IBM WebSphere Partner Gateway Enterprise
und Advanced Edition

Hub-Konfiguration

Version 6.0

IBM WebSphere Partner Gateway Enterprise
und Advanced Edition

Hub-Konfiguration

Version 6.0

Hinweis

Vor Verwendung dieser Informationen und des darin beschriebenen Produkts sollten die Informationen unter Anhang E, „Bemerkungen", auf Seite 321 gelesen werden.

Ausgabe Juni 2005

Diese Veröffentlichung ist eine Übersetzung des Handbuchs

IBM WebSphere Partner Gateway Enterprise and Advanced Editions Hub Configuration Guide,

herausgegeben von International Business Machines Corporation, USA

Informationen, die nur für bestimmte Länder Gültigkeit haben und für Deutschland, Österreich und die Schweiz nicht zutreffen, wurden in dieser Veröffentlichung im Originaltext übernommen.

Möglicherweise sind nicht alle in dieser Übersetzung aufgeführten Produkte in Deutschland angekündigt und verfügbar; vor Entscheidungen empfiehlt sich der Kontakt mit der zuständigen IBM Geschäftsstelle.

Änderung des Textes bleibt vorbehalten.

Herausgegeben von:
SW TSC Germany
Kst. 2877
Juni 2005

Inhaltsverzeichnis

Zu diesem Handbuch xi
Zielgruppe xi
Typografische Konventionen xi
Zugehörige Dokumente xii

Neu in diesem Release xiii
Neu in Release 6.0 xiii
Neu in Release 4.2.2 xiii

Kapitel 1. Einführung 1
Übersicht 1
Für die Hubkonfiguration benötigte Informationen 2
Übersicht über Transporte 2
Übersicht über Dokumentenflussdefinitionen 3
Übersicht über die Dokumentverarbeitung 8
Dokumentverarbeitungskomponenten mit Handler konfigurieren 10
Ziele 10
Document Manager 12
Gateways 17
Übersicht über die Hubkonfiguration 18
Hub konfigurieren 18
Teilnehmer erstellen 19
Dokumentverbindungen aufbauen 19

Kapitel 2. Die Konfiguration des Hubs vorbereiten 21
Verzeichnis für ein Dateiverzeichnisgateway erstellen 21
Den FTP-Server für das Empfangen von Dokumenten konfigurieren 21
Die erforderliche Verzeichnisstruktur auf dem FTP-Server konfigurieren 22
Verarbeitung der über FTP gesendeten Dateien 23
Zusätzliche FTP-Serverkonfiguration 24
Sicherheitsaspekte für den FTPS-Server 24
Den Hub für das JMS-Transportprotokoll konfigurieren 25
Verzeichnis für JMS erstellen 25
Die Standard-JMS-Konfiguration ändern 25
Warteschlangen und den Kanal erstellen 26
Ihrer Umgebung eine Java(TM)-Laufzeit hinzufügen 26
Die JMS-Konfiguration definieren 27
FTP-Scripts für FTP-Scripting-Ziele und -Gateways verwenden 28
Zuordnungen vom Data Interchange Services-Client verwenden 28

Kapitel 3. Den Server starten und Community Console anzeigen 29
WebSphere MQ starten 29
Die WebSphere Partner Gateway-Komponenten starten 29
An Community Console anmelden 30

Kapitel 4. Community Console konfigurieren 33
Locale-Informationen und Konsolbranding angeben 33
Konsolbranding durchführen 33
Style-Sheet ändern 34
Die Konsoldaten lokalisieren 34
Kennwortrichtlinie konfigurieren 35
Berechtigungen konfigurieren 36
Benutzern Berechtigungen erteilen 36
Berechtigungen aktivieren oder inaktivieren 37

Kapitel 5. Ziele definieren 39
Übersicht 39
Benutzerdefinierte Handler hochladen 40
Globale Transportwerte konfigurieren 41
HTTP/S-Ziel konfigurieren 41
Zieldetails 42
Zielkonfiguration 42
Handler 42
FTP-Ziel konfigurieren. 42
Zieldetails 43
Zielkonfiguration 43
Handler 44
SMTP-Ziel konfigurieren 44
Zieldetails 44
Zielkonfiguration 44
Zeitplan 44
JMS-Ziel konfigurieren 45
Zieldetails 45
Zielkonfiguration 45
Handler 46
Dateisystemziel konfigurieren 47
Zieldetails 47
Zielkonfiguration 47
Handler 47
FTP-Scripting-Ziel konfigurieren 48
Das FTP-Script erstellen 48
FTP-Scripting-Befehle 48
Zieldetails 49
Zielkonfiguration 50
Benutzerdefinierte Attribute 51
Zeitplan 51
Handler 51
Ziel für benutzerdefinierten Transport konfigurieren. 52
Konfigurationspunkte ändern 52
Vorverarbeitung 53
Synchronprüfung 56
Nachverarbeitung 57
Die Konfigurationsliste ändern 57

Kapitel 6. Schritte und Aktionen für feste Arbeitsabläufe konfigurieren 59
Handler hochladen 59
Feste Arbeitsabläufe konfigurieren. 60
Eingangsarbeitsabläufe 61
Ausgangsarbeitsablauf. 61
Aktionen konfigurieren 62
Benutzerdefinierte Aktion ändern 62
Aktionen erstellen 63

Kapitel 7. Dokumentenflüsse konfigurieren 65
Übersicht 65
Schritt 1: Sicherstellen, dass die Dokumentenflussdefinition verfügbar ist. 65
Schritt 2: Interaktionen erstellen 66
Schritt 3: Teilnehmerprofile, Gateways und B2B-Funktionalität erstellen 66
Schritt 4: Verbindungen aktivieren. 67
Ein Beispieldokumentenfluss 67
Binäre Dokumente 69
EDI-Dokumente mit Pass-Through-Aktion 69
Dokumentenflussdefinitionen erstellen 70
Interaktionen erstellen. 70
RosettaNet-Dokumente 71

Übersicht . . . 71
RNIF- und PIP-Dokumentenflusspakete . . . 72
Dokumentenflussdefinitionen erstellen . . . 74
Attributwerte konfigurieren . . . 75
Interaktionen erstellen . . . 76
Web-Services . . . 79
Die Teilnehmer für einen Web-Service angeben . . . 79
Dokumentenflussdefinitionen erstellen . . . 80
Interaktionen erstellen . . . 84
Einschränkungen und Begrenzungen der Web-Serviceunterstützung . . . 84
cXML-Dokumente . . . 84
Übersicht . . . 84
Dokumentenflussdefinitionen erstellen . . . 88
Interaktionen erstellen . . . 88
Angepasste XML-Dokumente . . . 89
Übersicht . . . 89
Protokolldefinitionsformat erstellen . . . 89
Dokumentenflussdefinition erstellen . . . 90
XML-Format erstellen . . . 91
Validierungszuordnungen verwenden . . . 91
Validierungszuordnungen hinzufügen . . . 91
Zuordnungen zu Dokumentenflussdefinitionen zuordnen . . . 92
Dokumente anzeigen . . . 92

Kapitel 8. EDI-Dokumentenflüsse konfigurieren . . . 93
Übersicht über EDI . . . 93
Die EDI-Austauschstruktur . . . 93
Zuordnungen . . . 95
Überblick über XML- und ROD-Dokumente . . . 96
XML-Dokumente . . . 96
ROD-Dokumente . . . 96
Verteiler und mehrere Dokumente . . . 96
Übersicht - Dokumentenflüsse erstellen und Attribute festlegen . . . 97
Schritt 1: Sicherstellen, dass die Dokumentenflussdefinition verfügbar ist . . . 97
Schritt 2: Interaktionen erstellen . . . 98
Schritt 3: Teilnehmerprofile, Gateways und B2B-Funktionalität erstellen . . . 98
Schritt 4: Verbindungen aktivieren . . . 99
Übersicht über mögliche Dokumentenflüsse . . . 99
Dokumentenfluss: EDI zu EDI . . . 99
Dokumentenfluss: EDI zu XML oder ROD . . . 100
Dokumentenfluss: XML oder ROD zu EDI . . . 101
Dokumentenfluss: Mehrere XML- oder ROD-Dokumente zu EDI-Austausch . . . 102
Dokumentenfluss: XML zu ROD oder ROD zu XML . . . 103
Dokumentenfluss: XML zu XML oder ROD zu ROD . . . 103
Verarbeitung von EDI-Austauschvorgängen . . . 104
Verarbeitung von XML- oder ROD-Dokumenten . . . 107
EDI-Umgebung konfigurieren . . . 108
Programm zur Umschlagsgenerierung . . . 108
Umschlagsprofile . . . 110
Verbindungsprofile . . . 115
Kontrollnummern . . . 118
Initialisierung der Kontrollnummer . . . 120
Aktuelle Kontrollnummern . . . 121
Allgemeine Schritte für das Definieren von Dokumentaustauschvorgängen . . . 122
Zuordnungen importieren . . . 122
Dokumentenfluss konfigurieren: EDI zu EDI . . . 124
Dokumentenfluss konfigurieren: EDI zu XML oder ROD . . . 126
Dokumentenfluss konfigurieren: XML oder ROD zu EDI . . . 128
Dokumentenfluss konfigurieren: Mehrere XML- oder ROD-Dokumente in einer Datei zu EDI . . . 129
Dokumentenfluss konfigurieren: XML zu ROD oder ROD zu XML . . . 131
Dokumentenfluss konfigurieren: XML zu XML oder ROD zu ROD . . . 131

Bestätigungen konfigurieren . . . 132
Dem Dokumentenfluss eine Bestätigung hinzufügen . . . 133
EDI-Austauschvorgänge und -Transaktionen anzeigen . . . 135

Kapitel 9. Das Community Manager-Profil und B2B-Funktionalität erstellen . . . 137
Das Community Manager-Profil erstellen . . . 137
B2B-Funktionalität konfigurieren . . . 139

Kapitel 10. Gateways erstellen . . . 141
Übersicht . . . 141
Globale Transportwerte konfigurieren . . . 142
Forward Proxy konfigurieren . . . 143
HTTP-Gateway konfigurieren . . . 144
Gateway-Details . . . 144
Gatewaykonfiguration . . . 144
HTTPS-Gateway konfigurieren . . . 145
Gateway-Details . . . 145
Gatewaykonfiguration . . . 146
FTP-Gateway konfigurieren . . . 147
Gateway-Details . . . 147
Gatewaykonfiguration . . . 147
SMTP-Gateway konfigurieren . . . 148
Gateway-Details . . . 148
Gatewaykonfiguration . . . 148
JMS-Gateway konfigurieren . . . 149
Gateway-Details . . . 149
Gatewaykonfiguration . . . 149
Dateiverzeichnisgateway konfigurieren . . . 151
Gateway-Details . . . 151
Gatewaykonfiguration . . . 152
FTPS-Gateway konfigurieren . . . 152
Gateway-Details . . . 153
Gatewaykonfiguration . . . 153
FTP-Scripting-Gateway konfigurieren . . . 154
Das FTP-Script erstellen . . . 154
FTP-Scriptbefehle . . . 154
FTP-Scripting-Gateways . . . 155
Gateway-Details . . . 156
Gatewaykonfiguration . . . 156
Benutzerdefinierte Attribute . . . 157
Zeitplan . . . 157
Handler konfigurieren . . . 158
Gateway für benutzerdefinierten Transport konfigurieren . . . 158
Standardgateway angeben . . . 159

Kapitel 11. Teilnehmer und ihre B2B-Funktionalität erstellen . . . 161
Teilnehmerprofile erstellen . . . 161
B2B-Funktionalität konfigurieren . . . 163

Kapitel 12. Verbindungen verwalten . . . 165
Übersicht . . . 165
Teilnehmerverbindungen aktivieren . . . 165
Attribute angeben oder ändern . . . 166

Kapitel 13. Sicherheit für Eingangs- und Ausgangsaustauschvorgänge konfigurieren 169
Begriffe und Konzepte für Sicherheit . . . 169
In WebSphere Partner Gateway verwendete Sicherheitsmechanismen und Protokolle . . . 169
Das Dienstprogramm iKeyman . . . 170
Community Console . . . 171
Keystores und Truststores . . . 171

Zertifikatketten . . . 172
Primäre und sekundäre Zertifikate . . . 172
Die Verschlüsselungsstufe ändern . . . 173
SSL-Zertifikate erstellen und installieren . . . 173
SSL-Handshake . . . 174
Eingehende SSL-Zertifikate . . . 175
Ausgehende SSL-Zertifikate . . . 177
Zertifikatswiderrufsliste hinzufügen . . . 179
Zugriff auf CRL-Verteilungspunkte aktivieren . . . 180
Unterschriftszertifikate erstellen und installieren . . . 181
Eingehendes Unterschriftszertifikat . . . 181
Ausgehendes Unterschriftszertifikat . . . 182
Verschlüsselungszertifikate erstellen und installieren . . . 183
Eingehendes Verschlüsselungszertifikat . . . 183
Ausgehendes Verschlüsselungszertifikat . . . 185
Eingangs-SSL für Konsole und Empfänger konfigurieren . . . 186
Übersicht über Zertifikate . . . 187

Kapitel 14. Die Konfiguration fertig stellen . . . 189
Die Verwendung von APIs aktivieren . . . 189
Die für Ereignisse verwendeten Warteschlangen angeben . . . 189
Alertfähige Ereignisse angeben . . . 191
Benutzerdefinierten Transport aktualisieren . . . 191

Anhang A. Grundlegende Beispiele . . . 193
Basiskonfiguration – EDI-Pass-Through-Dokumente austauschen . . . 193
Den Hub konfigurieren . . . 193
Teilnehmer und Teilnehmerverbindungen erstellen . . . 195
Basiskonfiguration - Sicherheit für eingehende und ausgehende Dokumente konfigurieren . . . 199
SSL-Authentifizierung für Eingangsdokumente konfigurieren . . . 199
Verschlüsselung konfigurieren . . . 201
Dokumentunterzeichnung konfigurieren . . . 203
Die Basiskonfiguration erweitern . . . 205
FTP-Ziel erstellen . . . 205
Den Hub zum Empfangen von Binärdateien konfigurieren . . . 205
Den Hub für angepasste XML-Dokumente konfigurieren . . . 207

Anhang B. EDI-Beispiele . . . 211
Beispiel: EDI zu ROD . . . 211
Umschlag vom EDI-Austausch entfernen und EDI-Austausch transformieren . . . 211
Dem Austausch TA1 hinzufügen . . . 217
FA-Zuordnung hinzufügen . . . 221
Beispiel: EDI zu XML . . . 225
Die Transformationszuordnung importieren . . . 225
Die Transformationszuordnung und Dokumentenflussdefinitionen prüfen . . . 225
Das Ziel konfigurieren . . . 226
Die Interaktionen erstellen . . . 226
Die Teilnehmer erstellen . . . 227
Die Gateways erstellen . . . 228
B2B-Funktionalität konfigurieren . . . 228
Die Verbindungen aktivieren . . . 230
Beispiel: XML zu EDI . . . 230
Die Transformationszuordnung importieren . . . 230
Die Transformationszuordnung und Dokumentenflussdefinitionen prüfen . . . 231
Das Ziel konfigurieren . . . 231
Die Interaktionen erstellen . . . 232
Die Teilnehmer erstellen . . . 232
Die Gateways erstellen . . . 233
B2B-Funktionalität konfigurieren . . . 234
Das Umschlagsprofil erstellen . . . 235

Das XML-Format erstellen . . . 236
Die Verbindungen aktivieren . . . 236
Attribute konfigurieren . . . 237
Beispiel: ROD zu EDI . . . 237
Die Transformationszuordnung importieren . . . 238
Die Transformationszuordnung und Dokumentenflussdefinitionen prüfen . . . 238
Das Ziel konfigurieren . . . 239
Die Interaktionen erstellen . . . 239
Die Teilnehmer erstellen . . . 240
Die Gateways erstellen . . . 241
B2B-Funktionalität konfigurieren . . . 242
Das Umschlagsprofil erstellen . . . 243
Die Verbindungen aktivieren . . . 243
Attribute konfigurieren . . . 244

Anhang C. Zusätzliche RosettaNet-Informationen . . . 245
PIPs inaktivieren . . . 245
Fehlerbenachrichtigung bereitstellen . . . 245
0A1 PIP . . . 245
Kontaktinformationen aktualisieren . . . 246
RosettaNet-Attributwerte bearbeiten . . . 246
PIP-Dokumentenflusspakete erstellen . . . 247
Die XSD-Dateien erstellen . . . 248
Die XML-Datei erstellen . . . 254
Das Paket erstellen . . . 257
Informationen zur Validierung . . . 258
Kardinalität . . . 258
Format . . . 258
Aufzählung . . . 259
Inhalt der PIP-Dokumentenflusspakete . . . 259
0A1 Notification of Failure V1.0 . . . 259
0A1 Notification of Failure V02.00 . . . 260
2A1 Distribute New Product Information . . . 260
2A12 Distribute Product Master . . . 262
3A1 Request Quote . . . 262
3A2 Request Price and Availability . . . 263
3A4 Request Purchase Order V02.00 . . . 264
3A4 Request Purchase Order V02.02 . . . 266
3A5 Query Order Status . . . 267
3A6 Distribute Order Status . . . 268
3A7 Notify of Purchase Order Update . . . 269
3A8 Request Purchase Order Change V01.02 . . . 270
3A8 Request Purchase Order Change V01.03 . . . 272
3A9 Request Purchase Order Cancellation . . . 273
3B2 Notify of Advance Shipment . . . 274
3B3 Distribute Shipment Status . . . 275
3B11 Notify of Shipping Order . . . 276
3B12 Request Shipping Order . . . 277
3B13 Notify of Shipping Order Confirmation . . . 278
3B14 Request Shipping Order Cancellation . . . 279
3B18 Notify of Shipping Documentation . . . 279
3C1 Return Product . . . 281
3C3 Notify of Invoice . . . 282
3C4 Notify of Invoice Reject . . . 283
3C6 Notify of Remittance Advice . . . 284
3C7 Notify of Self-Billing Invoice . . . 284
3D8 Distribute Work in Process . . . 285
4A1 Notify of Strategic Forecast . . . 286
4A3 Notify of Threshold Release Forecast . . . 287
4A4 Notify of Planning Release Forecast . . . 288
4A5 Notify of Forecast Reply . . . 289

4B2 Notify of Shipment Receipt 290
4B3 Notify of Consumption 291
4C1 Distribute Inventory Report V02.01 291
4C1 Distribute Inventory Report V02.03 292
5C1 Distribute Product List. 293
5C2 Request Design Registration 294
5C4 Distribute Registration Status 295
5D1 Request Ship From Stock And Debit Authorization 295
6C1 Query Service Entitlement 296
6C2 Request Warranty Claim 297
7B1 Distribute Work in Process 298
7B5 Notify Of Manufacturing Work Order. 299
7B6 Notify Of Manufacturing Work Order Reply 300

Anhang D. Attribute. 301
EDI-Attribute 301
Attribute für Umschlagsprofil 301
Attribute für Dokumentenflussdefinition und Verbindung 305
Data Interchange Services-Clientmerkmale. 313
AS-Attribute. 314
RosettaNet-Attribute 318
Backend Integration-Attribute 320

Anhang E. Bemerkungen 321
Informationen zur Programmierschnittstelle 323
Marken und Servicemarken 324

Index 325

Zu diesem Handbuch

Diese Dokumentation beschreibt, wie Sie den IBM (R) WebSphere (R) Partner Gateway-Server konfigurieren.

Zielgruppe

Diese Dokumentation richtet sich an die Person, die für das Konfigurieren des WebSphere Partner Gateway-Servers, auch Hub genannt, verantwortlich ist. Um den Hub zu konfigurieren, sollten Sie der Hubadmin sein. Der Hubadmin ist in der Lage, alle Funktionen der WebSphere Partner Gateway Community Console zu konfigurieren und den Hub zu betreiben.

Typografische Konventionen

Diese Dokumentation verwendet die folgenden Konventionen.

Tabelle 1. Typographische Konventionen

Konvention	Beschreibung
`Monospaceschrift`	Text in dieser Schriftart gibt von Ihnen einzugebenden Text, Werte für Argumente oder Befehlsoptionen, Beispiele oder Codebeispiele oder Informationen, die das System in der Anzeige druckt (Nachrichtentext oder Eingabeaufforderungen), an.
Fettdruck	Text in Fettdruck gibt die Bedienelemente der grafischen Benutzerschnittstelle (z. B. Online-Schaltflächennamen, Menünamen oder Menüoptionen) und Spaltenüberschriften in Tabellen und Text an.
Kursivschrift	Text in Kursivschrift gibt eine Hervorhebung, Buchtitel, neue Begriffe sowie im Text definierte Begriffe, Variablennamen oder Buchstaben des Alphabets, die als solche verwendet werden, an.
`Kursive Monospaceschrift`	Text in kursiver Monospaceschrift gibt Variablennamen innerhalb eines in Monospaceschrift verfassten Textes an.
Produktverz	*Produktverz* steht für das Verzeichnis, in dem das Programm installiert ist.Alle IBM WebSphere Partner Gateway-Pfadnamen sind relativ zum Verzeichnis, in dem das Produkt IBM WebSphere Partner Gateway auf Ihrem System installiert ist.
`%text%` und *`$text`*	Text in Prozentzeichen (%) gibt den Wert für den `Text` der Windows(R)-Systemvariablen bzw. -Benutzervariablen an. Die entsprechende Notation in einer UNIX(R)-Umgebung ist $*text*. Sie gibt den Wert für den *text* der UNIX-Umgebungsvariablen an.
Unterstrichener farbiger Text	Unterstrichener farbiger Text gibt einen Querverweis an. Klicken Sie auf den Text, um das Objekt des Verweises aufzurufen.
Text in einer blauen Kontur	(Nur in PDF-Dateien) Eine Kontur um den Text herum gib einen Querverweis an. Klicken Sie auf den umrandeten Text, um das Objekt des Verweises aufzurufen. Diese Konvention für PDF-Dateien entspricht in dieser Tabelle der Konvention “Unterstrichener farbiger Text”.

Tabelle 1. Typographische Konventionen (Forts.)

Konvention	Beschreibung
" " (Anführungszeichen)	(Nur in PDF-Dateien) Anführungszeichen umgeben Querverweise auf andere Abschnitte in der Dokumentation.
{ }	In einer Syntaxzeile umgeben geschweifte Klammern eine Gruppe von Optionen, von denen Sie nur eine auswählen dürfen.
[ ]	In einer Syntaxzeile umgeben eckige Klammern optionale Parameter.
< >	Spitze Klammern umgeben variable Elemente eines Namens, um sie voneinander zu unterscheiden. Beispiel: <*servername*><*connectorname*>tmp.log.
/, \	Backslashes (\) werden als Trennzeichen in Verzeichnispfaden von Windows-Installationen verwendet. Setzen Sie für UNIX-Installationen Schrägstriche (/) für Backslashes ein.

Zugehörige Dokumente

Der vollständige Dokumentationssatz, der für dieses Produkt verfügbar ist, enthält umfassende Informationen zum Installieren, Konfigurieren, Verwalten und Verwenden von WebSphere Partner Gateway Enterprise und Advanced Edition.

Sie können diese Dokumentation von der folgenden Site herunterladen oder sie dort direkt online lesen:
http://www.ibm.com/software/integration/wspartnergateway/library/infocenter

Anmerkung: Wichtige Informationen zu diesem Produkt sind unter Umständen in den technischen Hinweisen und Eilnachrichten der technischen Unterstützung enthalten, die nach Veröffentlichung dieser Dokumentation herausgegeben wurden. Diese können Sie auf der Unterstützungswebsite von WebSphere Partner Gateway unter der folgenden Adresse finden:
http://www.ibm.com/software/integration/wspartnergateway/support. Wählen Sie den Teilbereich Ihres Interesses aus, und durchsuchen Sie die technischen Hinweise und Einblendungsabschnitte.

Neu in diesem Release

Neu in Release 6.0

WebSphere Partner Gateway (das in früheren Releases WebSphere Business Integration Connect genannt wurde) verfügt über die folgenden neuen Funktionen:

- Die Funktionalität zum Entfernen des Umschlags von EDI-Transaktionen sowie zum Prüfen und Umsetzen der EDI-Transaktionen mit diesen Umschlägen
- Die Funktionalität zum Versehen einzelner EDI-Transaktionen mit einem Umschlag, bevor sie zugestellt werden
- Die Funktionalität zum Empfangen mehrerer Dokumente mit satzorientierten Daten und XML-Dokumente oder EDI-Austauschvorgänge in einer einzelnen Datei und zum Aufteilen dieser Elemente in einzelne Dokumente oder Austauschvorgänge
- Die Funktionalität zum Übersetzen jeglicher Kombination von ROD-, XML- und EDI-Dokumenten
- Die Einführung eines neuen Transports, FTP-Scripting, das sowohl für Ziele als auch für Gateways verwendet werden kann, zum Kommunizieren mit VANs (Mehrwertnetzen - Value Added Networks) sowie mit anderen FTP-Servern
- Die Funktionalität zum Unterstützen von mehr als einem Zertifikat für bestimmte Funktionen, so dass das sekundäre Zertifikat verwendet werden kann, falls das primäre Zertifikat verfällt
- Die Fähigkeit zum Senden von Dokumenten von einem HTTP- oder HTTPS-Gateway über einen Proxy-Server an Teilnehmer

Beachten Sie, dass WebSphere Partner Gateway Version 6.0 den RC5-Algorithmus nicht unterstützt.

Neu in Release 4.2.2

Version 4.2.2 ist das erste Release von *Hub-Konfigurationshandbuch* .

Kapitel 1. Einführung

Nachdem Sie WebSphere Partner Gateway installiert haben und bevor Dokumente zwischen Community Manager und Teilnehmern ausgetauscht werden können, müssen Sie den WebSphere Partner Gateway-Server (den Hub) konfigurieren.

Dieses Kapitel behandelt die folgenden Themen:

- „Übersicht"
- „Für die Hubkonfiguration benötigte Informationen" auf Seite 2
- „Übersicht über die Dokumentverarbeitung" auf Seite 8
- „Dokumentverarbeitungskomponenten mit Handler konfigurieren" auf Seite 10
- „Übersicht über die Hubkonfiguration" auf Seite 18

Übersicht

Die Zielsetzung lautet, Community Manager zu aktivieren, damit er ein Dokument bzw. eine Gruppe von Dokumenten (elektronisch) an einen Teilnehmer sendet oder ein Dokument bzw. eine Gruppe von Dokumenten von einem Teilnehmer empfängt. Der Hub verwaltet den Empfang von Dokumenten, die Transformation in andere Formate (falls erforderlich) und die Übermittlung der Dokumente. Der Hub kann auch so konfiguriert werden, dass er Sicherheit für Eingangs- und Ausgangsdokumente bereitstellt.

Die zwischen dem Hub und dem Teilnehmer ausgetauschten Dokumente sind in der Regel im Standardformat und stellen eine bestimmte Geschäftsinteraktion dar. Der Teilnehmer könnte z. B. eine Bestellungsanforderung als einen RosettaNet-3A4-PIP, ein cXML-OrderRequest-Dokument oder einen EDI-X12-Austausch mit einer 850-Transaktion senden. Der Hub transformiert das Dokument in ein Format, das von einer Anwendung im Community Manager verwendet werden kann. In ähnlicher Weise könnte eine Community Manager-Back-End-Anwendung eine Bestellungsantwort in ihrem eigenen angepassten Format senden, das in ein Standardformat transformiert wird. Das transformierte Dokument wird dann zum Teilnehmer gesendet.

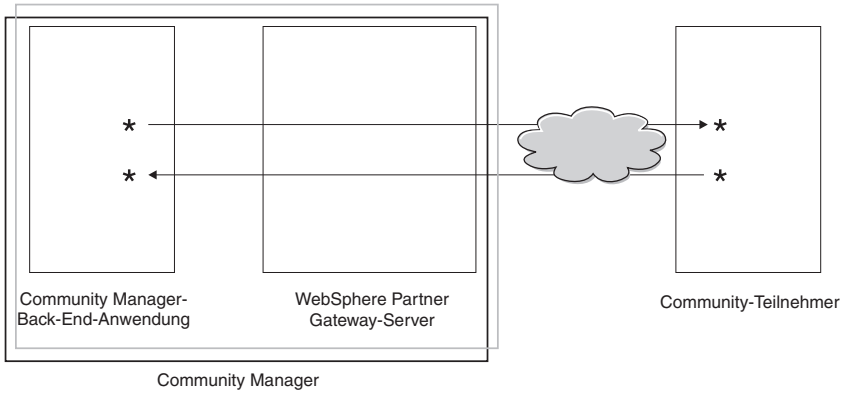

Abbildung 1. Dokumentenfluss durch den Hub

In diesem Handbuch erfahren Sie, wie Sie den Hub konfigurieren, und dann wie Sie die Teilnehmer definieren. Sie erfahren außerdem, wie Sie die Sicherheit für den Hub konfigurieren.

In Abb. 1 auf Seite 1 sehen Sie, dass Community Manager der Eigner des WebSphere Partner Gateway-Servers und der Community Manager-Back-End-Anwendung ist. Community Manager ist das Unternehmen, das Eigner des Hubs ist, Community Manager ist aber auch ein Teilnehmer des Hubs. Wie Sie in späteren Kapiteln feststellen können, definieren Sie ein Profil für Community Manager genauso wie für Teilnehmer.

Anmerkung: Diese Dokumentation zeigt Ihnen, wie Sie Verbindungen erstellen, die von der Community Manager-Back-End-Anwendung zu einem Teilnehmergateway und von einem Teilnehmer zum Community Manager-Gateway fließen. Nachdem die Dokumente am Community Manager-Gateway angekommen sind, möchten Sie diese wahrscheinlich in eine Back-End-Anwendung, wie WebSphere InterChange Server oder WebSphere MQ Broker, integrieren. Die erforderlichen Aufgaben für die Integration zwischen WebSphere Partner Gateway und solchen Back-End-Anwendungen werden im Handbuch *Unternehmensintegration* definiert.

Für die Hubkonfiguration benötigte Informationen

Sie benötigen einige Informationen über die Typen der Austauschvorgänge, an denen Community Manager teilnimmt, um den Hub zu konfigurieren. Sie benötigen z. B. die folgenden Informationen:

- Die Dokumenttypen (z. B. EDI-X12 oder angepasstes XML), die Community Manager und seine Teilnehmer durch den Hub senden.
- Die Transporttypen (z. B. HTTP oder FTP), die Community Manager und seine Teilnehmer zum Senden der Dokumente verwenden.
- Muss ein auf dem Hub eingehendes Dokument in mehrere Dokumente aufgeteilt werden oder müssen einzelne auf dem Hub eingehende Dokumente gruppiert werden, bevor sie weitergesendet werden?
- Werden die Dokumente vor ihrer Übermittlung transformiert?
- Werden die Dokumente vor ihrer Übermittlung geprüft?
- Werden die Dokumente verschlüsselt oder digital unterzeichnet oder wird eine andere Sicherheitstechnik verwendet?

Wenn Sie diese Informationen ermittelt haben, können Sie mit der Konfiguration des Hubs beginnen.

Nachdem Sie den Hub definiert haben, können Sie Ihre Teilnehmer mit den Informationen, wie z. B. IP-Adresse und DUNS-Nummern, definieren, die Sie von den Teilnehmern erhalten haben. Wie zuvor angemerkt, definieren Sie auch Community Manager als einen speziellen Typ von Hubteilnehmer.

Übersicht über Transporte

Dokumente können von Teilnehmern an WebSphere Partner Gateway (den Hub) über eine Vielzahl von Transporten gesendet werden. Ein Teilnehmer kann Dokumente über öffentliche Netze unter Verwendung von HTTP, HTTPS, JMS, FTP, FTPS, FTP-Scripting, SMTP oder ein Dateiverzeichnis senden. Ein Teilnehmer kann Dokumente unter Verwendung des FTP-Scripting-Transports über VAN (Value Added Network - Mehrwertnetz), einem privaten Netz, senden. Sie können auch Ihren eigenen Transport erstellen.

Anmerkung: Wenn der Transport **Dateiverzeichnis** zwischen einem Teilnehmer und dem Hub verwendet wird, sollte sich der Administrator um alle sicherheitsrelevanten Themen kümmern.

Ebenso sendet der Hub Dokumente an Back-End-Anwendungen über eine Vielzahl von Transporten. Die am meisten verwendeten Transporte zwischen dem Hub und Back-End-Anwendungen sind HTTP, HTTPS, JMS und Dateiverzeichnis.

Abb. 2 zeigt die verschiedenen Transporte, die verwendet werden können.

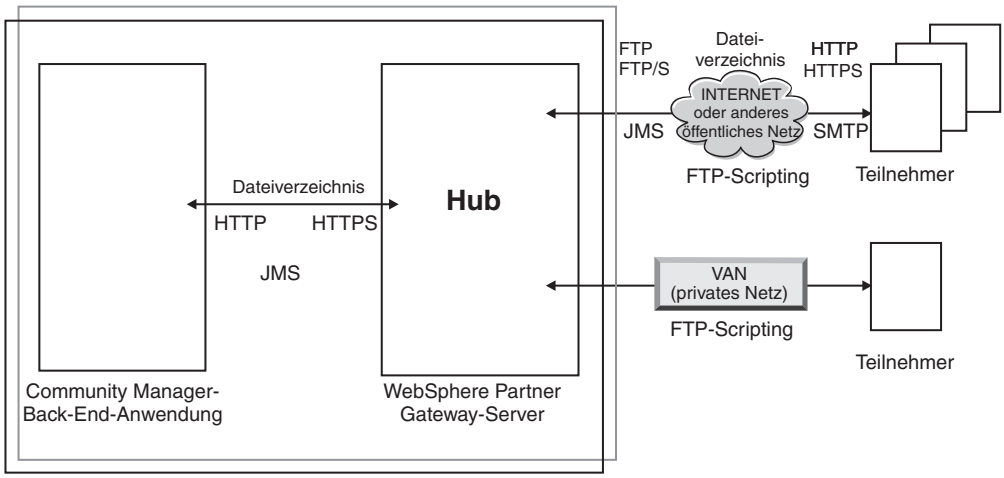

Abbildung 2. Transporte, die von WebSphere Partner Gateway unterstützt werden

Der Transporttyp, mit dem Dokumente gesendet und empfangen werden, beeinflusst das Einrichten von Zielen und Gateways. Ein Ziel ist ein Einstiegspunkt in den Hub. Es ist der Ort, an dem Dokumente, die von Teilnehmern oder Back-End-Anwendungen gesendet wurden, auf dem Hub empfangen werden. Ein Gateway ist ein Einstiegspunkt in den Computer des Teilnehmers oder des Back-End-Systems. Es ist der Ort, an den der Hub Dokumente sendet. Sie müssen einiges an Konfigurationsarbeit leisten, wie in Kapitel 2, „Die Konfiguration des Hubs vorbereiten", auf Seite 21 beschrieben, um die Verwendung der Transporte FTP, FTPS, FTP-Scripting, JMS und Dateiverzeichnis vorzubereiten.

Übersicht über Dokumentenflussdefinitionen

Wenn Sie den Austausch von Dokumenten zwischen den Teilnehmern und Community Manager definieren, geben Sie mehrere Dinge bezüglich des Dokuments an:

- Das *Paket*, das das Dokument umgibt
- Das Geschäfts*protokoll*, das das Dokument definiert
- Den Typ des *Dokumentenflusses*

Das Paket des Dokuments, das Protokoll des Dokuments und der Dokumentenfluss bilden gemeinsam die *Dokumentenflussdefinition*. Die Dokumentenflussdefinition gibt dem Hub Informationen darüber, wie das Dokument zu verarbeiten ist. Angenommen, Sie verwenden z. B. die folgende vom System bereitgestellte Dokumentenflussdefintion:

- Paket: AS
- Protokoll: EDI-X12
- Dokumentenfluss: ISA

Der Hub extrahiert die AS-Headerinformationen (und verwendet sie, um die Quelle und das Ziel des Dokuments zu ermitteln). Er weiß, an welcher Stelle im Dokument er bestimmte Informationen, aufgrund ihrer Position im Dokument, findet. Den drei Teilen der Dokumentenflussdefinition sind Attribute zugeordnet. Sie können die vom System bereitgestellten Attribute ändern bzw. ihnen etwas hinzufügen.

Paket

Das Paket stellt Informationen bereit, die die Übertragung des Dokuments betreffen. Wie im vorherigen Abschnitt erwähnt, verwendet der Hub im Falle eines AS-Pakets die Informationen im AS-Header, um die Quelle und das Ziel für das Dokument zu ermitteln. Wenn ein Teilnehmer einen RosettaNet-PIP (PIP - Partner Interface Process) an Community Manager sendet, wird der PIP als RNIF gepackt.

Abb. 3 zeigt die Pakettypen, die für Dokumente festgelegt werden können, die zwischen dem Hub und einem Community-Teilnehmer und zwischen dem Hub und einer Back-End-Anwendung ausgetauscht werden

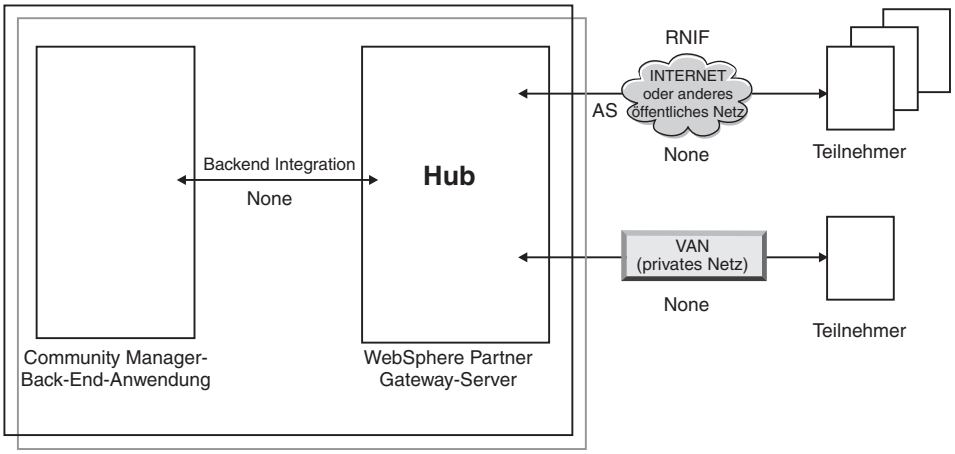

Abbildung 3. Pakettypen für Dokumente

Pakete sind bestimmten Protokollen zugeordnet. Ein Teilnehmer muss z. B. ein RNIF-Paket angeben, wenn er ein RosettaNet-Dokument an den Hub sendet.

Backend Integration: Wie in Abbildung Abb. 3 gezeigt wird, ist **Backend Integration** nur zwischen dem Hub und der Back-End-Anwendung verfügbar. Wenn Sie das Paket **Backend Integration** angeben, werden Dokumenten, die vom Hub an das Back-End-System gesendet werden, bestimmte Headerinformationen hinzugefügt. Ebenso muss eine Back-End-Anwendung Headerinformationen hinzufügen, wenn sie Dokumente mit dem Paket **Backend Integration** an den Hub sendet. Das Paket **Backend Integration** und die Anforderungen an die Headerinformationen werden im Handbuch *Unternehmensintegration* beschrieben.

