continued)

Field name	Required?	Description	Default
UNH0204 (Controlling Agency)	No	The code identifying a controlling agency.	UN

Document flow definition and connection attributes

This section lists document flow definition attributes for the envelope. Some of these attributes can be set only at the protocol or connection level, as indicated.

Separator and delimiter attributes

This section lists the characters used as delimiters or separators within an EDI interchange. Table 91 shows the attribute as it appears on the Community Console, the corresponding term in X12 and EDIFACT (ISO 9735 Version 4, Release 1), whether the attribute is required, and a description of the attribute. Following the table is an example of how these characters appear in an EDI document.

Attribute descriptions: The separator and delimiter attributes are listed in Table 91.

Note: Some characters (as noted) can be hexadecimal values. These can be Unicode values or values from another type of encoding. For Unicode, use the format \unnnn. For other encoding, use the form 0xnn.

Table 91. Envelope profile attributes

Attribute	X12 term	EDIFACT term	Description
Segment delimiter	segment terminator	segment terminator	This is a single character, which appears at the last character of a segment. The character can be a hexadecimal value. The default value is based on the EDI type. **X12** ~ (tilde) **EDIFACT** ‘ (single quote) **UCS** ~ (tilde)
Data element delimiter	data element separator	data element separator	This is a single character, which separates the data elements of a segment. The character can be a hexadecimal value. The default value is the based on the EDI type. **X12** * (asterisk) **EDIFACT** + (plus sign) **UCS** * (asterisk)

Table 91. Envelope profile attributes (continued)

Attribute	X12 term	EDIFACT term	Description
Subelement delimiter	component element separator	component data element separator	This is a single character, which separates the component elements of a composite data element. The character can be a hexadecimal value. The default value is the based on the EDI type. **X12** \ (back slash) **EDIFACT** : (colon) **UCS** \ (back slash)
Release character		release character	This is a single character, which overrides the meaning of the next character, allowing a separator character to appear within a data element. The character can be a hexadecimal value. It applies to EDIFACT only. **EDIFACT** ? (question mark)
Repeating data element separator	repetition separator	repetition separator	This is a single character, which separates the instances of a repeating data element. This character can be a hexadecimal value. The default value is based on the EDI type for X12 or EDIFACT. **X12** ^ (hat sign, accent circumflex) **EDIFACT** * (asterisk)
Decimal notation		decimal notation (deprecated)	This attribute was used in decimal formatting or parsing and is now deprecated. It can be a period or comma only. The default value is a period.

Example EDI structure: This section shows a simple EDI interchange and how the attributes described in Table 91 on page 275 are used in an interchange.

An EDI message consists of a series of segments in a particular order. A segment consists of a series of elements. In a segment, an element can be a simple data element, which contains only one item of information. An element can also be a composite data element, containing two or more simple data elements. The simple elements that make up a composite element are called component data elements.

There is no nesting of composite data elements. A composite element can contain only simple data elements, not other composites. Although not shown here, a component data element can also be defined as a repeating data element.

Consider the following example:

```
ABC*123*AA\BB\CC*001^002^003*star?*power~
```

In this example:

- ″ABC″ is the segment name (EDIFACT calls this the ″segment tag″); this would be called an ″ABC segment″

- ″*″ (asterisk) is the data element separator.

  The corresponding attribute name on the Community Console is Segment delimiter.
- ″123″ is the first data element, a simple data element (which might be referred to as ABC01 is some contexts)
- ″AA\BB\CC″ is the second data element (ABC02), a composite element made up of component data elements
  - ″\ ″ (backslash) is the component data element separator

    The corresponding attribute name on the Community Console is the Data element delimiter.
  - ″AA″ is the first component data element of ABC02 (which might be designated ABC0201)
  - ″BB″ is the second component data element of ABC02 (ABC0202)
  - ″CC″ is the third component data element of ABC02 (ABC0203)
- ″001^002^003″ is the third data element (ABC03), a repeating data element
  - ″^″ (hat sign) is the repetition separator

    The corresponding attribute name on the Community Console is the Repeating data element character.
  - ″001″,″002″, ″003″ are the repetitions (all would be designated ABC03)
- ″star?*power″ is the fourth data element (ABC04)
  - ″?″ (question mark) is the release character, meaning the following asterisk is not treated as a data element separator
  - ″star*power″ is the resulting value of ABC04
- ″~″ (tilde) is the segment terminator.

  The corresponding attribute name on the Community Console is Segment delimiter.

Additional EDI attributes

This section lists additional EDI attributes that you can set at the document flow definition level or the connection level.

Table 92. Additional EDI attributes

Attribute	Required	Description	Restrictions	Default
Segment output	No	Used in EDI/XML transformation, this indicates whether a line break should occur after each EDI segment or XML element.	Limited to protocol or connection	Yes
Allow documents with duplicate document IDs	No	Yes indicates that duplicate document IDs (interchange control numbers) are allowed. No indicates that duplicate interchange control numbers should be treated as an error.	Limited to protocol or connection	No
Max error level at Transformation	No	Indicates the maximum number of errors that can occur during a transformation before the transformation fails. Valid values are 0, 1, or 2. If the transformation map contains an Error command to indicate a user-specified error, and the level parameter of the Error command is greater than this value, the transformation fails.	Limited to protocol or connection	0

Table 92. Additional EDI attributes (continued)

Attribute	**Required**	**Description**	**Restrictions**	**Default**
FA Map	No	Provides the map to use for converting the internal generic FA to the specific FA. **Note:** You select this attribute from a list of maps identified as FA maps (map type of "K").	Limited to protocol or connection	
Envelope Profile	Yes	The EDI envelope profile name to use for enveloping. All envelope profiles that you have defined are available from the list.		
XMLNS Active	No	Do namespace processing for the input XML document. This attribute is used by the XML transformation step. Valid values are Yes or No.		Schema: Yes DTD: No
Max validation error level	No	The maximum acceptable validation error level (the error severity to accept before considering the transaction ″failed″). Valid values are 0, 1, or 2. **0** Allow only validation with no errors **1** Do not fail documents that have only simple element validation errors **2** Do not fail documents that have element or segment validation errors.		0
Validation level	No	Indicates the level of checking to be performed at the transaction level. A value of 2 means to use the values set for the Alphanumeric validation table and Char Set validation table attributes. This attribute also applies to the Detailed validation of segments attribute if that attribute is set to Yes. Valid values are 0, 1, or 2. **0** Only perform basic validation, such as checking for missing mandatory elements and segments and minimum or maximum lengths. Do not validate element values against the data types or code lists specified in the transaction definition. **1** Perform level 0 validation, plus validate the element values against the code lists specified for the data element. **2** Perform level 1 validation, plus validate that the element value is correct for the data type of the element.		0

Table 92. Additional EDI attributes (continued)