AS: Das Paket **AS** ist nur zwischen Teilnehmern und dem Hub verfügbar. Das Paket **AS** kann für Dokumente verwendet werden, die mit den Standards AS1 oder AS2 konform sind. AS1 ist ein Standard, der für das sichere Übertragen von Dokumenten über SMTP verwendet wird, und AS2 ist ein Standard, der für das sichere Übertragen von von Dokumenten über HTTP oder HTTPS verwendet wird. Dokumente, die von einem Teilnehmer mit dem Paket **AS** gesendet wurden, haben entweder AS1- oder AS2-Headerinformationen. An einen Teilnehmer gesendete Dokumente, der AS1- oder AS2-Header erwartet, müssen (auf dem Hub) als Paket **AS** gepackt werden.

None: Das Paket **None** kann verwendet werden, um Dokumente zwischen dem Hub und Teilnehmern sowie zwischen dem Hub und einer Back-End-Anwendung zu senden und zu empfangen. Es werden keine Headerinformationen hinzugefügt (oder erwartet), wenn ein Dokument als Paket **None** gepackt wird.

RNIF: Das Paket **RNIF** wird auf dem Installationsdatenträger bereitgestellt. Sie laden das Paket **RNIF** (zusammmen mit den PIPs, die Sie austauschen wollen) wie in „RosettaNet-Dokumente" auf Seite 71 beschrieben hoch. Das Paket **RNIF** wird verwendet, um RosettaNet-Dokumente vom Teilnehmer an den Hub bzw. vom Hub an den Teilnehmer zu senden.

N/A: Einige Dokumentenflüsse enden entweder in WebSphere Partner Gateway oder sie stammen intern von WebSphere Partner Gateway. Für Dokumentenflüsse, die in WebSphere Partner Gateway enden, ist kein Paket erforderlich. Dokumentenflüsse, die intern von WebSphere Partner Gateway stammen, verfügen über kein Quellenpaket. Deshalb wird für solche Dokumentenflüsse das Paket **N/A** angegeben.

Bei den meisten Übertragungen in einer Richtung zwischen dem Teilnehmer und Community Manager (oder umgekehrt) empfängt WebSphere Partner Gateway ein Dokument von einem Teilnehmer und sendet es an Community Manager. Wenn Sie in WebSphere Partner Gateway die Teilnehmerverbindung erstellen, geben Sie das Paket an, in dem WebSphere Partner Gateway das Dokument empfangen wird, sowie das Paket, das WebSphere Partner Gateway verwenden wird, um das Dokument zu senden. In Abb. 4 fließt ein als AS gepacktes Dokument von einem Teilnehmer zur Community Manager-Back-End-Anwendung. Das Dokument wird dem Community Manager-Gateway ohne Transportheader übermittelt. In Abb. 4 ist dem Austausch von Dokumenten eine Aktion zugeordnet.

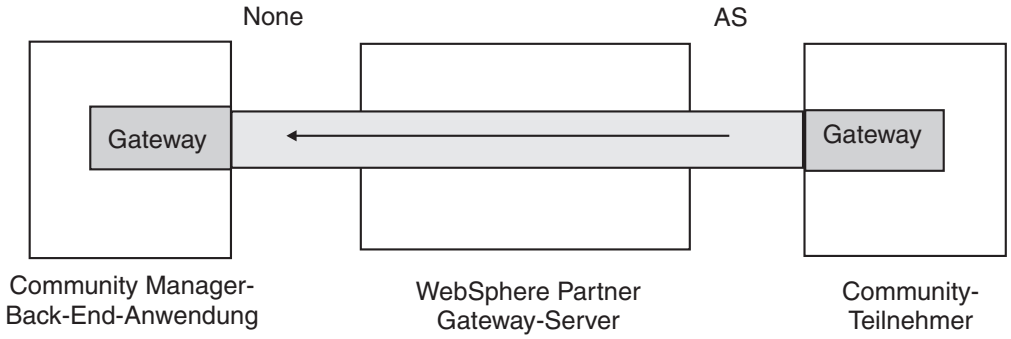

Abbildung 4. Typische Einwegverbindung

Bestimmte Protokolle beziehen jedoch mehrere Aktivitäten mit ein, wie z. B. Umschlagsentfernung und Transformation, einige dieser Aktivitäten stellen Zwischenschritte im Gesamtaustausch dar. Wenn z. B. ein Teilnehmer einen EDI-Austausch an den Hub mit Community Manager als Endziel sendet, wird der Umschlag des Austauschs entfernt und die einzelnen EDI-Transaktionen werden verarbeitet. Dem ursprünglichen EDI-Austausch ist ein Paket zugeordnet, wenn er vom Teilnehmer gesendet wird. Da jedoch der Austausch selbst Community Manager nicht übermittelt wird (sein Umschlag wird im Hub entfernt und keine weitere Verarbeitung des Austauschs erfolgt), wird der Austausch nicht gepackt. Wenn Sie die Interaktion für den Schritt zum Entfernen des Umschlags definieren, geben Sie daher ein Paket für die Sendeseite ein, aber für die Empfangsseite geben Sie **N/A** an.

Der Prozess für das Definieren der Dokumentenflussdefinitionen, die für einen EDI-Austausch erforderlich sind, wird in Kapitel 8, „EDI-Dokumentenflüsse konfigurieren", auf Seite 93 beschrieben.

Protokolle

Die folgenden Protokolle werden vom System bereitgestellt:

- Binary

  Das Protokoll **Binary** kann mit den Paketen **AS**, **None** und **Backend Integration** verwendet werden. Ein binäres Dokument enthält keine Daten über die Quelle oder das Ziel des Dokuments.

- EDI-X12, EDI-Consent, EDI-EDIFACT

  Diese EDI-Protokolle können mit den Paketen **AS** oder **None** verwendet werden. Wie in „N/A" auf Seite 5 beschrieben, geben Sie das Paket **N/A** an, falls die EDI-Transaktion oder der EDI-Austausch vom Hub stammt bzw. dort endet. X12 und EDIFACT sind EDI-Standards, die für den Austausch von Daten verwendet werden. EDI-Consent bezieht sich auf andere Inhaltstypen als X12 oder EDIFACT.

- Web Service

  Anforderungen des Protokolls **Web Service** können nur mit dem Paket **None** verwendet werden.

- cXML

  cXML-Dokumente können nur mit dem Paket **None** verwendet werden.

- XMLEvent

  XMLEvent ist ein besonderes Protokoll, mit dem Ereignisbenachrichtigungen für Dokumente bereitgestellt werden, die von und zur Back-End-Anwendung fließen. Es kann nur mit dem Paket **Backend Integration** verwendet werden. Dieses Protokoll wird im Handbuch *Unternehmensintegration* beschrieben.

Wenn Sie die Pakete **RNIF** hochladen, erhalten Sie außerdem die zugeordneten Protokolle (RosettaNet und RNSC). RosettaNet ist das zwischen dem Teilnehmer und dem Hub verwendete Protokoll. Es wird dem Paket **RNIF** zugeordnet. RNSC ist das zwischen dem Hub und der Community Manager-Back-End-Anwendung verwendete Protokoll. Es wird dem Paket **Backend Integration** zugeordnet.

Für EDI-Transaktionen bzw. XML- oder ROD-Dokumente, die transformiert werden, importieren Sie eine Transformationszuordnung vom Data Interchange Services-Client. Im Data Interchange Services-Client werden Wörterbücher für das Protokoll definiert, das dieser Transformation zugeordnet ist. Ein Wörterbuch enthält Informationen zu allen EDI-Dokumentdefinitionen, EDI-Segmenten, zusammengesetzten EDI-Datenelementen und EDI-Datenelementen, die den EDI-Standard ausmachen. Detaillierte Informationen zu einem bestimmten EDI-Standard finden Sie in den entsprechenden Handbüchern der jeweiligen EDI-Standards. Informationen zum Data Interchange Services-Client finden Sie im *Mapping Guide* oder in der Onlinehilfe, die mit dem Data Interchange Services-Client bereitgestellt wird.

Anmerkung: Die Sender- und Empfänger-IDs müssen Teil der ROD-Dokumentdefinition sein, die der Transformationszuordnung zugeordnet ist. Die Informationen, die zum Ermitteln des Dokumenttyps und der Wörterbuchwerte nötig sind, müssen ebenso in der Dokumentdefinition vorhanden sein. Stellen Sie sicher, dass der Zuordnungsexperte des Data Interchange Services-Clients diese Anforderungen kennt, wenn er die Transformationszuordnung erstellt.

Sie können angepasste Protokolle erstellen, um genau zu definieren, wie ein Dokument strukturiert sein soll. Bei XML-Dokumenten können Sie ein XML-Format definieren, wie in „Angepasste XML-Dokumente" auf Seite 89 beschrieben.

Dokumentenfluss

Das Dokument selbst kann in einer Vielzahl von Formaten vorliegen. Es gibt die folgenden vom System bereitgestellten Dokumentenflüsse und ihnen zugeordneten Protokolle:

- **Binary** kann mit dem Protokoll **Binary** verwendet werden.
- **ISA** stellt den X12-Austausch (Umschlag) dar und ist dem Protokoll **EDI-X12** zugeordnet.
- **BG** stellt den EDI-Consent-Umschlag dar und ist dem Protokoll **EDI-Consent** zugeordnet.
- **UNB** stellt den EDIFACT-Umschlag dar und ist dem Protokoll **EDI-EDIFACT** zugeordnet.
- **XMLEvent** kann mit dem Protokoll **XMLEvent** verwendet werden.

Die folgende Liste beschreibt weitere Dokumenttypen und die Quelle ihrer Definition:

- Ein RosettaNet-PIP, den Sie vom Installationsdatenträger hochladen, kann mit dem Protokoll **RosettaNet** verwendet werden.
- Ein Web-Service, den Sie als WSDL-Datei hochladen, kann mit dem Protokoll **Web Service** verwendet werden.
- Ein cXML-Dokument, das Sie durch Angabe des cXML-Dokumenttyps erstellen.
- Eine bestimmte EDI-Standardtransaktion, die Sie vom Data Interchange Services-Client importieren.
- Ein ROD-Dokument (Dokument mit satzorientierten Daten) oder ein XML-Dokument, das Sie vom Data Interchange Services-Client importieren.

Sie können ebenfalls Ihre eigenen Dokumentenflüsse erstellen, wie in „Angepasste XML-Dokumente" auf Seite 89 beschrieben.

Übersicht über die Dokumentverarbeitung

Bevor Sie mit der Konfiguration des Hubs beginnen, ist es hilfreich, sich eine Übersicht über die Komponenten von WebSphere Partner Gateway zu verschaffen und darüber, wie sie zur Verarbeitung von Dokumenten verwendet werden.

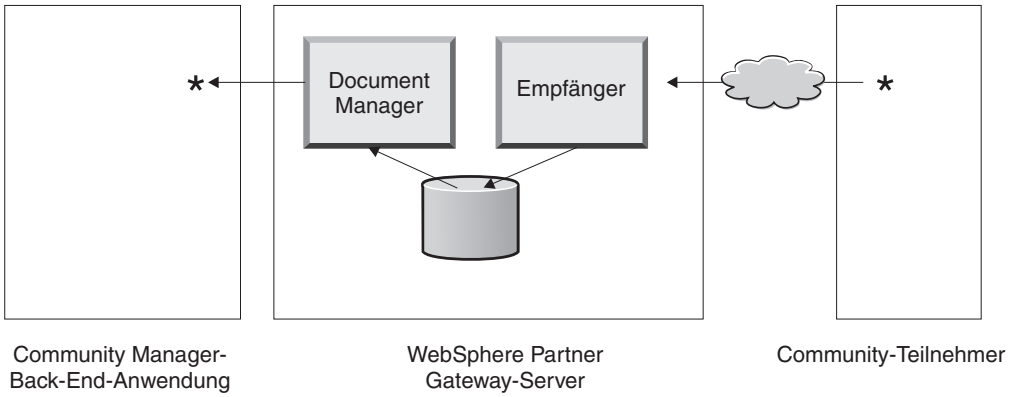

Abbildung 5. Die Komponenten "Empfänger" und "Document Manager"

Abb. 5 ist ein Beispiel dafür, wie ein Dokument von einem Teilnehmer gesendet, vom Hub empfangen, auf dem Hub verarbeitet und an eine Community Manager-Back-End-Anwendung gesendet wird.

Anmerkung: Zur Veranschaulichung sind in der Zeichnung dieser Dokumentation ein Empfänger und ein Document Manager abgebildet, die auf derselben Servermaschine installiert sind. (Die dritte Komponente wird nicht gezeigt, sie ist die Schnittstellt zu WebSphere Partner Gateway.) Tatsächlich können diese Komponenten mehrfach vorkommen und sie können auf verschiedenen Servern installiert sein. Alle Komponenten müssen dasselbe gemeinsame Dateisystem verwenden. Informationen zu den verschiedenen Topologien, die für die Konfiguration von WebSphere Partner Gateway verwendet werden können, finden Sie im *Installationshandbuch*.

Ein Dokument wird in WebSphere Partner Gateway hinein von der Empfängerkomponente empfangen. Der Empfänger ist verantwortlich für das Überwachen der Transporte für eingehende Dokumente, das Abrufen der eingehenden Dokumente, das Ausführen einiger grundlegender Verarbeitungsschritte an ihnen und dann für das Stellen dieser Dokumente in eine Warteschlange, so dass Document Manager sie abrufen kann.

Empfänger sind transportspezifisch. Die Instanzen von transportspezifischen Empfängern werden als *Ziele* bezeichnet. Sie konfigurieren ein Ziel für jeden Transporttyp, den der Hub unterstützen wird. Wenn Teilnehmer z. B. Dokumente über HTTP senden, konfigurieren Sie ein HTTP-Ziel, um diese zu empfangen.

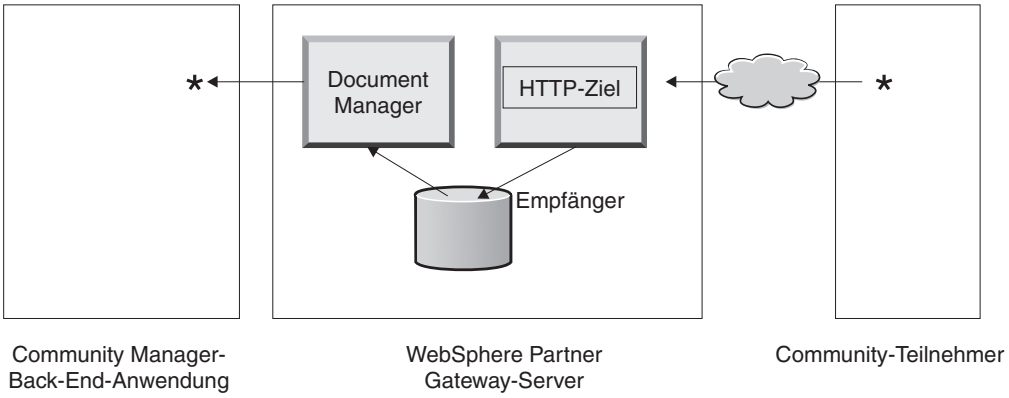

Abbildung 6. Ein HTTP-Ziel

Wenn die Community Manager-Back-End-Anwendung Dokumente über JMS senden wird, konfigurieren Sie ein JMS-Ziel auf dem Hub, um sie zu empfangen.

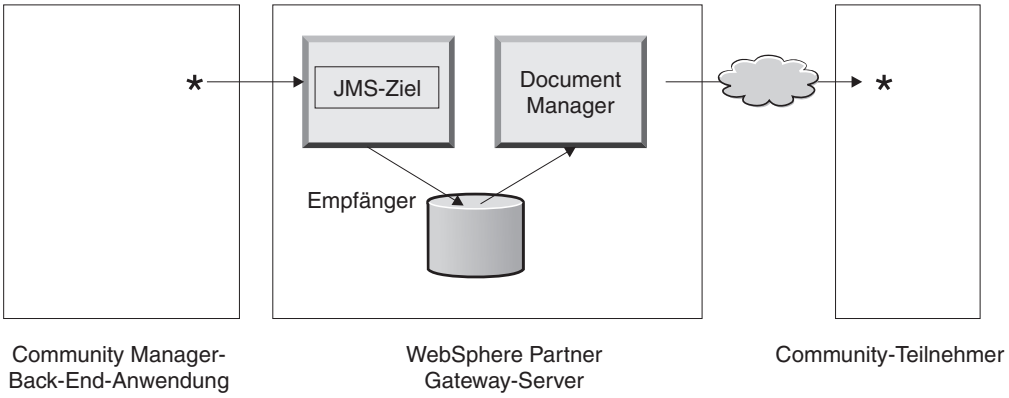

Abbildung 7. Ein JMS-Ziel

Wie in „Übersicht über Transporte" auf Seite 2 beschrieben, unterstützt WebSphere Partner Gateway eine Vielzahl von Transporten, aber Sie können auch Ihren eigenen benutzerdefinierten Transport hochladen, um ein Ziel zu definieren (wie in „Ziel für benutzerdefinierten Transport konfigurieren" auf Seite 52 beschrieben).

Der Empfänger sendet das Dokument an ein gemeinsam benutztes Dateisystem. Bei mehreren Dokumenten, die sich in einer einzelnen Datei befinden (z. B. gemeinsam gesendete XML- oder ROD-Dokumente oder EDI-Austauschvorgänge), teilt das Ziel die Dokumente oder Austauschvorgänge auf, bevor es diese an das gemeinsam genutzte Dateisystem sendet. Die Document Manager-Komponente empfängt das Dokument vom Dateisystem und legt die Route-Informationen fest und ob eine Transformation erforderlich ist.

Community Manager könnte z. B. ein EDI-X12-Dokument im Paket **None** an den Hub senden, das an einen Teilnehmer gesendet werden soll, der das EDI-X12-Dokument in einem Paket **AS2** erwartet. Der Teilnehmer stellt den HTTP-URL bereit, an den das Dokument im Paket **AS2** gesendet werden soll, und Document Manager packt das Dokument wie vom Teilnehmer erwartet. Document Manager verwendet die Konfiguration des Gateways für diesen Teilnehmer (welcher für den HTTP-URL konfiguiert worden sein muss, von dem der Teilnehmer den Empfang der AS2-Dokumente erwartet), um das Dokument an den Teilnehmer zu senden.

Dokumentverarbeitungskomponenten mit Handler konfigurieren

Dieser Abschnitt beschreibt detailliert die Komponenten von WebSphere Partner Gateway und zeigt Ihnen die verschiedenen Punkte auf, an denen Sie das vom System bereitgestellte Verhalten der Komponenten für die Verarbeitung eines Geschäftsdokuments ändern können (bzw. müssen).

Sie verwenden *Handler*, um das vom System bereitgestellte Verhalten von Zielen, Gateways, Schritten für festen Arbeitsablauf und Aktionen zu ändern. Es gibt zwei Handlertypen: die von WebSphere Partner Gateway bereitgestellten Handler und die benutzerdefinierten Handler. Wenn Sie Informationen zur Erstellung von Handlern benötigen, lesen Sie das Handbuch *Programmer Guide*.

Nachdem ein Handler erstellt worden ist, laden Sie ihn hoch, um ihn zur Verfügung zu stellen. Sie laden nur benutzerdefinierte Handler hoch. Die Handler, die von WebSphere Partner Gateway bereitgestellt wurden, sind bereits verfügbar.

Die folgenden Abschnitte beschreiben die Verarbeitungspunkte, an denen Sie Handler angeben können.

Ziele

Ziele verfügen über drei *Konfigurationspunkte*, für die Handler angegeben werden können: Vorverarbeitung, Synchronprüfung und Nachverarbeitung.

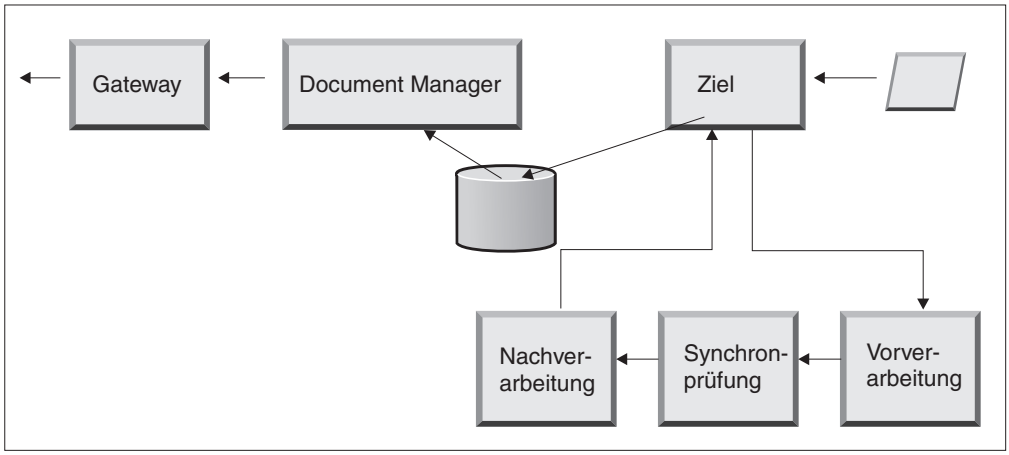

Abbildung 8. Konfigurationspunkte für Ziele

Die Verarbeitung findet in der folgenden Reihenfolge statt:

1. Der Empfänger ruft die Vorverarbeitungs- und Synchronprüfungsschritte auf, nachdem er das Dokument empfangen hat.
2. Dann ruft er Document Manager zur Verarbeitung des Dokuments auf.
3. Bei synchronen Abläufen stellt Document Manager eine Synchronantwort bereit. Der Empfänger ruft dann den Nachverarbeitungsschritt mit der Antwort auf, die von Document Manager zurückgegeben wurde.

Die Schritte werden in den folgenden Abschnitten beschrieben:

- Vorverarbeitung

  Der Vorverarbeitungsschritt wird im Allgemeinen für eine beliebige Verarbeitung des Dokuments verwendet, die ausgeführt werden muss, bevor das Dokument von Document Manager verarbeitet werden kann. Wenn Sie z. B. mehrere ROD-Dokumente in einer einzelnen Datei empfangen, konfigurieren Sie den ROD-Verteilerhandler, wenn Sie das Ziel definieren. Sie können den ROD-Verteiler zusammen mit zwei weiteren vom System bereitgestellten Verteilern verwenden, wenn Sie ein Ziel konfigurieren. Wenn Sie zusätzliche Handler für den Vorverarbeitungsschritt erstellen, sind diese Handler ebenfalls verfügbar.

  Informationen darüber, wie Sie den Vorverarbeitungs-Konfigurationspunkt konfigurieren, finden Sie in „Vorverarbeitung" auf Seite 53.

- Synchronprüfung

  Die Synchronprüfung wird verwendet, um zu ermitteln, ob WebSphere Partner Gateway das Dokument synchron oder asynchron verarbeiten soll. Im Fall von z. B. AS2-Dokumenten, die über HTTP empfangen wurden, ermittelt sie, ob eine MDN (Message Disposition Notification - Nachrichtendispositions-Benachrichtigung) über dieselbe HTTP-Verbindung synchron zurückgegeben werden soll. WebSphere Partner Gateway stellt eine Vielzahl von Handlern für die Synchronprüfung bereit. Die Liste mit Handlern variiert abhängig von dem Transport, der dem Ziel zugeordnet ist.

  Die Synchronprüfung wird nur auf die Transporte (wie z. B. HTTP, HTTPS und JMS) angewendet, die eine synchrone Datenübertragung unterstützen.

  Anmerkung: Für AS2-, cXML-, RNIF- oder SOAP-Dokumente, die in synchronen Austauschvorgängen verwendet werden, müssen Sie den zugeordneten Synchronprüfungshandler auf dem HTTP- oder HTTPS-Ziel angeben.

  Informationen darüber, wie Sie den Synchronprüfungs-Konfigurationspunkt konfigurieren, finden Sie in „Synchronprüfung" auf Seite 56.

- Nachverarbeitung

  Die Nachbearbeitung wird für die Verarbeitung des Antwortdokuments verwendet, das der Hub als Ergebnis einer synchronen Transaktion sendet.

  Informationen darüber, wie Sie den Nachverarbeitungs-Konfigurationspunkt konfigurieren, finden Sie in „Nachverarbeitung" auf Seite 57.

Document Manager

Dokumente, die von Zielen empfangen werden, werden von Document Manager zur weiteren Verarbeitung vom gemeinsamen Dateisystem abgerufen. Document Manager verwendet Teilnehmerverbindungen, um die Dokumente weiterzuleiten. Alle Dokumente, die durch Document Manager fließen, durchlaufen eine Reihe von Arbeitsabläufen: fester Eingangsarbeitsablauf, variabler Arbeitsablauf und fester Ausgangsarbeitsablauf. Am Ende des Eingangsarbeitsablaufs ist die Teilnehmerverbindung ermittelt. Die Teilnehmerverbindung gibt die Aktion an, die für dieses Dokument ausgeführt werden soll. Nach dem Ausführen des variablen Arbeitsablaufs führt Document Manager den festen Ausgangsarbeitsablauf für dieses Dokument aus.

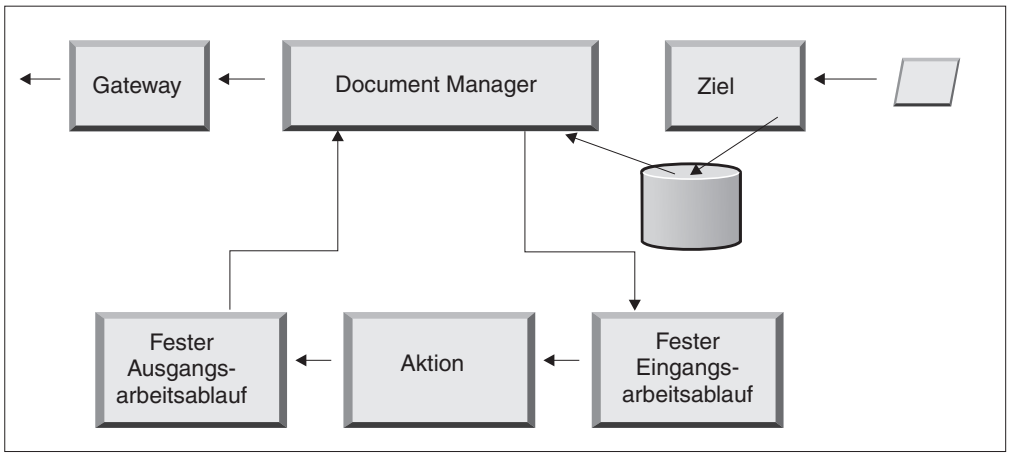

Abbildung 9. Feste Arbeitsabläufe und Aktionen

Abb. 9 zeigt den Pfad, den ein Dokument, wie z. B. ein RosettaNet-PIP oder ein Web-Service, nehmen würde. Einige Dokumente erfordern jedoch mehrere konfigurierte Verarbeitungsabläufe. Ein EDI-Austausch kann z. B. aus mehreren Transaktionen bestehen. Der erste Verarbeitungsablauf verwendet eine Aktion, um den Umschlag von der Gruppe einzelner Transaktionen zu entfernen. Jede dieser Transaktionen wird erneut eingeführt und in ihrem eigenen konfigurierten Verarbeitungsablauf verarbeitet.

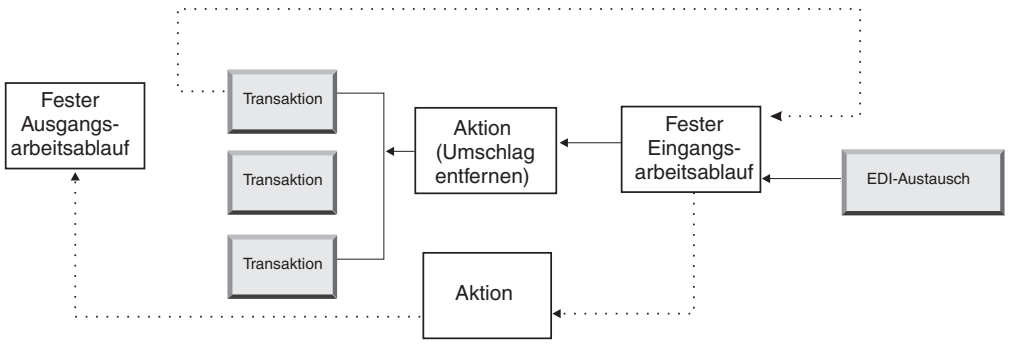

Abbildung 10. Feste Arbeitsabläufe und Aktionen für einen EDI-Austauschvorgang

Fester Eingangsarbeitsablauf

Der feste Eingangsarbeitsablauf besteht aus der Standardgruppe von Verarbeitungsschritten, die für alle Dokumente ausgeführt wird, die von einem Empfänger bei Document Manager eingehen. Der Arbeitsablauf ist fest, da die Anzahl und die Schritttypen immer gleich sind. Sie können jedoch über Benutzerexits angepasste Handler für die Verarbeitung der folgenden Schritte bereitstellen: Protokoll entpacken und Protokoll verarbeiten. Der letzte Schritt des festen Eingangsarbeitsablaufs führt eine Teilnehmerverbindungs-Suchfunktion aus, welche den variablen Arbeitsablauf ermittelt, der für dieses Geschäftsdokument ausgeführt wird.

Wenn z. B. eine AS2-Nachricht empfangen wird, wird die Nachricht entschlüsselt und die Absender- und Empfängergeschäfts-IDs werden abgerufen. Die Schritte für festen Eingangsarbeitsablauf konvertieren das AS2-Dokument zur weiteren Verarbeitung durch WebSphere Partner Gateway in einfachen Text und extrahieren Informationen, um die Aktion für die Nachricht zu bestimmen.

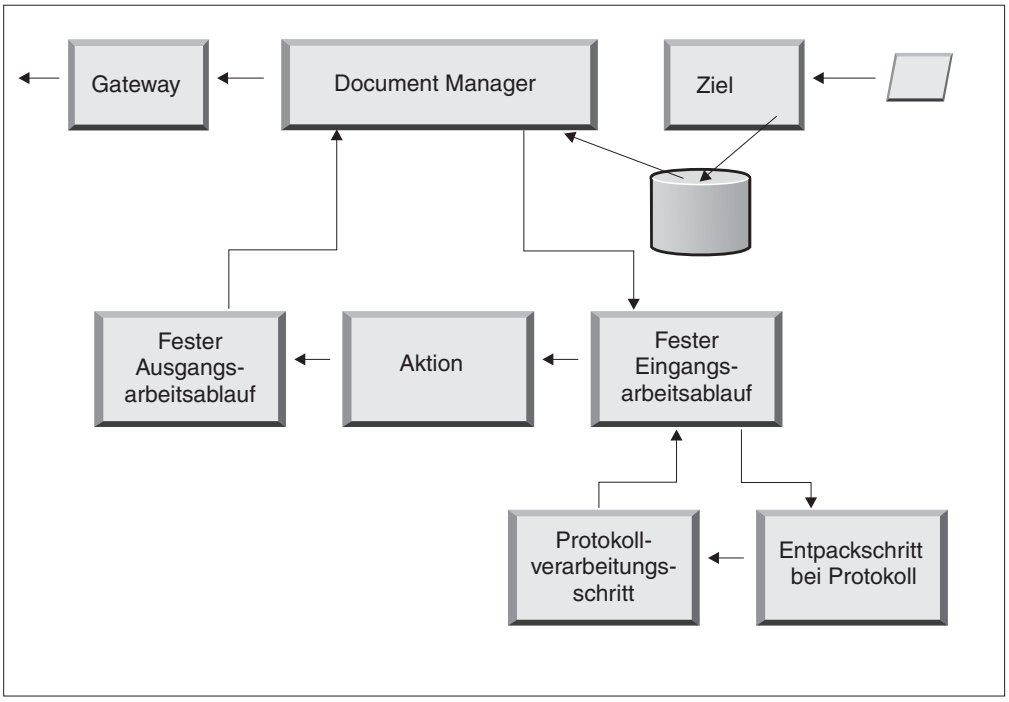

Abbildung 11. Schritte für festen Eingangsarbeitsablauf

Protokoll entpacken: Während des Entpackens eines Protokolls wird ein Dokument entpackt, so dass es weiter verarbeitet werden kann. Dieser Prozess kann Entschlüsselung, Dekomprimierung, Signaturprüfung, Route-Informationen, Benutzerauthentifizierung oder Extraktion von Geschäftsdokumentteilen einschließen.

WebSphere Partner Gateway bietet Handler für die Pakete **RNIF**, **AS**, **Backend Integration** und **None**. Wenn Handler für andere Pakettypen notwendig sind, können sie als Benutzerexits gestaltet werden. Weitere Informationen zum Schreiben von Benutzerexits finden Sie im Handbuch *Programmer Guide*.

Sie können den Entpackschritt bei Protokoll nicht ändern, aber Sie können dem Schritt durch Hinzufügen von Handlern Logik hinzufügen.

Informationen darüber, wie Sie diesen Schritt konfigurieren, finden Sie in „Feste Arbeitsabläufe konfigurieren" auf Seite 60.

Protokollverarbeitungsschritt: Die Protokollverarbeitung bezieht das Ermitteln protokollspezifischer Informationen mit ein, wozu das Parsing der Nachricht gehören kann, um Route-Informationen (wie z. B. die Absender-ID und die Empfänger-ID), Protokollinformationen und Dokumentenflussinformationen zu ermitteln. WebSphere Partner Gateway bietet die Verarbeitung für eine Vielzahl von Protokollen, wie in „Handler für das Verarbeiten des Protokolls" auf Seite 61 aufgelistet. Die Verarbeitung anderer Protokolle, z. B. CSV (durch Kommata getrennter Wert), kann mit einem Benutzerexit bereitstellt werden.

Sie können den Protokollverarbeitungsschritt nicht ändern, aber Sie können dem Schritt durch Hinzufügen von Handlern Logik hinzufügen.

Informationen darüber, wie Sie diesen Schritt konfigurieren, finden Sie in „Feste Arbeitsabläufe konfigurieren" auf Seite 60.

Sie können den Standardhandler verwenden, der auf das Protokoll für Ihr Dokument angewendet wird, oder Sie können einen anderen Handler für die Schritte für festen Arbeitsablauf, Protokoll entpacken und Protokoll verarbeiten, angeben.

Aktionen

Der nächste Schritt in der Verarbeitungsreihenfolge tritt auf der Basis der Aktionen auf, die für den Dokumentenaustausch konfiguriert wurden. Aktionen bestehen aus einer variierenden Anzahl Schritte, die am Dokument ausgeführt werden können. Beispiele für Aktionen sind die Validierung eines Dokuments, so dass es einer bestimmten Gruppe von Regeln entspricht, und die Transformation des Dokuments in das vom Empfänger benötigte Format.

Wenn für das Dokument keine spezifischen Schritte erforderlich sind, kann es die vom System bereitgestellte Pass-Through-Aktion verwenden, die keine Änderungen am Dokument vornimmt.

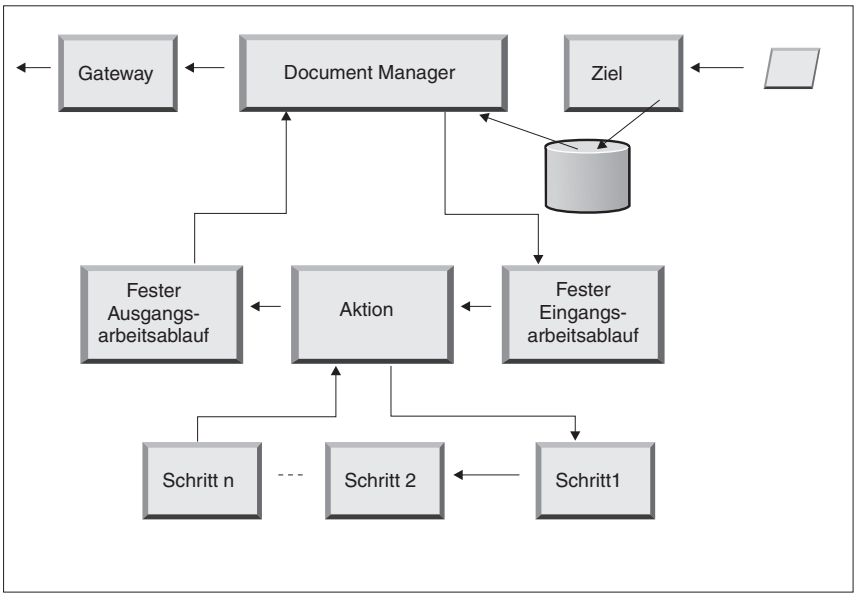

Abbildung 12. Aktionsschritte

Sie können keine vom System bereitgestellte Aktion ändern. Sie können jedoch eine Aktion erstellen (und der Konfigurationsliste Handler hinzufügen) oder eine vom System bereitgestellte Aktion kopieren und dann die Liste der Handler ändern.

Informationen zum Erstellen oder Kopieren einer vom System bereitgestellten Aktion oder zum Konfigurieren einer benutzerdefinierten Aktion finden Sie in „Aktionen konfigurieren” auf Seite 62.

Fester Ausgangsarbeitsablauf

Der feste Ausgangsarbeitsablauf besteht aus einem Schritt: dem Packen des Dokuments mit seinen Protokollinformationen. Wenn ein Dokument z. B. so konfiguriert wurde, dass es von einer Back-End-Anwendung unter Verwendung des Pakets **Backend Integration** empfangen wird, werden dem Dokument bestimmte Headerinformationen hinzugefügt, bevor es an das Gateway übermittelt wird.

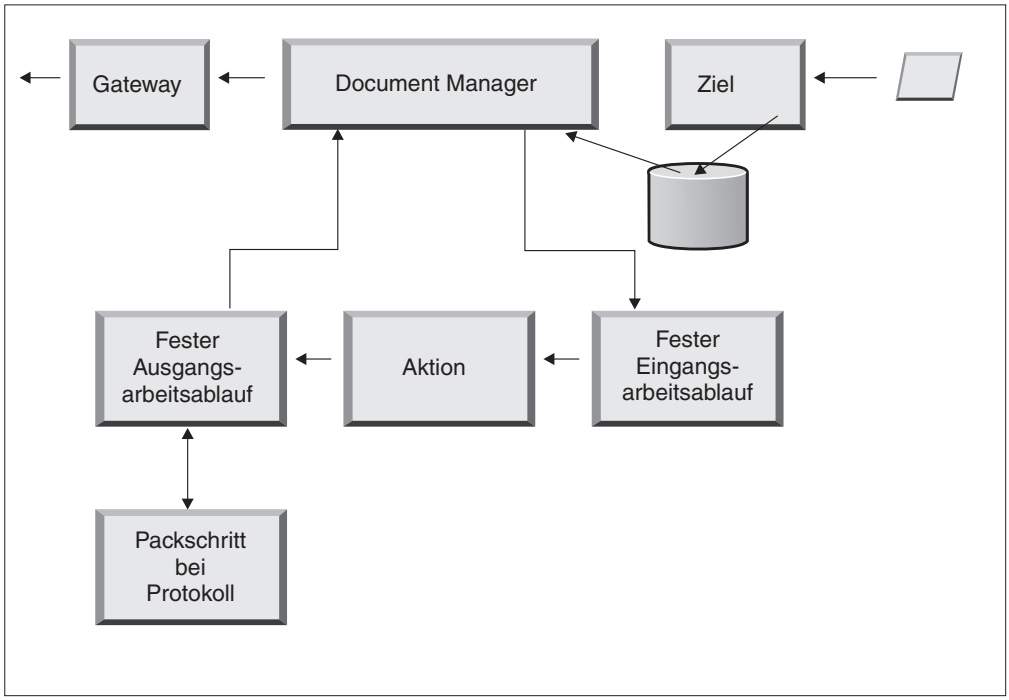

Abbildung 13. Schritte für festen Ausgangsarbeitsablauf

WebSphere Partner Gateway bietet Handler für eine Vielzahl von Paketen und Protokollen, wie in „Ausgangsarbeitsablauf" auf Seite 61 aufgelistet. Wenn weitere Pakethandler erforderlich sind, können sie als Benutzerexitschritte gestaltet werden. Normalerweise decken diese Schritte mindestens einen der folgenden Prozesse ab:

- Assemblieren oder mit Umschlag versehen
- Verschlüsseln
- Signieren
- Komprimieren
- Geschäftsprotokollspezifische Transportheader festlegen

Sie können den Protokollpackschritt nicht ändern, aber Sie können dem Schritt durch Hinzufügen von Handlern Logik hinzufügen.