Attribute	Required	Description	Restrictions	Default
Char set validation table	No	Indicates the table to use for character set validation. This table is used only when the Validation level attribute is 2. This attribute refers to the virtual code lists table. The user can create new code lists in the Code Lists tab of the Mapping area in the Data Interchange Services client. This area also contains code lists that are used for other purposes, such as validation of certain EDI elements.		CHARSET
Alphanumeric validation table	No	Indicates the table to use for alphanumeric validation. This table is used only when the Validation level attribute is 2. The attribute refers to the virtual code list tables. The user can create new code lists in the Code Lists tab of the Mapping area in the Data Interchange Services client. This area also contains code lists that are used for other purposes, such as validation of certain EDI elements.		ALPHANUM
Generate group level info only in functional Ack	No	This attribute applies to EDI-X12. The values are Yes or No. **Yes** Generate group level information only for functional acknowledgment. **No** Generate full functional acknowledgment detail (for each individual transaction and segments and elements within a transaction).	Limited to protocol or connection	No
Century control year	No	When dates are being converted from two-digit years to four-digit years, two-digit years after this value are assumed to have a century value of "19". Two-digit years equal to or before this value are assumed to have a century value of "20". The valid range is 0-99.	Limited to protocol or connection	10

Table 92. Additional EDI attributes (continued)

Attribute	Required	Description	Restrictions	Default
Detailed validation of segment	No	This attribute applies to the following segment headers and trailers: • X12 – ISA, IEA – GS, GE – ST, SE • EDIFACT – UNA – UNB, UNZ – UNG, UNE – UNH, UNT • UNTUCS – BG, EG – GS, GE – ST, SE Valid values are Yes or No. **Yes** Perform detailed envelope segment validation. The depth of checking is controlled by the Validation level attribute. **No** Do not perform detailed envelope segment validation.	Limited to protocol or connection	No
TA1 override	No	Allow generation of a TA1 request if indicated in the Interchange envelope segment. Applies only to EDI-X12. If set to Yes, a TA1 is generated if specified in the Interchange envelope segment. If set to No, a TA1 is not generated, even if it was specified in the Interchange envelope segment.	Limited to protocol or connection	Yes
Discard on error	No	This attribute is used in polymorphic processing. In the case of a batch that results from de-enveloping, this attribute indicates whether to discard the entire batch if any of the transactions fail. Valid values are Yes and No.	Limited to protocol or connection	No
Connection Profile Qualifier1	No	This attribute is used by the Enveloper to determine which profile to use for an interchange connection. Transactions with different values for this attribute are put into different interchanges.		
Interchange qualifier	No	The code used to identify the format of the interchange sender or receiver identifier.		

Table 92. Additional EDI attributes (continued)

Attribute	Required	Description	Restrictions	Default
Interchange identifier	No	Identifies the specific sender or receiver of the document. The type of data entered is determined by the Interchange qualifier attribute.		
Interchange usage indicator	No	Indicates whether the source documents being translated are classified as Production, Test, or Information documents. Valid values are P, T, and I.		
Group application sender identifier	No	Identifies the specific sender of the transaction. This attribute, when agreed to by trading partners, facilitates addressing within a company.		
Group application receiver identifier	No	Identifies the specific receiver or application of the transaction. This attribute, when agreed to by trading partners, facilitates addressing within a company.		
Interchange reverse routing	No	Indicates the address to which the recipient should address any replies.		
Interchange routing address	No	The sub-address code for onward routing.		
Group application sender qualifier	No	The code used to identify the format of the group application sender identifier.		
Group application receiver qualifier	No	The code used to identify the format of the group application receiver identifier.		
Group application password	No	This attribute defines security information.		

Data Interchange Services client properties

This section lists the properties that can be set as part of the transformation map in the Data Interchange Services client and their corresponding WebSphere Partner Gateway attributes.

Table 93. Map properties and their corresponding attributes

Data Interchange Services client property	Overrides WebSphere Partner Gateway attribute
AckReq	Acknowledge Requested
Alphanum	Alphanumeric validation table
Charset	Char set validation table
CtlNumFlag	Control numbers by Transaction Id
EdiDecNot (Decimal notation)	Decimal notation
EdiDeDlm (Data element separator)	Data element delimiter
EdiDeSep (Repeating data element separator)	Repeating data element separator
EdifactGrp	Create Groups for EDI
EdiRlsChar (Release character)	Release character
EdiSeDlm (Component data element separator)	Subelement delimiter
EdiSegDlm (Segment terminator)	Segment delimiter
EnvProfName	Envelope profile

Table 93. Map properties and their corresponding attributes (continued)

Data Interchange Services client property	Overrides WebSphere Partner Gateway attribute
EnvType	Envelope type
MaxDocs	Max Transactions Number
Reroute	Interchange reverse routing
SegOutput	Segment output
ValLevel	Validation level
ValErrLevel	Max validation error level
ValMap	Validation map

Table 94 lists additional Data Interchange Services client properties and their associated WebSphere Partner Gateway attributes.

Table 94. Data Interchange Services client properties and their associated attributes

Data Interchange Services client property	Overrides WebSphere Partner Gateway attribute
IchgCtlNum	Interchange control number
IchgSndrQl	Interchange sender qualifier
IchgSndrId	Interchange sender ID
IchgRcvrQl	Interchange receiver qualifier
IchgRcvrId	Interchange receiver ID
IchgDate	Interchange date
IchgTime	Interchange time
IchgPswd	Interchange password
IchgUsgInd	Interchange usage indicator
IchgAppRef	Interchange application reference
IchgVerRel	Interchange version and release
IchgGrpCnt	Number of groups in interchange
IchgCtlTotal	Control total from interchange trailer segment
IchgTrxCnt	Number of documents in interchange
GrpCtlNum	Group control number
GrpFuncGrpId	Functional group ID
GrpAppSndrId	Group application sender ID
GrpAppRcvrId	Group application receiver ID
GrpDate	Group date
GrpTime	Group time
GrpPswd	Group password
GrpVer Group version.	Group version
GrpRel Group release.	Group release
GrpTrxCnt	Number of documents in group
TrxCtlNum	Transaction control number
TrxCode	Transaction code
TrxVer	Transaction version
TrxRel	Transaction release

Table 94. Data Interchange Services client properties and their associated attributes (continued)

Data Interchange Services client property	Overrides WebSphere Partner Gateway attribute
TrxSegCnt	Number of EDI Segments in the document

AS attributes

This section describes the AS attributes.

Table 95. AS attributes

Attribute	Required	Description	Restrictions	Default
Time to Acknowledge	No	The amount of time to wait for an MDN acknowledgment before resending the original request. This attribute works in conjunction with Retry Count. The units are in minutes.	Limited to package or connection	30
Retry Count	No	The number of times to send a request if an MDN is not received. This attribute works in conjunction with Time to Acknowledge. For example, if this attribute is set to 3, the request can potentially be sent four times (the initial time and then the three retries).	Limited to package or connection	3
AS Compressed	No	Compress the data. This attribute works in conjunction with the AS Compress Before Sign attribute.	Limited to package or connection	No
AS Compress Before Sign	No	Indicates whether AS compression should be applied to both the payload and signature or only to the payload. If you select Yes, the payload is compressed before the message is signed. This attribute works in conjunction with the AS Compressed attribute.	Limited to package or connection	Yes
AS Encrypted	No	Indicates whether encryption should be performed. **Note:** This is not the same as SSL encryption. For the TO side of an exchange (when you are sending documents to a partner), this specifies whether to encrypt the document. For the FROM side of an exchange (when you are receiving documents from a partner), if the attribute is set to Yes, an AS request sent from the partner must be encrypted. If the attribute is set to No, the document from the partner can be encrypted or un-encrypted. Valid values are Yes or No. **Yes** Encryption is required. **No** Encryption is not required.	Limited to package or connection	No

Table 95. AS attributes (continued)

Attribute	Required	Description	Restrictions	Default
AS MDN Requested	No	Specifies whether an MDN reply is required. If set to Yes, this attribute causes the “transport Disposition-notification-to” header to be filled in with the value from the AS MDN Email Address attribute. Valid values are Yes and No. **Yes** Request an MDN. **No** Do not request an MDN.	Limited to package or connection	Yes
AS MDN Email Address	Yes if the ″AS MDN Asynchronous″ attribute is Yes and you are using AS1.	Specifies the e-mail address for the partner to use when sending an asynchronous MDN. This attribute is used in conjunction with the AS MDN Requested attribute. The value of AS MDN Email Address is used in the “Disposition-notification-to” field. For AS1 only, this attribute works in conjunction with the AS MDN Asynchronous attribute of the format mailto:xxx@company.com.	Limited to package or connection	
AS MDN Http Url	Yes if the ″AS MDN Asynchronous″ attribute is Yes and you are using AS2.	This attribute applies to AS2 and is used to specify the URL to which a partner should send an asynchronous MDN. This attribute works in conjunction with the AS MDN Asynchronous attribute.	Limited to package or connection	
AS MDN Asynchronous	No	Specifies whether the MDN should be returned synchronously or asynchronously. The value of this attribute affects whether the AS MDN HTTP URL or AS MDN Email Address attribute is used. Valid values are Yes and No. **Yes** Asynchronous **No** Synchronous If this attribute is Yes, the ″receipt-delivery-option″ field is filled in based on the AS MDN HTTP URL attribute (for AS2) or the AS MDN Email Address attribute (for AS1).	Limited to package or connection	Yes

Table 95. AS attributes (continued)

Attribute	Required	Description	Restrictions	Default
AS MDN Signed	No	Indicates whether the request requires that a signed MDN be returned. This attribute works in conjunction with AS MDN Requested. If the value is Yes, the “Disposition-notification-options: signed-receipt-protocol” is filled in. Valid values are Yes and No. **Yes** Signed MDN requested **No** Signed MDN is not requested If this attribute is set to Yes, the MDN sent by the partner has to be signed. If this attribute is set to No, the MDN can be signed or unsigned.	Limited to package or connection	No
AS Message Digest Algorithm	No	The message digest algorithm to use when signing. This attribute is used in conjunction with the AS Signed and AS MDN Signed attributes. For signed MDNs, this value is used to fill in the “Disposition-notification-options: signed-receipt-micalg” header.	Limited to package or connection	sha1
AS Signed	No	Specifies whether to sign the document. For the TO side of an exchange (when you are sending documents to a partner), this specifies whether to sign the document. For the FROM side of the exchange (when you are receiving from a partner) if the attribute is set to Yes, an AS request sent from the partner must be signed. If the attribute is set to No, the document from the partner can be signed or unsigned. **Yes** Sign the document **No** Signed document is not required	Limited to package or connection	No
AS Business Id	No	The AS business ID to use in the “AS2-To” header. If a value is not supplied, WebSphere Partner Gateway uses the recipient business ID used in the source document. **Note:** The “AS2-From” header will be set from the original source document that came into WebSphere Partner Gateway and that is being sent out as AS.	Limited to package or connection	

RosettaNet attributes

This section describes RosettaNet attributes.

Table 96. RosettaNet attributes

Attribute	Required	Description	Restrictions	Default
Time To Acknowledge	Yes	The amount of time to wait for a Receipt Acknowledgment before resending the original request. This attribute works in conjunction with Retry Count. The units are in minutes. The default value is taken from the RosettaNet PIP specification document.	Limited to package or connection	120
Time To Perform	Yes	The amount of time to wait for a response to a request action before sending a failure notification message.	Limited to package or connection	
Retry count	Yes	The number of times to send a request when an Receipt Acknowledgment was not received. This attribute works in conjunction with Time to Acknowledge. For example, with a setting of 3, the request can potentially be sent 4 times (the initial time and the three retries). The default value is taken from the RosettaNet PIP specification document.	Limited to package or connection	3
Digital Signature Required	No	Indicates whether the PIP message requires a digital signature. The default value is taken from the RosettaNet PIP specification document.	Limited to package or connection	Yes
Non-Repudiation Required	No	Indicates whether to store the original document in the non-repudiation store. The default value is taken from the RosettaNet PIP specification document.	Limited to package or connection	Yes
Non-Repudiation of Receipt Required	No	Indicates whether to store the Receipt Acknowledgement document in the non-repudiation store. The default value is taken from the RosettaNet PIP specification document.	Limited to package or connection	Yes
Sync Supported		Indicates whether the PIP supports synchronous communication. The default value is provided based on the PIP specification.	Limited to package or connection. This attribute is available for RNIF 2.0 only.	
Sync Ack Required		Indicates whether the PIP requires a synchronous Receipt Acknowledgment. The default value is provided based on the PIP specification.	Limited to package or connection. This attribute is available for RNIF 2.0 only.	

Table 96. RosettaNet attributes (continued)

Attribute	Required	Description	Restrictions	Default
Global Supply Chain Code	Required for RNIF 1.1	The code identifying the supply chain for the participant's function. Valid values are: • Electronic Components • Information Technology • Semiconductor Technology	Limited to package or connection	
Encryption		This attribute indicates whether encryption should be performed. **Note:** This is not the same as SSL encryption. For the TO side of an exchange (when you are sending documents to a partner), this specifies whether to encrypt the document. For the FROM side of an exchange (when you are receiving documents from a partner), if the attribute is set to Yes, an RNIF request sent from the partner must be encrypted. If the attribute is set to No, the document from the partner can be encrypted or un-encrypted. Valid values are: **None** Encryption is not required. **Payload** Encrypt the RosettaNet Service Content only. **Payload and Container** Encrypt the RosettaNet service content and the service header together.	Limited to package or connection. This attribute is available for RNIF 2.0 only.	None

Backend Integration attribute

This section describes the attribute associated with Backend Integration packaging.