Informationen darüber, wie Sie diesen Arbeitsablaufschritt konfigurieren, finden Sie in „Feste Arbeitsabläufe konfigurieren" auf Seite 60.

Gateways

Nachdem das Dokument Document Manager verlassen hat, wird es vom Gateway an den beabsichtigten Empfänger gesendet. Das Gateway hat zwei Konfigurationspunkte: die Vorverarbeitung und die Nachverarbeitung.

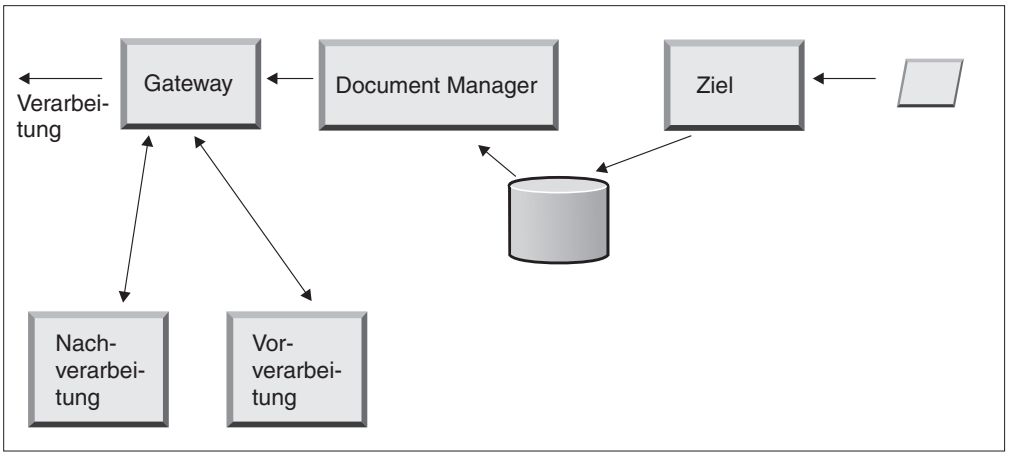

Abbildung 14. Konfigurationspunkte des Gateways

- Vorverarbeitung

  Die Vorverarbeitung wirkt sich auf die Verarbeitung eines Dokuments aus, bevor es an den Empfänger gesendet wird. (Die Verarbeitung ist das tatsächliche Senden des Dokuments.) Das System stellt keine Handler bereit, um den Vorverarbeitungsschritt zu konfigurieren. Sie können aber einen benutzerdefinierten Handler hochladen.
- Nachverarbeitung

  Die Nachverarbeitung richtet sich nach den Ergebnissen der Dokumentenübertragung (z. B. nach der Antwort, die es vom Empfänger während einer synchronen Datenübertragung empfängt). Das System stellt keine Handler bereit, um den Nachverarbeitungsschritt zu konfigurieren. Sie können aber einen benutzerdefinierten Handler hochladen.

Informationen darüber, wie Sie die Vorverarbeitungs- und Nachverarbeitungsschritte konfigurieren, finden Sie in „Handler konfigurieren” auf Seite 158.

Übersicht über die Hubkonfiguration

Nachdem Sie Ihre Geschäftsanforderungen analysiert haben, wie in „Für die Hubkonfiguration benötigte Informationen" auf Seite 2 beschrieben, konfigurieren Sie den Hub und erstellen Ihre Teilnehmerprofile. Dieser Abschnitt bietet eine Übersicht der zugehörigen Aufgaben auf höchster Ebene.

Anmerkung: Während Sie den Hub konfigurieren, entnehmen dem Handbuch *Verwaltung* Informationen zu Ereigniscodes und Tipps zur Fehlerbehebung.

Hub konfigurieren

Als Hubadministrator führen Sie die folgenden Aufgaben aus, um den Hub zu konfigurieren:

1. Führen Sie jede vorläufige Konfiguration (sofern erforderlich) für die verwendeten Transporte aus. Die vorläufige Konfiguration wird in Kapitel 2, „Die Konfiguration des Hubs vorbereiten", auf Seite 21 beschrieben.
2. Passen Sie optional die Konsole an, und ändern Sie das Standardkennwort und die Berechtigungsrichtlinie. Diese Aufgaben werden in Kapitel 4, „Community Console konfigurieren", auf Seite 33 beschrieben.
3. Erstellen Sie Ziele für die Transporttypen, mit denen Dokumente auf dem Hub (von Community Manager und von Teilnehmern) empfangen werden. Das Erstellen von Zielen wird in Kapitel 5, „Ziele definieren", auf Seite 39 beschrieben.

   Anmerkung: Wenn Sie das Ziel mit benutzerdefinierten Handlern konfigurieren, müssen Sie die Handler hochladen, bevor Sie das Ziel erstellen. Das Hochladen von Handlern wird in „Benutzerdefinierte Handler hochladen" auf Seite 40 beschrieben.
4. Konfigurieren Sie beliebige Schritte für Eingangsarbeitsablauf oder Aktionen. Dies ist ein *optionaler* Schritt. Er wird nur dann benötigt, wenn bestimmte Anforderungen an die Dokumentverarbeitung gestellt werden, die WebSphere Partner Gateway nicht bereitstellt. Wenn Sie das vom System bereitgestellte Verhalten von Arbeitsabläufen oder Aktionen nicht ändern müssen, überspringen Sie diesen Schritt. Das Konfigurieren der Arbeitsablaufschritte und Aktionen wird in Kapitel 6, „Schritte und Aktionen für feste Arbeitsabläufe konfigurieren", auf Seite 59. beschrieben.

   Anmerkung: Sie müssen die benutzerdefinierten Handler hochladen, bevor Sie Arbeitsabläufe oder Aktionen konfigurieren. Das Hochladen von benutzerdefinierten Handlern wird in „Handler hochladen" auf Seite 59 beschrieben.
5. Erstellen Sie Dokumentenflussdefinitionen (oder prüfen Sie, ob die von Ihnen benötigten bereits verfügbar sind), um die Dokumenttypen zu definieren, die Sie auf dem Hub senden und empfangen können.
6. Erstellen Sie Interaktionen, um die gültige Kombination von zwei Dokumentenflussdefinitionen anzuzeigen.

   Das Erstellen von Dokumentenflussdefinitionen und das Erstellen von Interaktionen wird in Kapitel 7, „Dokumentenflüsse konfigurieren", auf Seite 65 und Kapitel 8, „EDI-Dokumentenflüsse konfigurieren", auf Seite 93 beschrieben.

7. Erstellen Sie ein Profil für Community Manager, und stellen Sie Informationen zu Community Manager bereit, und erstellen Sie die Dokumenttypen, die Community Manager senden und empfangen kann (die B2B-Funktionalität von Community Manager). Das Erstellen des Profils wird in Kapitel 9, „Das Community Manager-Profil und B2B-Funktionalität erstellen", auf Seite 137 beschrieben.

Teilnehmer erstellen

Nachdem Sie den Hub konfiguriert haben, erstellen Sie ein Profil für jeden Teilnehmer, der mit Community Manager Dokumente austauschen wird. Nur der Hubadmin kann Teilnehmer erstellen.

Als Hubadmin können Sie auch die B2B-Funktionalität der Teilnehmer konfigurieren, die Gateways für Teilnehmer erstellen und Sicherheitsprofile für Teilnehmer konfigurieren. Diese Schritte können alternativ von den Teilnehmern selbst ausgeführt werden.

Das Erstellen von Teilnehmern wird in Kapitel 11, „Teilnehmer und ihre B2B-Funktionalität erstellen", auf Seite 161 beschrieben. Das Erstellen von Gateways wird in Kapitel 10, „Gateways erstellen", auf Seite 141 beschrieben. Die Konfiguration von Sicherheitsprofilen wird in Kapitel 13, „Sicherheit für Eingangs- und Ausgangsaustauschvorgänge konfigurieren", auf Seite 169 beschrieben.

Dokumentverbindungen aufbauen

Nachdem Sie den Hub konfiguriert und Teilnehmerprofile erstellt haben, können Sie nun Verbindungen konfigurieren. Verbindungen zeigen die gültigen Kombinationen von Absendern und von Empfängern sowie die Dokumente an, die sie austauschen können. Das Verwalten von Verbindungen wird in Kapitel 12, „Verbindungen verwalten", auf Seite 165 beschrieben.

Kapitel 2. Die Konfiguration des Hubs vorbereiten

In den nächsten Kapiteln werden Sie die in Kapitel 1, „Einführung” beschriebenen Ziele und Gateways konfigurieren. Abhängig von den Transporttypen, die Sie dazu verwenden, um Dokumente auf Zielen zu empfangen und diese von Gateways zu senden, müssen Sie die entsprechende Konfigurationsarbeit durchführen.

Dieses Kapitel behandelt die folgenden Themen:

- „Verzeichnis für ein Dateiverzeichnisgateway erstellen”
- „Den FTP-Server für das Empfangen von Dokumenten konfigurieren”
- „Den Hub für das JMS-Transportprotokoll konfigurieren” auf Seite 25

Es bietet ebenso eine kurze Übersicht über die FTP-Scripts, die für die FTP-Scripting-Ziele und -Gateways benötigt werden. Es beschreibt ferner den Data Interchange Services-Client, mit dem Transformations- und Validierungszuordnungen und Zuordnungen der funktionalen Bestätigungen für EDI-, XML- und ROD-Dokumente erstellt werden können.

- „FTP-Scripts für FTP-Scripting-Ziele und -Gateways verwenden” auf Seite 28
- „Zuordnungen vom Data Interchange Services-Client verwenden” auf Seite 28

Wenn Sie nicht beabsichtigen, einen der vorgenannten Ziel- oder Gateway-Typen zu konfigurieren, überspringen Sie dieses Kapitel, und fahren Sie mit Kapitel 3, „Den Server starten und Community Console anzeigen” fort.

Verzeichnis für ein Dateiverzeichnisgateway erstellen

Wenn Sie ein Dateiverzeichnisgateway verwenden, um Dokumente an Community Manager zu senden, müssen Sie zuerst ein Verzeichnis auf dem Dateisystem erstellen, das von Community Manager verwendet wird.

Angenommen, Sie wollen z. B. ein Verzeichnis namens **FileSystemGateway** unter dem Verzeichnis `c:\temp` einer Windows-Installation erstellen. Hierzu müssen Sie die folgenden Schritte ausführen:

1. Öffnen Sie einen Windows-Explorer.
2. Öffnen das Verzeichnis `C:\temp`.
3. Erstellen Sie einen neuen Ordner namens **FileSystemGateway**.

Den FTP-Server für das Empfangen von Dokumenten konfigurieren

Anmerkung: Dieser Abschnitt gilt nur für das Empfangen der Dokumente über FTP oder FTPS von Teilnehmern. Das Senden von Dokumenten an Teilnehmer wird in „FTP-Gateway konfigurieren” auf Seite 147 und „FTPS-Gateway konfigurieren” auf Seite 152 beschrieben.

Wenn Sie FTP oder FTPS als Transport für Eingangsdokumente verwenden, müssen Sie einen FTP-Server installieren. Wenn Sie vorhaben, FTP zu verwenden, und momentan noch keinen Server installiert haben, dann installieren Sie jetzt einen, bevor Sie fortfahren.

Stellen Sie sicher, dass eines der folgenden Szenarios auf Ihre Installation zutrifft:

- Der FTP-Server ist auf derselben Maschine wie WebSphere Partner Gateway installiert.
- Der Benutzer **bcguser** auf der WebSphere Partner Gateway-Maschine verfügt über den Schreib-/Lesezugriff für die Position, an der der FTP-Server Dateien speichert.

Die erforderliche Verzeichnisstruktur auf dem FTP-Server konfigurieren

Nachdem Sie den FTP-Server installiert haben, besteht der nächste Schritt darin, die erforderliche Verzeichnisstruktur unter dem Ausgangsverzeichnis des FTP-Servers zu erstellen. WebSphere Partner Gateway benötigt eine bestimmte Verzeichnisstruktur, die die Empfänger- und Document Manager-Komponenten verwenden, um den Teilnehmer korrekt identifizieren zu können, der ein Eingangsdokument sendet. Die Struktur wird in Abb. 15 dargestellt.

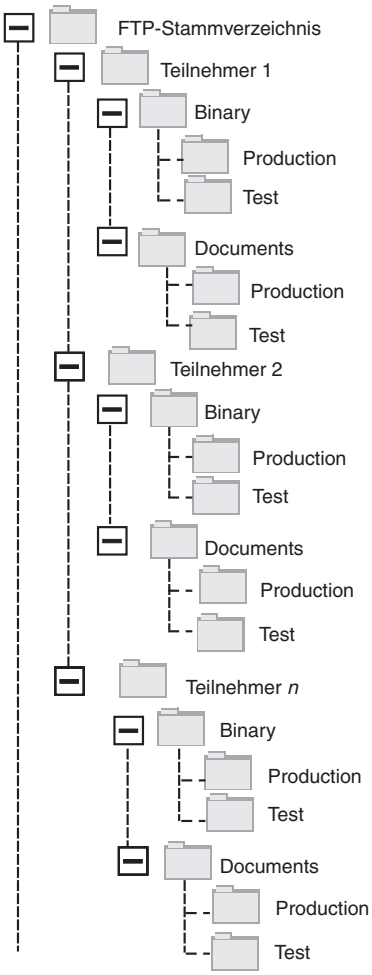

Abbildung 15. FTP-Verzeichnisstruktur

Jedes Teilnehmerverzeichnis enthält ein Verzeichnis **Binary** und ein Verzeichnis **Documents**. Die beiden Verzeichnisse **Binary** und **Documents** enthalten jeweils ein Verzeichnis **Production** und ein Verzeichnis **Test**.

Das Verzeichnis **Documents** wird verwendet, wenn ein Teilnehmer ein XML-Dokument, das die vollständigen Route-Informationen (unter Verwendung von FTP) enthält, an den Hub sendet. Dazu ist das Erstellen einer angepassten XML-Definition erforderlich.

Das Verzeichnis **Binary** wird verwendet, wenn ein Teilnehmer ein beliebiges anderes Dokument (unter Verwendung von FTP) an den Hub sendet.

Für jeden Teilnehmer, der FTP zum Senden oder Empfangen von Dokumenten verwendet, erstellen Sie die folgenden Ordner im Stammverzeichnis Ihres FTP-Servers:

1. Erstellen Sie einen Ordner für den Teilnehmer.

   Anmerkung: Der Name des Ordners sollte mit dem Namen übereinstimmen, den Sie als **Anmeldename des Unternehmens** angegeben haben, als Sie den Teilnehmer erstellten. Das Erstellen von Teilnehmern wird in „Teilnehmerprofile erstellen" auf Seite 161 beschrieben.
2. Erstellen Sie unter dem Teilnehmerordner die Unterordner namens `Binary` und `Documents`.
3. Erstellen Sie unter den Ordnern `Binary` und `Documents` die Unterordner namens `Production` und `Test`.

Verarbeitung der über FTP gesendeten Dateien

Es ist wichtig, dass Sie verstehen, wie Binär- und XML-Dateien vom FTP-Server verarbeitet werden.

Binärdateien

Binärdateien verfügen über eine erforderliche Dateinamensstruktur, da die Dateien von Document Manager nicht überprüft werden.

Die Dateinamensstruktur lautet wie folgt:
<zielteilnehmer_ID><eindeutiger_dateiname>

Wenn der Empfänger eine Binärdatei ermittelt, schreibt er sie in den gemeinsam benutzten Speicher und übermittelt sie zur Verarbeitung an Document Manager.

Der Name des Verzeichnisses, in der die Datei ermittelt wurde, wird zum Auswerten des Namens vom Absenderteilnehmer verwendet und der erste Teil des Dateinamens wird zum Auswerten des Namens vom Zielteilnehmer verwendet. Die Position des Verzeichnisses in der Verzeichnisstruktur wird verwendet, um auszuwerten, ob es sich bei der Transaktion um eine Produktions- oder eine Testtransaktion handelt.

Beispiel: Eine Datei namens `123456789.abcdefg1234567` wird im Verzeichnis `\ftproot\partnerZwei\binary\production` ermittelt. Document Manager kennt die folgenden Informationen:

- Der Name in `Absenderteilnehmer` ist `partnerZwei`, da die Datei im `partnerZwei`-Teil der Verzeichnisbaumstruktur gefunden wurde.
- Der Name in `Zielteilnehmer` ist `partnerEins`, da der erste Teil des Dateinamens `123456789` lautet, dies ist die DUNS-ID für **partnerEins**.

  Anmerkung: An dieser Stelle und im ganzen Handbuch sind die verwendeten DUNS-Nummern, nur als Beispiele zu verstehen.
- Der Transaktionstyp ist **Produktion**.

Document Manager sucht nach einer Teilnehmerverbindung des Typs **Produktion** von **partnerZwei** nach **partnerEins** für:

- Paket: None (N/A)
- Protokoll: Binary (1.0)
- Dokumentenfluss: Binary (1.0)

Document Manager verarbeitet dann die Datei.

XML-Dateien

An eine XML-Datei werden keine Dateinamensanforderungen gestellt, da die Datei von Document Manager überprüft wird und die Route-Informationen aus dem Dokument selbst extrahiert werden.

Wenn der Empfänger eine XML-Datei ermittelt, schreibt er sie in den gemeinsam benutzten Speicher und übermittelt sie zur Verarbeitung an Document Manager.

Document Manager vergleicht die XML-Datei mit den XML-Formaten, die definiert wurden, und wählt das erforderliche XML-Format aus. (Die Konfiguration von XML-Formaten wird in „Angepasste XML-Dokumente" auf Seite 89 beschrieben.) Der Name des Absenderteilnehmers und des Zielteilnehmers sowie die Route-Informationen werden aus der XML-Datei extrahiert.

Die Position des Verzeichnisses in der Verzeichnisstruktur wird verwendet, um auszuwerten, ob es sich bei der Transaktion um eine Produktions- oder eine Testtransaktion handelt.

Document Manager verwendet dann diese Informationen, um die richtige Teilnehmerverbindung zu finden, bevor die Datei verarbeitet wird.

Zusätzliche FTP-Serverkonfiguration

Nachdem Sie die erforderliche Verzeichnisstruktur erstellt haben, konfigurieren Sie Ihren FTP-Server für jeden Teilnehmer in der Hub-Community. Wie Sie Ihren FTP-Server konfigurieren, hängt vom verwendeten Server ab. Lesen Sie die Dokumentation des FTP-Servers, und führen Sie die folgenden Aufgaben aus:

1. Fügen Sie eine neue Gruppe hinzu (z. B. Teilnehmer).
2. Fügen Sie der neu erstellten Gruppe für jeden Teilnehmer, der Dokumente über FTP senden oder empfangen wird, einen Benutzer hinzu.
3. Konfigurieren Sie für jeden Teilnehmer den FTP-Server so, dass der eingehende Teilnehmer der jeweiligen Verzeichnisstruktur zugeordnet wird, die Sie in dem obigen Abschnitt „Die erforderliche Verzeichnisstruktur auf dem FTP-Server konfigurieren" auf Seite 22 erstellt haben. Zusätzliche Informationen finden Sie in der Dokumentation Ihres FTP-Servers.

Sicherheitsaspekte für den FTPS-Server

Wenn Sie einen FTPS-Server zum Empfangen von Eingangsdokumenten verwenden, werden die Sicherheitserwägungen für SSL-Sitzungen ausschließlich vom FTPS-Server und dem vom Teilnehmer verwendeten Client verarbeitet. Es gibt keine spezifische Sicherheitskonfiguration für WebSphere Partner Gateway bei FTPS-Eingangsdokumenten. WebSphere Partner Gateway ruft die Dokumente vom FTP-Ziel ab (dies wird in „FTP-Ziel konfigurieren" auf Seite 42 beschrieben), nachdem der Server erfolgreich die gesicherten Kanäle vereinbart und das Dokument empfangen hat. Lesen Sie in der Dokumentation des FTPS-Servers, welche Zertifikate benötigt werden (und wo diese benötigt werden), um erfolgreich einen gesicherten Kanal zu konfigurieren, den der Teilnehmer kontaktieren kann.

Stellen Sie für die Serverauthentifizierung den Teilnehmern das Zertifikat des Empfängers zur Verfügung. Wenn das Zertifikat von einer Zertifizierungsstelle (CA) ausgestellt wurde, stellen Sie auch die Zertifikatkette der Zertifizierungsstelle bereit. Wenn die Clientauthentifizierung vom FTPS-Server unterstützt wird, sollten die Zertifikate für die Clientauthentifizierung der Teilnehmer auf dem FTPS-Server angegeben werden. Informationen zum Angeben der Clientauthentifizierung und der Zertifikate für die Clientauthentifizierung finden Sie in der FTPS-Serverdokumentation.

Den Hub für das JMS-Transportprotokoll konfigurieren

Dieser Abschnitt beschreibt, wie Sie den Hub für die Verwendung des JMS-Transports konfigurieren. Wenn Sie den JMS-Transport zum Senden von Dokumenten vom Hub bzw. zum Empfangen von Dokumenten auf dem Hub verwenden, befolgen Sie die Prozeduren in diesem Abschnitt. Wenn Sie das JMS-Transport nicht verwenden, überspringen Sie diesen Abschnitt.

Anmerkung: Die Prozeduren in diesem Abschnitt beschrieben, wie Sie die JMS-Implementierung von WebSphere MQ verwenden, um die JMS-Umgebung zu konfigurieren. Die Prozedur beschreibt auch, wie Sie lokale Warteschlangen konfigurieren. Wenn Sie die Übertragung und ferne Warteschlangen konfigurieren wollen, lesen Sie die WebSphere MQ-Dokumentation.

In späteren Abschnitten dieser Dokumentation erfahren Sie, wie Sie JMS-Ziele oder -Gateways (oder beides) konfigurieren. Diese Aufgaben werden in „JMS-Ziel konfigurieren" auf Seite 45 und „JMS-Gateway konfigurieren" auf Seite 149 beschrieben.

Verzeichnis für JMS erstellen

Zunächst erstellen Sie ein Verzeichnis für JMS. Angenommen, Sie wollen z. B. ein Verzeichnis namens `JMS` im Verzeichnis `c:\temp` einer Windows-Installation erstellen. Hierzu müssen Sie die folgenden Schritte ausführen:

1. Öffnen Sie einen Windows-Explorer.
2. Öffnen das Verzeichnis `C:\temp`.
3. Erstellen Sie einen neuen Ordner namens **JMS**.

Die Standard-JMS-Konfiguration ändern

In diesem Abschnitt aktualisieren Sie die Datei `JMSAdmin.config`, die Teil der WebSphere MQ-Installation ist, um die Kontextfactory und die Provider-URL-Adresse zu ändern.

1. Navigieren Sie zum Verzeichnis `Java\bin` von WebSphere MQ. In einer Windows-Installation würden Sie z. B. zu `C:\IBM\MQ\Java\bin` navigieren.
2. Öffnen Sie die Datei `JMSAdmin.config` mit einem einfachen Texteditor, wie z. B. Editor oder vi.
3. Fügen Sie das Zeichen # am Anfang der folgenden Zeilen hinzu:

   ```
   INITIAL_CONTEXT_FACTORY=com.sun.jndi.ldap.LdapCtxFactory
   PROVIDER_URL=ldap://polaris/o=ibm,c=us
   ```

4. Entfernen Sie das Zeichen # vom Anfang der folgenden Zeilen:

   ```
   #INITIAL_CONTEXT_FACTORY=com.sun.jndi.fscontext.RefFSContextFactory
   #PROVIDER_URL=file:/C:/JNDI-Directory
   ```

5. Ändern Sie die Zeile `PROVIDER_URL=file:/C:/JNDI-Directory` so, dass der Name dem Namen des JMS-Verzeichnisses gleicht, das Sie in „Verzeichnis für

JMS erstellen" auf Seite 25 definiert haben. Wenn Sie z. B. das Verzeichnis `c:/temp/JMS` definieren, würde die Zeile wie folgt aussehen:

```
PROVIDER_URL=file:/c:/temp/JMS
```

6. Speichern Sie die Datei.

Warteschlangen und den Kanal erstellen

In diesem Abschnitt erstellen Sie mit WebSphere MQ die Warteschlangen, die Sie zum Senden und Empfangen von Dokumenten verwenden, und den Kanal für diese Kommunikation. Es wird davon ausgegangen, dass ein Warteschlangenmanager erstellt wurde. Der Name des Warteschlangenmanagers sollte eingesetzt werden, wo <*name_des_warteschlangenmanagers*> in den folgenden Schritten aufgeführt wird. Es wird ferner davon ausgegangen, dass ein Listener für diesen Warteschlangenmanager am TCP-Port 1414 gestartet wurde.

1. Öffnen Sie eine Eingabeaufforderung.
2. Geben Sie den folgenden Befehl ein, um den WebSphere MQ-Befehlsserver zu starten:

   ```
   strmqcsv <name_des_warteschlangenmanagers>
   ```

3. Geben Sie den folgenden Befehl ein, um die WebSphere MQ-Befehlsumgebung zu starten:

   ```
   runmqsc <name_des_warteschlangenmanagers>
   ```

4. Geben Sie den folgenden Befehl ein, um eine WebSphere MQ-Warteschlange zu erstellen, die Eingangsdokumente enthalten soll, die an den Hub gesendet wurden:

   ```
   def ql(<warteschlangenname>)
   ```

   Geben Sie z. B. Folgendes ein, um eine Warteschlange namens **JMSIN** zu erstellen:

   ```
   def ql(JMSIN)
   ```

5. Geben Sie den folgenden Befehl ein, um eine WebSphere MQ-Warteschlange zu erstellen, die Dokumente enthalten soll, die vom Hub gesendet wurden:

   ```
   def ql(<warteschlangenname>)
   ```

   Geben Sie z. B. Folgendes ein, um eine Warteschlange namens **JMSOUT** zu erstellen:

   ```
   def ql(JMSOUT)
   ```

6. Geben Sie den folgenden Befehl ein, um einen WebSphere MQ-Kanal zu erstellen, der für Dokumente verwendet werden soll, die an den und vom Hub gesendet wurden:

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

   Geben Sie z. B. Folgendes ein, um einen Kanal namens `java.channel` zu erstellen:

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

7. Geben Sie den folgenden Befehl ein, um die WebSphere MQ-Befehlsumgebung zu verlassen:

   ```
   end
   ```

Ihrer Umgebung eine Java(TM)-Laufzeit hinzufügen

Geben Sie den folgenden Befehl ein, um eine Java-Laufzeit Ihrem Systempfad hinzuzufügen:

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

Dabei steht *produktverz* für das Verzeichnis, in dem WebSphere Partner Gateway installiert ist.

Die JMS-Konfiguration definieren

Führen Sie die folgenden Schritte aus, um die JMS-Konfiguration zu definieren:

1. Wechseln Sie in das WebSphere MQ-Java-Verzeichnis (<*pfad_zum_Websphere_MQ-installationsverzeichnis*>\java\bin)
2. Starten Sie die JMSAdmin-Anwendung, indem Sie den folgenden Befehl eingeben:

   ```
   JMSAdmin
   ```

3. Definieren Sie einen neuen JMS-Kontext, indem Sie die folgenden Befehle an der Eingabeaufforderung `InitCtx>` eingeben:

   ```
   define ctx(<kontextname>)
   change ctx(<kontextname>)
   ```

   Wenn z. B. der *kontextname* JMS lautet, sehen die Befehle wie folgt aus:

   ```
   define ctx(JMS)
   change ctx(JMS)
   ```

4. Geben Sie an der Eingabeaufforderung `InitCtx/jms>` die folgende JMS-Konfiguration ein:

   ```
   define qcf(name_der_verbindungsfactory)
       tran(CLIENT)
   host(<Ihre_IP-adresse>)    port(1414)
       chan(java.channel)
       qmgr(<name_des_warteschlangenmanagers>)
   define q(<name>) queue(<warteschlangenname>) qmgr(<name_des_warteschlangenmanagers>)
   define q(<name>) queue(<warteschlangenname>) qmgr(<name_des_warteschlangenmanagers>)
   end
   ```

Die vorherigen Schritte haben die `.bindings`-Datei erstellt, die sich in einem Unterordner des Ordners befindet, den Sie in Schritt 5 auf Seite 25 angegeben haben. Der Name des Unterordners ist der Name, den Sie für Ihren JMS-Kontext angegeben haben.