Table 97. Backend Integration attribute

Attribute	Description	Default
Envelope Flag	This attribute indicates whether to wrap the document in an XML envelope. Valid values are Yes and No.	No

Appendix E. Notices

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

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

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

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

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

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

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

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

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

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

© Copyright IBM Corp. 2004, 2005

Burlingame, CA 94010
U.S.A

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

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

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

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

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

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

COPYRIGHT LICENSE

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

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

COPYRIGHT AND PERMISSION NOTICE

Copyright (c) 1995-2003 International Business Machines Corporation and others

All rights reserved.

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

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

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

Programming interface information

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

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

Trademarks and service marks

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

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

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

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

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

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

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

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

WebSphere Partner Gateway Enterprise and Advanced Editions includes software developed by the Eclipse Project (www.eclipse.org).

WebSphere Partner Gateway Enterprise and Advanced Editions, version 6.0.

Index

Special characters

- &DT99724 map 116
- &DT99735 map 116
- &DT99933 map 116
- &DTCTL map 116
- &DTCTL21 map 116
- &WDIEVAL map 116
- &X44TA1 map 116

Numerics

- 0A1 Notification of Failure
  - V02.02 PIP 231
  - V1.0 PIP 230
- 0A1 PIP 217
- 2048-byte encryption certificate maximum 150
- 2A1 Distribute New Product PIP 231
- 2A12 Distribute Product Master PIP 233
- 3A1 Request Quote PIP 233
- 3A2 Request Price and Availability PIP 234
- 3A4 Request Purchase Order
  - V02.00 PIP 235
  - V02.02 PIP 236
- 3A5 Query Order Status PIP 238
- 3A6 Distribute Order Status PIP 239
- 3A7 Notify of Purchase Order PIP 240
- 3A8 Request Purchase Order Change
  - V01.02 PIP 241
  - V01.03 PIP 242
- 3A9 Request Purchase Order Cancellation PIP 244
- 3B11 Notify of Shipping Order PIP 246
- 3B12 Request Shipping Order PIP 247
- 3B13 Notify of Shipping Order Confirmation PIP 248
- 3B14 Request Shipping Order Cancellation 249
- 3B18 Notify of Shipping Documentation PIP 250
- 3B2 Notify of Advance Shipment PIP 244
- 3B3 Distribute Shipment Status PIP 245
- 3C1 Return Product PIP 251
- 3C3 Notify of Invoice PIP 252
- 3C4 Notify of Invoice Reject PIP 253
- 3C6 Notify of Remittance Advice PIP 253
- 3C7 Notify of Self-Billing Invoice PIP 254
- 3D8 Distribute Work in Process PIP 255
- 4A1 Notify of Strategic Forecast PIP 256
- 4A3 Notify of Threshold Release Forecast PIP 257
- 4A4 Notify of Planning Release Forecast PIP 258
- 4A5 Notify of Forecast Reply PIP 258
- 4B2 Notify of Shipment Receipt PIP 259
- 4B3 Notify of Consumption PIP 260
- 4C1 Distribute Inventory Report
  - V02.01 PIP 261
  - V02.03 PIP 262
- 5C1 Distribute Product List PIP 263
- 5C2 Request Design Registration PIP 263
- 5C4 Distribute Registration Status PIP 264
- 5D1 Request Ship From Stock and Debit Authorization PIP 265
- 6C1 Query Service Entitlement PIP 266
- 6C2 Request Warranty Claim PIP 267
- 7B1 Distribute Work in Process PIP 267
- 7B5 Notify of Manufacturing Work Order PIP 268
- 7B6 Notify of Manufacturing Work Order Reply PIP 269

A

- Acknowledge Requested 99
- Acknowledgment Request 99
- actions
  - copying 52
  - creating 52
  - description 13
  - handlers 51
- Admin user
  - Community Manager 120
  - creation of 30
  - participant 140
- alertable events 166
- Allow Duplicate elements attribute 277
- Alphanumeric validation table attribute 279
- APIs, enabling 165
- Application Password 100
- Application Receiver 99
- Application Receiver ID 100
- Application Receiver ID Qualifier 100
- Application Reference 99
- Application Sender 99
- Application Sender ID 100
- Application Sender ID Qualifier 100
- AS attributes
  - AS Business ID 121, 144, 285
  - AS Compress Before Sign 283
  - AS Compressed 283
  - AS Encrypted 161, 162, 283
  - AS MDN Asynchronous 284
  - AS MDN Email Address 284
  - AS MDN Requested 284
  - AS MDN Signed 285
  - AS Message Digest Algorithm 285
  - AS Signed 158, 285
  - Retry Count 283
  - Time to Acknowledge 283
- AS Business ID attribute 121, 144, 285
- AS Compress Before Sign attribute 283
- AS Compressed attribute 283
- AS Encrypted attribute 161, 162, 283
- AS MDN Asynchronous attribute 284
- AS MDN Email Address attribute 284
- AS MDN Http Url attribute 284
- AS MDN Requested attribute 284
- AS MDN Signed attribute 285
- AS Message Digest Algorithm attribute 285
- AS packaging 4
- AS Signed attribute 158, 285
- AS1 standard 4
- AS2 standard 4
- AS2 SyncCheck handler 46
- ascii command 39, 135
- Association Assigned 100
- Association Assigned Code 100
- attributes
  - B2B capabilities 56, 86
  - connection profile 101
  - delimiter 275
  - document flow definition 55, 85
  - EDI document flow-level 109
  - EDI protocol-level 109
  - EDI, list of 271
  - EDIFACT envelope 273
  - envelope profile 97, 271
  - global transport 32
  - participant connection 57, 87
  - precedence 143
  - separator 275
  - splitter handler 43
  - UCS envelope 272
  - X12 envelope 271
- Authorization Information 98
- Authorization Information Qualifier 98

B

- B2B capabilities
  - attributes 56, 86
  - Community Manager 120
  - description 56, 86
  - participants 140
- Backend Integration packaging
  - creating 228
  - description 4
- banner, adding 27
- batch mode 95, 96
- BCG_BATCHDOCS attribute 43, 90, 95
- bcg.CRLDir property 156
- BCG.Properties file
  - bcg.CRLDir 156
  - updating 0A1 PIP contact information 217
- bcgChgPassword.jacl script 149
- bcgClientAuth.jacl script
  - resetting after using bcgssl.jacl 163
  - setting up client authentication 153
- bcgDISImport utility 107
- bcgreceiver servlet 33
- bcgssl.jacl script 162
- BG01 Communications ID 99

© Copyright IBM Corp. 2004, 2005

BG02 Communications Password 99
binary command 39, 135
Binary directory 18
binary documents 58
binary files
  naming convention 19
  processing 19
binary protocol 5
branding the Community Console 27
Business ID 120, 139, 140
business protocols 5
bye command 40, 135

C

calendar-based scheduling
  Enveloper 96
  FTP Scripting targets 42
  SMTP (POP3) target 36
cardinality 229
cd command 39, 135
Century control year attribute 279
certificate chains 150
certificate revocation list (CRL)
  adding 156
  distribution points 156
Certificate revoked or expired message 162
certificates
  expired, replacing 149
  format, converting 154
  intermediate 150
  list of 163
  primary 150
  revoked 156
  secondary 150
  self-signed 150
  signature 157, 158
  target 150
chaining, map 83
chains, certificate 150
Char set validation table attribute 279
client authentication
  configuring 153
  inbound SSL 153
  outbound SSL 155
commands, FTP 39, 135
Common Access Reference 100
common_LineNumber_R type elements 229
Communication Agreement ID 99
Communications ID 99
Communications Password 99
Community Console
  background header 27
  banner 27
  branding 27
  logging in 26
  logo, adding 27
  starting 25
Community Manager
  B2B capabilities 120
  description 2, 119
  profile 119
company logo, adding 27
component data element separator 276
component data elements 276, 277
component element separator 276
composite data element 276, 277
configuration points
  gateways 14, 137
  Postprocess 10, 46, 137
  Preprocess 9, 43, 137
  SyncCheck 10, 45
  synchronous exchanges 43
  target 9, 43
configuration points, gateway
  modifying 137
  Postprocess 15, 137
  Preprocess 15, 137
configuration points, target
  modifying 47
  overview 9
  Postprocess 10, 46
  Preprocess 9, 43
  SyncCheck 10, 45
Connection Profile Qualifier 1 attribute 102, 280
connection profiles
  attributes 101
  description 101
  for transactions 101
  interchanges 102
  setting up 102
connections, participant
  activating 143
  attributes 57, 87
  description 56, 86
contact information, 0A1 PIP 217
content-type headers, cXML 75
control numbers
  description 103
  initialization 105
  masks 103
  viewing 106
Control Numbers by Transaction ID 98, 272, 273, 274
control segments 82
Controlling Agency 100, 275
Create Groups for EDI 274
CRL (certificate revocation list)
  adding 156
  distribution points 156
CTLNUMFLAG (Control Numbers by Transaction ID) 272, 273, 274
custom XML protocol definitions 77
cXML documents
  content-type headers 75
  document flow definitions 76
  DTDs 73
  example 73
  message type 74
  request type 74
  response type 74
  root element 73
cXML protocol 6
cXML SyncCheck handler 46

D

Data element delimiter attribute 275, 277
data element separator 275, 277
data elements
  component 276
  composite 276
  description 81
  simple 276
Data Interchange Services
  maps, importing 107
Data Interchange Services client
  description 23, 107
  mapping specialist 23, 83
  properties 281
DayofMonth type element 230
de-enveloping interchanges 91
Decimal notation 276
Decimal notation attribute 276
default gateway, setting 138
delete command 39, 135
delimiter attributes 275
Detailed validation of segments attribute 280
digital signature
  description 148
  enabling 158
Digital Signature Required attribute 286
directories
  Binary 18
  Documents 18
  FTP server 18
  JMS 21
  Production 18
  Test 18
Discard on error attribute 280
Distribute Inventory Report
  V02.01 PIP 261
  V02.03 PIP 262
Distribute New Product Information PIP 231
Distribute Order Status PIP 239
Distribute Product List PIP 263
Distribute Product Master PIP 233
Distribute Registration Status PIP 264
Distribute Shipment Status PIP 245
Distribute Work in Process PIP 255, 267
document definitions, Data Interchange Services 107
document flow definitions
  attributes 55, 85
  description 55, 85
  ensuring availability 55, 85
  overview 3
  RNIF 61
  types 58
  validation maps, associating 79
  Web services 69
document flow packages, PIP 62
document flows
  custom 78
  description 6
Document Manager
  description 10
  starting 26
Document Viewer 80, 118
Documents directory 18
DTDs
  converting to XML schema 220
  cXML documents 73

E

- EDI
  - attributes, list of 271
  - data elements 81
  - interchanges 81
  - overview 81
  - segments 81
  - transactions 81
- EDI attributes
  - Allow Duplicate elements 277
  - Alphanumeric validation table 279
  - Century control year 279
  - Char set validation table 279
  - Connection Profile Qualifier 1 102, 280
  - Detailed validation of segments 280
  - Discard on error 280
  - FA map 278
  - Generate group level info only in functional Ack 279
  - Group application password 281
  - Group application receiver identifier 281
  - Group application receiver qualifier 281
  - Group application sender identifier 281
  - Group application sender qualifier 281
  - Interchange identifier 281
  - Interchange qualifier 280
  - Interchange reverse routing 281
  - Interchange routing address 281
  - Interchange usage indicator 281
  - Max error level at Transformation 277
  - Max validation error level 278
  - Segment output 277
  - TA1 override 280
  - Validation level 278
  - XMLNS Active 278
- EDI envelope attributes 99
  - BG01 Communications ID 99
  - BG02 Communications Password 99
  - Control Numbers by Transaction ID 98
  - CRPCTLLEN Group Control Number Length 272
  - CTLNUMFLAG Control Numbers by Transaction ID 272, 273, 274
  - delimiter 275
  - EDIFACTGRP Create Groups for EDI 274
  - Group Control Number Length 98, 271
  - GRPCTLLEN Group Control Number Length 273
  - GS01 Functional Group ID 99, 272, 273
  - GS02 Application Sender 99
  - GS03 Application Receiver 99
  - GS07 Group Agency 100
  - GS08 Group Version 100, 272, 273
  - INTCTLLEN Interchange Control Number Length 271, 272, 273
  - Interchange Control Number Length 98

- EDI envelope attributes *(continued)*
  - ISA01 Authorization Information Qualifier 98
  - ISA02 Authorization Information 98
  - ISA03 Security Information Qualifier 98
  - ISA04 Security Information 98
  - ISA11 Interchange Standards 98
  - ISA12 Interchange Version ID 99
  - ISA14 Acknowledge Requested 99
  - Max Transactions Number 98
  - MAXDOCS Max Transactions Number 272, 273, 274
  - separator 276
  - Transaction Control Number Length 98
  - TRXCTLLEN Transaction Control Number Length 272, 273, 274
  - UNB0101 Syntax ID 99
  - UNB0102 Syntax Version 99
  - UNB0601 Recipients Reference/Password 99
  - UNB0602 Recipients Reference/Password Qualifier 99
  - UNB07 Application Reference 99
  - UNB08 Priority 99
  - UNB09 Acknowledgment Request 99
  - UNB10 Communication Agreement ID 99
  - UNB11 Test Indicator (Usage Indicator) 99
  - UNG01 Functional Group ID 100, 274
  - UNG0201 Application Sender ID 100
  - UNG0202 Application Sender ID Qualifier 100
  - UNG0301 Application Receiver ID 100
  - UNG0302 Application Receiver ID Qualifier 100
  - UNG06 Controlling Agency 100
  - UNG0701 Message Version 100
  - UNG0703 Association Assigned 100
  - UNG0703 Message Release 100
  - UNG08 Application Password 100
  - UNH0201 Message Type 100, 274
  - UNH0202 Message Version 100, 274
  - UNH0203 Message Release 100, 274
  - UNH0204 Controlling Agency 100, 275
  - UNH0205 Association Assigned Code 100
  - UNH03 Common Access Reference 100
- EDI interchanges
  - processing of 91
  - structure 81, 82
- EDI splitter handler 44, 45
- EDI to EDI flow
  - description 87
  - setting up 108
- EDI to ROD flow
  - description 88
  - example 185
  - setting up 110
- EDI to XML flow
  - description 88