Als Beispiel wird die folgende JMSAdmin-Sitzung verwendet, um die Verbindungsfactory für Warteschlangen als `Hub` mit einer IP-Adresse von `sample.ibm.com` zu definieren, in der sich der MQ-Warteschlangenmanager (<*name_des_warteschlangenmanagers*> von `sample.queue.manager`) befindet. Das Beispiel verwendet die JMS-Warteschlangennamen und den Kanalnamen, die Sie in „Warteschlangen und den Kanal erstellen" auf Seite 26 erstellt haben.Beachten Sie, dass die Benutzereingabe an der Eingabeaufforderung > erfolgt.

```
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 diesem Beispiel würde sich die `.bindings` im folgenden Verzeichnis befinden: `c:/temp/JMS/JMS`. Dabei steht `c:/temp/JMS` für die PROVIDER_URL und `JMS` für den Kontextnamen.

FTP-Scripts für FTP-Scripting-Ziele und -Gateways verwenden

Das FTP-Scripting-Transport ermöglicht Ihnen, Daten an beliebige FTP-Services, einschließlich eines Mehrwertnetzes (VAN - Value Added Network) zu senden. Sie steuern die Operationen auf dem FTP-Server mit einer Scriptdatei, die FTP-Befehle enthält.

++Sie geben dieses Script an, wenn Sie das FTP-Scripting-Ziel oder -Gateway erstellen. WebSphere Partner Gateway ersetzt die Platzhalter im FTP-Script durch die tatsächlichen, von Ihnen eingegebenen Werte, wenn Sie das Ziel oder Gateway erstellen.

Die Operationen, die im Eingabescript definiert sind, werden auf dem FTP-Server in Aktionen übersetzt. Das Eingabescript besteht aus einer Gruppe unterstützter FTP-Befehle. Parameter für diese Befehle können das Format einer Variable annehmen, die während der Laufzeit ausgefüllt wird.

Informationen zum Erstellen eines FTP-Scripts für ein FTP-Scripting-Ziel finden Sie in „FTP-Scripting-Ziel konfigurieren" auf Seite 48. Informationen zum Erstellen eines FTP-Scripts für ein FTP-Scripting-Gateway finden Sie in „FTP-Scripting-Gateway konfigurieren" auf Seite 154.

Zuordnungen vom Data Interchange Services-Client verwenden

Um eine Umschlagsentfernung, eine Transformation und Validierung von EDI auszuführen oder Transformationen zwischen ROD, XML und EDI vorzunehmen, müssen Sie die zugehörigen Zuordnungen vom Data Interchange Services-Client importieren. Data Interchange Services ist ein separat installiertes Programm, das sich normalerweise auf einem anderen Computer befindet als dem, auf dem WebSphere Partner Gateway ausgeführt wird.

Der Data Interchange Services-Zuordnungsexperte erstellt Zuordnungen, die beschreiben, wie bestimmte Dokumente transformiert und validiert werden sollen. Sie könnten z. B. über eine Bestellung verfügen, die von einer Back-End-Anwendung erstellt wurde, welche Sie transformieren und einem Community-Teilnehmer als Standard-EDI-X12-Bestellung (850) zusenden wollen. Der Data Interchange Services-Zuordnungsexperte würde eine Zuordnung schreiben, die detailliert beschreibt, wie jedes Feld oder Datenstück von Ihrem Programm in das X12-Format transformiert werden soll. Die Zuordnung würde dann direkt nach WebSphere Partner Gateway exportiert werden, oder sie würde in eine Datei exportiert werden, welche Sie dann mit einem Befehlsscript importieren würden.

Detaillierte Informationen zum Importieren von Zuordnungen vom Data Interchange Services-Client finden Sie in „Zuordnungen importieren" auf Seite 122.

Kapitel 3. Den Server starten und Community Console anzeigen

In diesem Kapitel erfahren Sie, wie Sie den WebSphere Partner Gateway-Server starten und Community Console anzeigen. Es behandelt die folgenden Themen:

- „WebSphere MQ starten"
- „Die WebSphere Partner Gateway-Komponenten starten"
- „An Community Console anmelden" auf Seite 30

WebSphere MQ starten

Sofern noch nicht geschehen, starten Sie WebSphere MQ, indem Sie eine der folgenden Prozeduren ausführen:

- Für Unix-basierte Systeme:
  1. Geben Sie Folgendes ein:
     ```
     su mqm
     ```
  2. Geben Sie Folgendes ein:
     ```
     strmqm bcg.queue.manager
     ```
  3. Geben Sie Folgendes ein:
     ```
     runmqlsr -t tcp -p 9999 -m bcg.queue.manager &
     ```
  4. Warten Sie ungefähr 10 Sekunden, und drücken Sie dann die Eingabetaste, um zur Eingabeaufforderung zurückzukehren.
  5. Geben Sie Folgendes ein:
     ```
     strmqbrk -m bcg.queue.manager
     ```
- Für Windows-basierte Systeme:
  1. Geben Sie Folgendes ein:
     ```
     strmqm bcg.queue.manager
     ```
  2. Geben Sie Folgendes ein:
     ```
     runmqlsr -t tcp -p 9999 -m bcg.queue.manager
     ```
     Der Listener wird in diesem Fenster ausgeführt, schließen Sie es daher nicht.
  3. Öffnen Sie ein neues Fenster, und starten Sie den JMS-Broker (den Veröffentlichungs-/Subskriptionsbroker) mit dem folgenden Befehl:
     ```
     strmqbrk -m -bcg.queue.manager
     ```

Die WebSphere Partner Gateway-Komponenten starten

Zum Starten des Servers müssen Sie jede der drei Komponenten von WebSphere Partner Gateway starten: die Konsole, Document Manager und den Empfänger.

1. Wechseln Sie in das Verzeichnis \<*produktverz*\bin.
2. Geben Sie den folgenden Befehl ein, um die Konsole zu starten:
   - Für Unix-basierte Systeme:
     ```
     ./bcgStartServer.sh bcgconsole
     ```
   - Für Windows-basierte Systeme:
     ```
     bcgStartServer bcgconsole
     ```

3. Geben Sie den folgenden Befehl ein, um den Empfänger zu starten:
   ```
   ./bcgStartServer.sh bcgreceiver
   ```

   oder
   ```
   bcgStartServer bcgreceiver
   ```
4. Geben Sie den folgenden Befehl ein, um Document Manager zu starten:
   ```
   ./bcgStartServer.sh bcgdocmgr
   ```

   oder
   ```
   bcgStartServer bcgdocmgr
   ```

Nachdem Sie die Komponenten gestartet haben, starten Sie das Hilfesystem. Geben Sie den folgenden Befehl ein, um das Hilfesystem zu starten:
```
./bcgStartHelp.sh
```

oder
```
bcgStartHelp.bat
```

Nachdem die Komponenten gestartet sind, melden Sie sich an Community Console an, wie in „An Community Console anmelden" beschrieben.

Informationen zum Starten des Data Interchange Services-Clients finden Sie im *Mapping Guide*.

An Community Console anmelden

Community Console ist der Zugriffspunkt zu WebSphere Partner Gateway. Für die meisten Aufgaben, die Sie zum Konfigurieren des Hubs ausführen werden, ist es erforderlich, dass Sie als Hubadministrator (hubadmin) angemeldet sind. Der Hubadministrator ist der Superuser des Systems.

Stellen Sie sicher, dass Sie die IP-Adresse des Computers kennen, auf dem die Konsolkomponente aktiv ist. Sie geben diese Adresse im HTTP-Befehl ein.

1. Geben Sie in einem Browser die folgende URL-Adresse ein:
   ```
   http://<IP-adresse>:58080/console
   ```
2. Geben Sie die folgenden Informationen ein:
   a. Geben Sie als **Benutzername** Folgendes ein: `hubadmin`.
   b. Geben Sie als **Kennwort** Folgendes ein: `Pa55word`.

      Anmerkung: Wenn Sie sich bereits an Community Console angemeldet und das Standardkennwort **Pa55word** geändert haben, geben Sie Ihr neues Kennwort in das Feld **Kennwort** ein.
   c. Geben Sie als **Anmeldename des Unternehmens** Folgendes ein: `Operator`.

Die Seite **Teilnehmersuche** wird angezeigt. Diese Seite wird immer zuerst angezeigt, wenn Sie sich an Community Console anmelden.

Sie erfahren später in diesem Handbuch, wie Sie mit dieser Seite Teilnehmer definieren.

Wenn Sie jetzt auf **Suchen** klicken, sehen Sie, dass ein Teilnehmer, der **Community Operator**, aufgelistet ist. Der **Community Operator** wird von WebSphere Partner Gateway automatisch definiert.

Anmerkung: Wenn Sie das Standardkennwort **Pa55word** noch nicht in Ihr eigenes Kennwort geändert haben, werden Sie aufgefordert dies zu tun, bevor die Seite **Teilnehmersuche** angezeigt wird.

Kapitel 4. Community Console konfigurieren

Dieses Kapitel beschreibt, wie Sie Community Console konfigurieren, um anzugeben, was Teilnehmer anzeigen und wie sie sich an der Konsole anmelden können und welchen Zugriff sie auf verschiedene Konsolaufgaben haben. Dieses Kapitel behandelt die folgenden Themen:

- „Locale-Informationen und Konsolbranding angeben"
- „Kennwortrichtlinie konfigurieren" auf Seite 35
- „Berechtigungen konfigurieren" auf Seite 36

Sie müssen keine dieser Aufgaben ausführen, wenn Sie die von WebSphere Partner Gateway bereitgestellten Standardeinstellungen verwenden wollen.

Locale-Informationen und Konsolbranding angeben

Die Seiten von Community Console werden standardmäßig auf Englisch dargestellt. IBM stellt die Übersetzung des Inhalts in anderen Sprachen als eine Gruppe von Dateien zur Verfügung, die hochgeladen werden können. Andere Konsolelemente, die von IBM für unterschiedliche Locales bereitgestellt werden, sind die Bannergrafiken. Sie können optional Ihre eigenen Logografiken hochladen. Darüber hinaus können Sie Ihr eigenes angepasstes Style-Sheet hochladen, mit dem der Text auf den Seiten formatiert wird.

Sie führen diese Aufgaben mit der Seite **Locale hochladen** aus. Gehen Sie wie folgt vor, um die Seite **Locale hochladen** anzuzeigen:

1. Klicken Sie auf **Hubadmin > Konsolkonfiguration > Localekonfiguration**.
2. Klicken Sie auf **Erstellen**.
3. Wählen Sie eine Locale in der Liste **Locale** aus.

Die Konsole zeigt die Seite **Locale hochladen** an.

Sie können über die Seite **Locale hochladen** die folgenden Aufgaben ausführen:

- Konsolbranding durchführen, indem Sie ein eindeutiges Banner oder Logo (oder beides) hochladen
- Von IBM bereitgestellte Dateien hochladen, so dass Sie den Inhalt der Konsolelemente lokalisieren können

Konsolbranding durchführen

Sie können die Darstellung von Community Console anpassen, indem Sie die Brandingbilder ändern. Das Branding von Community Console besteht aus dem Import zweier Bilder: dem Kopfhintergrund und dem Firmenlogo.

- Der Kopfhintergrund erstreckt sich über den oberen Bereich von Community Console.
- Das Firmenlogo wird oben rechts in Community Console angezeigt.

Die Bilder müssen .JPG-Formatdateien sein und bestimmten Spezifikationen entsprechen, so dass sie in das Fenster von Community Console eingefügt werden können.

- Klicken Sie auf **Bildspezifikationen** im Fenster **Locale hochladen**, um die erforderlichen Spezifikationen für Banner und Logo anzuzeigen.
- Blättern Sie vor bis zum Abschnitt **Musterbilder** der Seite, und klicken Sie auf `sample_headerback.jpg` oder `sample_logo.jpg`, um Beispiele für ein Kopf- oder Logobild anzuzeigen.
- Klicken Sie auf **Musterbilder (Kopfhintergrund und Firmenlogo)**, um Beispiele für ein Banner oder Logo herunterzuladen, die Sie als Vorlage für die Erstellung Ihres eigenen Banners oder Logos verwenden wollen.

Nachdem Sie das Banner oder Logo (oder beides) erstellt haben, führen Sie die folgenden Schritte aus:

1. Führen Sie eine der folgenden Aufgaben aus, um das angepasste Banner hochzuladen:
   - Geben Sie in das Feld **Banner** den Pfad und den Namen der Bilddatei ein, die Sie für den Kopf/das Banner verwenden wollen.
   - Klicken Sie auf **Durchsuchen**, um zur JPG-Datei zu navigieren, die das Banner enthält und wählen Sie diese aus.
2. Führen Sie einen der folgenden Schritte aus, um das angepasste Logo hochzuladen:
   - Geben Sie in das Feld **Logo** den Pfad und den Namen der Datei ein, die Sie für das Firmenlogo verwenden wollen.
   - Klicken Sie auf **Durchsuchen**, um zur JPG-Datei zu navigieren, die das Logo enthält und wählen Sie dieses aus.
3. Klicken Sie auf **Hochladen**.

Anmerkung: Wenn Sie den Kopfhintergrund und das Firmenlogo ersetzt haben, müssen Sie Community Console erneut starten, damit die Änderungen wirksam werden.

Style-Sheet ändern

Wenn Sie ein Style-Sheet angeben wollen, das sich vom Standard-Style-Sheet unterscheidet (z. B. wenn Sie unterschiedlich große Schriftarten oder verschiedene Farben wünschen), führen Sie die folgenden Schritte aus:

1. Führen Sie eine der folgenden Aufgaben aus:
   - Geben Sie in das Feld **CSS** den Pfad und den Namen der Datei ein, die das angepasste Style-Sheet enthält.
   - Klicken Sie auf **Durchsuchen**, um zur Datei zu navigieren, die das Style-Sheet enthält, und wählen Sie diese aus.
2. Klicken Sie auf **Hochladen**.

Die Konsoldaten lokalisieren

Wenn Sie Ressourcenbündel oder andere Localedateien von IBM empfangen, können Sie diese mit der Seite **Locale hochladen** hochladen. Ressourcenbündel umfassen die folgenden Informationen:

- **Konsolbezeichnung**. Enthalten die Zeichenfolgen, die den gesamten Text der Schnittstelle darstellen
- **Ereignisbeschreibungen**. Enthalten die Zeichenfolgen zur Anzeige von Ereignisdetail (z. B. “Es wurde versucht, eine doppelte Verbindung zu erstellen”)
- **Ereignisnamen**. Enthalten die Zeichenfolgen, die für Ereignisnamen stehen (z. B. “Verbindung besteht bereits”)

- **EDI-Ereignisbeschreibungen**. Enthalten die Zeichenfolgen zur Anzeige von EDI-Ereignisdetail (z. B. "Fehler bei der FA-Abstimmung. Für die Konvertierungen in der EDI-Bestätigung wurden keine Aktivitäts-IDs gefunden.")
- **EDI-Ereignisnamen**. Enthalten die Zeichenfolgen, die für EDI-Ereignisnamen stehen (z. B. "Fehler bei der FA-Abstimmung")
- **Erweiterter Ereignistext**. Enthält die Zeichenfolgen, die zusätzliche Informationen zu Ereignissen bereitstellen (z. B. den Grund des Ereignisses und Informationen zur Fehlerbehebung)

Gehen Sie wie folgt vor, um ein Ressourcenbündel oder eine andere Localedatei hochzuladen:

1. Führen Sie für jedes Ressourcenbündel bzw. jede Datei eine der folgenden Aufgaben aus:
   - Geben Sie den Pfad und den Namen der Datei ein.
   - Klicken Sie auf **Durchsuchen**, um zur Datei zu navigieren, und wählen Sie die Datei aus.
2. Wenn Sie mit dem Hochladen der Dateien fertig sind, klicken Sie auf **Hochladen**.

Kennwortrichtlinie konfigurieren

Sie können eine Kennwortrichtlinie für die Hub-Community konfigurieren, wenn Sie andere Werte als die (vom System) festgelegten Standardwerte verwenden wollen. Die Kennwortrichtlinie gilt für alle Benutzer, die sich an Community Console anmelden.

Sie können die folgenden Elemente der Kennwortrichtlinie ändern:

- **Mindestlänge**. Stellt die Mindestanzahl Zeichen dar, die der Teilnehmer für das Kennwort verwenden muss. Die Standardwert ist 8 Zeichen.
- **Ablaufzeit**. Stellt die Anzahl Tage dar, bevor das Kennwort abläuft. Der Standardwert ist 30 Tage.
- **Einmaligkeit**. Gibt die Anzahl Kennwörter an, die sich in einer Protokolldatei befinden sollen. Ein Teilnehmer kann kein altes Kennwort verwenden, wenn es in der Protokolldatei vorhanden ist. Der Standardwert ist 10 Kennwörter.
- **Sonderzeichen**. Gibt an, wenn ausgewählt, dass Kennwörter mindestens drei der folgenden Typen von Sonderzeichen enthalten müssen:
  - Großbuchstaben
  - Kleinbuchstaben
  - Numerische Zeichen
  - Sonderzeichen

  Diese Einstellung ermöglicht genauere Sicherheitsanforderungen, wenn Kennwörter aus englischen Zeichen (ASCII) zusammengestellt werden. Die Standardeinstellung ist **Aus**. Es wird empfohlen, dass Sonderzeichen ausgeschaltet bleiben, wenn Kennwörter aus einem internationalen Zeichensatz zusammengestellt werden. Nichtenglische Zeichensätze enthalten unter Umständen nicht die erforderlichen drei oder vier Zeichentypen.

  Zu den vom System unterstützten Sonderzeichen gehören: '#', '@', '$', '&', '+'.
- **Prüfung auf Namensvariationen**. Verhindert, wenn ausgewählt, die Verwendung von Kennwörtern, die sich aus einer leicht zu erratenden Kombination des Anmeldenamens oder des vollständigen Namens vom Benutzer zusammensetzen. Dieses Feld ist standardmäßig ausgewählt.

Gehen Sie wie folgt vor, um die Standardwerte zu ändern:

1. Klicken Sie auf **Hubadmin > Konsolkonfiguration > Kennwortrichtlinie**. Die Seite **Kennwortrichtlinie** wird angezeigt.
2. Klicken Sie auf das Symbol **Bearbeiten**.
3. Ändern Sie die Standardwerte in die Werte, die Sie in Ihrer Kennwortrichtlinie verwenden wollen.
4. Klicken Sie auf **Speichern**.

Berechtigungen konfigurieren

Berechtigungen stellen Zugriffsrechte dar, über die ein Benutzer verfügen muss, um auf die verschiedenen Konsolmodule zuzugreifen.

Benutzern Berechtigungen erteilen

Bevor Sie Berechtigungen konfigurieren, ist es hilfreich zu verstehen, wie einzelnen Benutzern Berechtigungen erteilt werden. Alle drei Entitätstypen in der Hub-Community, in Community Operator, Community Manager und in den Teilnehmern verfügen über einen Administrator. Wenn Sie Community Manager oder einen Teilnehmer erstellen, erstellen Sie in Wirklichkeit den Administrator für diese Entität. (Im Fall von Community Operator wird der Hubadmin automatisch erstellt, wie auch ein weiterer Administrator für den Hub.)

Wenn Sie den Teilnehmer erstellen (wie in „Teilnehmerprofile erstellen" auf Seite 161 definiert), stellen Sie für den Teilnehmer Anmeldeinformationen bereit, wie z. B. den Anmeldenamen und das Kennwort. Nachdem der Teilnehmer sich angemeldet hat, erstellt der Teilnehmer zusätzliche Benutzer innerhalb der Organisation. Der Teilnehmer erstellt auch Gruppen und ordnet diesen Gruppen Benutzer zu. Eine Organisation will z. B. unter Umständen über eine Gruppe für Personen verfügen, die das Dokumentvolumen überwachen. Der Teilnehmer würde eine Gruppe **Volumen** erstellen und ihr Benutzer hinzufügen.

Anmerkung: Als Hubadmin können Sie ebenfalls die Benutzer und Gruppen für einen Teilnehmer definieren.

Der Administrator für den Teilnehmer würde dann dieser Gruppe von Benutzern Berechtigungen zuordnen. Der Administrator könnte z. B. beschließen, dass für die Gruppe **Volumen** nur die Dokumentvolumen- und die Dokumentanalyseberichte angezeigt werden sollen. Der Administrator würde auf der Seite **Gruppendetails** das Modul für Dokumentberichte aktivieren, aber alle anderen Module für die Gruppe **Volumen** inaktivieren.

Die Einstellung, die Sie als Hubadmin auf der Seite **Berechtigungen** vornehmen, bestimmt, ob ein Modul auf der Seite **Gruppendetails** aufgelistet wird.

Einige Module sind auf bestimmte Mitglieder der Hub-Community beschränkt (z. B. den Hubadmin). Wenn Sie daher selbst eines dieser Module für die Verwendung durch einen Teilnehmer aktivieren, wird das Modul nicht auf der Seite **Gruppendetails** für den Teilnehmer angezeigt.

Berechtigungen aktivieren oder inaktivieren

Sie können über die Seite **Berechtigungsliste** festlegen, welche Berechtigungen für die Zuordnung zu Gruppen von Benutzern verfügbar sind, indem Sie die Berechtigungen aktivieren oder inaktivieren. Sie können allerdings keine neuen Berechtigungen definieren.

Gehen Sie wie folgt vor, um die Standardberechtigungen zu ändern:

1. Klicken Sie auf **Hubadmin > Konsolkonfiguration > Berechtigungen**. Die Anzeige **Berechtigungsliste** wird angezeigt.
2. Wenn Sie die Standardwerte ändern wollen, führen Sie die folgenden Schritte aus:
   a. Klicken Sie auf die aktuelle Einstellung (**Aktiviert** oder **Inaktiviert**), um die Einstellung zu ändern.
   b. Wenn Sie aufgefordert werden, die Änderung zu bestätigen, klicken Sie auf **OK**.

Kapitel 5. Ziele definieren

Dieses Kapitel beschreibt, wie Sie Ziele auf WebSphere Partner Gateway installieren: Es behandelt die folgenden Themen:

- „Übersicht"
- „Benutzerdefinierte Handler hochladen" auf Seite 40
- „Globale Transportwerte konfigurieren" auf Seite 41
- „HTTP/S-Ziel konfigurieren" auf Seite 41
- „FTP-Ziel konfigurieren" auf Seite 42
- „SMTP-Ziel konfigurieren" auf Seite 44
- „JMS-Ziel konfigurieren" auf Seite 45
- „Dateisystemziel konfigurieren" auf Seite 47
- „FTP-Scripting-Ziel konfigurieren" auf Seite 48
- „Ziel für benutzerdefinierten Transport konfigurieren" auf Seite 52
- „Konfigurationspunkte ändern" auf Seite 52

Übersicht

Wie in „Übersicht über die Dokumentverarbeitung" auf Seite 8 beschrieben, ist der Empfänger für das Akzeptieren eingehender Dokumente von einem bestimmten Transport verantwortlich. Ein Ziel ist eine Instanz des Empfängers, die für eine besondere Implementierung konfiguriert ist.

Dokumente, die auf einem Ziel auf dem Hub empfangen werden, können von Community-Teilnehmern (zur letztendlichen Zustellung an Community Manager) oder von einer Community Manager-Back-End-Anwendung (zur letztendlichen Zustellung an Teilnehmer) kommen.

Abb. 16 auf Seite 40 zeigt einen WebSphere Partner Gateway-Server mit vier konfigurierten Zielen. Zwei der Ziele (HTTP/S und FTP/S) sind für Dokumente, die von Teilnehmern gesendet werden. Diese zwei Ziele stellen eine HTTP-URI und ein FTP-Verzeichnis dar. Sie stellen Ihren Teilnehmern Informationen zu diesen Zielen zur Verfügung, um anzugeben, wohin sie Ihnen Dokumente senden sollen. Die anderen zwei Ziele (JMS und Dateiverzeichnis) sind für Dokumente, die von der Community Manager-Back-End-Anwendung stammen. Diese Ziele stellen eine Warteschlange und ein Verzeichnis dar.

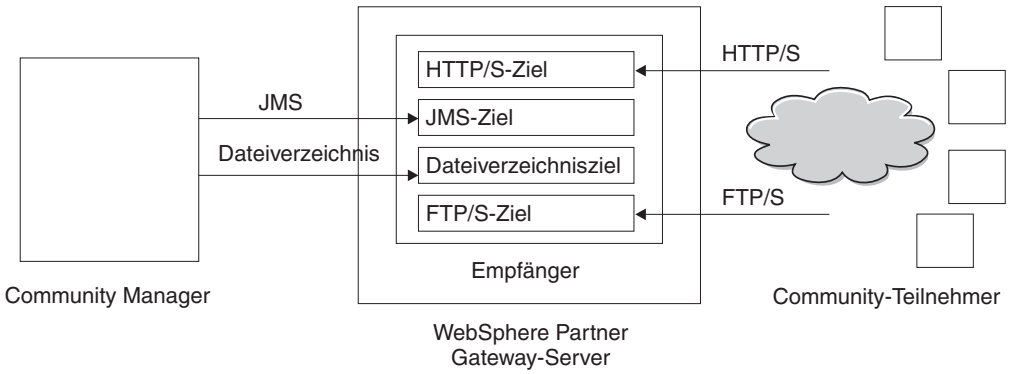

Abbildung 16. Transporte und zugeordnete Ziele

Sie konfigurieren mindestens ein Ziel für jeden Transporttyp, über den Dokumente an den Hub gesendet werden. Sie haben z. B. ein HTTP-Ziel, um beliebige Dokumente zu empfangen, die über den HTTP- oder HTTPS-Transport gesendet werden. Wenn Ihre Community-Teilnehmer Dokumente über FTP senden, konfigurieren Sie ein FTP-Ziel.

Die Empfängerkomponente ermitteln, wann eine Nachricht auf einem der Ziele eingeht. Einige Ziele ermitteln Nachrichten, indem Sie deren Transporte in regelmäßigen Intervallen oder zu geplanten Zeitpunkten abfragen, um festzustellen, ob neue Nachrichten eingegangen sind. Zu den abrufbasierten WebSphere Partner Gateway-Zielen gehören: JMS, FTP, SMTP, File und FTP-Scripting. Das HTTP/S-Ziel basiert auf Callbacks, das bedeutet, dass es eine Benachrichtigung vom Transport empfängt, wenn Nachrichten eingehen. Benutzerdefinierte Transporte können entweder abrufbasiert oder Callback-basiert sein.

Benutzerdefinierte Handler hochladen

Sie können Konfigurationspunkte für Ziele ändern, indem Sie einen Handler für das Ziel angeben. Der Handler kann von WebSphere Partner Gateway bereitgestellt werden oder es kann sich um einen benutzerdefinierten Handler handeln. Dieser Abschnitt beschreibt, wie Sie einen benutzerdefinierten Handler hochladen. Verwenden Sie diesen Abschnitt nur für benutzerdefinierte Handler. Die Handler, die von WebSphere Partner Gateway bereitgestellt werden, sind sofort einsatzbereit.

Führen Sie die folgenden Schritte aus, um einen Handler hochzuladen:

1. Klicken Sie im Hauptmenü auf **Hubadmin > Hubkonfiguration > Handler**.
2. Wählen Sie **Ziel** aus.

   Die Liste der Handler, die derzeit für Ziele definiert sind, wird angezeigt. Beachten Sie, dass die von WebSphere Partner Gateway bereitgestellten Handler die Provider-ID **Produkt** haben.
3. Klicken Sie auf der Seite **Handler-Liste** auf **Importieren**.
4. Geben Sie auf der Seite **Handler importieren** den Pfad zur XML-Datei an, die den Handler beschreibt, oder verwenden Sie **Durchsuchen**, um nach dieser XML-Datei zu suchen.

Nachdem ein Handler hochgeladen ist, können Sie mit ihm die Konfigurationspunkte von Zielen anpassen.

Globale Transportwerte konfigurieren

Sie setzen globale Transportattribute, die für alle HTTP/S- und FTP-Scripting-Ziele gelten. Wenn Sie keine HTTP/S- oder FTP-Scripting-Ziele definieren, können Sie diesen Abschnitt überspringen.

1. Klicken Sie auf **Hubadmin > Hubkonfiguration > Ziele**, um die Zielliste anzuzeigen.
2. Wählen Sie **Globale Transportattribute** in der Zielliste aus.
3. Wenn die Standardwerte für Ihre Konfiguration geeignet sind, klicken Sie auf **Abbrechen**. Andernfalls fahren Sie mit den übrigen Schritten in diesem Abschnitt fort.
4. Klicken Sie auf das Symbol **Bearbeiten** neben **Globale Attribute, nach Kategorie aufgelistet**.
5. Prüfen Sie und, falls notwendig, ändern Sie die Werte von **FTP-Scripting-Transport** und **FTP-Scripting - Ziele und Gateways**.

   Der FTP-Scripting-Transport verwendet einen Sperrmechanismus, der verhindert, dass mehr als eine FTP-Scripting-Instanz gleichzeitig auf dasselbe Ziel zugreift. Wenn ein FTP-Scripting-Transport bereit ist, Dokumente zu senden, fordert er diese Sperre an. Standardwerte werden für Folgendes bereitgestellt: wie lange eine Zielinstanz wartet, um die Sperre zu erhalten, und wie oft eine Zielinstanz versucht, die Sperre abzurufen, falls diese verwendet wird. Sie können diese Standardwerte verwenden bzw. diese ändern. Um mindestens einen Wert zu ändern, geben Sie den neuen Wert ein. Sie können Folgendes ändern:

   - Werte für **FTP-Scripting-Transport**
     - **Wiederholungszähler für Sperren**. Gibt an, wie oft das Ziel versucht, eine Sperre zu erhalten, wenn die Sperre gerade verwendet wird. Der Standardwert ist 3.
     - **Wiederholungsintervall für Sperren (Sekunden)**. Gibt an, wie viel Zeit zwischen den Versuchen, eine Sperre zu erhalten, verstreichen wird. Der Standardwert ist 260 Sekunden.
   - Werte für **FTP-Scripting - Ziele und Gateways**
     - **Maximale Sperrenzeit (Sekunden)**. Gibt an, wie lange das Ziel die Sperre beibehalten kann. Der Standardwert ist 240 Sekunden.
     - **Höchstalter der Warteschlange (Sekunden)**. Gibt an, wie lange das Ziel in einer Warteschlange warten wird, um die Sperre zu erhalten. Der Standardwert ist 740 Sekunden.
6. Prüfen Sie und, falls notwendig, ändern Sie die Werte für **HTTP/S-Transport**. Sie können Folgendes ändern:
   - **Zeitlimit für max. synchrone Verbindungen (Sekunden)**. Um die Anzahl Sekunden anzugeben, die eine synchrone Verbindung geöffnet bleiben kann. Der Standardwert ist 300 Sekunden.
   - **Max. gleichzeitige synchrone Verbindungen**. Um anzugeben, wie viele synchrone Verbindungen das System zulässt. Der Standardwert ist 100 Verbindungen.
7. Klicken Sie auf **Speichern**.

HTTP/S-Ziel konfigurieren

Die Empfängerkomponente verfügt über ein vordefiniertes Servlet **bcgreceiver**, das zum Empfangen von HTTP/S-POST-Nachrichten verwendet wird. Sie erstellen mindestens ein HTTP-Ziel, um auf die vom Servlet empfangenen Nachrichten zuzugreifen.

Die folgenden Schritte beschreiben, was Sie für ein HTTP/S-Ziel angeben müssen.

1. Klicken Sie auf **Hubadmin > Hubkonfiguration > Ziele**, um die Seite **Zielliste** anzuzeigen.
2. Klicken Sie auf der Seite **Zielliste** auf **Ziel erstellen**.

Zieldetails

Führen Sie die folgenden Schritte im Abschnitt **Zieldetails** aus:

1. Geben Sie einen Namen für das Ziel ein. Sie könnten das Ziel z. B. `HttpZiel1` nennen. Dies ist ein erforderliches Feld. Der Name, den Sie hier eingeben, wird in der Liste **Ziele** angezeigt.
2. Geben Sie optional den Status des Ziels an. **Aktiviert** ist die Standardeinstellung. Ein Ziel, das aktiviert ist, ist für das Akzeptieren von Dokumenten bereit. Ein Ziel, das inaktiviert ist, kann keine Dokumente akzeptieren.
3. Geben Sie optional eine Beschreibung für das Ziel ein.
4. Wählen Sie **HTTP/S** in der Liste **Transport** aus.

Zielkonfiguration

Führen Sie die folgenden Schritte im Abschnitt **Zielkonfiguration** aus:

1. Geben Sie optional den Gateway-Typ an. Der Gateway-Typ definiert die Art der Übertragung. Wenn Sie z. B. einen Dokumentenaustausch testen wollen, bevor Sie ihn in die Produktion einreihen, würden Sie **Test** eingeben. Die Standardeinstellung ist **Produktion**.
2. Geben Sie die URI für das HTTP/S-Ziel ein. Der Name muss mit **bcgreceiver** beginnen. Sie könnten z. B. bcgreceiver/submit eingeben. Dokumente, die beim Server über HTTP/S eingehen, würden dann an der Position bcgreceiver/submit empfangen.

   Anmerkung: Die Werte für **Synchronrouting** sind bereits ausgefüllt und Sie können diese über diese Seite nicht bearbeiten. Verwenden Sie die Seite **Globale Transportattribute**, um diese Werte zu ändern, wie in „Globale Transportwerte konfigurieren” auf Seite 41 beschrieben.

Handler

Wenn Sie Dateien mit mehreren EDI-Austauschvorgängen bzw. XML- oder ROD-Dokumenten empfangen, die aufgeteilt werden müssen, konfigurieren Sie den entsprechenden Verteilerhandler am Konfigurationspunkt **Vorverarbeitung**.

Wenn Sie bestimmte Geschäftsdokumenttypen (RosettaNet, cXML, SOAP und AS2) über einen synchronen Austausch senden oder empfangen, geben Sie einen Handler für das zugeordnete Protokoll am Konfigurationspunkt **Synchronprüfung** an. Darüber hinaus können Sie die Nachverarbeitungs-Konfigurationspunkte für das Ziel ändern.

In „Konfigurationspunkte ändern” auf Seite 52 erfahren Sie, wie Sie einen Konfigurationspunkt ändern. Ansonsten klicken Sie auf **Speichern**.

FTP-Ziel konfigurieren

Ein FTP-Ziel fragt Ihren FTP-Server in festgelegten Intervallen nach neuen Dokumenten ab.

Die folgenden Schritte beschreiben, was Sie für ein FTP-Ziel angeben müssen.

1. Klicken Sie auf **Hubadmin > Hubkonfiguration > Ziele**, um die Seite **Zielliste** anzuzeigen.
2. Klicken Sie auf der Seite **Zielliste** auf **Ziel erstellen**.

Zieldetails

Führen Sie die folgenden Schritte im Abschnitt **Zieldetails** aus:

1. Geben Sie einen Namen für das Ziel ein. Sie könnten das Ziel z. B. `FTPZiel1` nennen. Dies ist ein erforderliches Feld. Der Name, den Sie hier eingeben, wird in der Liste **Ziele** angezeigt.
2. Geben Sie optional den Status des Ziels an. **Aktiviert** ist die Standardeinstellung. Ein Ziel, das aktiviert ist, ist für das Akzeptieren von Dokumenten bereit. Ein Ziel, das inaktiviert ist, kann keine Dokumente akzeptieren.
3. Geben Sie optional eine Beschreibung für das Ziel ein.
4. Wählen Sie **FTP-Verzeichnis** in der Liste **Transport** aus.

Zielkonfiguration

Führen Sie die folgenden Schritte im Abschnitt **Zielkonfiguration** aus:

1. Geben Sie in das Feld **FTP-Stammverzeichnis** das Stammverzeichnis FTP-Servers ein. Document Manager fragt automatisch die Unterverzeichnisse der Teilnehmer innerhalb des FTP-Stammverzeichnisses nach Dokumentweiterleitungen ab. Dieses Feld ist erforderlich. Informationen zum Konfigurieren des Verzeichnisses für einen FTP-Server finden Sie in „Den FTP-Server für das Empfangen von Dokumenten konfigurieren" auf Seite 21.

   Anmerkung: Geben Sie als Verzeichnispfad nur das FTP-Stammverzeichnis ein. Schließen Sie die Unterverzeichnisse der Teilnehmer nicht mit ein.
2. Geben Sie optional einen Wert für **Nichtänderungsintervall für Datei** ein, um die Anzahl Sekunden anzugeben, die die Dateigröße unverändert bleiben muss, bevor Document Manager das Dokument zur Verarbeitung abruft. Dieser Nichtänderungszeitraum stellt sicher, dass ein Dokument vollständig übertragen wurde (und sich nicht mitten in der Übertragung befindet), wenn es von Document Manager abgerufen wird. Der Standardwert ist 3 Sekunden.
3. Geben Sie optional einen Wert für **Threadanzahl** ein, um die Anzahl Dokumente anzugeben, die Document Manager gleichzeitig verarbeiten kann. Der Standardwert 1 wird hier empfohlen.
4. Geben Sie optional einen Wert für **Ausschlussdateierw.** ein, um die Dokumententypen anzugeben, die Document Manager ignorieren sollte (von der Verarbeitung ausschließen), falls er die Dokumente im FTP-Verzeichnis findet. Wenn Sie z. B. wollen, dass Document Manager Spreadsheetdateien ignoriert, dann geben Sie in diesem Fall die Erweiterung ein, die ihnen zugeordnet ist. Nachdem Sie die Erweiterung eingegeben haben, klicken Sie auf **Hinzufügen**. Die Erweiterung wird dann der Liste mit Dateierweiterungen hinzugefügt, die ignoriert werden sollen. Die Standardeinstellung ist, dass keine Dateitypen ausgeschlossen werden.

   Anmerkung: Verwenden Sie vor der Dateinamenerweiterung keinen Punkt (Beispiel: .exe oder .txt). Verwenden Sie nur die Zeichen, die die Dateierweiterung bezeichnen.

Handler

Wenn Sie Dateien mit mehreren EDI-Austauschvorgängen bzw. XML- oder ROD-Dokumenten empfangen, die aufgeteilt werden müssen, konfigurieren Sie den entsprechenden Verteilerhandler am Konfigurationspunkt **Vorverarbeitung**.

In „Konfigurationspunkte ändern" auf Seite 52 erfahren Sie, wie Sie den Konfigurationspunkt **Vorverarbeitung** ändern. Ansonsten klicken Sie auf **Speichern**.

SMTP-Ziel konfigurieren

Ein SMTP-Ziel fragt Ihren POP3-E-Mail-Server, entsprechend dem von Ihnen angegebenen Zeitplan, nach neuen Dokumenten ab.

Die folgenden Schritte beschreiben, was Sie für ein SMTP-Ziel (POP3) angeben müssen.

1. Klicken Sie auf **Hubadmin > Hubkonfiguration > Ziele**, um die Seite **Zielliste** anzuzeigen.
2. Klicken Sie auf der Seite **Zielliste** auf **Ziel erstellen**.

Zieldetails

Führen Sie die folgenden Schritte im Abschnitt **Zieldetails** aus:

1. Geben Sie einen Namen für das Ziel ein. Sie könnten das Ziel z. B. `POP3Ziel1` nennen. Dies ist ein erforderliches Feld. Der Name, den Sie hier eingeben, wird in der Liste **Ziele** angezeigt.
2. Geben Sie optional den Status des Ziels an. **Aktiviert** ist die Standardeinstellung. Ein Ziel, das aktiviert ist, ist für das Akzeptieren von Dokumenten bereit. Ein Ziel, das inaktiviert ist, kann keine Dokumente akzeptieren.
3. Geben Sie optional eine Beschreibung für das Ziel ein.
4. Wählen Sie **POP3** in der Liste **Transport** aus.

Zielkonfiguration

Führen Sie die folgenden Schritte im Abschnitt **Zielkonfiguration** der Seite aus:

1. Geben Sie optional den Gateway-Typ an. Der Gateway-Typ definiert die Art der Übertragung. Wenn Sie z. B. einen Dokumentenaustausch testen wollen, bevor Sie ihn in die Produktion einreihen, würden Sie **Test** eingeben. Die Standardeinstellung ist **Produktion**.
2. Geben Sie die Position des POP3-Servers ein, wohin E-Mails zugestellt werden. Sie könnten z. B. eine IP-Adresse eingeben.
3. Geben Sie optional eine Portnummer ein. Wenn Sie nichts eingeben, wird der Wert 110 verwendet.
4. Geben Sie die Benutzer-ID und das Kennwort ein, die erforderlich sind, um auf den E-Mail-Server zuzugreifen, falls eine Benutzer-ID und ein Kennwort benötigt werden.
5. Geben Sie optional einen Wert für **Threadanzahl** ein, um die Anzahl Dokumente anzugeben, die Document Manager gleichzeitig verarbeiten kann. Der Standardwert 1 wird hier empfohlen.

Zeitplan

Führen Sie die folgenden Schritte im Abschnitt **Zeitplan** der Seite aus:

1. Wählen Sie **Intervallbasierte Zeitplanung** oder **Kalenderbasierte Zeitplanung** aus.
2. Führen Sie eine der folgenden Schrittegruppen aus:
   - Wenn Sie **Intervallbasierte Zeitplanung** auswählen, dann wählen Sie die Anzahl Sekunden aus, die verstreichen sollen, bevor der POP3-Server erneut abgefragt wird, oder akzeptieren Sie den Standardwert. Wenn Sie den Standardwert auswählen, wird der POP3-Server alle 5 Sekunden abgefragt.
   - Wenn Sie **Kalenderbasierte Zeitplanung** auswählen, dann wählen Sie den Zeitplanungstyp (**Täglicher Zeitplan**, **Wöchentlicher Zeitplan** oder **Angepasster Zeitplan**) aus.
     – Wenn Sie **Täglicher Zeitplan** auswählen, dann wählen Sie die Uhrzeit (Stunde und Minute) aus, wann der POP3-Server abgefragt werden soll.
     – Wenn Sie **Wöchentlicher Zeitplan** auswählen, dann wählen Sie mindestens einen Tag in der Woche zusätzlich zur Uhrzeit aus.
     – Wenn Sie **Angepasster Zeitplan** auswählen, dann wählen Sie die Uhrzeit und schließlich noch **Bereich** oder **Ausgewählte Tage** für die Woche und den Monat aus. Mit **Bereich** geben Sie das Startdatum und das Enddatum an. (Sie können z. B. auf **Mo** und **Fr** klicken, wenn Sie wollen, dass der Server nur an Wochentagen zu einer bestimmten Uhrzeit abgefragt wird.) Mit der Option **Ausgewählte Tage** wählen Sie bestimmte Tage in der Woche und im Monat aus.

JMS-Ziel konfigurieren

Ein JMS-Ziel fragt eine JMS-Warteschlange, entsprechend dem von Ihnen angegebenen Zeitplan, nach neuen Dokumenten ab.

Die folgenden Schritte beschreiben, was Sie für ein JMS-Ziel angeben müssen.

1. Klicken Sie auf **Hubadmin > Hubkonfiguration > Ziele**, um die Seite **Zielliste** anzuzeigen.
2. Klicken Sie auf der Seite **Zielliste** auf **Ziel erstellen**.

Zieldetails

Führen Sie die folgenden Schritte im Abschnitt **Zieldetails** aus:

1. Geben Sie einen Namen für das Ziel ein. Sie könnten das Ziel z. B. `JMSZiel1` nennen. Dies ist ein erforderliches Feld. Der Name, den Sie hier eingeben, wird in der Liste **Ziele** angezeigt.
2. Geben Sie optional den Status des Ziels an. **Aktiviert** ist die Standardeinstellung. Ein Ziel, das aktiviert ist, ist für das Akzeptieren von Dokumenten bereit. Ein Ziel, das inaktiviert ist, kann keine Dokumente akzeptieren.
3. Geben Sie optional eine Beschreibung für das Ziel ein.
4. Wählen Sie **JMS** in der Liste **Transport** aus.

Zielkonfiguration

Führen Sie die folgenden Schritte im Abschnitt **Zielkonfiguration** der Seite aus:

1. Geben Sie optional den Gateway-Typ an. Der Gateway-Typ definiert die Art der Übertragung. Wenn Sie z. B. einen Dokumentenaustausch testen wollen, bevor Sie ihn in die Produktion einreihen, würden Sie **Test** eingeben. Die Standardeinstellung ist **Produktion**.
2. Geben Sie die URL-Adresse des JMS-Providers ein. Diese sollte mit dem Wert übereinstimmen, den Sie eingegeben haben (der Dateisystempfad zur `.bin-`

dungs-Datei), als Sie WebSphere Partner Gateway für JMS konfiguriert haben (Schritt 5 auf Seite 25). Sie können den Unterordner für den JMS-Kontext auch als Teil des JMS-Provider-URLs angeben.

Sie würden z. B. ohne den JMS-Kontext `c:/temp/JMS` eingeben. Mit dem JMS-Kontext würden Sie `c:/temp/JMS/JMS` eingeben.

3. Geben Sie die Benutzer-ID und das Kennwort ein, die erforderlich sind, um auf die JMS-Warteschlange zuzugreifen, falls eine Benutzer-ID und ein Kennwort benötigt werden.
4. Geben Sie einen Wert für den Namen der JMS-Warteschlange ein. Dies ist ein erforderliches Feld. Dieser Name sollte mit dem Namen übereinstimmen, den Sie mit dem Befehl `define q` angegeben haben, als Sie die `.bindungs`-Datei erstellt haben (Schritt 4 auf Seite 27).

   Wenn Sie den Unterordner für den JMS-Kontext in Schritt 2 auf Seite 45 eingegeben haben, geben Sie hier nur den Namen der Warteschlange ein (z. B. `inQ`). Wenn Sie den Unterordner für den JMS-Kontext nicht im JMS-Provider-URL eingegeben haben, geben Sie den Unterordner vor dem Factory-Namen ein (z. B. `JMS/inQ`).
5. Geben Sie einen Wert für den JMS-Factory-Namen ein. Dies ist ein erforderliches Feld. Dieser Name sollte mit dem Namen übereinstimmen, den Sie mit dem Befehl `define qcf` angegeben haben, als Sie die `.bindungs`-Datei erstellt haben (Schritt 4 auf Seite 27).

   Wenn Sie den Unterordner für den JMS-Kontext in Schritt 2 auf Seite 45 eingegeben haben, geben Sie hier nur den Factory-Namen ein (z. B. `Hub`). Wenn Sie den Unterordner für den JMS-Kontext nicht im JMS-Provider-URL eingegeben haben, geben Sie den Unterordner vor dem Factory-Namen ein (z. B. `JMS/Hub`).
6. Geben Sie optional das Provider-URL-Paket ein.
7. Geben Sie den JNDI-Factory-Namen ein. Wenn Sie nichts eingeben, wird der Wert `com.sun.jndi.fscontext.RefFSContextFactory` verwendet. Dies ist ein erforderliches Feld.
8. Geben Sie optional einen Wert für **Zeitlimit** ein, um die Anzahl Sekunden anzugeben, die das Ziel die JMS-Warteschlange auf Dokumente hin überwacht. Dieses Feld ist optional.
9. Geben Sie optional einen Wert für **Threadanzahl** ein, um die Anzahl Dokumente anzugeben, die Document Manager gleichzeitig verarbeitet. Der Standardwert 1 wird hier empfohlen.

Wenn Sie z. B. ein JMS-Ziel konfigurieren wollen, das mit dem JMS-Konfigurationsbeispiel in „Den Hub für das JMS-Transportprotokoll konfigurieren" auf Seite 25 übereinstimmt, würden Sie wie folgt vorgehen:

1. Geben Sie den Wert **JMSTarget** in das Feld **Zielname** ein.
2. Geben Sie den Wert **file:/C:/TEMP/JMS/JMS** in das Feld **JMS-Provider-URL** ein.
3. Geben Sie den Wert **inQ** in das Feld **JMS-Warteschlangenname** ein.
4. Geben Sie den Wert **Hub** in das Feld **JMS-Factory-Name** ein.

Handler

Wenn Sie Dateien mit mehreren EDI-Austauschvorgängen bzw. XML- oder ROD-Dokumenten empfangen, die aufgeteilt werden müssen, konfigurieren Sie den entsprechenden Verteilerhandler am Konfigurationspunkt **Vorverarbeitung**.

In „Konfigurationspunkte ändern" auf Seite 52 erfahren Sie, wie Sie Konfigurationspunkte für dieses Ziel ändern. Ansonsten klicken Sie auf **Speichern**.

Dateisystemziel konfigurieren

Ein Dateisystemziel fragt ein Verzeichnis entsprechend einem festgelegten Intervall nach neuen Dokumenten ab.

Die folgenden Schritte beschreiben, was Sie für ein Dateisystemziel angeben müssen.

1. Klicken Sie auf **Hubadmin > Hubkonfiguration > Ziele**, um die Seite **Zielliste** anzuzeigen.
2. Klicken Sie auf der Seite **Zielliste** auf **Ziel erstellen**.

Zieldetails

Führen Sie die folgenden Schritte im Abschnitt **Zieldetails** aus:

1. Geben Sie einen Namen für das Ziel ein. Sie könnten das Ziel z. B. `DateiZiel1` nennen. Dies ist ein erforderliches Feld. Der Name, den Sie hier eingeben, wird in der Liste **Ziele** angezeigt.
2. Geben Sie optional den Status des Ziels an. **Aktiviert** ist die Standardeinstellung. Ein Ziel, das aktiviert ist, ist für das Akzeptieren von Dokumenten bereit. Ein Ziel, das inaktiviert ist, kann keine Dokumente akzeptieren.
3. Geben Sie optional eine Beschreibung für das Ziel ein.
4. Wählen Sie **Dateiverzeichnis** in der Liste **Transport** aus.

Zielkonfiguration

Führen Sie die folgenden Schritte im Abschnitt **Zielkonfiguration** der Seite aus:

1. Geben Sie optional den Gateway-Typ an. Der Gateway-Typ definiert die Art der Übertragung. Wenn Sie z. B. einen Dokumentenaustausch testen wollen, bevor Sie ihn in die Produktion einreihen, würden Sie **Test** eingeben. Die Standardeinstellung ist **Produktion**.
2. Geben Sie einen Wert für **Dokumentstammverzeichnispfad** ein, um das Verzeichnis anzugeben, in dem die Dokumente empfangen werden.
3. Geben Sie optional einen Wert für **Abfrageintervall** ein, um anzugeben, wie häufig das Verzeichnis nach neuen Dokumenten abgefragt werden soll. Wenn Sie nichts eingeben, wird das Verzeichnis alle 5 Sekunden abgefragt.
4. Geben Sie optional einen Wert für **Nichtänderungsintervall für Datei** ein, um die Anzahl Sekunden anzugeben, die die Dateigröße unverändert bleiben muss, bevor Document Manager das Dokument zur Verarbeitung abruft. Dieser Nichtänderungszeitraum stellt sicher, dass ein Dokument vollständig übertragen wurde (und sich nicht mitten in der Übertragung befindet), wenn es von Document Manager abgerufen wird. Der Standardwert ist 3 Sekunden.
5. Geben Sie optional einen Wert für **Threadanzahl** ein, um die Anzahl Dokumente anzugeben, die Document Manager gleichzeitig verarbeiten kann. Der Standardwert 1 wird hier empfohlen.

Handler

Wenn Sie Dateien mit mehreren EDI-Austauschvorgängen bzw. XML- oder ROD-Dokumenten empfangen, die aufgeteilt werden müssen, konfigurieren Sie den entsprechenden Verteilerhandler am Konfigurationspunkt **Vorverarbeitung**.

In „Konfigurationspunkte ändern” auf Seite 52 erfahren Sie, wie Sie den Konfigurationspunkt **Vorverarbeitung** ändern. Ansonsten klicken Sie auf **Speichern**.

FTP-Scripting-Ziel konfigurieren

Ein FTP-Scripting-Ziel ist ein Abfrageziel, das entsprechend dem von Ihnen festgelegten Zeitplan ausgeführt wird. Das Verhalten eines FTP-Scripting-Ziels wird von einem FTP-Befehlsscript geregelt.

Das FTP-Ziel fragt ein Verzeichnis auf Ihrem FTP-Server ab, im Gegensatz dazu fragt das FTP-Scripting-Ziel Verzeichnisse auf einem anderen Server ab (z. B. ein VAN).

Das FTP-Script erstellen

Die FTP-Server können bestimmte Anforderungen an die Befehle stellen, die sie akzeptieren. Um ein FTP-Scripting-Ziel zu verwenden, erstellen Sie eine Datei mit allen FTP-Befehlen, die der FTP-Server erfordert, zu dem Sie eine Verbindung herstellen. (Sie müssen diese Informationen vom Administrator des FTP-Servers anfordern.)

1. Erstellen Sie ein Script für die Ziele, um die Aktionen anzugeben, die Sie ausführen wollen. Das folgende Script ist ein Beispiel für das Herstellen einer Verbindung zu dem angegebenen FTP-Server (mit dem angegebenen Namen und Kennwort), für das Wechseln zum angegebenen Verzeichnis auf dem FTP-Server und für das Empfangen aller Dateien in diesem Verzeichnis:

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

   Die Platzhalter (z. B. %BCGSERVERIP%) werden ersetzt, wenn das Ziel aktiviert wird durch die Werte, die Sie eingeben, wenn Sie eine bestimmte Instanz eines FTP-Scripting-Ziels erstellen. %BCGOPTION% ist in diesem Beispiel der Name des Verzeichnisses im Befehl `cd`. Die Scriptparameter und ihre zugeordneten Felder des FTP-Scripting-Ziels werden in Tabelle 2 gezeigt:

Tabelle 2. Zuordnung der Scriptparameter zu den Feldeinträgen für das FTP-Scripting-Ziel

Scriptparameter	**Feldeintrag für das FTP-Scripting-Ziel**
%BCGSERVERIP%	Server-IP
%BCGUSERID%	Benutzer-ID
%BCGPASSWORD%	Kennwort
%BCGOPTIONx%	Option*x* unter **Benutzerdefinierte Attribute**

2. Speichern Sie die Datei.

FTP-Scripting-Befehle

Sie können die folgenden Befehle verwenden, wenn Sie das Script erstellen:

- ascii, binary, passive

  Diese Befehle werden nicht an den FTP-Server gesendet. Sie ändern den Modus für die Übertragung (ascii, binary oder passive) zum FTP-Server.
- cd

  Dieser Befehl wechselt zum angegebenen Verzeichnis.
- delete

  Dieser Befehl entfernt eine Datei vom FTP-Server.
- get

Dieser Befehl verfügt über ein einzelnes Argument: das ist der Name der Datei, die vom fernen System abgerufen werden soll. Die angeforderte Datei wird dann auf WebSphere Partner Gateway übertragen. Verwenden Sie diesen Befehl nur, wenn Sie eine einzelne Datei abrufen und der Name bekannt ist. Andernfalls sollte der Befehl `mget` mit Platzhaltern verwendet werden.

- getdel

  Dieser Befehl ist mit dem Befehl `get` identisch, außer dass die Datei vom fernen System entfernt wird, wenn WebSphere Partner Gateway die Datei zur Verarbeitung abruft.

- mget

  Dieser Befehl verfügt über ein einzelnes Argument, das eine Dateigruppe beschreibt, die abgerufen werden soll. Die Beschreibung kann die Standardplatzhalterzeichen ('*' und '?') umfassen. Mindestens eine Datei wird dann vom fernen System abgerufen.

- mgetdel

  Dieser Befehl verfügt über ein einzelnes Argument, das eine Dateigruppe beschreibt, die abgerufen und dann vom FTP-Server gelöscht werden soll. Die Beschreibung kann die Standardplatzhalterzeichen ('*' und '?') umfassen. Mindestens eine Datei wird vom fernen System abgerufen und dann auf dem fernen System gelöscht.

- mkdir

  Dieser Befehl erstellt ein Verzeichnis auf dem FTP-Server.

- open

  Dieser Befehl verwendet drei Parameter: die IP-Adresse des FTP-Servers, den Benutzernamen und ein Kennwort. Diese Parameter stimmen mit den Variablen %BCGSERVERIP%, %BCGUSERID% und %BCGPASSWORD% überein.

  Die erste Zeile Ihres FTP-Scripting-Zielscripts sollte daher wie folgt lauten:

  ```
  open %BCGSERVERIP% %BCGUSERID% %BCGPASSWORD%
  ```

- quit, bye

  Dieser Befehl beendet eine vorhandene Verbindung zu einem FTP-Server.

- quote

  Dieser Befehl gibt an, dass alles nach dem Befehl `QUOTE` an das ferne System als Befehl gesendet werden soll. Dies ermöglicht Ihnen, Befehle an einen fernen FTP-Server zu senden, die möglicherweise nicht im Standard-FTP-Protokoll definiert sind.

- rename

  Dieser Befehl benennt eine Datei auf dem FTP-Server um.

- rmdir

  Dieser Befehl entfernt ein Verzeichnis vom FTP-Server.

- site

  Dieser Befehl kann verwendet werden, um sitespezifische Befehle auf dem fernen System abzusetzen. Das ferne System bestimmt, ob der Inhalt dieses Befehls gültig ist.

Zieldetails

Die folgenden Schritte beschreiben, was Sie für ein FTP-Scripting-Ziel angeben müssen.

1. Klicken Sie auf **Hubadmin > Hubkonfiguration > Ziele**, um die Seite **Zielliste** anzuzeigen.
2. Klicken Sie auf der Seite **Zielliste** auf **Ziel erstellen**.

Führen Sie die folgenden Schritte im Abschnitt **Zieldetails** aus:

1. Geben Sie einen Namen für das Ziel ein. Sie könnten das Ziel z. B. `FTPScriptingZiel1` nennen. Dies ist ein erforderliches Feld. Der Name, den Sie hier eingeben, wird in der Liste **Ziele** angezeigt.
2. Geben Sie optional den Status des Ziels an. **Aktiviert** ist die Standardeinstellung. Ein Ziel, das aktiviert ist, ist für das Akzeptieren von Dokumenten bereit. Ein Ziel, das inaktiviert ist, kann keine Dokumente akzeptieren.
3. Geben Sie optional eine Beschreibung für das Ziel ein.
4. Wählen Sie **FTP-Scripting** in der Liste **Transport** aus.

Zielkonfiguration

Führen Sie die folgenden Schritte im Abschnitt **Zielkonfiguration** der Seite aus:

1. Geben Sie optional den Gateway-Typ an. Der Gateway-Typ definiert die Art der Übertragung. Wenn Sie z. B. einen Dokumentenaustausch testen wollen, bevor Sie ihn in die Produktion einreihen, würden Sie **Test** eingeben. Die Standardeinstellung ist **Produktion**.
2. Geben Sie die Server-IP-Adresse des FTP-Servers ein, zu dem Sie eine Verbindung herstellen. Der Wert, den Sie hier eingeben, wird %BCGSERVERIP% ersetzen, wenn das FTP-Script ausgeführt wird.
3. Geben Sie die Benutzer-ID und das Kennwort ein, mit denen Sie auf den Server zugreifen. Die Werte, die Sie hier eingeben, werden %BCGUSERID% und %BCGPASSWORD% ersetzen, wenn das FTP-Script ausgeführt wird.
4. Geben Sie an, ob das Ziel im SSL-Modus (Secure Sockets Layer) betrieben wird. Falls ja, müssen Sie Zertifikate mit Ihren Teilnehmern austauschen, wie in Kapitel 13, „Sicherheit für Eingangs- und Ausgangsaustauschvorgänge konfigurieren", auf Seite 169 beschrieben.
5. Laden Sie die Scriptdatei hoch, indem Sie die folgenden Schritte befolgen:
   a. Klicken Sie auf **Scriptdatei hochladen**.
   b. Geben Sie den Namen der Datei ein, die das Script für die Verarbeitung von Dokumenten enthält, oder navigieren Sie mit **Durchsuchen** zu der Datei.
   c. Klicken Sie auf **Datei laden**, um die Scriptdatei in das Textfeld **Momentan geladene Scriptdatei** zu laden.
   d. Wenn es sich um die gewünschte Scriptdatei handelt, klicken Sie auf **Speichern**.
   e. Klicken Sie auf **Fenster schließen**.
6. Geben Sie für **Verbindungszeitlimit** die Anzahl Sekunden ein, die ein Socket ohne Datenverkehr geöffnet bleibt.
7. Geben Sie im Feld **Benutzer sperren** an, ob das Ziel eine Sperre anfordern wird, so dass keine anderen Instanzen eines FTP-Scripting-Ziels gleichzeitig auf dasselbe FTP-Serververzeichnis zugreifen können.

Anmerkung: Die Werte für **Attribute des globalen FTP-Scripting** sind bereits ausgefüllt und Sie können diese über diese Seite nicht bearbeiten. Verwenden Sie die Seite **Globale Transportattribute**, um diese Werte zu ändern, wie in „Globale Transportwerte konfigurieren" auf Seite 41 beschrieben.

Benutzerdefinierte Attribute

Wenn Sie zusätzliche Attribute angeben wollen, führen Sie die folgenden Schritte aus. Der Wert, den Sie für die Option eingeben, wird %BCGOPTION*x*% ersetzen, wenn das FTP-Script ausgeführt wird (dabei entspricht *x* der Optionsnummer).

1. Klicken Sie auf **Neu**.
2. Geben Sie einen Wert neben **Option 1** ein.
3. Wenn Sie zusätzliche Attribute anzugeben haben, klicken Sie wieder auf **Neu**, und geben Sie einen Wert ein.
4. Wiederholen Sie Schritt 3 so oft wie nötig, um alle Attribute zu definieren.

Angenommen, Ihr FTP-Script sieht z. B. wie folgt aus:

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

%BCGOPTION% wäre in diesem Fall ein Verzeichnisname.

Zeitplan

Geben Sie an, ob Sie intervallbasierte Zeitplanung oder kalenderbasierte Zeitplanung verwenden wollen.

- Wenn Sie **Intervallbasierte Zeitplanung** auswählen, dann wählen Sie die Anzahl Sekunden aus, die verstreichen sollen, bevor der FTP-Server abgefragt wird, oder akzeptieren Sie den Standardwert.
- Wenn Sie **Kalenderbasierte Zeitplanung** auswählen, dann wählen Sie den Zeitplanungstyp (**Täglicher Zeitplan**, **Wöchentlicher Zeitplan** oder **Angepasster Zeitplan**) aus.
  - Wenn Sie **Täglicher Zeitplan** auswählen, dann geben Sie die Uhrzeit ein, wann der FTP-Server abgefragt werden soll.
  - Wenn Sie **Wöchentlicher Zeitplan** auswählen, dann wählen Sie mindestens einen Tag in der Woche zusätzlich zur Uhrzeit aus.
  - Wenn Sie **Angepasster Zeitplan** auswählen, dann wählen Sie die Uhrzeit und schließlich noch **Bereich** oder **Ausgewählte Tage** für die Woche und den Monat aus. Mit **Bereich** geben Sie das Startdatum und das Enddatum an. (Sie können z. B. auf **Mo** und **Fr** klicken, wenn Sie wollen, dass der Server nur an Wochentagen zu einer bestimmten Uhrzeit abgefragt wird.) Mit der Option **Ausgewählte Tage** wählen Sie bestimmte Tage in der Woche und im Monat aus.

Handler

Wenn Sie Dateien mit mehreren EDI-Austauschvorgängen bzw. XML- oder ROD-Dokumenten empfangen, die aufgeteilt werden müssen, konfigurieren Sie den entsprechenden Verteilerhandler am Konfigurationspunkt **Vorverarbeitung**.

In „Konfigurationspunkte ändern” auf Seite 52 erfahren Sie, wie Sie den Konfigurationspunkt **Vorverarbeitung** ändern. Ansonsten klicken Sie auf **Speichern**.

Ziel für benutzerdefinierten Transport konfigurieren

Wenn Sie ein Ziel für einen benutzerdefinierten Transport definieren, werden die Feldnamen und andere Informationen innerhalb der Datei definiert, die den Transport beschreibt.

Führen Sie die folgenden Schritte aus:

1. Klicken Sie auf **Hubadmin > Hubkonfiguration > Ziele**.
2. Klicken Sie auf **Transporttypen verwalten**.
3. Geben Sie den Namen einer XML-Datei ein, die den Transport definiert oder verwenden Sie **Durchsuchen**, um zur Datei zu navigieren.
4. Klicken Sie auf **Hochladen**.

   Anmerkung: Sie können aus der **Zielliste** auch einen benutzerdefinierten Transporttyp löschen. Sie können keinen Transport löschen, der von WebSphere Partner Gateway bereitgestellt wurde. Ebenfalls können Sie keinen benutzerdefinierten Transport löschen, nachdem er zum Erstellen eines Ziels verwendet wurde.
5. Klicken Sie auf **Ziel erstellen**.
6. Geben Sie einen Namen für das Ziel ein. Dies ist ein erforderliches Feld. Der Name, den Sie hier eingeben, wird in der Liste **Ziele** angezeigt.
7. Geben Sie optional den Status des Ziels an. **Aktiviert** ist die Standardeinstellung. Ein Ziel, das aktiviert ist, ist für das Akzeptieren von Dokumenten bereit. Ein Ziel, das inaktiviert ist, kann keine Dokumente akzeptieren.
8. Geben Sie optional eine Beschreibung für das Ziel ein.
9. Wählen Sie den benutzerdefinierten Transport in der Liste aus.
10. Füllen Sie die Felder aus (die für jeden benutzerdefinierten Transport eindeutig sind).
11. Wenn Sie Konfigurationspunkte für dieses Ziel ändern wollen, lesen Sie „Konfigurationspunkte ändern". Ansonsten klicken Sie auf **Speichern**.

Konfigurationspunkte ändern

Die Anzahl verfügbarer Konfigurationspunkte und die Anzahl zugeordneter Handler für diese Konfigurationspunkte variiert je nach konfiguriertem Zieltyp. Der Konfigurationspunkt **Synchronprüfung** ist z. B. nur für HTTP/S- und JMS-Ziele verfügbar.

Für bestimmte Geschäftsprotokolle (RosettaNet, cXML, SOAP, und AS2), die in synchrone Austauschvorgänge einbezogen werden, müssen Sie einen Handler für das Protokoll im Konfigurationspunkt **Synchronprüfung** angeben. Sie können auch die Art und Weise ändern, wie Ziele Dokumente verarbeiten, indem Sie einen hochgeladenen benutzerdefinierten Handler oder einen vom System bereitgestellten Prozess auf die Vorverarbeitungs- und Nachverarbeitungspunkte des Ziels anwenden.

Um einen benutzerdefinierten Handler auf diese Konfigurationspunkte anzuwenden, müssen Sie zuerst den Handler hochladen, wie in „Benutzerdefinierte Handler hochladen" auf Seite 40 beschrieben. Sie können auch einen vom System bereitgestellten Handler verwenden, der bereits verfügbar ist und nicht mehr hochgeladen werden muss.

Vorverarbeitung

Der Vorverarbeitungs-Konfigurationshandler ist auf allen Zieltypen verfügbar, er ist jedoch nicht auf SMTP-Ziele anwendbar.

Vorverarbeitungsattribute

Tabelle 3 beschreibt die Attribute, die Sie für einen Vorverarbeitungshandler festlegen können und listet die Verteilerhandler auf, auf die die Attribute angewendet werden.

Die ROD-Attribute, die in dieser Tabelle als Beispiele verwendet werden, entsprechen denen, die in „Beispiel: ROD zu EDI" auf Seite 237 verwendet wurden. Im Beispiel sind die ROD-Attribute in der Zuordnung **S_DT_ROD_TO_EDI.eif** enthalten, welche die folgende Dokumentenflussdefinition einschließt:

- Paket: None (Version N/A)
- Protokoll: ROD_TO_EDI_DICT (Version ALL)
- Dokumentenfluss: DTROD-TO-EDI_ROD (Version ALL)

Das ROD-Metawörterbuch und -Metadokument, die diesem Dokumentenfluss zugeordnet sind, lauten ROD_TO_EDI_DICT und DTROD-TO-EDI_ROD.

Tabelle 3. Attribute für Verteilerhandler

Attribut	Beschreibung	Verteiler-handler
Encoding	Die Zeichencodierung des Dokuments. Der Standardwert ist ASCII.	ROD Generic XML EDI
BATCHDOCS	Wenn BCG_BATCHDOCS aktiv ist, fügt der Verteiler den Dokumenten Stapel-IDs hinzu, nachdem die Dokumente aufgeteilt wurden. Wenn die Dokumente in EDI-Transaktionen transformiert werden, die mit einem Umschlag versehen werden sollen, verwendet das Programm zur Umschlagsgenerierung die Stapel-IDs, um sicherzustellen, dass die Transaktionen, wenn möglich, in denselben EDI-Austausch gestellt werden, bevor sie zugestellt werden. Beachten Sie, dass für das Stapelattribut des Programms zur Umschlagsgenerierung der Standardwert **On** (Ein) festgelegt sein muss. Siehe „Stapelbetrieb" auf Seite 109.	ROD Generic XML
From Packaging Name	Das Paket, das dem Dokument zugeordnet ist. Dieser Wert muss mit dem Paket übereinstimmen, das in der Dokumentenflussdefinition angegeben ist. Für ein Dokument im Paket **None** sollte dieser Wert z. B. **None** sein.	ROD Generic
From Packaging Version	Die Version des Pakets, das in **From Packaging Name** angegeben ist. Wenn das Dokument z. B. im Paket **None** gepackt ist, würde dieser Wert **N/A** sein.	ROD Generic
From Protocol Name	Das Protokoll, das dem Dokument zugeordnet ist. Dieser Wert muss mit dem Protokoll übereinstimmen, das in der Dokumentenflussdefinition angegeben ist. Für ein ROD-Dokument könnte dieser Wert z. B. **ROD-TO-EDI_DICT** sein.	ROD Generic
From Protocol Version	Die Version des Pakets, das in **From Protocol Name** angegeben ist. Für das Protokoll ROD-TO-EDI_DICT würde der Wert z. B. **ALL** sein.	ROD Generic

Tabelle 3. Attribute für Verteilerhandler (Forts.)

Attribut	Beschreibung	Verteiler-handler
From Process Code	Der Prozess (Dokumentenfluss), der diesem Dokument zugeordnet ist. Dieser Wert muss mit dem Dokumentenfluss in der Dokumentenflussdefinition übereinstimmen. Für ein ROD-Dokument könnte dieser Wert z. B. **DTROD-TO-EDI_ROD** sein.	ROD Generic
From Process Version	Die Version des Prozesses, der in **From Process Code** angegeben ist. Für DTROD-TO-EDI_ROD würde dieser Wert z. B. **ALL** sein.	ROD Generic
Metadictionary	Das Metawörterbuch stellt Informationen bereit, mit denen WebSphere Partner Gateway die Daten interpretieren kann. Für ein ROD-Dokument könnte dieser Wert z. B. **ROD-TO-EDI_DICT** sein.	ROD Generic
Metadocument	Das Metadokument stellt Informationen bereit, mit denen WebSphere Partner Gateway die Daten interpretieren kann. Für ein ROD-Dokument könnte dieser Wert z. B. **DTROD-TO-EDI_ROD** sein.	ROD Generic
Metasyntax	Die Metasyntax beschreibt das Format des Dokuments, das aufgeteilt wird. Der Standardwert ist **rod**.	ROD Generic

Hinweise:

1. Es wird nur ein ROD-Dokumenttyp pro Zielinstanz unterstützt.
2. Wenn für ein Ziel mehr als ein Verteilerhandler konfiguriert wurde (z. B. wenn die ROD-, XML- und EDI-Verteilerhandler konfiguriert wurden), muss der ROD-Verteilerhandler in der **Konfigurationsliste** als letztes aufgeführt sein.

Den Vorverarbeitungs-Konfigurationspunkt ändern

Führen Sie die folgenden Schritte aus, um den Vorverarbeitungs-Konfigurationspunkt zu ändern:

1. Wählen Sie **Vorverarbeitung** in der Liste **Konfigurationspunkt-Handler** aus.

   Vier Vorverarbeitungshandler werden (standardmäßig) bereitgestellt und in der **Verfügbarkeitsliste** gezeigt.

   - 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

   Anmerkung: Die Vorverarbeitungshandler werden nicht auf SMTP-Ziele angewendet.
2. Wenn Sie mehrere EDI-Austauschvorgänge oder XML- oder ROD-Dokumente empfangen, die aufgeteilt werden müssen, stellen Sie sicher, dass Sie die entsprechenden Verteilerhandler auswählen. Führen Sie die folgenden Schritte aus, um den Vorverarbeitungsschritt zu konfigurieren:

a. Wählen Sie einen Handler in der **Verfügbarkeitsliste** aus, und klicken Sie auf **Hinzufügen**. Beachten Sie, dass der Handler von der **Verfügbarkeitsliste** in die **Konfigurationsliste** versetzt wird, wie in Abb. 17 dargestellt:

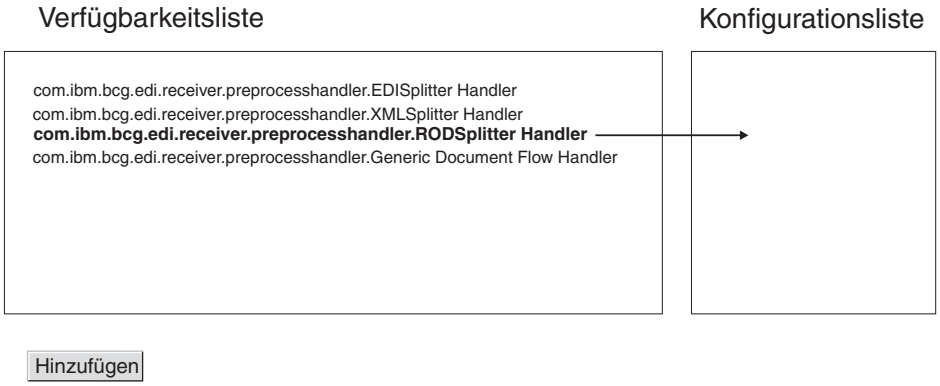

Abbildung 17. Vorverarbeitungsschritt für ein Ziel konfigurieren

b. Wiederholen Sie diesen Schritt für jeden Handler, den Sie der Konfigurationsliste hinzufügen wollen.

   Denken Sie daran, dass Handler für Ziele in der Reihenfolge aufgerufen werden, in der sie in der **Konfigurationsliste** angezeigt werden. Der erste verfügbare Handler verarbeitet die Anforderung und die in der Liste nachfolgenden Handler werden nicht aufgerufen.

c. Konfigurieren Sie den Handler, indem Sie ihn auswählen und auf **Konfigurieren** klicken:
   - Wenn Sie EDISplitterHandler hinzugefügt haben, können Sie sein Attribut **Encoding** ändern. Die Standardcodierung ist ASCII.
   - Wenn Sie XMLSplitterHandler hinzugefügt haben, können Sie sein Attribut **BCGBATCHDOCS** ändern. Die Standardeinstellung ist **ON**. Informationen zu diesem Attribut finden Sie in „Vorverarbeitungsattribute" auf Seite 53.
   - Wenn Sie RODSplitterHandler hinzugefügt haben, können Sie Werte für 11 Attribute angeben. **Encoding**, **BATCHDOCS** und **Metasyntax** haben Standardwerte. Für die anderen Attribute müssen Sie einen Wert für **From Packaging Name**, **From Packaging Version**, **From Protocol Name**, **From Protocol Version**, **From Process Code**, **From Process Version**, **Metadictionary** und **Metadocument** eingeben. Informationen zu diesen Attributen finden Sie in „Vorverarbeitungsattribute" auf Seite 53.
   - Wenn Sie GenericDocumentFlowHandler hinzugefügt haben, können Sie Werte für 11 Attribute angeben. **Encoding** und **BATCHDOCS** haben Standardwerte. Für die anderen Attribute müssen Sie einen Wert für **From Packaging Name**, **From Packaging Version From Protocol Name**, **From Protocol Version**, **From Process Code**, **From Process Version**, **Metadictionary**, **Metadocument** und **Metasyntax** eingeben. Informationen zu diesen Attributen finden Sie in „Vorverarbeitungsattribute" auf Seite 53.

Synchronprüfung

Der Konfigurationspunkt **Synchronprüfung** ist nur für HTTP/S- und JMS-Ziele verfügbar.

Führen Sie die folgenden Schritte aus, um einen Handler für ein Geschäftsprotokoll anzugeben, das in einem synchronen Austausch einbezogen ist:

1. Wählen Sie **Synchronprüfung** in der Liste **Konfigurationspunkt-Handler** aus.

   Sechs Synchronprüfungshandler werden (standardmäßig) für ein HTTP/S-Ziel bereitgestellt. Diese Handler werden in der **Verfügbarkeitsliste** gezeigt:

   - 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

   Wenn Sie z. B. ein HTTP/S-Ziel konfigurieren, sieht die **Verfügbarkeitsliste** wie folgt aus:

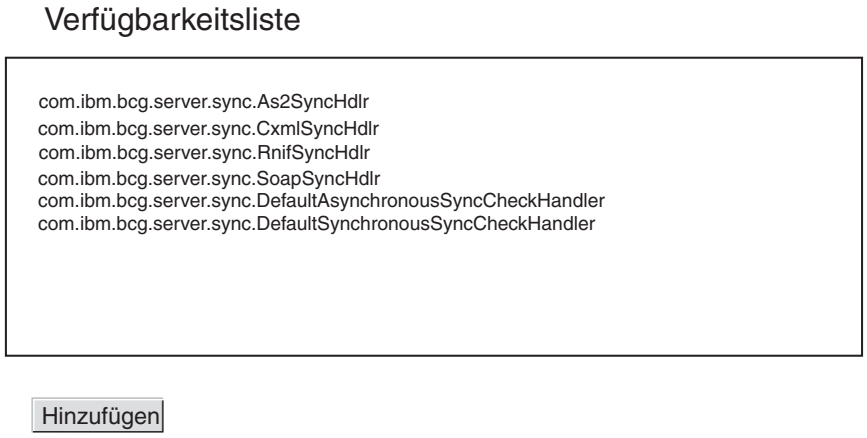

Abbildung 18. Liste verfügbarer Handler für einen HTTP/S-Synchronprüfungs-Konfigurationspunkt

Wie Sie der Namenskonvention entnehmen können, sind die ersten vier Handler spezifisch für die vier Dokumenttypen, die für synchrone Transaktionen verwendet werden können. Jede Anforderung, die **DefaultAsynchronousSyncCheckHandler** verwendet, wird als asynchrone Anforderung behandelt. Jede Anforderung, die **DefaultSynchronousSyncCheckHandler** verwendet, wird als synchrone Anforderung behandelt.

DefaultAsynchronousSyncCheckHandler und **DefaultSynchronousSyncCheckHandler** können mit anderen Zielen, wie z. B. einem JMS-Ziel, verwendet werden.

2. Wenn Sie synchrone Dokumente auf diesem Ziel empfangen, führen Sie die folgenden Schritte aus:
   a. Wählen Sie mindestens einen Handler in der **Verfügbarkeitsliste** aus, und klicken Sie auf **Hinzufügen**.
   b. Wiederholen Sie diesen Schritt, wenn Sie der Liste weitere Handler hinzufügen wollen. Denken Sie daran, dass Handler für Ziele in der Reihenfolge aufgerufen werden, in der sie in der **Konfigurationsliste** angezeigt werden. Der erste verfügbare Handler verarbeitet die Anforderung und die in der Liste nachfolgenden Handler werden nicht aufgerufen.

   Bei HTTP- und HTTPS-Zielen empfiehlt es sich, den spezifischen Handler für die Synchronprüfung, z. B. `com.ibm.bcg.server.sync.As2SyncHdlr` für AS2-Transaktionen, aufzulisten, bevor Sie die Standardhandler für die Synchronprüfung auflisten.

Nachverarbeitung

Für den Nachverarbeitungsschritt werden standardmäßig keine Handler bereitgestellt, und daher sind auch standardmäßig keine Handler in der **Verfügbarkeitsliste** aufgelistet. Sie können jedoch einen Handler für diesen Konfigurationspunkt für alle Zieltypen hochladen, die die synchrone Übertragung unterstützen. Für den Nachbearbeitungsschritt sind folgende Handlertypen verfügbar:

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

Sie fügen einen Nachbearbeitungshandler hinzu, indem Sie einen Handler hochladen, der einem dieser Handlertypen entspricht. Sie verwenden die Auswahl **Importieren** der Seite **Handlerliste**, um einen benutzerdefinierten Handler hochzuladen. Wenn Sie einen benutzerdefinierten Zielhandler hochladen, wird der Handler der **Handlerliste** hinzugefügt. Der Handler wird auch in der **Verfügbarkeitsliste** für den Konfigurationspunkttyp angezeigt, zu dem er gehört.

Führen Sie die folgenden Schritte aus, um den Nachverarbeitungs-Konfigurationspunkt zu ändern:

1. Wählen Sie **Nachverarbeitung** in der Liste **Konfigurationspunkt-Handler** aus.
2. Wählen Sie einen benutzerdefinierten Handler in der **Verfügbarkeitsliste** aus, und klicken Sie auf **Hinzufügen**. Beachten Sie, dass der Handler von der **Verfügbarkeitsliste** in die **Konfigurationsliste** versetzt wird.

Die Konfigurationsliste ändern

Wenn Sie die Reihenfolge der Handler ändern müssen, löschen Sie einen Handler, oder konfigurieren Sie Attribute für den Handler. Führen Sie den entsprechenden Schritt aus:

- Entfernen Sie einen Handler, indem Sie den Handler in der **Konfigurationsliste** auswählen, und klicken Sie auf **Entfernen**. Der Handler wird in die **Verfügbarkeitsliste** versetzt.
- Ändern Sie die Reihenfolge, in der der Handler verwendet wird, indem Sie den Handler auswählen und auf **Nach oben** oder **Nach unten** klicken.
- Konfigurieren Sie den Handler, indem Sie ihn in der **Konfigurationsliste** auswählen und auf **Konfigurieren** klicken. Die Liste der Attribute, die konfiguriert werden können, wird angezeigt.

Kapitel 6. Schritte und Aktionen für feste Arbeitsabläufe konfigurieren

Dieses Kapitel beschreibt optionale Aufgaben, die Sie ausführen können, um feste Eingangs- und Ausgangsarbeitsabläufe und Aktionen zu konfigurieren. Wenn Sie das vom System bereitgestellte Verhalten von Arbeitsabläufen oder Aktionen nicht ändern müssen, überspringen Sie dieses Kapitel.

Dieses Kapitel behandelt die folgenden Themen:

- „Handler hochladen"
- „Feste Arbeitsabläufe konfigurieren" auf Seite 60
- „Aktionen konfigurieren" auf Seite 62

Handler hochladen

Wenn Sie Komponenten modifizieren, laden Sie zuerst die Handler für diese Komponenten hoch, bevor Sie die Komponenten erstellen oder konfigurieren. Sie müssen nur die benutzerdefinierten Handler für die Komponenten hochladen, die sie benötigen. Wenn Sie z. B. Ihren eigenen Validierungsschritt hinzufügen, müssen Sie den Handler von der Seite **Aktionen** der Seite **Handler** hochladen (wie in den Schritten 1 bis 4 beschrieben).

Anmerkung: Wie in „Dokumentverarbeitungskomponenten mit Handler konfigurieren" auf Seite 10 erwähnt, laden Sie nur benutzerdefinierte Handler hoch. Die Handler, die von WebSphere Partner Gateway bereitgestellt wurden, sind bereits verfügbar.

Sie können feste Arbeitsabläufe und Aktionen ändern und neue Aktionen erstellen. Sie ändern diese Komponenten durch den Handler, den Sie ihnen zuordnen.

Anmerkung: Sie können die gültigen Handlertypen für Aktionen und feste Arbeitsabläufe auflisten, indem Sie auf **Hubadmin > Hubkonfiguration > Handler > Aktionen > Handlertypen** oder auf **Hubadmin > Hubkonfiguration > Handler > Fester Arbeitsablauf > Handlertypen** klicken. Bestätigen Sie mit dieser Liste, dass Ihr Handler ein gültiger Typ ist, bevor Sie ihn hochladen. Er muss einer der zulässigen Typen sein oder er wird nicht erfolgreich hochgeladen.

Führen Sie die folgenden Schritte aus, um einen Handler hochzuladen:

1. Klicken Sie im Hauptmenü auf **Hubadmin > Hubkonfiguration > Handler**.
2. Wählen Sie den Handlertyp (**Aktion** oder **Fester Arbeitsablauf**) aus.

   Die Liste der Handler, die derzeit für die bestimmte Komponente definiert sind, wird angezeigt. Beachten Sie, dass die von WebSphere Partner Gateway bereitgestellten Handler aufgelistet werden. Sie haben die Provider-ID **Produkt**.
3. Klicken Sie auf der Seite **Handler-Liste** auf **Importieren**.
4. Geben Sie auf der Seite **Handler importieren** den Pfad zur XML-Datei an, die den Handler beschreibt, oder verwenden Sie **Durchsuchen**, um nach dieser XML-Datei zu suchen.
5. Klicken Sie auf **Hochladen**.

Nachdem ein Handler hochgeladen ist, können Sie mit ihm neue Aktionen und Arbeitsabläufe erstellen.

Anmerkung: Sie können benutzerdefinierte Handler aktualisieren, indem Sie die geänderte XML-Datei hochladen. Für einen Aktionshandler würden Sie z. B. auf **Hubadmin > Hubkonfiguration > Handler > Aktion** und dann auf **Importieren** klicken.

Sie können die von WebSphere Partner Gateway bereitgestellten Handler nicht ändern oder löschen.

Feste Arbeitsabläufe konfigurieren

In Kapitel 1, „Einführung" wurden die zwei Schritte für festen Eingangsarbeitsablauf beschrieben, die Sie konfigurieren können: Ein Schritt für das Entpacken eines Protokolls und einen Schritt für das Parsing des Protokolls. Für Ausgangsarbeitsabläufe ist ein Schritt für das Packen des Protokolls vorhanden.

Wenn Sie einen benutzerdefinierten Handler verwenden, um einen Arbeitsablaufschritt zu konfigurieren, laden Sie den Handler hoch, wie in „Handler hochladen" auf Seite 59 beschrieben.

Führen Sie die folgenden Schritte aus, um einen festen Arbeitsablauf zu konfigurieren:

1. Klicken Sie auf **Hubadmin > Hubkonfiguration > Fester Arbeitsablauf**.
2. Klicken Sie entweder auf **Eingang** oder auf **Ausgang**.
3. Klicken Sie auf das Symbol **Details anzeigen** neben dem Namen des Schritts, den Sie konfigurieren wollen.

   Der Schritt wird zusammen mit einer Liste der Handler aufgelistet, die bereits für diesen Schritt konfiguriert wurden. Eine Liste der Standardhandler finden Sie in „Eingangsarbeitsabläufe" auf Seite 61 und „Ausgangsarbeitsablauf" auf Seite 61.
4. Klicken Sie auf das Symbol **Bearbeiten**, um die Liste der Handler zu bearbeiten.
5. Führen Sie mindestens eine der folgenden Aufgaben für jeden Schritt aus, den Sie ändern wollen.
   a. Fügen Sie einen Handler hinzu, indem Sie den Handler in der **Verfügbarkeitsliste** auswählen, und klicken Sie auf **Hinzufügen**. (Ein Handler wird in der **Verfügbarkeitsliste** angezeigt, wenn Sie einen benutzerdefinierten Handler hochgeladen haben, oder wenn Sie zuvor einen Handler aus der **Konfigurationsliste** entfernt haben.) Der Handler wird in die **Konfigurationsliste** versetzt.
   b. Entfernen Sie einen Handler, indem Sie den Handler in der **Konfigurationsliste** auswählen, und klicken Sie auf **Entfernen**. Der Handler wird in die **Verfügbarkeitsliste** versetzt.
   c. Ändern Sie die Reihenfolge, in der die Handler aufgerufen werden, indem Sie den Handler auswählen und auf **Nach oben** oder **Nach unten** klicken.

      Handler werden in der Reihenfolge aufgerufen, in der sie in der **Konfigurationsliste** aufgelistet sind. Der erste verfügbare Handler, der die Anforderung verarbeiten kann, ist derjenige, der die Anforderung bearbeitet.

Wenn Sie erwarten, eine große Anzahl von Dokumenten eines bestimmten Typs (z. B. ROD-Dokumente) zu empfangen, können Sie den Handler, der diesem Dokumenttyp (in diesem Beispiel: com.ibm.bcg.edi.business.process-.RODScannerHandler) zugeordnet ist, an den Anfang der Liste setzen.

6. Klicken Sie auf **Speichern**.

Eingangsarbeitsabläufe

Dieser Abschnitt listet die Handler auf, die für Eingangsarbeitsabläufe konfiguriert wurden.

Handler für das Entpacken des Protokolls

Standardmäßig sind für den Schritt für das Entpacken des Protokolls die folgenden Handler konfiguriert:

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

Handler für das Verarbeiten des Protokolls

Standardmäßig sind für den Schritt für das Verarbeiten des Protokolls die folgenden Handler konfiguriert:

- 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

Ausgangsarbeitsablauf

Standardmäßig sind für den Schritt für das Packen des Protokolls die folgenden Handler konfiguriert:

- 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

Aktionen konfigurieren

In Kapitel 1, „Einführung" wird beschrieben, dass Aktionen aus mindestens einem Schritt bestehen können. WebSphere Partner Gateway stellt eine Reihe von Standardaktionen bereit. Sie können der Liste der Aktionen etwas hinzufügen, indem Sie mindestens einen Aktionshandler (dies sind Schritte in der Aktion) hochladen, den Sie dann in einer Aktion verwenden können. Sie können ebenfalls neue Aktionen erstellen, wie in „Aktionen erstellen" auf Seite 63 beschrieben.

Anmerkung: Sie können die Aktionen nicht ändern, die von WebSphere Partner Gateway bereitgestellt wurden, obwohl Sie eine dieser Aktionen kopieren und ändern können, wie in „Aktion kopieren" auf Seite 63 beschrieben.

Wenn Sie einen benutzerdefinierten Handler verwenden, um eine Aktion zu konfigurieren, laden Sie den Handler hoch, wie in „Handler hochladen" auf Seite 59 beschrieben.

Benutzerdefinierte Aktion ändern

Führen Sie die folgenden Schritte aus, um eine benutzerdefinierte Aktion zu konfigurieren:

1. Klicken Sie auf **Hubadmin > Hubkonfiguration > Aktionen**.
2. Klicken Sie auf das Symbol **Details anzeigen** neben dem Namen der benutzerdefinierten Aktion, die Sie konfigurieren wollen.

   Die Aktion wird zusammen mit einer Liste der Handler (Aktionsschritte) aufgelistet, die bereits für diese Aktion konfiguriert wurden.
3. Führen Sie mindestens einen der folgenden Schritte für jede Aktion aus, die Sie modifizieren wollen.
   a. Fügen Sie einen Schritt hinzu, indem Sie den zugeordneten Handler in der **Verfügbarkeitsliste** auswählen, und klicken Sie auf **Hinzufügen**. Der Handler wird in die **Konfigurationsliste** versetzt.
   b. Entfernen Sie einen Handler, indem Sie den Handler in der **Konfigurationsliste** auswählen, und klicken Sie auf **Entfernen**. Der Handler wird in die **Verfügbarkeitsliste** versetzt.
   c. Ändern Sie die Reihenfolge, in der die Handler aufgerufen werden, indem Sie den Handler auswählen und auf **Nach oben** oder **Nach unten** klicken.
   d. Damit ein Handler mehrfach verarbeitet werden kann, wählen Sie ihn aus, und klicken Sie dann auf **Wiederholen**.

      Denken Sie daran, dass alle Handler, die für eine Aktion konfiguriert wurden, aufgerufen werden und die Schritte, die die Handler darstellen, in der Reihenfolge ausgeführt werden, in der sie in der **Konfigurationsliste** angezeigt werden.
   e. Konfigurieren Sie den Handler, indem Sie ihn in der **Konfigurationsliste** auswählen und auf **Konfigurieren** klicken. Die Liste der Attribute, die konfiguriert werden können, wird angezeigt.
4. Klicken Sie auf **Speichern**.

Aktionen erstellen

Sie können eine Aktion auf eine der folgenden Weisen erstellen:

- Erstellen Sie eine neue Aktion, und ordnen Sie der Aktion Handler zu.
- Kopieren Sie eine vom Produkt bereitgestellte Aktion und, falls nötig, modifizieren Sie die ihr zugeordneten Handler.

Neue Aktion erstellen

Führen Sie die folgenden Schritte aus, um eine neue Aktion zu erstellen:

1. Klicken Sie auf **Hubadmin > Hubkonfiguration > Aktionen**.
2. Klicken Sie auf **Erstellen**.
3. Geben Sie einen Namen für die Aktion ein. Dieses Feld ist erforderlich.
4. Geben Sie eine optionale Beschreibung der Aktion ein.
5. Geben Sie an, ob die Aktion zur Verwendung aktiviert ist.
6. Fügen Sie für jeden Schritt, der als Teil der Aktion aufgerufen wird, den zugeordneten Handler hinzu, indem Sie ihn in der **Verfügbarkeitsliste** auswählen und auf **Hinzufügen** klicken. Der Handler wird in die **Konfigurationsliste** versetzt.

   Denken Sie daran, dass Handler von der Aktion in der Reihenfolge aufgerufen werden, in der sie in der **Konfigurationsliste** angezeigt werden. Stellen Sie sicher, dass Sie die Handler in der richtigen Reihenfolge anordnen. Sie können mit den Schaltflächen **Nach oben** oder **Nach unten** die Reihenfolge der Handler ändern oder mit der Schaltfläche **Wiederholen** bewirken, dass ein Handler mehr als einmal verarbeitet wird.
7. Konfigurieren Sie einen Handler, indem Sie ihn in der **Konfigurationsliste** auswählen und auf **Konfigurieren** klicken. Die Liste der Attribute, die konfiguriert werden können, wird angezeigt.
8. Klicken Sie auf **Speichern**.

Aktion kopieren

Führen Sie die folgenden Schritte aus, um eine Aktion zu erstellen, indem Sie eine vorhandene Aktion kopieren:

1. Klicken Sie auf **Hubadmin > Hubkonfiguration > Aktionen**.
2. Klicken Sie in der Liste **Aktionen** auf das Symbol **Kopieren** neben der Aktion, die Sie kopieren wollen.
3. Geben Sie einen Namen für die Aktion ein. Dieses Feld ist erforderlich.
4. Geben Sie eine optionale Beschreibung der Aktion ein.
5. Geben Sie an, ob die Aktion zur Verwendung aktiviert ist.

6. Beachten Sie, dass schon mindestens ein Schritt in der **Konfigurationsliste** vorhanden ist. Dies sind die Schritte, die der kopierten Aktion zugeordnet sind. Wenn Sie z. B. die vom System bereitgestellte Aktion **Community Manager - Abbruch des RosettaNet-Prozesses** geklont haben, würden Ihre Verfügbarkeits- und Konfigurationsliste die folgenden Handler enthalten:

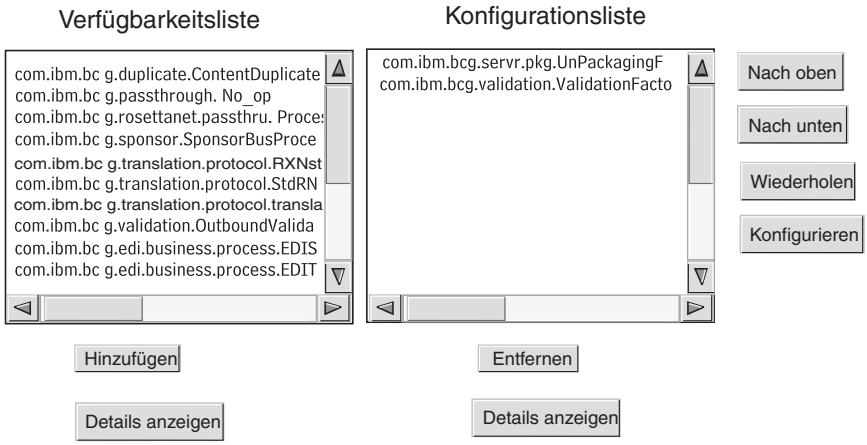

Abbildung 19. Aktion klonen

Führen Sie mindestens einen der folgenden Schritte aus, um die **Konfigurationsliste** zu ändern:

a. Fügen Sie einen Schritt hinzu, indem Sie den zugeordneten Handler in der **Verfügbarkeitsliste** auswählen, und klicken Sie auf **Hinzufügen**. Der Handler wird in die **Konfigurationsliste** versetzt.

b. Entfernen Sie einen Schritt, indem Sie den zugeordneten Handler in der **Konfigurationsliste** auswählen, und klicken Sie auf **Entfernen**. Der Handler wird in die **Verfügbarkeitsliste** versetzt.

c. Ändern Sie die Reihenfolge, in der die Handler aufgerufen werden, indem Sie den Handler auswählen und auf **Nach oben** oder **Nach unten** klicken.

   Denken Sie daran, dass alle Handler, die für eine Aktion konfiguriert wurden, aufgerufen werden und die Schritte, die den Handlern zugeordnet sind, in der Reihenfolge ausgeführt werden, in der sie in der **Konfigurationsliste** angezeigt werden.

d. Konfigurieren Sie den Schritt, indem Sie ihn in der **Konfigurationsliste** auswählen und auf **Konfigurieren** klicken. Die Liste der Attribute, die konfiguriert werden können, wird angezeigt.

7. Klicken Sie auf **Speichern**.

Kapitel 7. Dokumentenflüsse konfigurieren

Dieses Kapitel beschreibt, wie Sie die Nicht-EDI-Dokumente konfigurieren, die Sie mit Ihren Community-Teilnehmern und mit Ihren Back-End-Anwendungen austauschen werden. Das Konfigurieren von Dokumentenflüssen und Interaktionen für EDI-Dokumente, mit Ausnahme der EDI-Dokumente, die weitergeleitet werden, wird in Kapitel 8, „EDI-Dokumentenflüsse konfigurieren", auf Seite 93 beschrieben. Kapitel 8 beschreibt außerdem, wie Sie Dokumentenflüsse und Interaktionen für XML-Dokumente und satzorientierte Datendokumente (ROD-Dokumente) konfigurieren.

Das Kapitel behandelt die folgenden Themen:

- „Übersicht"
- „Binäre Dokumente" auf Seite 69
- „EDI-Dokumente mit Pass-Through-Aktion" auf Seite 69
- „RosettaNet-Dokumente" auf Seite 71
- „Web-Services" auf Seite 79
- „cXML-Dokumente" auf Seite 84
- „Angepasste XML-Dokumente" auf Seite 89

Übersicht

Eine Dokumentenflussdefinition besteht aus mindestens einem Paket, einem Protokoll und einem Dokumentenfluss. Für einige Protokolle kann eine Aktivität, eine Aktion und ein Signal angegeben werden. Die Dokumentenflussdefinitionen geben die Dokumenttypen an, die von WebSphere Partner Gateway verarbeitet werden.

Ein Paket bezieht sich auf die Logik, die erforderlich ist, um ein Dokument gemäß einer Spezifikation, wie z. B. AS2, zu packen. Eine Protokollübertragung ist die Logik, die erforderlich ist, um ein Dokument zu verarbeiten, das mit einem bestimmten Protokoll, wie z. B. EDI-X12, konform ist. Ein Dokumentenfluss beschreibt, wie das Dokument aussehen wird.

Die folgenden Abschnitte beschreiben kurz den Gesamtablauf für das Konfigurieren eines Dokumentenflusses zwischen Community Manager und einem Teilnehmer.

Schritt 1: Sicherstellen, dass die Dokumentenflussdefinition verfügbar ist

Überprüfen Sie, ob eine Dokumentenflussdefinition von denen vorhanden ist, die auf dem System vordefiniert sind. Wenn der Fluss nicht bereits vorhanden ist, erstellen Sie ihn, indem Sie die notwendigen Dateien hochladen oder indem Sie manuell eine angepasste Definition erstellen.

Sie können als ein Teil der Erstellung der Dokumentenflussdefinition bestimmte Attribute ändern. Attribute werden verwendet, um verschiedene Dokumentverarbeitungs- und Routing-Funktionen auszuführen, wie z. B. Validierung, Verschlüsselungsüberprüfung und Wiederholungszähler. Die Attribute, die Sie auf der Dokumentenfluss-Definitionsebene festlegen, liefern eine globale Einstellung für das zugeordnete Paket und Protokoll sowie den zugeordneten Dokumenten-

fluss. Die Attribute, die zur Verfügung stehen, variieren je nach Dokumentenflussdefinition. Die Attribute für EDI-Dokumentenflussdefinitionen unterscheiden sich z. B. von den Attributen für RosettaNet-Dokumentenflussdefinitionen.

Wenn Sie z. B. einen Wert für **Bestätigungszeit** im Paket **AS** angeben, wird dieser auf alle Dokumente angewendet, die mit AS gepackt werden. (**Bestätigungszeit** gibt die Wartezeit für eine MDN-Bestätigung (Message Disposition Notification - Nachrichtendispositionsbenachrichtigung) an, bevor die ursprüngliche Anforderung erneut gesendet wird.) Wenn Sie später das Attribut **Bestätigungszeit** auf der B2B-Funktionalitätsebene festlegen, überschreibt diese Einstellung diejenige, die auf der Dokumentenfluss-Definitionsebene festgelegt wurde.

Bei Attributen, die auf allen Ebenen der Dokumentenflussdefinition festgelegt werden können, haben die auf Dokumentenflussebene festgelegten Werte Vorrang vor den auf Protokollebene festgelegten Werten und die auf Protokollebene festgelegten Attribute haben Vorrang vor denen auf der Paketebene.

Sie müssen den Dokumentenfluss auf der Seite **Dokumentenflussdefinitionen verwalten** auflisten, bevor Sie Interaktionen erstellen können.

Schritt 2: Interaktionen erstellen