- EDI to XML flow *(continued)*
  - example 197
  - setting up 110
- EDI with passthrough flow
  - example 169
  - setting up 59
- EDI-Consent protocol 5
- EDI-EDIFACT protocol 5
- EDI-X12 interchange structure 82
- EDI-X12 protocol 5
- EDIFACT envelope attributes 273
- EDIFACTGRP (Create Groups for EDI) 274
- Encoding attribute 43
- encryption
  - description 148
  - enabling 161, 162
- Encryption attribute 287
- encryption certificates, limits on length 150
- enumeration 230
- envelope attributes 97
- Envelope Flag attribute 287
- envelope profiles
  - attributes 97, 271
  - creating 97
  - description 96
  - General attributes 98
  - Group attributes 99
  - Interchange attributes 98
  - Transaction attributes 100
- Envelope Type 272, 273, 274
- Enveloper
  - batch mode 96
  - default values, modifying 96
  - description 95
  - interval-based scheduling 96
  - locking 95
  - maximum lock time 96
  - queue age 96
- ENVTYPE Envelope Type 272, 273, 274
- event queues, specifying 165
- Event Viewer 162
- events, alertable 166
- examples
  - EDI to ROD 185
  - EDI to XML 197
  - EDI with passthrough 169
  - functional acknowledgments 194
  - ROD to EDI 209
  - security 174
  - TA1 acknowledgment 190
  - XML to EDI 202
- expired certificate, replacing 149

F

- FA (functional acknowledgment)
  - description 116
  - example 194
- FA (functional acknowledgment) maps
  - description 83
  - system-supplied 116
- FA map attribute 278
- failure notification, PIP processing 217
- file-directory gateways 17
- file-system targets 38

format, validation maps 229
From Packaging Name attribute 44
From Packaging Version attribute 44
From Process Code attribute 44
From Process Version attribute 44
From Protocol Name attribute 44
From Protocol Version attribute 44
FTP commands
  ascii 39, 135
  binary 39, 135
  bye 40, 135
  cd 39, 135
  delete 39, 135
  get 39
  getdel 40
  mget 40
  mgetdel 40
  mkdir 40, 135
  mput 135
  open 40, 135
  passive 39, 135
  quit 40, 135
  quote 40, 135
  rename 40
  rmdir 40, 135
  site 40, 135
FTP gateways 128
FTP Scripting targets 39
FTP scripts
  commands allowed in 39, 135
  description 23
  gateways 134
  targets 39
FTP server
  Binary directory 18
  configuring 20
  directory structure 18
  Documents directory 18
FTP targets 34
FTPS server, security considerations 20
functional acknowledgment maps
  description 83
  importing 107
  system-supplied 116
functional acknowledgments
  description 116
  example 194
Functional Group ID 99, 100, 272, 274

G

gateways
  configuration points 14
  default 138
  description 14
  file-directory 17, 132
  FTP 128
  FTP Scripting 134, 135
  FTPS 133
  HTTP 125
  HTTPS 127
  JMS 130
  Postprocess configuration point 15, 137
  Preprocess configuration point 15, 137
  SMTP 129
gateways *(continued)*
  transports supported 123
  user-defined transports 138
General attributes, envelope profile 98
Generate group level info only in function Ack attribute 279
Generic Document Flow Handler 45
get command 39
getdel command 40
Global Supply Chain Code attribute 287
global transport attributes
  gateway 124
  target 32
GlobalLocationIdentifier type element 230
Group Agency 100
Group application password attribute 281
Group application receiver identifier attribute 281
Group application receiver qualifier attribute 281
Group application sender identifier attribute 281
Group application sender qualifier attribute 281
Group attributes, envelope profile 99
Group Control Number Length 98, 271, 272, 273
Group Version 100, 272, 273
groups, EDI
  description 82
  header segments 82
  trailer segments 82
GRPCTLLEN (Group Control Number Length) 271, 272, 273
GS attributes 99
GS01 Functional Group ID 99, 272, 273
GS02 Application Sender 99
GS03 Application Receiver 99
GS07 Group Agency 100
GS08 Group Version 100, 272, 273

H

handler types 49
handlers
  description 9
  Protocol Packaging 51
  Protocol Processing 50
  Protocol Unpackaging 50
  uploading 32, 49
  user-defined 49
Handlers List page 47
handshake, SSL 151
header background, adding 27
header segment 82
help system, starting 26
HTTP targets
  setting up 33
  SyncCheck handlers 46
Hub Admin user xi, 26

I

IBM Key Management Tool (ikeyman)
  description 148
  location 148
ikeyman utility
  description 148
  location 148
inbound fixed workflows
  description 11
  handlers 50
  user-defined handlers 50
inbound signature certificates 157
inbound SSL
  client authentication 153
  configuring with non-default key stores 162
  server authentication 152
INTCTLLEN (Interchange Control Number Length) 271, 272, 273
interactions
  cXML documents 76
  description 56, 86
  RosettaNet documents 65
  Web services 72
Interchange Control Number Length 98, 271, 272, 273
Interchange identifier attribute 281
Interchange qualifier attribute 280
Interchange reverse routing attribute 281
Interchange routing address attribute 281
Interchange Standards ID 98
Interchange usage indicator attribute 281
Interchange Version ID 99
interchanges
  connection profiles 102
  processing of 91
  structure 81
intermediate certificates 150
interval-based scheduling
  Enveloper 96
  FTP Scripting targets 42
  SMTP (POP3) target 36
ISA01 Authorization Information Qualifier 98
ISA02 Authorization Information 98
ISA03 Security Information Qualifier 98
ISA04 Security Information 98
ISA11 Interchange Standards ID 98
ISA12 Interchange Version ID 99
ISA14 Acknowledge Requested 99
ISA15 Test Indicator 99

J

Java run time, adding 22
JMS configuration, defining 22
JMS context, defining 22
JMS directories, creating 21
JMS gateways 130
JMS targets
  setting up 36
  SyncCheck handlers 46
JMS, modifying default configuration 21

JMSAdmin.config file 21
JRE jurisdiction policy files 150
jurisdiction policy files, JRE 150

K

key stores
  default password 149
  description 148
  using non-default 162
keys
  private 148
  public 148

L

locks
  Enveloper 95, 96
  FTP Scripting transport 32, 124
logging in to the Community Console 26
logo, adding company 27

M

map chaining 83
mapping specialist 23, 83
maps
  functional acknowledgment 83
  importing 107
  transformation 83
  validation 79, 84
masks, control number 103
Max error level at transformation attribute 277
Max Transactions Number 98, 272, 273, 274
Max validation error level attribute 278
MAXDOCS (Max Transactions Number) 272, 273, 274
Maximum Lock Time field 96
Maximum Queue Age field 96
maxOccurs attribute 229
Message Release 100, 274
Message Release ID 100
Message Type 100, 274
Message Version 100, 274
Metadictionary attribute 44
Metadocument attribute 44
Metasyntax attribute 44
mget command 40
mgetdel command 40
minOccurs attribute 229
mkdir command 40, 135
mput command 135
multiple certificates 150
multiple documents in one file 84

N

N/A specification 4
No attributes were found message 218
No valid encryption certificate found message 162
non-repudiation 148
Non-Repudiation of Receipt Required attribute 286
Non-Repudiation Required attribute 286
None packaging 4
Notification of Failure
  V02.00 PIP 231
  V1.0 PIP 230
Notify of Advance Shipment PIP 244
Notify of Consumption PIP 260
Notify of Forecast Reply PIP 258
Notify of Invoice PIP 252
Notify of Invoice Reject PIP 253
Notify Of Manufacturing Work Order PIP 268
Notify Of Manufacturing Work Order Reply PIP 269
Notify of Planning Release Forecast PIP 258
Notify of Purchase Order Update PIP 240
Notify of Remittance Advice PIP 253
Notify of Self-Billing Invoice PIP 254
Notify of Shipment Receipt PIP 259
Notify of Shipping Documentation PIP 250
Notify of Shipping Order Confirmation PIP 248
Notify of Shipping Order PIP 246
Notify of Strategic Forecast PIP 256
Notify of Threshold Release Forecast PIP 257

O

open command 40, 135
outbound fixed workflows
  description 13
  handlers 51
  user-defined handlers 50
outbound signature certificates 158
outbound SSL
  client authentication 155
  server authentication 154

P

packaging
  AS 4
  Backend Integration 4
  description 3
  N/A concept 4
  None 4
  RNIF 4
participant connections
  activating 143
  attributes 57, 87
  description 56, 86
participants
  B2B capabilities 140
  creating 139
Partner Interface Process (PIP) 60
passive command 39, 135
password policy, setting 29
passwords
  default 26
  key store default 149
passwords *(continued)*
  trust store default 149
permissions
  changing default 30
  description 29
PIP package contents
  0A1 Notification of Failure 230
  0A1 Notification of Failure V02.00 231
  2A1 Distribute New Product Information 231
  2A12 Distribute Product Master 233
  3A1 Request Quote 233
  3A2 Request Price and Availability 234
  3A4 Request Purchase Order V02.00 235
  3A4 Request Purchase Order V02.02 236
  3A5 Query Order Status 238
  3A6 Distribute Order Status 239
  3A7 Notify of Purchase Order Update 240
  3A8 Request Purchase Order Change V01.02 241
  3A8 Request Purchase Order Change V01.03 242
  3A9 Request Purchase Order Cancellation 244
  3B11 Notify of Shipping Order 246
  3B12 Request Shipping Order 247
  3B13 Notify of Shipping Order Confirmation 248
  3B14 Request Shipping Order Cancellation 249
  3B18 Notify of Shipping Documentation 250
  3B2 Notify of Advance Shipment 244
  3B3 Distribute Shipment Status 245
  3C1 Return Product 251
  3C3 Notify of Invoice 252
  3C4 Notify of Invoice Reject 253
  3C6 Notify of Remittance Advice 253
  3C7 Notify of Self-Billing Invoice 254
  3D8 Distribute Work in Process 255
  4A1 Notify of Strategic Forecast 256
  4A3 Notify of Threshold Release Forecast 257
  4A4 Notify of Planning Release Forecast 258
  4A5 Notify of Forecast Reply 258
  4B2 Notify of Shipment Receipt 259
  4B3 Notify of Consumption 260
  4C1 Distribute Inventory Report V02.01 261
  4C1 Distribute Inventory Report V02.03 262
  5C1 Distribute Product List 263
  5C2 Distribute Product List 263
  5C4 Distribute Registration Status 264
  5D1 Request Ship From Stock and Debit Authorization 265
  6C1 Query Service Entitlement 266
  6C2 Request Warranty Claim 267
  7B1 Distribute Work in Process 267

- PIP package contents *(continued)*
  - 7B5 Notify Of Manufacturing Work Order 268
  - 7B6 Notify Of Manufacturing Work Order Reply 269
- PIP packages
  - creating 219
  - updating 219
- PIP release notes 219
- PIPs
  - 0A1 217
  - deactivating 217
  - description 60
  - document flow package contents 230
  - document flow packages 62
  - failure notification 217
  - list of supported 61
  - message processing 60
  - uploading packages 64
  - XML schema files, creating schemas 219
  - XSD file, creating 219
- POP3 targets 35
- Postprocess configuration point
  - gateway 15, 137
  - handler types 47
  - target 10, 46
- Preprocess configuration point
  - gateway 15, 137
  - target 9, 43
- primary certificates
  - description 150
  - outbound digital signature 158
  - outbound encryption 161
  - outbound SSL 155
- Priority 99
- private key 148
- private WSDL files 69
- Production directory 18
- profiles
  - Community Manager 119
  - connection 101
  - envelope 96
  - participant 139
- properties
  - Data Interchange Services client 281
  - transformation map 281
- Protocol Packaging
  - handlers 51
  - step, description 13
- Protocol Processing
  - handlers 50
  - step, description 12
- Protocol Unpackaging
  - handlers 50
  - step, description 12
- protocols
  - binary 5
  - custom XML 77
  - cXML 6
  - EDI-Consent 5
  - EDI-EDIFACT 5
  - EDI-X12 5
  - list 5
  - RNSC 6
  - RosettaNet 6
  - Web service 6
- protocols *(continued)*
  - XMLEvent 6
- public key 148
- public WSDL files 69

Q

- Qualifier1 field 102
- Query Order Status PIP 238
- Query Service Entitlement PIP 266
- queue age, Enveloper 96
- queues
  - event 165
  - JMS, creating 21
- quit command 40, 135
- quote command 40, 135

R

- raw documents, viewing 80, 118
- Receiver
  - description 7, 31
  - starting 25
- Recipients Reference/Password 99
- Recipients Reference/Password Qualifier 99
- record-oriented data (ROD) documents 84
- Release character 276
- Release character attribute 276, 277
- rename command 40
- Repeating data element character attribute 277
- Repeating data element separator attribute 276
- repitition separator 276
- Request Purchase Order
  - V02.00 PIP 235
  - V02.02 PIP 236
- Request Purchase Order Cancellation PIP 244
- Request Purchase Order Change
  - V01.02 PIP 241
  - V01.03 PIP 242
- Request Quote PIP 233
- Request Ship From Stock and Debit Authorization PIP 265
- Request Shipping Order Cancellation PIP 249
- Request Shipping Order PIP 247
- Request Warranty Claim PIP 267
- resource bundles 28
- Retry Count attribute 283, 286
- Return Product PIP 251
- revoked certificates 156
- rmdir command 40, 135
- RNIF packages
  - creating 228
  - location 61
- RNIF packaging 4
- RNIF SyncCheck handler 46
- RNIF, description of 60
- RNSC messages 60
- RNSC protocol 6
- ROD documents
  - description 84
- ROD documents *(continued)*
  - processing of 94
- ROD documents to EDI flow
  - description 89
  - setting up 113
- ROD splitter handler 44, 45, 84
- ROD to EDI flow
  - description 88
  - example 209
  - setting up 112
- ROD to ROD flow
  - description 91
  - setting up 115
- ROD to XML flow
  - description 90
  - setting up 114
- root CA (certifying authority) 150
- RosettaNet
  - description 60
  - Web site 60
- RosettaNet attributes
  - Digital Signature Required 286
  - editing 218
  - Encryption 64, 287
  - Global Supply Chain Code 64, 287
  - Non-Repudiation of Receipt Required 286
  - Non-Repudiation Required 286
  - Retry Count 286
  - Sync Ack Required 64, 286
  - Sync Supported 64, 286
  - Time to Acknowledge 286
  - Time to Perform 286
- RosettaNet Implementation Framework 60
- RosettaNet messages
  - event notification 61
  - versions supported 60
- RosettaNet protocol 6
- RosettaNet Service Content messages 60
- RosettaNet XML message guidelines 219
- RosettaNet XML message schema 219

S

- scheduling
  - Enveloper 96
  - FTP Scripting targets 42
  - SMTP (POP3) target 36
- schemas
  - PIP packages 219
  - WSDL files 70
- secondary certificates
  - description 150
  - outbound digital signature 158
  - outbound encryption 161
  - outbound SSL 155
- security
  - certificate list 163
  - example 174
  - FTPS server considerations 20
  - overview 147
  - types supported 147
- Security Information 98
- Security Information Qualifier 98
- Security Sockets Layer (SSL) description 147

segment delimiter 275
Segment delimiter 275
Segment delimiter attribute 277
segment name 81, 277
Segment output attribute 277
segment tag 81, 277
segment terminator 275, 277
segment, description 276
segments, EDI 81
self-signed certificate 150
separator attributes 275
server authentication
  inbound SSL 152
  outbound SSL 154
service segments 82
signature certificates
  inbound 157
  outbound 158
simple data element 276
site command 40, 135
SMTP gateways 129
SMTP targets 35
SOAP SyncCheck handler 46
splitter handlers
  attributes 43
  description 84
  list of 44
splitters 84
SSL certificates
  client authentication, inbound 153
  client authentication, outbound 155
  inbound 152
  server authentication, inbound 152
  server authentication, outbound 154
SSL description 147
SSL handshake 151
style sheet, changing 28
Subelement delimiter attribute 276
Sync Ack Required attribute 286
Sync Supported attribute 286
SyncCheck configuration point
  description 10
  HTTP/S target 46
  JMS target 46
  list of handlers 45
  order of handlers 46
  when required 43
synchronous exchanges, configuration point requirement 43
Syntax ID 99
Syntax Version 99

T

TA1 acknowledgments
  description 117
  example 190
TA1 override attribute 280
target certificates 150
targets
  configuration points 9, 43
  description 7, 31
  file-system 38
  FTP 34
  FTP Scripting 39
  global transport attributes 32
  HTTP 33

targets *(continued)*
  JMS 36
  Postprocess configuration point 46
  Preprocess configuration point 43
  SMTP 35
  splitter handler 43
  SyncCheck configuration point 43
Test directory 18
Test Indicator 99
Test Indicator (Usage Indicator) 99
Time to Acknowledge attribute 283, 286
Time to Perform attribute 286
trailer segment 82
Transaction attributes, envelope profile 100
Transaction Control Number Length 98, 272, 273, 274
transactions, EDI
  connection profiles 101
  description 81, 82
  header segments 82
  trailer segments 82
transformation maps
  description 83
  importing 107
  properties 281
transports
  gateway, system-supplied 123
  overview 2
transports, user-defined
  deleting 42, 138
  gateway 138
  target 42
  updating 167
trust anchor 150
trust stores
  default password 149
  description 149
TRXCTLLEN (Transaction Control Number Length) 272, 273, 274

U

UCS
  description 81
  envelope attributes 272
UN/EDIFACT 81
UNB0101 Syntax ID 99
UNB0102 Syntax Version 99
UNB0601 Recipients Reference/Password 99
UNB0602 Recipients Reference/Password Qualifier 99
UNB07 Application Reference 99
UNB08 Priority 99
UNB09 Acknowledgment Request 99
UNB10 Communication Agreement ID 99
UNB11 Test Indicator (Usage Indicator) 99
UNG01 Functional Group ID 100, 274
UNG0201 Application Sender ID 100
UNG0202 Application Sender ID Qualifier 100
UNG0301 Application Receiver ID 100
UNG0302 Application Receiver ID Qualifier 100

UNG06 Controlling Agency 100
UNG0701 Message Version 100
UNG0702 Message Release 100
UNG0703 Association Assigned 100
UNG08 Application Password 100
UNH0201 Message Type 100, 274
UNH0202 Message Version 100, 274
UNH0203 Message Release 100, 274
UNH0204 Controlling Agency 100, 275
UNH0205 Association Assigned Code 100
UNH03 Common Access Reference 100
Use Batch Mode field 96
user-defined handlers
  updating 49
  uploading 32, 49
  workflow 50
user-defined transports
  deleting 42, 138
  gateway 138
  target 42
  updating 167

V

Validate Client SSL certificate option 153
Validation level attribute 278
validation maps
  adding 79
  description 79
  document flow definitions, associating 79
  format 229
  importing 107
  RosettaNet 229
  standard EDI 84

W

Web service protocol 6
Web services
  document flow definitions 69
  participants, identifying 68
  restrictions 72
  standards supported 72
WebSphere MQ
  modifying JMS implementation 21
  starting 25
workflows
  inbound fixed 11
  outbound fixed 13
  user-defined handlers 50
WSDL files
  importing 69
  private 69
  public 69
  XML schemas 70
  ZIP archive requirements 70

X

X12
  description 81
  interchange structure 82
X12 envelopes, attributes 271

XML documents
description 84
processing of 94
XML documents to EDI flow
description 89
setting up 113
XML files
creating for Backend Integration packages 226
creating for RNIF packages 226
processing 19
XML formats
creating 77, 78
description 77
XML protocol definitions, custom 77
XML schemas
converting from DTD file 220
PIP packages 219
WDSL files 70
XML splitter handler 44, 45
XML to EDI flow
description 88
example 202
setting up 112
XML to ROD flow
description 90
setting up 114
XML to XML flow
description 91
setting up 115
XML-based APIs, enabling 165
XMLEvent protocol 6, 67
XMLNS Active attribute 278

Z

ZIP archive requirements for WSDL files 70

Printed in USA