Erstellen Sie Interaktionen für die Dokumentenflüsse, die definiert worden sind. Die Interaktion teilt WebSphere Partner Gateway mit, welche Aktionen an einem Dokument ausgeführt werden sollen. Für einige Austauschvorgänge benötigen Sie nur zwei Dokumentenflüsse: Der eine beschreibt das Dokument, das auf dem Hub vom Teilnehmer oder Community Manager empfangen wird und der andere beschreibt das Dokument, das vom Hub zum Teilnehmer oder Community Manager gesendet wird. Wenn der Hub jedoch einen EDI-Austauschvorgang sendet oder empfängt, der in einzelne Transaktionen aufgeteilt wird bzw. in dem Bestätigungen erforderlich sind, dann erstellen Sie tatsächlich mehrere Interaktionen, um den Austausch auszuführen.

Schritt 3: Teilnehmerprofile, Gateways und B2B-Funktionalität erstellen

Erstellen Sie Teilnehmerprofile für Community Manager und die Community-Teilnehmer. Definieren Sie Gateways, die bestimmen, wohin Dokumente gesendet werden, und B2B-Funktionalität, die die Dokumente angeben, welche Community Manager und die Teilnehmer senden und empfangen können. Die Seite **B2B-Funktionalität** listet alle Dokumentenflüsse auf, die definiert worden sind.

Sie können Attribute auf der B2B-Funktionalitätsebene festlegen. Jedes Attribut, das Sie auf dieser Ebene festlegen, überschreibt die auf der Dokumentenfluss-Definitionsebene festgelegten Attribute. Wenn Sie z. B. die **Bestätigungszeit** auf der Dokumentenfluss-Definitionsebene für das Paket **AS** auf 30 und auf der B2B-Funktionalitätsebene dann aber auf 60 setzen, wird der Wert 60 verwendet. Wenn Sie ein Attribut auf der B2B-Ebene festlegen, können Sie das Attribut an einen bestimmten Teilnehmer anpassen.

Sie müssen die Profile und B2B-Funktionalität von Community Manager und den Teilnehmern definiert haben, bevor Sie Verbindungen zwischen ihnen erstellen können.

Schritt 4: Verbindungen aktivieren

Aktivieren Sie Verbindungen zwischen Community Manager und Teilnehmern. Die verfügbaren Verbindungen basieren auf der B2B-Funktionalität der Teilnehmer. Die B2B-Funktionalität basiert auf den von Ihnen erstellten Interaktionen. Die Interaktionen hängen von den Dokumentenflussdefinitionen ab, die zur Verfügung stehen.

Für einige Austauschvorgänge ist nur eine Verbindung erforderlich. Wenn z. B. ein Teilnehmer ein binäres Dokument an eine Community Manager-Back-End-Anwendung sendet, wird nur eine Verbindung benötigt. Für den Austausch von EDI-Austauschvorgängen, in denen der Umschlag des Austauschs entfernt wird und die einzelnen Transaktionen umgesetzt werden, sind jedoch mehrere Verbindungen konfiguriert.

Anmerkung: Für EDI-Austauschvorgänge, die unverändert weitergeleitet werden, ist nur eine Verbindung erforderlich.

Sie können Attribute auf der Verbindungsebene festlegen. Jedes Attribut, das Sie auf dieser Ebene festlegen, überschreibt die auf der B2B-Attributebene festgelegten Attribute. Wenn Sie z. B. die **Bestätigungszeit** auf der B2B-Funktionalitätsebene für das Paket **AS** auf 60 und diese dann aber auf 120 setzen, wird der Wert 120 verwendet. Wenn Sie einen Wert für ein Attribut auf der Verbindungsebene festlegen, können Sie das Attribut, abhängig von den Routing-Anforderungen der Teilnehmer und der Anwendungen, die beteiligt sind, noch weiter anpassen.

Ein Beispieldokumentenfluss

Standardmäßig sind mehrere Packmethoden aktiviert. Um die Gesamtprozedur für das Erstellen von Dokumentenflussdefinitionen zu veranschaulichen, wird der Fall betrachtet, in dem Sie eine Vereinbarung mit einem Community-Teilnehmer haben, um einen EDI-Austauschvorgang zu empfangen, der mit dem EDI-X12-Standard konform ist. Der Teilnehmer wird das Dokument in einem Paket **AS2** senden. Sie werden angeben, dass der Austausch unverändert (ohne Umsetzung) an eine Back-End-Anwendung ohne Paket gesendet wird.

1. Prüfen Sie auf der Seite **Dokumentenflussdefinitionen verwalten**, ob die Dokumentenflussdefinition aktiviert ist, die den Dokumenttyp beschreibt, welcher vom Community-Teilnehmer in den Hub fließt.
   a. Klicken Sie auf **Hubadmin > Hubkonfiguration > Dokumentenflussdefinition**.
   b. Klicken Sie auf das Symbol **Erweitern** neben **Paket: AS**. Beachten Sie, dass **EDI-X12** bereits aufgelistet ist.
   c. Klicken Sie auf das Symbol **Erweitern** neben **Protokoll: EDI-X12**. Beachten Sie, dass **Dokumentenfluss: ISA** bereits aufgelistet ist.
2. Prüfen Sie, während die Seite **Dokumentenflussdefinitionen verwalten** noch angezeigt ist, ob die zweite Dokumentenflussdefinition aktiviert ist, die den Dokumenttyp beschreibt, welcher zur Back-End-Anwendung fließt.
   a. Klicken Sie auf das Symbol **Erweitern** neben **Paket: None**. Beachten Sie, dass **EDI-X12** bereits aufgelistet ist.
   b. Klicken Sie auf das Symbol **Erweitern** neben **Protokoll: EDI-X12**. Beachten Sie, dass **Dokumentenfluss: ISA** bereits aufgelistet ist.
3. Erstellen Sie eine Interaktion, die beschreibt, ob der Dokumentenfluss ein Quell- oder ein Zieldokumentenfluss sein wird.
   a. Klicken Sie, während die Seite **Dokumentenflussdefinitionen verwalten** noch angezeigt ist, auf **Interaktionen verwalten**.

b. Klicken Sie auf **Interaktion erstellen**.
c. Erweitern Sie in der Spalte **Quelle** den Eintrag **Paket: AS**, **Protokoll: EDI-X12 (ALL)**, und klicken Sie dann auf **Dokumentenfluss: ISA**.
d. Erweitern Sie in der Spalte **Ziel** den Eintrag **Paket: None**, **Protokoll: EDI-X12 (ALL)**, und klicken Sie dann auf **Dokumentenfluss: ISA**.
e. In diesem Beispiel gibt es keine Umsetzung. Treffen Sie daher keine Auswahl in der Liste **Transformationszuordnung**.
f. Wählen Sie in der Liste **Aktion** die Option **Pass-Through** aus.
g. Klicken Sie auf **Speichern**.

Sie haben gerade angegeben, dass der Hub in der Lage ist, EDI-X12-Austauschvorgänge (ISA-Standard) in einem AS-Paket zu akzeptieren. Sie haben außerdem angegeben, dass der Hub in der Lage ist, EDI-X12-Austauschvorgänge (ISA-Standard) ohne Paket zu senden. Darüber hinaus haben Sie angegeben, dass beim Austausch keine Umsetzung stattfinden soll. Der Austausch wird einfach bis zur Back-End-Anwendung weitergeleitet, nachdem die AS-Header entfernt wurden.

Sie haben noch nicht angegeben, welcher Community-Teilnehmer in der Lage ist, diesen Austauschtyp zum Hub zu senden. Sie definieren dies, wenn Sie das Teilnehmerprofil und die B2B-Funktionalität der Teilnehmer konfigurieren. (Sie definieren außerdem ein Profil und die B2B-Funktionalität für das Community Manager-Back-End-System.) Nachdem Sie diese Aufgaben ausgeführt haben, erstellen Sie dann eine Verbindung zwischen dem Community-Teilnehmer und der Back-End-Anwendung. Abb. 20 zeigt die Verbindung zwischen dem Teilnehmer und der Community Manager-Back-End-Anwendung für dieses Beispiel.

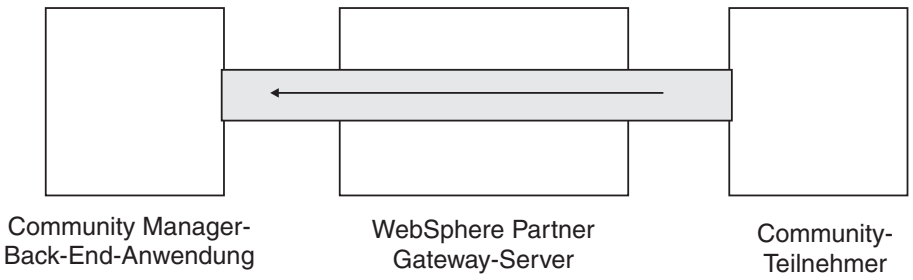

Abbildung 20. Eine Einwegverbindung von einem Teilnehmer zu Community Manager

Sie prüfen mit der Seite **Verbindungen verwalten** (**Kontenadmin > Teilnehmerverbindungen**), ob eine Verbindung vorhanden ist. Sie wählen auf der Seite **Verbindungen verwalten** den Teilnehmer in der Liste **Quelle** und Community Manager in der Liste **Ziel** aus, und Sie klicken dann auf **Suchen**. Die eine verfügbare Verbindung wird aufgelistet. Falls nötig, können Sie Attribute und Aktionen ändern, wie in den nachfolgenden Abschnitten beschrieben wird.

Es gibt drei Typen von Dokumentenflussdefinitionen. Die einen Definitionen werden mit dem System bereitgestellt und können über die Konsole ausgewählt werden. Die anderen Definitionen sind bereits definiert, aber noch nicht auf der Community Console; sie laden diese Definitionen entweder vom WebSphere Partner Gateway-Installationsdatenträger oder einer anderen Speicherposition hoch. Die übrigen Definitionen erstellen Sie selber. Für jeden Typ von Dokumentenflussdefinition können (oder müssen) Sie Attribute angeben oder Zuordnungen hochladen, die den Dokumentenfluss noch weiter definieren.

Binäre Dokumente

Binäre Dokumente werden unverändert durch den Hub weitergeleitet und daher ist das Austauschen von binären Dokumenten zwischen einem Community-Teilnehmer und einer Community Manager-Back-End-Anwendung ein unkomplizierter Prozess. Das binäre Protokoll ist bereits für die Pakete **AS**, **None** und **Backend Integration** verfügbar. Daher ist „Schritt 1: Sicherstellen, dass die Dokumentenflussdefinition verfügbar ist" auf Seite 65 bereits erledigt.

Anmerkung: Sie können Attribute auf jeder Ebene (Paket, Protokoll oder Dokumentenfluss) hinzufügen, um die Standardverarbeitung zu ändern, indem Sie auf das Symbol **Attributwerte bearbeiten** klicken. Standardmäßig werden keine Attribute dem binären Protokoll oder dem Dokumentenfluss zugeordnet.

Ebenso wurden vier Interaktionen für binäre Dokumente bereits standardmäßig bereitgestellt, und für diese Interaktionen müssen Sie Schritt 2: Interaktionen erstellen nicht ausführen. Interaktionen werden für die folgenden Austauschvorgänge bereitgestellt:

Tabelle 4. Vom System bereitgestellte Interaktionen

Paket/Protokoll/Dokumentenfluss der Quelle	Paket/Protokoll/Dokumentenfluss des Ziels
AS/Binary/Binary	Backend Integration/Binary/Binary
Backend Integration/Binary/Binary	AS/Binary/Binary
AS/Binary/Binary	None/Binary/Binary
None/Binary/Binary	AS/Binary/Binary

Für den Austausch binärer Dokumente müssen Sie noch Folgendes ausführen:

- Schritt 3: Teilnehmerprofile, Gateways und B2B-Funktionalität erstellen wird in Kapitel 9, „Das Community Manager-Profil und B2B-Funktionalität erstellen", auf Seite 137, Kapitel 11, „Teilnehmer und ihre B2B-Funktionalität erstellen", auf Seite 161 und Kapitel 10, „Gateways erstellen", auf Seite 141 beschrieben.
- Schritt 4: Verbindungen aktivieren wird in Kapitel 12, „Verbindungen verwalten", auf Seite 165 beschrieben.

EDI-Dokumente mit Pass-Through-Aktion

WebSphere Partner Gateway stellt für EDI-Austauschvorgänge die Funktion zum Entfernen des Umschlags und zum Umsetzen bereit. Dieser Prozess wird in Kapitel 8, „EDI-Dokumentenflüsse konfigurieren", auf Seite 93 beschrieben.

Abb. 21 auf Seite 70 zeigt den Ablauf eines EDI-Austauschs, der von einem Teilnehmer an Community Manager weitergeleitet wird.

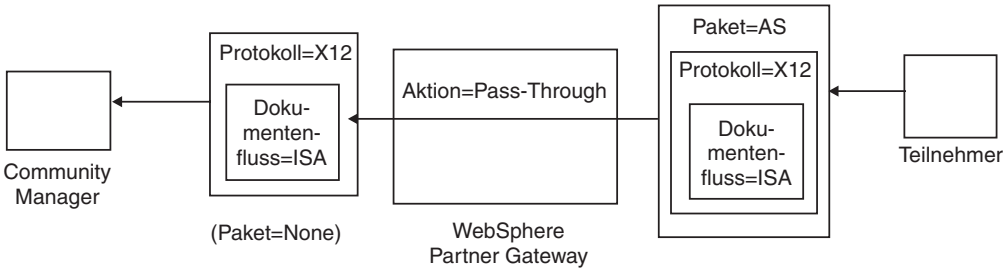

Abbildung 21. Eingehender EDI-Austausch mit Pass-Through-Aktion

In diesem Beispiel werden die AS2-Header entfernt, ansonsten wird der Austausch aber nicht verändert und fließt durch das System zum Gateway von Community Manager.

Dokumentenflussdefinitionen erstellen

Der Dokumentenfluss für EDI-Austauschvorgänge mit Pass-Through wird bereits standardmäßig auf der Seite **Dokumentenflussdefinitionen verwalten** bereitgestellt, wie in „Ein Beispieldokumentenfluss" auf Seite 67 beschrieben. Wenn Sie ein Attribut mit Standardwert ändern wollen oder ein Attribut ohne zugeordneten Wert festlegen wollen, können Sie die Seite **Dokumentenflussdefinitionen verwalten** zur Ausführung dieser Aufgabe verwenden.

Angenommen, Sie wollen z. B. das Attribut **Bestätigungszeit** für ein mit AS gepacktes EDI-Dokument ändern. Sie müssen hierzu die folgenden Schritte ausführen:

1. Klicken Sie auf **Hubadmin > Hubkonfiguration > Dokumentenflussdefinition**.
2. Klicken Sie auf das Symbol **Attributwerte bearbeiten** neben **Paket: AS**.
3. Blättern Sie auf der Seite bis zum Abschnitt mit dem Titel **Attribute für Dokumentenflusskontexte** vor.
4. Geben Sie in der Zeile **Bestätigungszeit** einen anderen Wert in die Spalte **Aktualisieren** ein.
5. Klicken Sie auf **Speichern**.

Beachten Sie, dass Sie in diesem Beispiel ein Paketattribut geändert haben. Die Attribute für Protokoll (z. B. EDI-X12) und Dokumentenfluss (z. B. ISA) sind für eine Pass-Through-Aktion nicht wichtig. Dieses Paketattribut wird auf alle Dokumente angewendet, die in einem AS-Paket gepackt werden.

Interaktionen erstellen

Führen Sie die folgenden Schritte aus, um die Interaktion für einen EDI-Austausch mit Pass-Through-Aktion zu erstellen:

1. Klicken Sie auf **Hubadmin > Hubkonfiguration > Dokumentenflussdefinition**.
2. Klicken Sie über die Seite **Dokumentenflussdefinitionen verwalten** auf **Interaktionen verwalten**.
3. Klicken Sie auf **Interaktion erstellen**.
4. Erweitern Sie unter **Quelle** den Eintrag **Paket: AS** und **Protokoll: EDI-X12**, und wählen Sie dann **Dokumentenfluss: ISA** aus.
5. Erweitern Sie unter **Ziel** den Eintrag **Paket: None** und **Protokoll: EDI-X12**, und wählen Sie dann **Dokumentenfluss: ISA** aus.

6. Wählen Sie in der Liste **Aktion** die Option **Pass-Through** aus.

Mit den Schritten 1 auf Seite 70 bis 6 wurde WebSphere Partner Gateway aktiviert, um einen EDI-X12-Austausch im AS-Paket von einem Quellenteilnehmer zu akzeptieren, einen EDI-X12-Austausch ohne Paket an den Zielteilnehmer zu senden und den Austausch von der Quelle an das Ziel weiterzuleiten.

Wenn Sie eine Interaktion konfigurieren wollen, deren Quellendokument als **None/EDI-X12/ISA** gepackt und deren Zieldokument als **AS/EDI-X12/ISA** gepackt ist, erweitern Sie **Paket: None** in Schritt 4 auf Seite 70 (in der Spalte **Quelle**), und erweitern Sie **Paket: AS** im Schritt 5 auf Seite 70 (in der Spalte **Ziel**).

RosettaNet-Dokumente

Dieser Abschnitt bietet eine Übersicht über RosettaNet-Dokumente und zeigt Ihnen, wie Sie Dokumentenflussdefinitionen und Interaktionen für diese Dokumente konfigurieren.

Übersicht

RosettaNet ist eine Organisation, die offene Standards zur Verfügung stellt, um den Austausch von Geschäftsnachrichten zwischen Handelspartnern zu unterstützen. Weitere Informationen zu RosettaNet finden Sie unter der Internetadresse: http://www.rosettanet.org. Die Standards schließen RNIF- (RosettaNet Implementation Framework) und PIP-Spezifikationen (Partner Interface Process) mit ein. RNIF definiert, wie Handelspartner Nachrichten austauschen, indem es ein Gerüst aus Nachrichtenpaketen, Übertragungsprotokollen und Sicherheit bereitstellt. Es gibt zwei freigegebene Versionen: 1.1 und 2.0. Ein PIP definiert einen öffentlichen Geschäftsprozess und die XML-basierten Nachrichtenformate, um den Prozess zu unterstützen.

WebSphere Partner Gateway unterstützt RosettaNet-Nachrichtenübertragung mit RNIF 1.1 und 2.0. Wenn der Hub eine PIP-Nachricht empfängt, validiert und wandelt er die Nachricht um, um sie an das entsprechende Back-End-System zu senden. WebSphere Partner Gateway stellt ein Protokoll zum Packen der umgewandelten Nachricht in eine RNSC-Nachricht (RosettaNet Service Content) bereit, die das Back-End-System bearbeiten kann. Informationen zu den Paketen, die für diese Nachrichten verwendet werden, um Route-Informationen bereitzustellen, finden Sie im Handbuch *Unternehmensintegration*.

Der Hub kann auch RNSC-Nachrichten von Back-End-Systemen empfangen und die entsprechende PIP-Nachricht erstellen und die Nachricht an den entsprechenden Handelspartner (einen Teilnehmer) senden. Sie stellen die Dokumentenflussdefinitionen für die RNIF-Version und die PIPs bereit, die Sie verwenden wollen.

Neben der Bereitstellung der Routing-Funktion für RosettaNet-Nachrichten verwaltet WebSphere Partner Gateway einen Status für jede Nachricht, die es bearbeitet. Dadurch kann es beliebige Nachrichten erneut senden, die fehlgeschlagen sind, bis die Anzahl Versuche den angegebenen Schwellenwert erreicht hat. Der Ereignisbenachrichtigungsmechanismus warnt Back-End-Systeme, wenn eine PIP-Nachricht nicht zugestellt werden kann. Der Hub kann außerdem automatisch 0A1 PIPs generieren, die an die entsprechenden Teilnehmer gesendet werden, wenn er bestimmte Ereignisbenachrichtigungsnachrichten von Back-End-Systemen empfängt. Weitere Informationen zur Ereignisbenachrichtigung finden Sie im Handbuch *Unternehmensintegration*.

RNIF- und PIP-Dokumentenflusspakete

Zur Unterstützung der RosettaNet-Nachrichtenübermittlung stellt WebSphere Partner Gateway zwei Gruppen von komprimierten Dateien, auch Pakete genannt, bereit. Die *RNIF-Pakete* bestehen aus Dokumentenflussdefinitionen, die zur Unterstützung des RNIF-Protokolls erforderlich sind. Diese Pakete befinden sich im Verzeichnis `B2BIntegrate`.

Für RNIF V1.1 gibt es folgende Pakete:

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

Für RNIF V02.00 gibt es folgende Pakete:

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

Das erste Paket in jedem Paar bietet die Dokumentenflussdefinitionen, die zur Unterstützung der RosettaNet-Kommunikation mit Teilnehmern erforderlich sind, und das zweite Paket bietet die Dokumentenflussdefinitionen, die zur Unterstützung der RosettaNet-Kommunikation mit Back-End-Systemen erforderlich sind.

Die zweite Gruppe von Paketen besteht aus PIP-Dokumentenflusspaketen. Jedes PIP-Dokumentenflusspaket hat ein Verzeichnis `Packages`, in dem sich eine XML-Datei und ein Verzeichnis `GuidelineMaps` mit XSD-Dateien befinden. Die XML-Datei gibt die Dokumentenflussdefinitionen an, die definieren, wie WebSphere Partner Gateway den PIP bearbeitet, und die die ausgetauschten Nachrichten und Signale definieren. Die XSD-Dateien geben das Format der PIP-Nachrichten an und definieren akzeptable Werte für XML-Elemente in den Nachrichten. Die komprimierten Dateien für 0A1 PIPs verfügen auch über eine XML-Datei, die der Hub als Vorlage zur Erstellung von 0A1-Dokumenten verwendet.

WebSphere Partner Gateway stellt für die folgenden PIPs PIP-Dokumentenflusspakete bereit:

- 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

Für jeden PIP gibt es vier PIP-Dokumentenflusspakete:

- Für RNIF 1.1-Nachrichtenübermittlung mit Teilnehmern
- Für RNIF 1.1-Nachrichtenübermittlung mit Back-End-Systemen
- Für RNIF 2.0-Nachrichtenübermittlung mit Teilnehmern
- Für RNIF 2.0-Nachrichtenübermittlung mit Back-End-Systemen

Jedes PIP-Dokumentenflusspaket folgt einer spezifischen Namenskonvention, mit der Sie erkennen können, ob das Paket für Nachrichten zwischen WebSphere Partner Gateway und Teilnehmern oder zwischen WebSphere Partner Gateway und Back-End-Systemen ist. Die Namenskonvention gibt auch die RNIF-Version, den PIP und die PIP-Version an, die das Paket unterstützt. Für PIP-Dokumentenflusspakete, die für die Nachrichtenübermittlung zwischen WebSphere Partner Gateway und Teilnehmern verwendet werden, gilt folgendes Format:

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

Für PIP-Dokumentenflusspakete, die für die Nachrichtenübermittlung zwischen WebSphere Partner Gateway und Back-End-Systemen verwendet werden, gilt folgendes Format:

`BCG_Package_RNSC<Backend_Integration-version>_RNIF<RNIF-version>_`
`<PIP><PIP-version>.zip`

BCG_Package_RNIF1.1_3A4V02.02.zip ist z. B. für das Validieren der Dokumente für Version 02.02 des 3A4 PIP, die zwischen Teilnehmern und WebSphere Partner Gateway mit dem RNIF 1.1-Protokoll gesendet werden. Bei PIP-Dokumentenflusspaketen für die Kommunikation mit Back-End-Systemen muss der Name des Pakets ebenfalls das Protokoll angeben, das zum Senden der RosettaNet-Inhalte an Back-End-Systeme verwendet wird. Informationen zu den Paketen, die für diese Nachrichten verwendet werden, finden Sie im Handbuch *Unternehmensintegration*.

Dokumentenflussdefinitionen erstellen

Für die RosettaNet-Nachrichtenübermittlung benötigt WebSphere Partner Gateway die RNIF-Pakete für die Version von RNIF, mit der die Nachrichten gesendet werden. Für jeden PIP, den WebSphere Partner Gateway unterstützt, benötigt es die zwei PIP-Dokumentenflusspakete für die RNIF-Version. WebSphere Partner Gateway benötigt z. B. die folgenden Pakete, um den 3A4 PIP über RNIF 2.0 zu unterstützen:

- 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

Das erste Paket unterstützt die RosettaNet-Nachrichtenübermittlung mit Teilnehmern und das zweite Paket unterstützt die RosettaNet-Nachrichtenübermittlung mit Back-End-Systemen. Das dritte und vierte Paket aktivieren WebSphere Partner Gateway für das Übergeben von 3A4-Nachrichten zwischen Teilnehmern und Back-End-Systemen mit RNIF 2.0.

Gehen Sie wie folgt vor, um RosettaNet-Pakete hochzuladen:

1. Klicken Sie auf **Hubadmin > Hubkonfiguration > Dokumentenflussdefinition**.
2. Klicken Sie auf **Pakete hoch-/herunterladen**.
3. Wählen Sie **Nein** für **WSDL-Paket** aus.
4. Klicken Sie auf **Durchsuchen**, und wählen Sie das RNIF-Paket für die Kommunikation mit Teilnehmern aus.

   Die RNIF-Pakete befinden sich auf dem Installationsdatenträger standardmäßig im Verzeichnis B2BIntegrate/Rosettanet. Wenn Sie z. B. das Paket mit RNIF Version 2.00 hochladen, würden Sie zum Verzeichnis B2BIntegrate/Rosettanet blättern und Package_RNIF_V0200.zip auswählen.
5. Stellen Sie sicher, dass **In Datenbank festschreiben** auf **Ja** gesetzt ist.
6. Klicken Sie auf **Hochladen**.
7. Klicken Sie erneut auf **Durchsuchen**, und wählen Sie das RNIF-Paket für die Kommunikation mit Back-End-Anwendungen aus.

   Wenn Sie z. B. das Paket mit RNIF Version 2.00 hochladen, würden Sie zum Verzeichnis B2BIntegrate/Rosettanet blättern und Package_RNSC_1.0_RNIF_V02.00.zip auswählen.
8. Klicken Sie auf **Hochladen**.

   Die Pakete, die für die Kommunikation mit Teilnehmern oder mit dem Back-End-System benötigt werden, sind jetzt auf dem System installiert. Wenn Sie die Seite **Dokumentenflussdefinitionen verwalten** überprüfen, finden Sie einen Eintrag für **Paket: RNIF/Protokoll: RosettaNet**, der das Paket für die Kommunikation mit Teilnehmern darstellt, und einen Eintrag für **Paket: Backend Integration/Protokoll: RNSC**, der das Paket für die Kommunikation mit Back-End-Anwendungen darstellt.

9. Laden Sie für jeden PIP, den Sie unterstützen wollen, das PIP-Dokumentenflusspaket für den PIP und für die unterstützte RNIF-Version hoch. Führen Sie die folgenden Schritte aus, um z. B. den 3A6 PIP (Notify of Remittance Advice) hochzuladen, der zu einem Teilnehmer gesendet werden soll:
   a. Klicken Sie auf **Durchsuchen**, und wählen Sie `BCG_Package_RNIFV02.00_3C6V02.02` im Verzeichnis `B2BIntegrate/Rosettanet` aus.
   b. Stellen Sie sicher, dass **In Datenbank festschreiben** auf **Ja** gesetzt ist.
   c. Klicken Sie auf **Hochladen**.

   Der 3C6V02.02 PIP wird jetzt als Dokumentenfluss unter **Paket:RNIF/Protokoll:RosettaNet** auf der Seite **Dokumentenflussdefinitionen verwalten** angezeigt. Darüber hinaus werden eine Aktivität, eine Aktion und zwei Signale angezeigt. Sie werden in den Upload des PIP einbezogen.

   Führen Sie die folgenden Schritte aus, um den 3A6 PIP hochzuladen, der zu einer Back-End-Anwendung gesendet werden soll:
   a. Klicken Sie auf **Durchsuchen**, und wählen Sie `BCG_Package_RNSC1.0_RNIFV02.00_3C6V02.02.zip` aus.
   b. Stellen Sie sicher, dass **In Datenbank festschreiben** auf **Ja** gesetzt ist.
   c. Klicken Sie auf **Hochladen**.

   Der 3C6V02.02 PIP wird jetzt als Dokumentenfluss unter **Paket:Backend Integration/Protokoll:RNSC** auf der Seite **Dokumentenflussdefinitionen verwalten** angezeigt. Wenn WebSphere Partner Gateway kein Paket für den PIP oder die PIP-Version bereitstellt, die Sie verwenden wollen, können Sie Ihre eigenen erstellen und hochladen. Weitere Informationen finden Sie in „PIP-Dokumentenflusspakete erstellen" auf Seite 247.

Attributwerte konfigurieren

Für PIP-Dokumentenflussdefinitionen sind die meisten Attributwerte bereits gesetzt und müssen nicht konfiguriert werden. Allerdings müssen Sie die folgenden Attribute festlegen:

RNIF (1.0)-Paket

- **Globaler Lieferkettencode** - Geben Sie den Typ der Lieferkette an, die vom Teilnehmer verwendet wird. Zu den Typen gehören **Elektronische Komponenten**, **Informationstechnologie** und **Halbleiterfertigung**. Dieses Attribut hat keinen Standardwert.

RNIF (V02.00)-Paket

- **Verschlüsselung** - Legen Sie fest, ob die PIPs verschlüsselte Nutzinformationen, einen verschlüsselten Container und verschlüsselte Nutzinformationen oder keine Verschlüsselung haben müssen. Der Standardwert ist **Kein(e)**.
- **Sync-Bestätigung erforderlich** - Setzen Sie auf **Ja**, wenn der Teilnehmer die Empfangsbestätigung empfangen möchte. Setzen Sie auf **Nein**, wenn 200 angefordert wurden.
- **Sync unterstützt** - Legen Sie fest, ob der PIP Austauschvorgänge für Synchronnachrichten unterstützt. Der Standardwert ist **Nein**.

Beachten Sie, dass die PIPs, für die WebSphere Partner Gateway PIP-Dokumentenflusspakete bereitstellt, nicht synchron sind. Folglich müssen Sie die Attribute **Sync-Bestätigung erforderlich** und **Sync unterstützt** für diese PIPs nicht ändern.

Anmerkung: Das Verhalten des Attributs **Sync-Bestätigung erforderlich** ist für Einweg- und Zweiwege-PIPs verschieden. Bei einem Zweiwege-PIP nimmt, wenn **Sync-Bestätigung erforderlich** auf **Nein** gesetzt ist, diese Einstellung die Vorrangstellung ein, wenn **Nichtablehnung des Empfangs** auf **Ja** gesetzt ist. Angenommen, Sie senden z. B. ein 3A7 PIP mit den folgenden Einstellungen:

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

Sie empfangen für ein Zweiwege-PIP eine Fehlernachricht für ein Eingangsdokument. Bei einem Einweg-PIP sehen Sie allerdings das Eingangsdokument auf der Konsole und 0KB 200 wird an den Teilnehmer zurückgegeben.

Führen Sie die folgenden Schritte aus, um die Attribute festzulegen:

1. Klicken Sie auf **Hubadmin > Hubkonfiguration > Dokumentenflussdefinition**.
2. Klicken Sie auf das Symbol **Erweitern**, um einen Knoten individuell zur entsprechenden Dokumentenflussdefinitions-Ebene zu erweitern, oder wählen Sie **Alle** aus, um alle angezeigten Dokumentenflussdefinitions-Knoten zu erweitern.
3. Klicken Sie in der Spalte **Aktionen** auf das Symbol **Attributwerte bearbeiten** für das Paket (z. B. **Paket: RNIF (1.1)** oder **Paket: RNIF (V02.00)**), das Sie bearbeiten wollen.
4. Gehen Sie im Abschnitt **Attribute für Dokumentenflusskontexte** in die Spalte **Aktualisieren** des Attributs, das Sie festlegen wollen, und wählen Sie den neuen Wert aus, bzw. geben Sie ihn dort ein. Wiederholen Sie dies für jedes Attribut, das Sie festlegen wollen.
5. Klicken Sie auf **Speichern**.

Anmerkung: Sie können auch RosettaNet-Attribute auf der Verbindungsebene aktualisieren, indem Sie für die Quelle oder das Ziel auf **Attribute** klicken, und dann die Werte in die Spalte **Aktualisieren** eingeben oder dort ändern. Lesen Sie „Attribute angeben oder ändern” auf Seite 166.

Interaktionen erstellen

Der folgende Prozess beschreibt, wie Sie eine Interaktion zwischen einem Back-End-System und einem Teilnehmer erstellen. Beachten Sie, dass Sie eine Interaktion für jeden PIP erstellen müssen, den Sie senden wollen, und eine Interaktion für jeden PIP, den Sie empfangen wollen.

Bevor Sie anfangen, stellen Sie sicher, dass die entsprechenden RNIF-Dokumentenflussdefinitionen hochgeladen wurden und dass die Pakete für den PIP, den Sie verwenden wollen, hochgeladen wurden. Wenn Sie über die Funktion zum Generieren eines 0A1 PIP (Notification of Failure) verfügen wollen, stellen Sie sicher, dass Sie den PIP hochgeladen haben, wie in Schritt 9 auf Seite 75 beschrieben.

Führen Sie die folgenden Schritte aus, um eine Interaktion für einen besonderen PIP zu erstellen:

1. Klicken Sie auf **Hubadmin > Hubkonfiguration > Dokumentenflussdefinition**.
2. Klicken Sie auf **Interaktionen verwalten**.

3. Klicken Sie auf **Interaktion erstellen**.
4. Erweitern Sie die Baumstruktur **Quelle** auf die Ebene **Aktion**, und erweitern Sie die Baumstruktur **Ziel** auf die Ebene **Aktion**.
5. Wählen Sie in den Baumstrukturen die Dokumentenflussdefinitionen aus, die für den Quellenkontext und den Zielkontext verwendet werden sollen. Wenn z. B. der Teilnehmer der Initiator eines 3C6 PIP (eines PIP mit einer Aktion) ist, wählen Sie die folgenden Dokumentenflussdefinitionen aus:

Tabelle 5. 3C6 PIP von einem Teilnehmer initiiert

Quelle	**Ziel**
Paket: RNIF (V02.00)	Paket: Backend Integration (1.0)
Protokoll: RosettaNet (V02.00)	Protokoll: RNSC (1.0)
Dokumentenfluss: 3C6 (V01.00)	Dokumentenfluss: 3C6 (V01.00)
Aktivität: Notify of Remittance Advice	Aktivität: Notify of Remittance Advice
Aktion: Remittance Advice Notification Action	Aktion: Remittance Advice Notification Action

Wenn das Back-End-System der Initiator des 3C6 PIP ist, wählen Sie die folgenden Dokumentenflussdefinitionen aus:

Tabelle 6. 3C6 PIP von einem Back-End-System initiiert

Quelle	**Ziel**
Paket: Backend Integration (1.0)	Paket: RNIF (V02.00)
Protokoll: RNSC (1.0)	Protokoll: RosettaNet (V02.00)
Dokumentenfluss: 3C6 (V01.00)	Dokumentenfluss: 3C6 (V01.00)
Aktivität: Notify of Remittance Advice	Aktivität: Notify of Remittance Advice
Aktion: Remittance Advice Notification Action	Aktion: Remittance Advice Notification Action

Für einen Doppelaktions-PIP, wie z. B. 3A4 von einem Teilnehmer initiiert, wählen Sie die folgenden Dokumentenflussdefinitionen für die erste Aktion aus:

Tabelle 7. 3A4 PIP von einem Teilnehmer initiiert

Quelle	**Ziel**
Paket: RNIF (V02.00)	Paket: Backend Integration (1.0)
Protokoll: RosettaNet (V02.00)	Protokoll: RNSC (1.0)
Dokumentenfluss: 3A4 (V02.02)	Dokumentenfluss: 3A4 (V02.02)
Aktivität: Request Purchase Order	Aktivität: Request Purchase Order
Aktion: Purchase Order Request Action	Aktion: Purchase Order Request Action

Wenn ein Back-End-System den Doppelaktions-3A4 PIP initiiert, wählen Sie die folgenden Dokumentenflussdefinitionen für die erste Aktion aus:

Tabelle 8. 3A4 PIP von einem Back-End-System initiiert

Quelle	**Ziel**
Paket: Backend Integration (1.0)	Paket: RNIF (V02.00)
Protokoll: RNSC (1.0)	Protokoll: RosettaNet (V02.00)
Dokumentenfluss: 3A4 (V02.02)	Dokumentenfluss: 3A4 (V02.02)

Tabelle 8. 3A4 PIP von einem Back-End-System initiiert (Forts.)

Quelle	Ziel
Aktivität: Request Purchase Order	Aktivität: Request Purchase Order
Aktion: Purchase Order Request Action	Aktion: Purchase Order Request Action

6. Wählen Sie im Feld **Aktion** den Eintrag **Bidirektionale Konvertierung von RosettaNet und RosettaNet-Service-Content mit Validierung** aus.
7. Klicken Sie auf **Speichern**.
8. Wenn Sie einen Doppelaktions-PIP konfigurieren, wiederholen Sie die benötigten Schritte, um die Interaktion für die zweite Aktion zu erstellen. Wählen Sie z. B. die folgenden Dokumentenflussdefinitionen für die zweite Aktion für einen von einem Teilnehmer initiierten 3A4 PIP aus. Dies ist die Aktion, bei der das Back-End-System die Antwort sendet.

Tabelle 9. 3A4 PIP von einem Teilnehmer initiiert (zweite Aktion)

Quelle	Ziel
Paket: Backend Integration (1.0)	Paket: RNIF (V02.00)
Protokoll: RNSC (1.0)	Protokoll: RosettaNet (V02.00)
Dokumentenfluss: 3A4 (V02.02)	Dokumentenfluss: 3A4 (V02.02)
Aktivität: Request Purchase Order	Aktivität: Request Purchase Order
Aktion: Purchase Order Confirmation Action	Aktion: Purchase Order Confirmation Action

Wählen Sie für die zweite Aktion für einen von einem Back-End-System initiierten 3A4 PIP die folgenden Dokumentenflussdefinitionen aus:

Tabelle 10. 3A4 PIP von einem Back-End-System initiiert (zweite Aktion)

Quelle	Ziel
Paket: RNIF (V02.00)	Paket: Backend Integration (1.0)
Protokoll: RosettaNet (V02.00)	Protokoll: RNSC (1.0)
Dokumentenfluss: 3A4 (V02.02)	Dokumentenfluss: 3A4 (V02.02)
Aktivität: Request Purchase Order	Aktivität: Request Purchase Order
Aktion: Purchase Order Confirmation Action	Aktion: Purchase Order Confirmation Action

9. Wenn Sie **0A1 Notification of Failure** generieren wollen, erstellen Sie eine Interaktion für XMLEvent.
   a. Klicken Sie auf **Hubadmin > Hubkonfiguration > Dokumentenflussdefinition**.
   b. Klicken Sie auf **Interaktionen verwalten**.
   c. Klicken Sie auf **Interaktion erstellen**.
   d. Erweitern Sie die Baumstruktur **Quelle** auf die Ebene **Dokumentenfluss**, und erweitern Sie die Baumstruktur **Ziel** auf die Ebene **Dokumentenfluss**.
   e. Wählen Sie die folgenden Dokumentenflussdefinitionen aus:

Tabelle 11. Dokumentenflussdefinition für XMLEvent

Quelle	Ziel
Paket: Backend Integration (1.0)	Paket: Backend Integration (1.0)
Protokoll: XMLEvent (1.0)	Protokoll: XMLEvent (1.0)
Dokumentenfluss: XMLEvent (1.0)	Dokumentenfluss: XMLEvent (1.0)

f. Wählen Sie im Feld **Aktion** die Option **Pass-Through** aus.

g. Klicken Sie auf **Speichern**.

10. Erstellen Sie eine Interaktion für XMLEvent zu 0A1 RNSC.

a. Klicken Sie auf **Hubadmin > Hubkonfiguration > Dokumentenfluss-definition**.

b. Klicken Sie auf **Interaktionen verwalten**.

c. Klicken Sie auf **Interaktion erstellen**.

d. Erweitern Sie die Baumstruktur **Quelle** auf die Ebene **Dokumentenfluss**, und erweitern Sie die Baumstruktur **Ziel** auf die Ebene **Aktivität**.

e. Wählen Sie die folgenden Dokumentenflussdefinitionen aus:

Tabelle 12. Dokumentenflussdefinition für XMLEvent zu 0A1

Quelle	Ziel
Paket: Backend Integration (1.0)	Paket: Backend Integration (1.0)
Protokoll: XMLEvent (1.0)	Protokoll: RNSC (1.0)
Dokumentenfluss: XMLEvent (1.0)	Dokumentenfluss: 0A1 (V02.00)
	Aktivität: Distribute Notification of Failure.

f. Wählen Sie im Feld **Aktion** den Eintrag **Bidirektionale Konvertierung von RosettaNet und XML mit Validierung** aus.

g. Klicken Sie auf **Speichern**.

Web-Services

Ein Teilnehmer kann einen Web-Service anfordern, der von Community Manager bereitgestellt wird. In ähnlicher Weise kann Community Manager einen Web-Service anfordern, der von einem Teilnehmer bereitgestellt wird. Der Teilnehmer oder Community Manager rufen den WebSphere Partner Gateway-Server auf, um den Web-Service zu erhalten. WebSphere Partner Gateway agiert als Proxy-Server, der die Web-Serviceanforderung an den Web-Service-Provider übergibt und die Antwort synchron vom Provider an den Requester zurückgibt.

Dieser Abschnitt enthält die folgenden Informationen für das Konfigurieren eines Web-Services zur Verwendung durch einen Teilnehmer oder Community Manager:

- Die Teilnehmer für einen Web-Service angeben
- Dokumentenflussdefinition für einen Web-Service konfigurieren
- Dokumentenflussdefinitionen der B2B-Funktionalität des Teilnehmers hinzufügen
- Einschränkungen und Begrenzungen der Web-Serviceunterstützung

Die Teilnehmer für einen Web-Service angeben

Wenn ein Web-Service von Community Manager zur Verwendung durch Teilnehmer bereitgestellt wird, erfordert WebSphere Partner Gateway, dass ein Teilnehmer sich selbst angibt. Wenn die Web-Serviceanforderung übergeben wird, legen Sie die Identität auf eine der folgenden zwei Arten fest:

1. Verwenden Sie die HTTP-Basisauthentifizierung mit einer Benutzer-ID im Format *<geschäfts-id_des_teilnehmers>/<konsolbenutzername>* (Beispiel: 123456789/joesmith) und ein Kennwort, das dem Kennwort des Konsolbenutzernamens entspricht.

2. Stellen Sie ein SSL-Clientzertifikat bereit, das zuvor in WebSphere Partner Gateway für den Teilnehmer geladen wurde.

Wenn der Web-Service von einem Teilnehmer für die Verwendung durch Community Manager zur Verfügung gestellt wird, sollte die öffentliche URL-Adresse, mit der Community Manager den Web-Service aufruft, die Abfragezeichenfolge `?to=<geschäfts-ID_des_teilnehmers>` enthalten. Beispiel:

`http://<IP-adresse>/bcgreceiver/Receiver?to=123456789`

Dadurch erfährt WebSphere Partner Gateway, dass der Provider des Web-Services der Teilnehmer mit der Geschäfts-ID 123456789 ist.

Dokumentenflussdefinitionen erstellen

Um die Dokumentenflussdefinition zu konfigurieren, laden Sie entweder die WSDL-Dateien (Web Service Definition Language) hoch, die den Web-Service definieren, oder Sie geben die entsprechenden Dokumentenflussdefinitionen manuell über Community Console ein.

Die WSDL-Dateien für einen Web-Service hochladen

Die Definition für einen Web-Service sollte in einer primären WSDL-Datei mit der Erweiterung `.wsdl` enthalten sein, welche zusätzliche WSDL-Dateien über das Element `import` importieren könnte.Wenn importierte Dateien vorhanden sind, können diese mit der Primärdatei unter Verwendung einer der folgenden Methoden hochgeladen werden:

- Wenn der Dateipfad oder (HTTP) URL im Attribut `location` von jedem Element `import` vom Community Console-Server (nicht die Maschine des Benutzers) erreicht werden kann, kann die Primärdatei direkt hochgeladen werden und die importierten Dateien werden automatisch hochgeladen.
- Wenn alle importierten Dateien und die Primärdatei in eine einzelne Datei komprimiert sind, jede mit einem Pfad, der dem Pfad (sofern vorhanden) im Importattribut `location` entspricht, wird das Hochladen der komprimierten Datei alle enthaltenen Primär- und Import-WSDL-Dateien hochladen.

Angenommen, die Primär-WSDL-Datei `helloworldRPC.wsdl` enthält z. B. das folgende Importelement:

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

Und angenommen, die importierte WSDL-Datei `bindingRPC.wsdl` enthält das folgende Importelement:

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

Die Datei sollte das Folgende enthalten:

```
Name                        Path

helloworldRPC.wsdl

bindingRPC.wsdl

porttypeRPC.wsdl            port\
```

Wenn eine WSDL-Dateidefinition eines Web-Services hochgeladen wird, wird die ursprüngliche WSDL als Validierungszuordnung gespeichert. (Web-Servicenach-

richten werden tatsächlich von WebSphere Partner Gateway nicht validiert. Sie werden direkt mit dem ursprünglichen Serviceendpunkt-URL weitergeleitet.) Dies wird als *private* WSDL bezeichnet.

Daneben wird eine öffentliche WSDL gespeichert, bei der der private URL durch den Ziel-URL ersetzt wird, der auf der Seite **Pakete hoch-/herunterlade** angegeben ist. Die öffentliche WSDL wird den Benutzern des Web-Services zur Verfügung gestellt, die den Web-Service am URL des Ziels (dem öffentlichen URL) aufrufen werden. WebSphere Partner Gateway wird dann die Web-Serviceanforderung an ein Gateway weiterleiten, das der private URL des ursprünglichen Web-Service-Providers ist. WebSphere Partner Gateway agiert als Proxy-Server, der die Web-Serviceanforderung an einen privaten Provider-URL weiterleitet, welcher für den Web-Servicebenutzer verdeckt ist.

Sowohl die private als auch die öffentliche WSDL (einschließlich aller importierten Dateien) können von Community Console hochgeladen werden, nachdem die WSDL hochgeladen wurde.

WSDL-Dateien mit Community Console hochladen: WebSphere Partner Gateway stellt eine Möglichkeit zum Importieren von WSDL-Dateien bereit. Wenn ein Web-Service in einer einzelnen WSDL-Datei definiert ist, können Sie die WSDL-Datei direkt hochladen. Wenn der Web-Service mit mehreren WSDL-Dateien definiert ist, dies ist der Fall, wenn Sie WSDL-Dateien innerhalb einer Primär-WSDL-Datei importiert haben, würden diese in einem komprimierten Archiv hochgeladen.

Wichtig: Die WSDL-Dateien in dem komprimierten Archiv müssen in einem Verzeichnis sein, das im WSDL-Importelement angegeben ist. Angenommen, Sie verfügen z. B. über das folgende Importelement:

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

Die Verzeichnisstruktur im komprimierten Archiv würde wie folgt lauten: `path1/bindingRPC.wsdl`.

Sehen Sie sich jetzt dieses Beispiel an:

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

Die Datei `bindingRPC.wsdl` würde sich im komprimierten Archiv auf der Stammverzeichnisebene befinden.

Gehen Sie wie folgt vor, um eine einzelne WSDL-Datei oder ein einzelnes gezipptes Archiv hochzuladen:

1. Klicken Sie auf **Hubadmin** > **Hubkonfiguration** > **Dokumentenflussdefinition**.
2. Klicken Sie auf **Pakete hoch-/herunterladen**.
3. Klicken Sie für **WSDL-Paket** auf **Ja**.
4. Führen Sie für **Öffentliche Web-Service-URL-Adresse** einen der folgenden Schritte aus:
   - Geben Sie für einen von Community Manager bereitgestellten Web-Service (der von einem Teilnehmer aufgerufen wird), die öffentliche URL-Adresse des Web-Services ein. Beispiel:

     `https://<ziel_host:port>/bcgreceiver/Receiver`

Die URL-Adresse ist in der Regel dieselbe wie das HTTP-Produktionsziel, das in **Ziele** definiert ist.

- Geben Sie für einen von einem Teilnehmer bereitgestellten Web-Service (der von Community Manager aufgerufen wird), die öffentliche URL-Adresse des Teilnehmers mit einer Abfragezeichenfolge ein: Beispiel:

  `https://<ziel_host:port>/bcgreceiver/Receiver?to=<geschäfts-id des teilnehmers>`

5. Klicken Sie auf **Durchsuchen**, und wählen Sie die WSDL-Datei oder das komprimierte Archiv aus.
6. Wählen Sie für **In Datenbank festschreiben** die Option **Nein** aus, wenn Sie die Datei in Testmodus hochladen wollen. Wenn Sie **Nein** auswählen, wird die Datei nicht auf dem System installiert. Verwenden Sie die vom System generierten Nachrichten, die im Fenster **Nachrichten** angezeigt werden, um Fehler bei der Hochladeoperation zu beheben. Wählen Sie **Ja** aus, um die Datei in die Systemdatenbank hochzuladen.
7. Wählen Sie für **Daten überschreiben** die Option **Ja** aus, um eine Datei zu ersetzen, die sich gerade in der Datenbank befindet. Wählen Sie **Nein** aus, um die Datei der Datenbank hinzuzufügen.
8. Klicken Sie auf **Hochladen**. Die WSDL-Datei wird auf dem System installiert.

Pakete mit Schemadateien validieren: Eine Gruppe von XML-Schemata, die die XML-Dateien beschreiben, welche über die Konsole hochgeladen werden können, wird auf dem WebSphere Partner Gateway-Installationsdatenträger bereitgestellt. Hochgeladene Dateien werden mit diesen Schemata validiert. Die Schemadateien sind eine hilfreiche Referenz zur Bestimmung von Fehlerursachen, wenn eine Datei aufgrund eines XML-Fehlers nicht hochgeladen werden kann. Zu diesen Dateien gehören `wsdl.xsd`, `wsdlhttp.xsd` und `wsdlsoap.xsd`, die das Schema enthalten, das die gültigen WSDL-Dateien (WSDL - Web Service Definition Language) beschreibt.

Die Dateien befinden sich in: `B2BIntegrate\packagingSchemas`

Die Dokumentenflussdefinition manuell erstellen

Um die entsprechenden Dokumentenflussdefinitionen manuell einzugeben, befolgen Sie die Prozeduren in diesem Abschnitt. Sie müssen auch die Einträge **Dokumentenfluss**, **Aktivität** und **Aktion** einzeln unter **Protokoll: Web Service** erstellen. Beachten Sie dabei besonders die Anforderungen für die Aktion und ihre Beziehung zu den empfangenen SOAP-Nachrichten.

In Bezug auf die Hierarchie von **Paket/Protokoll/Dokumentenfluss/Aktivität/Aktion** der Dokumentenflussdefinitionen wird ein unterstützter Web-Service wie folgt dargestellt:

- **Paket: None**
- **Protokoll: Web Service (1.0)**
- **Dokumentenfluss:** {*<web-service-namespace>*:*<web-service-name>*} (Name und Code). Dieser muss unter den Dokumentenflüssen für das Web-Service-Protokoll eindeutig sein. Dies ist in der Regel der WSDL-Namespace und -Name.
- **Aktivität:** Eine Aktivität für jede Web-Service-Operation mit Name und Code:

  {*<operationsnamespace>*}:*<operationsname>*
- **Aktion:** Eine Aktion für die Eingabenachricht jeder Operation mit Name und Code:

  {*<namespace_des_angebenden_xml-elements = erstes_untergeordnetes_element_von_soap:body>*}:
  <name_des_angebenden_xml-elements = erstes_untergeordnetes_element_von_soap:body>

Die Aktionen sind die kritischen Definitionen, da WebSphere Partner Gateway den Namespace und den Namen einer Aktion verwendet, um eine eingehende Web-Serviceanforderungs-SOAP-Nachricht zu erkennen und diese auf einer definierten Teilnehmerverbindung basierend entsprechend weiterzuleiten. Der Namespace und Name des ersten untergeordneten XML-Elements vom Element `soap:body` der empfangenen SOAP-Nachricht muss mit einem Namespace und Namen einer bekannten Aktion in den Dokumentenflussdefinitionen von WebSphere Partner Gateway übereinstimmen.

Angenommen, eine Web-Serviceanforderungs-SOAP-Nachricht für eine SOAP-Bindung **document-literal**) sieht z. B. wie folgt aus:

```
<?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 würde nach einer definierten Web-Serviceaktion mit diesem Code suchen:

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

Beispiel einer SOAP-Anforderungsnachricht im RPC-Bindungsstil:

```
<?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 würde nach einer definierten Web-Serviceaktion mit diesem Code suchen:

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

Bei einer RPC-Bindung sollte der Namespace und Name des ersten untergeordneten Elements vom `soap:body` einer SOAP-Anforderungsnachricht der Namespace und Name der gültigen Web-Serviceoperation sein.

Bei einer Bindung **document-literal** sollte der Namespace und Name des ersten untergeordneten Elements vom `soap:body` einer SOAP-Anforderungsnachricht der

Namespace und Name des XML-Attributs `element` im Element `part` der Eingabedefinition `message` für den Web-Service sein.

Interaktionen erstellen

Zum Erstellen einer Interaktion für einen Web-Service verwenden Sie dieselbe Web-Service-Dokumentenflussaktion für sowohl die Quelle als auch das Ziel.

Verwenden Sie die folgende Prozedur, um Interaktionen zu erstellen.

1. Klicken Sie auf **Hubadmin** > **Hubkonfiguration** > **Dokumentenflussdefinition**.
2. Klicken Sie auf **Interaktionen verwalten**.
3. Klicken Sie auf **Interaktion erstellen**.
4. Erweitern Sie unter **Quelle** den Eintrag **Paket: None > Protokoll: Web Service > Dokumentenfluss: <** *dokumentenfluss*> **> Aktion:** <*aktion*>. Wiederholen Sie diesen Schritt in der Spalte **Ziel**.
5. Wählen Sie **Pass-Through** in der Liste **Aktion** unten auf der Seite aus. (**Pass-Through** ist die einzige gültige Option, die von WebSphere Partner Gateway für einen Web-Service unterstützt wird.)

Einschränkungen und Begrenzungen der Web-Serviceunterstützung

WebSphere Partner Gateway unterstützt die folgenden Standards:

- WSDL 1.1
- SOAP 1.1
- WS-I Basic Profile v. 1.0 (enthält wichtige Einschränkungen im Format der SOAP-Nachrichten für die Bindung **document-literal**)

Anmerkung:

- SOAP/HTTP-Bindung wird unterstützt.
- Erneute Bindeoperation wird nicht unterstützt.
- Die Bindungsarten **RPC-encoded/RPC-literal** und **document-literal** werden unterstützt (gemäß den Einschränkungen im WS-I Basic Profile).
- Soap With Attachments wird nicht unterstützt.

cXML-Dokumente

Dieser Abschnitt enthält eine Übersicht über die cXML-Unterstützung und Informationen dazu, wie Sie Dokumentenflussdefinitionen für cXML-Austauschvorgänge erstellen.

Übersicht

WebSphere Partner Gateway Document Manager gibt ein cXML-Dokument durch den Stammelementnamen des XML-Dokuments, der `cXML` lautet, und die Version an, die mit dem cXML-DOCTYPE (DTD) angegeben wird. Der folgende DOCTYPE ist z. B. cXML-Version 1.2.009:

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

Document Manager führt die DTD-Validierung für cXML-Dokumente aus; WebSphere Partner Gateway stellt jedoch keine cXML-DTDs bereit. Sie können diese unter `www.cxml.org` herunterladen, und sie dann in WebSphere Partner Gateway über das Validierungszuordnungsmodul in Community Console hochladen.

Nachdem Sie die DTD hochgeladen haben, ordnen Sie diese dem cXML-Dokumentenfluss zu. Weitere Informationen zum Zuordnen der DTD zum cXML-Dokumentenfluss finden Sie in „Zuordnungen zu Dokumentenflussdefinitionen zuordnen” auf Seite 92.

Document Manager verwendet zwei Attribute des cXML-Rootelements für die Dokumentverwaltung: **payloadID** und **timestamp**. **payloadID** und **timestamp** werden als Dokument-ID-Nummer und Dokumentzeitmarke verwendet. Beide können in Community Console für die Dokumentverwaltung angezeigt werden.

Die Elemente **From** und **To** im cXML-Header enthalten das Element **Credential**, das für die Dokumentweiterleitung und -authentifizierung verwendet wird. Das Beispiel stellt die Elemente **From** und **To** als die Quelle und das Ziel des cXML-Dokuments dar.

Anmerkung: An dieser Stelle und im ganzen Handbuch sind die verwendeten DUNS-Nummern, nur als Beispiele zu verstehen.

```
<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>
```

Wenn mehr als ein Element **Credential** verwendet wird, verwendet Document Manager die DUNS-Nummer als Geschäftskennung für die Weiterleitung und Authentifizierung. In dem Fall, wenn keine DUNS-Nummer vorgegeben ist, wird das erste Element **Credential** verwendet.

WebSphere Partner Gateway verwendet nicht die Informationen im Absenderelement.

Bei einer synchronen Transaktion wird der Header **From** und **To** in einem cXML-Antwortdokument nicht verwendet. Das Antwortdokument wird über dieselbe HTTP-Verbindung gesendet, die vom Anforderungsdokument hergestellt wurde.

cXML-Dokumenttypen

Es gibt die folgenden drei cXML-Dokumenttypen: Anforderung, Antwort oder Nachricht.

Anforderung: Es gibt viele Typen von cXML-Anforderungen. Das Element `Request` im cXML-Dokument entspricht der Dokumentenflussdefinition in WebSphere Partner Gateway. Typische Anforderungselemente:

- OrderRequest
- ProfileRequest
- PunchOutSetupRequest
- StatusUpdateRequest

- GetPendingRequest
- ConfirmationRequest
- ShipNoticeRequest

Die folgende Tabelle zeigt die Beziehung zwischen den Elementen in einem cXML-Anforderungsdokument und den Dokumentenflussdefinitionen in WebSphere Partner Gateway:

cXML-Element	**Dokumentenflussdefinition**
cXML-DOCTYPE	Protokoll
DTD-Version	Protokollversion
Anforderungstyp Beispiel: OrderRequest	Dokumentenfluss

Antwort: Der Zielteilnehmer sendet eine cXML-Antwort, um den Quellenteilnehmer über die Ergebnisse der cXML-Anforderung zu informieren. Da die Ergebnisse einiger Anforderungen unter Umständen über keine Daten verfügen, kann das Element `Response` optional nichts außer einem Element `Status` enthalten. Ein Element `Response` kann auch Daten der Anwendungsebene enthalten. Während Punchout sind z. B. die Daten der Anwendungsebene in einem Element `PunchOutSetupResponse` enthalten. Zu den typischen Elementen `Response` gehören:
- ProfileResponse
- PunchOutSetupResponse
- GetPendingResponse

Die folgende Tabelle zeigt die Beziehung zwischen den Elementen in einem cXML-Antwortdokument und den Dokumentenflussdefinitionen in WebSphere Partner Gateway:

cXML-Element	**Dokumentenflussdefinition**
cXML-DOCTYPE	Protokoll
DTD-Version	Protokollversion
Antworttyp Beispiel: ProfileResponse	Dokumentenfluss

Nachricht: Eine cXML-Nachricht enthält die WebSphere Partner Gateway-Dokumentenflussinformation im cXML-Element `Message`. Es kann optional ein Element `Status` enthalten, das mit dem im Element `Response` identisch ist. Es würde in Nachrichten verwendet, die Antworten auf Anforderungsnachrichten sind.

Der Inhalt der Nachricht ist durch die Geschäftsanforderungen der Benutzer kundenspezifisch. Das Element direkt unterhalb dem Element `<Message>` entspricht dem Dokumentenfluss, der in WebSphere Partner Gateway erstellt wurde.Im folgenden Beispiel ist SubscriptionChangeMessage der Dokumentenfluss:

```
<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>
```

Die folgende Tabelle zeigt die Beziehung zwischen den Elementen in einer cXML-Nachricht und den Dokumentenflussdefinitionen in WebSphere Partner Gateway:

cXML-Element	Dokumentenflussdefinition
cXML-DOCTYPE	Protokoll
DTD-Version	Protokollversion
Nachricht	Dokumentenfluss

Sie können den Unterschied zwischen einer Einwegnachricht und einem Anforderungs-/Antwortdokument am einfachsten dadurch feststellen, ob ein Element `Message` anstelle eines Anforderungs- oder Antwortelements vorhanden ist.

Eine Nachricht kann über die folgenden Attribute verfügen:

- `deploymentMode`. Gibt an, ob die Nachricht ein Testdokument oder ein Produktionsdokument ist. Zulässige Werte sind **production** (Standardwert) oder **test**.
- `inReplyTo`. Gibt an, auf welche Nachricht diese Nachricht antwortet. Der Inhalt des Attributs `inReplyTo` ist die `payloadID` einer Nachricht, die zuvor empfangen wurde. Diese würde für die Erstellung einer Zweiwegetransaktion mit vielen Nachrichten verwendet werden.

Die Header ″Content-Type″ und angehängte Dokumente

Alle cXML-Dokumente müssen einen Header **Content-Type** enthalten. Für cXML-Dokumente ohne Anhänge werden die folgenden Header **Content-Type** verwendet:

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

Das cXML-Protokoll unterstützt das Anhängen von externen Dateien über MIME. Käufer müssen z. B. oft die Bestellungen mit unterstützenden Kurzinformationen, Zeichnungen oder per Fax verdeutlichen. Einer der Header **Content-Type**, die unten in der Liste gezeigt werden, muss in cXML-Dokumenten verwendet werden, die Anhänge enthalten:

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

Das Element `boundary` ist ein beliebiger eindeutiger Text, der den Hauptteil vom payload-Abschnitt (Nutzinformationen) der MIME-Nachricht trennt. Weitere Informationen finden Sie im *cXML User Guide* unter `www.cxml.org`.

Gültige cXML-Interaktionen

WebSphere Partner Gateway unterstützt die folgenden cXML-Dokumentenflussdefinitionsinteraktionen:

- Vom Teilnehmer zu Community Manager: None/cXML zu None/cXML mit Pass-Through und Validierung
- Vom Community Manager zum Teilnehmer:
  - None/cXML zu None/cXML mit Pass-Through und Validierung
  - None/XML zu None/cXML mit Pass-Through, Validierung und Transformation

Dokumentenflussdefinitionen erstellen

Verwenden Sie den folgenden Prozess, um eine neue Dokumentenflussdefinition für ein cXML-Dokument zu erstellen.

Anmerkung: Sie müssen sicherstellen, dass die korrekte Version von cXML definiert ist, bevor Sie eine cXML-Dokumentenflussdefinition erstellen. Der Standardwert ist Version 1.2.009.

1. Klicken Sie auf **Hubadmin** > **Hubkonfiguration** > **Dokumentenflussdefinition**.
2. Klicken Sie auf **Dokumentenflussdefinition erstellen**. Die Seite **Dokumentenflussdefinitionen erstellen** wird angezeigt.
3. Wählen Sie **Dokumentenfluss** als Dokumentenflusstyp aus.
4. Führen Sie eine der folgenden Aufgaben abhängig vom Dokumenttyp aus:
   - Geben Sie für Anforderungen den Anforderungstyp, z. B. `OrderRequest`, in die Felder **Code** und **Name** ein.
   - Geben Sie für Antworten, falls das Element `Response` über keine untergeordneten Tags außer `<Status>` verfügt, `Response` ein. Andernfalls geben Sie den nächsten Tag-Namen ein, der auf `<Status>` folgt. Im nachfolgenden Beispiel würden Sie `Response` für das erste Element `Response` und `ProfileResponse` für das zweite Element eingeben.

     ```
     <cXML>
         <Response>
             <Status code="200" text="OK"/>
         </Response>
     </cXML>
     <cXML>
         <Response>
             <Status code="200" text="OK"/>
        <ProfileResponse>
         </Response>
     </cXML>
     ```
5. Geben Sie **1.0** für **Version** ein.

   Die Versionsnummer dient nur zu Referenzzwecken. Die tatsächliche Protokollversion wird von der DTD-Version im cXML-Dokument abgeleitet.
6. Geben Sie eine optionale **Beschreibung** ein.
7. Wählen Sie **Ja** für **Dokumentebene** aus.
8. Wählen Sie **Aktiviert** als **Status** aus.
9. Wählen Sie **Ja** für alle Attribute **Sichtbarkeit** aus.
10. Klicken Sie auf den Ordner **Paket: None**, um die Paketauswahloptionen zu erweitern.
11. Wählen Sie **Protokoll: cXML (1.2.009): cXML** aus.
12. Klicken Sie auf **Speichern**.

Interaktionen erstellen

Nachdem Sie die Dokumentenflussdefinition erstellt haben, konfigurieren Sie eine Interaktion für das cXML-Dokument.

Verwenden Sie die folgende Prozedur, um Interaktionen zu erstellen.

1. Klicken Sie auf **Hubadmin** > **Hubkonfiguration** > **Dokumentenflussdefinition**.
2. Klicken Sie auf **Interaktionen verwalten**.
3. Klicken Sie auf **Interaktion erstellen**.

4. Wenn das cXML-Dokument die Quelle ist, erweitern Sie unter **Quelle** den Eintrag **Paket: None** und **Protokoll: cXML**, und wählen Sie **Dokumentenfluss**<*dokumentenfluss*> aus. Wenn das cXML-Dokument das Ziel ist, erweitern Sie **Paket: None** und **Protokoll: cXML**, und wählen Sie **Dokumentenfluss:** <*dokumentenfluss*> in der Spalte **Ziel** aus.
5. Erweitern Sie die Quellen- bzw. Zielspalte für die andere Hälfte der Interaktion (das Dokument, das in cXML konvertiert wird, bzw. das Dokument, das von cXML transformiert wird), und erweitern Sie sein Paket und Protokoll, und wählen Sie seinen Dokumentenfluss aus.
6. Wählen Sie **Pass-Through** in der Liste **Aktion** unten auf der Seite aus. (**Pass-Through** ist die einzige gültige Option, die für cXML-Dokumente unterstützt wird.)

Angepasste XML-Dokumente

Dieser Abschnitt beschreibt, wie Sie angepasste XML-Dokumente erstellen.

Übersicht

XML (Extensible Markup Language) ist das universale Format für gegliederte Dokumente und Daten im Web. Sie können mit der Seite **XML-Formate verwalten** angepasste XML-Formate erstellen und verwalten, die der Liste verfügbarer Dokumentenflussdefinitionen hinzugefügt werden können.

Ein XML-Format definiert die Pfade innerhalb einer Gruppe von XML-Dokumenten. Dies ermöglicht Document Manager, die Werte abzurufen, die ein Eingangsdokument eindeutig identifizieren, und auf die Informationen im Dokument zuzugreifen, die für die ordnungsgemäße Weiterleitung und Verarbeitung nötig sind.

Das Erstellen eines XML-Formats ist ein Prozess, der aus mehreren Schritten besteht. Sie müssen Folgendes ausführen:

1. Erstellen Sie ein Protokoll für das Format, und ordnen Sie es einem Paket bzw. Paketen zu.
2. Erstellen Sie einen Dokumentenfluss für das Format, und ordnen Sie ihn dem neu erstellten Protokoll zu.
3. Erstellen Sie das Format.

Sie erstellen dann eine gültige Interaktion für das neu erstellte Format.

Diese Schritte werden in den folgenden Abschnitten beschrieben. Sie können auch ein Beispiel zu diesen Schritten in „Den Hub für angepasste XML-Dokumente konfigurieren" auf Seite 207 finden.

Protokolldefinitionsformat erstellen

Die folgenden Schritte beschreiben, wie Sie ein angepasstes XML-Protokolldefinitionsformat erstellen:

1. Klicken Sie auf **Hubadmin > Hubkonfiguration > Dokumentenflussdefinition > Dokumentenflussdefinition erstellen**.
2. Wählen Sie als **Dokumentenflusstyp** den Eintrag **Protokoll** aus.

3. Geben Sie für **Code** den Wert für den Objekttyp an, den Sie im vorherigen Schritt ausgewählt haben. Sie könnten z. B. `XML` eingeben.
4. Geben Sie für **Name** eine Kennung für die Dokumentenflussdefinition ein. Sie könnten z. B. für ein angepasstes XML-Protokoll `Custom_XML` eingeben. Dieses Feld ist erforderlich.
5. Geben Sie als **Version** die Nummer **1.0** ein.
6. Geben Sie eine optionale Beschreibung des Protokolls ein.
7. Setzen Sie **Dokumentebene** auf **Nein**, da Sie ein Protokoll definieren, und keinen Dokumentenfluss, den werden Sie im nächsten Abschnitt definieren.
8. Setzen Sie **Status** auf **Aktiviert**.
9. Legen Sie für dieses Protokoll **Sichtbarkeit** fest. Sie wollen es möglicherweise für alle Teilnehmer sichtbar machen.
10. Wählen Sie die Pakete aus, in denen dieses neue Protokoll gepackt sein wird. Wenn Sie z. B. wollen, dass dieses Protokoll den Paketen **AS**, **None** und **Backend Integration** zugeordnet werden soll, wählen Sie **Paket: AS**, **Paket: None**, und **Paket: Backend Integration** aus.
11. Klicken Sie auf **Speichern**.

Dokumentenflussdefinition erstellen

Verwenden Sie als Nächstes wieder die Seite **Dokumentenflussdefinition erstellen**, um einen Dokumentenfluss zu erstellen.

1. Klicken Sie auf **Hubadmin > Hubkonfiguration > Dokumentenflussdefinition > Dokumentenflussdefinition erstellen**.
2. Wählen Sie als **Dokumentenflusstyp** den Eintrag **Dokumentenfluss** aus.
3. Geben Sie für **Code** den Wert für den Objekttyp (Dokumentenfluss) an, den Sie im vorherigen Schritt ausgewählt haben.
4. Geben Sie für **Name** eine Kennung für die Dokumentenflussdefinition ein. Sie könnten z. B. `XML_Tester` als einen Namen für den Dokumentenfluss eingeben. Dieses Feld ist erforderlich.
5. Geben Sie als **Version** die Nummer **1.0** ein.
6. Geben Sie eine optionale Beschreibung des Protokolls ein.
7. Setzen Sie die **Dokumentebene** auf **Ja**, weil Sie eine Dokumentebene definieren.
8. Setzen Sie **Status** auf **Aktiviert**.
9. Legen Sie für diesen Fluss **Sichtbarkeit** fest. Sie wollen es möglicherweise für alle Teilnehmer sichtbar machen.
10. Klicken Sie auf das Symbol **Erweitern**, um jedes Paket zu erweitern, das Sie in Schritt 10 ausgewählt haben. Erweitern Sie den Ordner, und wählen Sie den Namen des Protokolls aus, das Sie im vorherigen Abschnitt erstellt haben (z. B. das Protokoll: CustomXML).
11. Klicken Sie auf **Speichern**.

Die Seite **Dokumentenflussdefinitionen verwalten** enthält nun einen Dokumentenfluss von `XML_Tester` und ein Protokoll `CustomXML` unter den Paketen **AS**, **None** und **Backend Integration**.

XML-Format erstellen

Nachdem Sie ein angepasstes XML-Protokoll erstellt (und es einem Paket oder einer Gruppe von Paketen zugeordnet) sowie einen zugeordneten Dokumentenfluss erstellt haben, können Sie das XML-Format erstellen.

Verwenden Sie die folgende Prozedur, um ein XML-Format zu erstellen:

1. Klicken Sie auf **Hubadmin > Hubkonfiguration > XML-Formate**.
2. Klicken Sie auf **XML-Format erstellen**.
3. Wählen Sie für **Routing-Format** die Dokumentenflussdefinition aus, der dieses Format zugeordnet ist.
4. Wählen Sie für **Dateityp** den Eintrag **XML** aus.

   Anmerkung: XML ist die einzige Option, die für diesen Dateityp verfügbar ist.
5. Wählen Sie für **Kennungstyp** das Element aus, das zur Angabe des Eingangsdokumententyps verwendet wird. Die Auswahlmöglichkeiten sind **DTD**, **Namespace**, oder **Root-Tag**.
6. Für jedes Feld, für das eine Auswahlmöglichkeit angeboten wird, wählen Sie entweder **Elementpfad**, dies ist der Pfad zu dem Wert im Dokument, oder **Konstante** aus, dies ist der tatsächliche Wert im Dokument. Stellen Sie dann einen Wert bereit.
   a. Geben Sie für **Quellengeschäfts-ID/Zielgeschäfts-ID** den Pfad der Geschäfts-ID ein. Dieses Feld ist erforderlich.
   b. Geben Sie für **Quellendokumentenfluss** und **Quellendokumentenflussversion** einen Ausdruck ein, der den Pfad zum Dokumentenfluss und den Versionswert innerhalb des XML-Dokuments definiert. Dieses Feld ist erforderlich.
   c. Geben Sie für **Dokumentkennung** den Pfad für die Dokument-ID-Nummer ein.
   d. Geben Sie für **Dokumentzeitmarke** den Pfad für die Zeitmarke der Dokumenterstellung ein.
   e. Geben Sie für **Duplikatprüfschlüssel 1-5** die Pfade ein, mit denen die Weiterleitung einer Kopie eines Dokuments angegeben werden.
7. Klicken Sie auf **Speichern**.

Validierungszuordnungen verwenden

WebSphere Partner Gateway verwendet Validierungszuordnungen, um die Struktur von bestimmten Dokumenten zu validieren. Wenn Sie einem Dokument eine Validierungszuordnung zuordnen wollen, stellen Sie zuerst sicher, dass die Validierungszuordnung WebSphere Partner Gateway zur Verfügung steht, wie in „Validierungszuordnungen hinzufügen" beschrieben.

Validierungszuordnungen hinzufügen

Eine Aktion kann über eine zugeordnete Validierungszuordnung verfügen, um sicherzustellen, dass der Zielteilnehmer bzw. das Back-End-System das Dokument syntaktisch analysieren kann. Beachten Sie, dass eine Validierungszuordnung nur die *Struktur* des Dokuments validiert. Sie validiert nicht den Inhalt der Nachricht.

Anmerkung: Sobald Sie eine Validierungszuordnung einer Dokumentenflussdefinition zugeordnet haben, können Sie diese Zuordnung nicht mehr aufheben.

Verwenden Sie die folgende Prozedur, um dem Hub eine neue Validierungszuordnung hinzuzufügen.

1. Speichern Sie die Validierungszuordnungsdatei auf dem Hub oder an der Position, von der WebSphere Partner Gateway Dateien lesen kann.
2. Klicken Sie auf **Hubadmin > Hubkonfiguration > Zuordnungen > Validierungszuordnungen**.
3. Klicken Sie auf **Erstellen**.
4. Geben Sie eine Beschreibung für die Validierungszuordnung ein.
5. Navigieren Sie zur Schemadatei, mit der Sie Dokumente validieren wollen, und klicken Sie auf **Öffnen**.
6. Klicken Sie auf **Speichern**.

Zuordnungen zu Dokumentenflussdefinitionen zuordnen

Verwenden Sie die folgende Prozedur, um eine Validierungszuordnung einer Dokumentenflussdefinition zuzuordnen.

1. Klicken Sie auf **Hubadmin > Hubkonfiguration > Zuordnungen > Validierungszuordnungen**.
2. Klicken Sie auf das Symbol **Details anzeigen** neben der Validierungszuordnung, die Sie der Dokumentenflussdefinition zuordnen wollen.
3. Klicken Sie auf das Symbol **Erweitern** neben einem Paket, um es einzeln auf die gewünschte Ebene, z. B. **Aktion** für ein RosettaNet-Dokument, zu erweitern.
4. Wählen Sie die Dokumentenflussdefinition aus, die Sie der Validierungszuordnung zuordnen wollen.
5. Klicken Sie auf **Speichern**.

Dokumente anzeigen

Die **Dokumentanzeige** zeigt Informationen zu den Dokumenten an, die einen Dokumentenfluss ausmachen. Sie können unformatierte Dokumente und zugeordnete Dokumentverarbeitungsdetails und Ereignisse mit Hilfe von bestimmten Suchkriterien anzeigen. Diese Informationen sind nützlich, wenn Sie zu ermitteln versuchen, ob ein Dokument erfolgreich zugestellt wurde bzw. worin die Ursache eines Fehlers besteht.

Klicken Sie auf **Anzeigen > Dokumentanzeige**, um die Dokumentanzeige anzuzeigen. Informationen zur Verwendung der Dokumentanzeige finden Sie im Handbuch *Verwaltung*.

Kapitel 8. EDI-Dokumentenflüsse konfigurieren

Dieses Kapitel beschreibt, wie Sie die Dokumentenflussdefinitionen und Interaktionen für Standard-EDI-Austauschvorgänge konfigurieren. Darüber hinaus beschreibt dieses Kapitel das Empfangen und Transformieren von XML- und ROD-Dokumenten (ROD - satzorientierte Daten). Dieses Kapitel behandelt die folgenden Themen.

- „Übersicht über EDI"
- „Überblick über XML- und ROD-Dokumente" auf Seite 96
- „Übersicht - Dokumentenflüsse erstellen und Attribute festlegen" auf Seite 97
- „Übersicht über mögliche Dokumentenflüsse" auf Seite 99
- „Verarbeitung von EDI-Austauschvorgängen" auf Seite 104
- „Verarbeitung von XML- oder ROD-Dokumenten" auf Seite 107
- „EDI-Umgebung konfigurieren" auf Seite 108
- „Allgemeine Schritte für das Definieren von Dokumentaustauschvorgängen" auf Seite 122
- „EDI-Austauschvorgänge und -Transaktionen anzeigen" auf Seite 135

Es besteht auch die Möglichkeit, einen EDI-Austausch ohne Entfernen des Umschlags oder Transformation weiterzuleiten. Die Schritte für das Erstellen von Interaktionen für diesen Austauschtyp werden in „EDI-Dokumente mit Pass-Through-Aktion" auf Seite 69 beschrieben.

Übersicht über EDI

EDI ist eine Methode zum Übertragen von Geschäftsinformationen über ein Netz zwischen Geschäftspartnern, die vereinbart haben, einem genehmigten nationalen Standard oder Industriestandard für das Konvertieren und Austauschen von Informationen zu folgen. WebSphere Partner Gateway stellt das Entfernen von Umschlägen, das Transformieren und das Versehen mit Umschlägen für die folgenden EDI-Standards bereit:

- X12 ist ein einheitlicher EDI-Standard, der vom American National Standards Institute genehmigt wurde
- UN/EDIFACT (United Nations Electronic Data Interchange for Administration Commerce and Support)
- UCS (Uniform Communication Standard)

Die folgenden Abschnitte bieten eine kurze Übersicht über EDI-Austauschvorgänge, die den X12-, EDIFACT- und UCS-Standards entsprechen, sowie über Transaktionen und Gruppen, die in den Austauschvorgängen enthalten sind. Darüber hinaus wird beschrieben, wie XML- und ROD-Dokumente und EDI-Austauschvorgänge transformiert werden.

Die EDI-Austauschstruktur

Ein EDI-Austausch enthält mindestens eine Geschäftstransaktion. In X12 und zugehörigen Standards wird eine Geschäftstransaktion als *Transaktionsgruppe* bezeichnet. In EDIFACT und zugehörigen Standards wird eine Geschäftstransaktion als *Nachricht* bezeichnet. Diese Dokumentation verwendet im Allgemeinen den Begriff *Transaktion* oder *Geschäftstransaktion*, um eine X12- oder UCS-Transaktionsgruppe oder eine EDIFACT-Nachricht zu bezeichnen.

EDI-Austauschvorgänge bestehen aus *Segmenten*, die abwechselnd *Datenelemente* enthalten. Datenelemente stellen z. B. einen Namen, eine Menge, ein Datum oder eine Zeit dar.Ein Segment ist eine Gruppe zusammengehöriger Datenelemente. Segmente werden durch einen Segmentnamen oder Segment-Tag identifiziert, die am Anfang des Segments angezeigt werden. (Datenelemente werden nicht anhand des Namens identifiziert, sondern sie werden mit für diesen Zweck reservierten besonderen Trennzeichen abgegrenzt.)

In einigen Fällen ist es hilfreich, die Detail- oder Datensegmente in einer Transaktion von anderen Segmenten unterscheiden zu können, die für Verwaltungszwecke verwendet werden. Die Verwaltungssegmente werden in X12 *Steuerungssegmente* und in EDIFACT *Servicesegmente* genannt. Die *Umschlags*segmente, die die EDI-Austauschabgrenzung bilden, sind ein Beispiel für diese Steuerungs- oder Servicesegmente.

EDI-Austauschvorgänge können drei Segmentebenen enthalten. Auf jeder Ebene gibt es am Anfang ein Headersegment und am Ende ein Trailersegment.

Ein Austausch verfügt immer über ein Austauschheadersegment und ein Austauschtrailersegment.

Ein Austausch kann ein oder mehrere Gruppen enthalten. Eine Gruppe enthält abwechselnd mindestens eine zusammengehörige Transaktion. Die Gruppenebene ist in EDIFACT optional, aber in X12 und zugehörigen Standards ist sie erforderlich. Wenn Gruppen vorhanden sind, gibt es ein Gruppenheader- und ein Gruppentrailersegment für jede Gruppe.

Eine Gruppe oder ein Austausch ohne Gruppen enthält mindestens eine Transaktion. Jede Transaktion verfügt über einen Transaktionsgruppenheader und einen Transaktionsgruppentrailer.

Eine Transaktion stellt ein Geschäftsdokument, wie z. B. eine Bestellung, dar. Der Inhalt des Geschäftsdokuments wird von den Detailsegmenten zwischen dem Transaktionsgruppenheader und dem Transaktionsgruppentrailer dargestellt.

Jeder EDI-Standard stellt seine eigene Methode für das Anzeigen der Daten innerhalb eines Austauschs bereit. Die folgende Tabelle listet die Segmente für jeden der drei unterstützten EDI-Standards auf.

Tabelle 13. Segmente für unterstützte EDI-Standards

Standardsegment	**X12**	**UCS**	**EDIFACT**
Austauschstart	ISA	BG	UNB
Austauschende	IEA	EG	UNZ
Gruppenstart	GS	GS	UNG
Gruppenende	GE	GE	UNE
Transaktionsstart	ST	ST	UNH
Transaktionsende	SE	SE	UNT

Abb. 22 auf Seite 95 zeigt ein Beispiel eines X12-Austauschs und die Segmente, die den Austausch ausmachen.

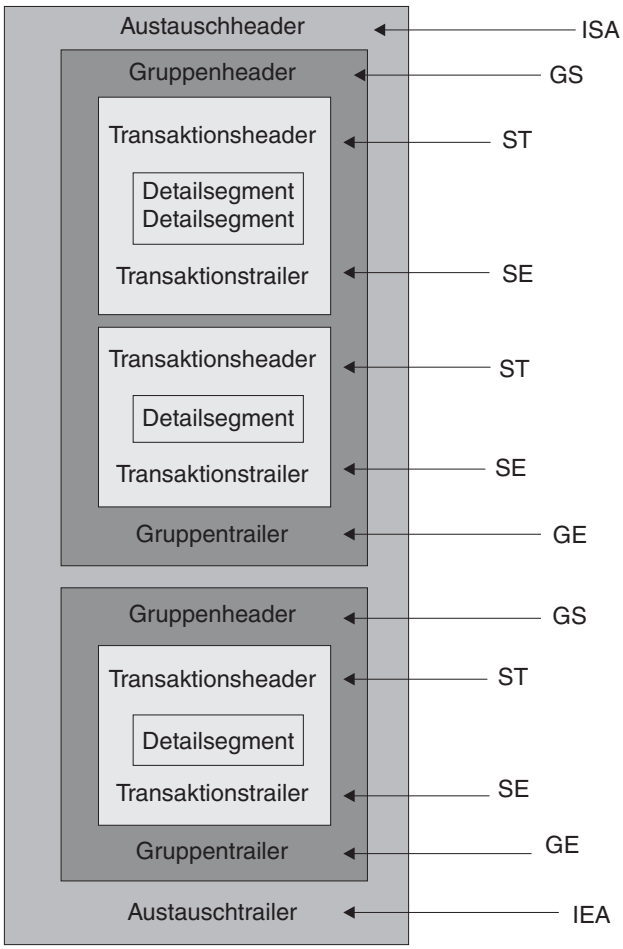

Abbildung 22. Ein Austauschumschlag

Zuordnungen

Der Zuordnungsexperte des Data Interchange Services-Clients erstellt Transformationszuordnungen, die beschreiben, wie ein Dokument in einem Format in ein Dokument eines anderen Formats geändert wird. Sie können z. B. über eine Transformationszuordnung verfügen, die eine X12-Transaktion in eine EDIFACT-Nachricht ändert. Sie können eine EDI-Transaktion auch in ein XML-Dokument oder ein satzorientiertes Datendokument transformieren.

Die Transformationszuordnung kann auch mehrere Dokumente von einem einzelnen Dokument erstellen. Dieser Zuordnungstyp verwendet eine *Zuordnungsverkettung*, die mehrere Ausgaben von einer einzelnen Konvertierung herstellt. Bei der Zuordnungsverkettung wird, nachdem ein Quellendokument erfolgreich in ein Zieldokument konvertiert wurde, mit einer anschließenden Zuordnung das Quellendokument erneut konvertiert, um ein weiteres Zieldokument herzustellen. Dies kann so oft wie gewünscht wiederholt werden, um die gewünschte Anzahl Dokumente herzustellen.

Zusätzlich zu Transformationszuordnungen können Sie Zuordnungen der funktionalen Bestätigungen und Validierungszuordnungen verwenden. Zuordnungen der funktionalen Bestätigungen bieten Anweisungen dazu, wie eine funktionale Bestätigung hergestellt wird, die den Absender eines EDI-Dokuments darüber informiert,

dass das Dokument angekommen ist. Mehrere EDI-Standardzuordnungen der funktionalen Bestätigungen werden bei der Installation von WebSphere Partner Gateway installiert. Eine Liste mit diesen Zuordnungen finden Sie in „Funktionale Bestätigungen" auf Seite 132. Zusätzliche Zuordnungen der funktionalen Bestätigungen können vom Zuordnungsexperten des Data Interchange Services-Clients erstellt werden. WebSphere Partner Gateway generiert eine funktionale Bestätigung, wenn eine EDI-Transaktion validiert wird, und der EDI-Transaktion eine Zuordnung der funktionalen Bestätigungen zugeordnet ist. Das Quellendokument muss ein EDI-Dokument sein.

WebSphere Partner Gateway stellt eine Standardebene der Validierung für das EDI-Dokument bereit. Wenn eine funktionale Bestätigung generiert wird, werden die Ergebnisse von der Validierung eines EDI-Dokuments gespeichert. Validierungszuordnungen werden erstellt, um eine zusätzliche Validierung eines EDI-Dokuments bereitzustellen. Die Generierung einer funktionalen Bestätigung verwendet die Zuordnung der funktionalen Bestätigungen und die Ergebnisse von der Validierung des EDI-Dokuments. Die Zuordnung der funktionalen Bestätigungen enthält Zuordnungsbefehle, die angeben, wie die Validierungsergebnisse zu verwenden sind, um eine bestimmte funktionale Bestätigung zu erstellen. Wenn ein Dokument vom Validierungsprozess für die Konvertierung akzeptiert wird, wird die geeignete Datentransformationszuordnung verwendet, um das Quellendokument zu konvertieren.

Überblick über XML- und ROD-Dokumente

Der Zuordnungsexperte des Data Interchange Services-Clients kann Dokumentdefinitionen für XML- und ROD-Dokumente (ROD - satzorientierte Daten) erstellen, und dann Transformationszuordnungen erstellen, die einen Dokumenttyp in einen anderen Dokumenttyp ändern.

XML-Dokumente

XML-Dokumente werden entweder von einer XML-DTD oder einem XML-Schema definiert. Der Zuordnungsexperte des Data Interchange Services-Client erstellt eine Transformationszuordnung auf der Basis der DTD oder des Schemas, die beschreiben, wie das XML-Dokument in ein anderes Format konvertiert werden soll. Ein XML-Dokument kann in ein anderes XML-Dokument, ein satzorientiertes Datendokument oder eine EDI-Transaktion transformiert werden.

ROD-Dokumente

Der Begriff *satzorientierte Daten (ROD - record-oriented data)* bezieht sich auf Dokumente, die einem proprietären Format entsprechen. Der Zuordnungsexperte des Data Interchange Services-Clients definiert eine ROD-Dokumentdefinition, die sich auf die Art und Weise bezieht, wie eine Geschäftsanwendung Daten in einem Dokument strukturiert. Nachdem eine Dokumentdefinition definiert wurde, kann der Zuordnungsexperte eine Zuordnung erstellen, um das ROD-Dokument in ein anderes ROD-Dokument, ein XML-Dokument oder eine EDI-Transaktion zu transformieren.

Verteiler und mehrere Dokumente

XML- oder ROD-Dokumente können in den Hub als einzelne Dokumente oder als Gruppe von Dokumenten innerhalb derselben Datei gelangen.Mehrere Dokumente könnten in dieselbe Datei gestellt werden, wenn z. B. ein terminierter Job auf dem Teilnehmer oder Community Manager regelmäßig zu sendende Dokumente hochlädt. Wenn mehrere XML- oder ROD-Dokumente in einer Datei ankommen, ruft

der Empfänger den zugeordneten Verteilerhandler (XMLSplitterHander oder RODSplitterHandler) auf, um die Gruppe von Dokumenten aufzuteilen. (Die Verteilerhandler werden konfiguriert, wenn Sie ein Ziel erstellen. Weitere Informationen finden Sie in „Vorverarbeitung" auf Seite 53.) Die Dokumente werden dann erneut in den Document Manager eingeführt, um individuell verarbeitet zu werden.

Anmerkung: Die Absender- und Empfänger-IDs müssen Teil der ROD-Dokumentdefinition sein, die der Transformationszuordnung zugeordnet ist. Die Informationen, die zum Ermitteln des Dokumenttyps und der Wörterbuchwerte nötig sind, müssen ebenso in der Dokumentdefinition vorhanden sein. Stellen Sie sicher, dass der Zuordnungsexperte des Data Interchange Services-Clients diese Anforderungen kennt, wenn er die Transformationszuordnung erstellt.

Mehrere EDI-Austauschvorgänge können auch in einer Datei gesendet werden. Wenn mehrere EDI-Austauschvorgänge in einer Datei ankommen, ruft der Empfänger den Handler `EDISplitterHandler` auf, um die Gruppe von Austauschvorgängen aufzuteilen. Die Austauschvorgänge werden dann erneut in Document Manager eingeführt, um individuell verarbeitet zu werden.

Anmerkung: Das Aufteilen wird am Austausch vorgenommen und nicht an den einzelnen Transaktionen innerhalb des Austauschs. Von den Transaktionen innerhalb des Austauschs wird der Umschlag entfernt.

Übersicht - Dokumentenflüsse erstellen und Attribute festlegen

Eine Dokumentenflussdefinition besteht aus mindestens einem Paket, einem Protokoll und einem Dokumentenfluss. Die Dokumentenflussdefinitionen geben die Dokumenttypen an, die von WebSphere Partner Gateway verarbeitet werden.

Ein Paket bezieht sich auf die Logik, die erforderlich ist, um ein Dokument gemäß einer Spezifikation, wie z. B. AS2, zu packen. Eine Protokollübertragung ist die Logik, die erforderlich ist, um ein Dokument zu verarbeiten, das mit einem bestimmten Protokoll, wie z. B. EDI-X12, konform ist. Ein Dokumentenfluss beschreibt, wie das Dokument aussehen wird.

Die folgenden Abschnitte beschreiben kurz den Gesamtablauf für das Konfigurieren eines Dokumentenflusses zwischen Community Manager und einem Teilnehmer. Die Abschnitte beschreiben auch die Punkte, an denen Sie Attribute festlegen können.

Schritt 1: Sicherstellen, dass die Dokumentenflussdefinition verfügbar ist

Bevor Sie ein Dokument senden oder empfangen können, muss eine Dokumentenflussdefinition für das Dokument definiert sein. WebSphere Partner Gateway bietet mehrere Standard-Dokumentenflussdefinitionen einschließlich derjenigen, die funktionale Bestätigungen darstellen. Wenn Sie Transformationszuordnungen für EDI-Transaktionen bzw. XML- oder ROD-Dokumente importieren, werden die zugeordneten Dokumentenflussdefinitionen auf der Seite **Dokumentenflussdefinitionen** angezeigt. Ebenso wird, wenn Sie eine Zuordnung der funktionalen Bestätigungen importieren, die noch nicht definiert ist, die Dokumentenflussdefinition für die Bestätigung auf der Seite **Dokumentenflussdefinitionen** angezeigt. Sie können auch Ihre eigenen Dokumentenflussdefinitionen erstellen.

Sie können als ein Teil der Erstellung der Dokumentenflussdefinition bestimmte Attribute ändern. Attribute werden verwendet, um verschiedene Dokument-

verarbeitungs- und Routing-Funktionen auszuführen, wie z. B. Validierung, Verschlüsselungsüberprüfung und Wiederholungszähler. Die Attribute, die Sie auf der Dokumentenfluss-Definitionsebene festlegen, liefern eine globale Einstellung für das zugeordnete Paket und Protokoll sowie den zugeordneten Dokumentenfluss. Die Attribute, die zur Verfügung stehen, variieren je nach Dokumentenflussdefinition. Attribute für EDI-Dokumentenflussdefinitionen unterscheiden sich von den Attributen für RosettaNet-Dokumentenflussdefinitionen.

Wenn Sie z. B. einen Wert für **TA1-Anforderung zulassen** auf der Dokumentenflussebene **ISA** angeben, wird diese Einstellung auf alle ISA-Dokumente angewendet. Wenn Sie später **TA1-Anforderung zulassen** auf B2B-Funktionalitätsebene für einen Teilnehmer oder Community Manager festlegen, überschreibt diese Einstellung diejenige, die auf Dokumentenflussdefinitions-Ebene festgelegt wurde.

Bei Attributen, die auf mehreren Ebenen der Dokumentenflussdefinition festgelegt werden können, haben die auf Dokumentenflussebene festgelegten Werte Vorrang vor den auf Protokollebene festgelegten Werten und die auf Protokollebene festgelegten Attribute haben Vorrang vor denen auf der Paketebene. Wenn Sie z. B. ein Umschlagsprofil auf der Protokollebene `&X44TA1` angeben, aber ein anderes Umschlagsprofil auf der Dokumentenflussebene `TA1` angeben, wird das von Ihnen angegebene Umschlagsprofil auf der Dokumentenflussebene `TA1` verwendet.

Sie müssen den Dokumentenfluss auf der Seite **Dokumentenflussdefinitionen verwalten** auflisten, bevor Sie Interaktionen erstellen können.

Schritt 2: Interaktionen erstellen

Sie legen als Nächstes Interaktionen fest, welche für das Erstellen von Teilnehmerverbindungen als Schablone dienen. Interaktionen teilen mit, wie das Dokument ankommt, welche Verarbeitung an dem Dokument ausgeführt wird und wie das Dokument vom Hub gesendet wird.

Für einige Protokolle benötigen Sie nur zwei Dokumentenflüsse: Der eine beschreibt das Dokument, das auf dem Hub vom Teilnehmer oder Community Manager empfangen wird und der andere beschreibt das Dokument, das vom Hub zum Teilnehmer oder Community Manager gesendet wird. Wenn der Hub jedoch einen EDI-Austauschvorgang sendet oder empfängt, von dem der Umschlag entfernt wird, so dass einzelne Transaktionen entstehen, bzw. in dem Bestätigungen erforderlich sind, dann erstellen Sie tatsächlich mehrere Interaktionen. Wenn Sie z. B. auf dem Hub einen EDI-Austausch empfangen, verfügen Sie über eine Interaktion, die beschreibt, wie der Austausch an den Hub gesendet und wie er auf dem Hub verarbeitet wird. Darüber hinaus verfügen Sie über eine Interaktion für jede Transaktion auf dem Hub, die beschreibt, wie die Transaktion verarbeitet wird. Für EDI-Austauschvorgänge, die den Hub verlassen, verfügen Sie über eine Interaktion, die beschreibt, wie der Austauschumschlag an den Empfänger gesendet wird.

Schritt 3: Teilnehmerprofile, Gateways und B2B-Funktionalität erstellen

Als Nächstes erstellen Sie Teilnehmerprofile für Community Manager und die Community-Teilnehmer. Sie definieren Gateways, die bestimmen, wohin Dokumente gesendet werden, und B2B-Funktionalität, die die Dokumente angeben, welche Community Manager oder ein Teilnehmer senden und empfangen kann. Die Seite **B2B-Funktionalität** listet alle Dokumentenflüsse auf, die definiert worden sind.

Sie können Attribute auf der B2B-Funktionalitätsebene festlegen. Jedes Attribut, das Sie auf dieser Ebene festlegen, überschreibt die auf der Dokumentenflussdefinitions-Ebene festgelegten Attribute. Wenn Sie z. B. für **TA1-Anforderung zulassen** auf Dokumentenflussdefinitions-Ebene für ISA-Dokumente **Nein** festlegen, aber für dieses Attribut auf B2B-Funktionalitätsebene **Ja** festlegen, wird der Wert **Ja** verwendet. Wenn Sie ein Attribut auf der B2B-Ebene festlegen, können Sie das Attribut an einen bestimmten Teilnehmer anpassen.

Wenn Sie das Umschlagsprofil auf Protokoll- oder Dokumentenflussebene auf der Seite **Dokumentenflussdefinitionen verwalten** festlegen, und Sie für dieses Profil dann auf der Seite **B2B-Funktionalität** einen anderen Wert festlegen, wird der letztere Wert verwendet.

Sie müssen die Profile und B2B-Funktionalität von Community Manager und den Teilnehmern definiert haben, bevor Sie Verbindungen zwischen ihnen erstellen können.

Schritt 4: Verbindungen aktivieren

Schließlich aktivieren Sie Verbindungen zwischen Community Manager und den Teilnehmern. Die verfügbaren Verbindungen basieren auf der B2B-Funktionalität der Teilnehmer und der von Ihnen erstellten Interaktionen. Die Interaktionen hängen von den Dokumentenflussdefinitionen ab, die zur Verfügung stehen.

Für einige Austauschvorgänge ist nur eine Verbindung erforderlich. Wenn z. B. ein Teilnehmer ein binäres Dokument an eine Community Manager-Back-End-Anwendung sendet, wird nur eine Verbindung benötigt. Für den Austausch von EDI-Austauschvorgängen, in denen der Umschlag des Austauschs entfernt wird und die einzelnen Transaktionen transformiert werden, sind jedoch mehrere Verbindungen konfiguriert.

Anmerkung: Für EDI-Austauschvorgänge, die unverändert weitergeleitet werden, ist nur eine Verbindung erforderlich.

Sie können Attribute auf der Verbindungsebene festlegen. Jedes Attribut, das Sie auf dieser Ebene festlegen, überschreibt die auf der B2B-Attributebene festgelegten Attribute. Wenn Sie z. B. für **TA1-Anforderung zulassen** auf B2B-Funktionalitätsebene **Ja** festlegen, aber für dieses Attribut auf Verbindungsebene **Nein** festlegen, wird der Wert **Nein** verwendet. Wenn Sie einen Wert für ein Attribut auf der Verbindungsebene festlegen, können Sie das Attribut, abhängig von den Routing-Anforderungen der Teilnehmer und der Anwendungen, die beteiligt sind, noch weiter anpassen.

Übersicht über mögliche Dokumentenflüsse

Dieser Abschnitt gibt Ihnen eine kurze Übersicht über die Transformationstypen, die WebSphere Partner Gateway ausführen kann. In „Allgemeine Schritte für das Definieren von Dokumentaustauschvorgängen" auf Seite 122 werden die Details dieser Transformationen beschrieben und wie Sie diese festlegen müssen.

Dokumentenfluss: EDI zu EDI

WebSphere Partner Gateway kann einen EDI-Austausch von einem Teilnehmer oder Community Manager akzeptieren, ihn in einen anderen EDI-Austauschtyp (z. B. EDI-X12 zu EDIFACT) transformieren und das Dokument zu Community Manager oder dem Teilnehmer senden.

Die folgenden Schritte treten auf, wenn ein EDI-Austausch in einen anderen EDI-Austausch transformiert wird:

1. Vom EDI-Austausch, der auf dem Hub empfangen wird, wird der Umschlag entfernt.
2. Die einzelnen Transaktionen innerhalb des EDI-Austauschs werden zu dem EDI-Format des Empfängers transformiert.
3. Die transformierten EDI-Transaktionen werden mit einem Umschlag versehen und an den Empfänger gesendet.

Abb. 23 zeigt einen X12-Austausch, der aus drei Transaktionen besteht, von denen der Umschlag # entfernt wird. Die Transaktionen werden in EDIFACT-Format transformiert, dann mit einem Umschlag versehen und an den Teilnehmer gesendet.

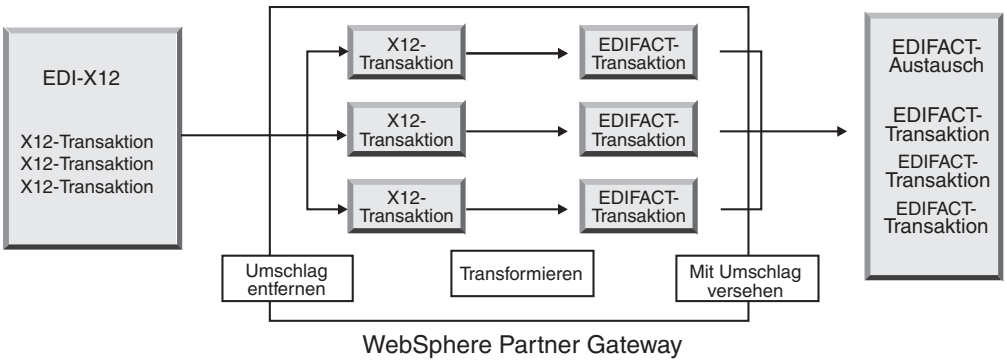

Abbildung 23. Dokumentenfluss: EDI-Austausch zu EDI-Austausch

Jeder Transaktion wurde eine Transformationszuordnung zugeordnet, die angibt, wie die Transaktion transformiert wird. Die Transaktion kann in eine einzelne Transaktion transformiert werden, oder, falls die Zuordnungsverkettung zur Erstellung der Zuordnung verwendet wurde, in mehrere Transaktionen transformiert werden. Wenn der Stapelbetrieb des Programms zur Umschlagsgenerierung aktiviert ist, verlassen Transaktionen, die auf dem Hub in einem Umschlag eintreffen, den Hub in einem Umschlag. Wenn jedoch Umschlagsunterbrechungspunkte, z. B. verschiedene Werte für EDI-Attribute oder ein unterschiedliches Umschlagsprofil, vorhanden sind oder wenn der Stapelbetrieb inaktiviert wurde, verlassen die Transaktionen den Hub in unterschiedlichen Umschlägen. Eine allgemeine Beschreibung des Programms zur Umschlagsgenerierung, dies die Komponente ist, die eine Gruppe von Transaktionen, welche an einen Teilnehmer gesendet werden sollen, zusammenstellt, sie mit einem Umschlag versieht und sendet, finden Sie in „Programm zur Umschlagsgenerierung" auf Seite 108. Weitere Informationen zum Stapelbetrieb finden Sie in „Stapelbetrieb" auf Seite 109.

Der Transaktion könnte auch eine Validierungszuordnung zugeordnet sein.

Dokumentenfluss: EDI zu XML oder ROD

WebSphere Partner Gateway kann einen EDI-Austausch von einem Teilnehmer oder Community Manager akzeptieren, den Umschlag vom Austausch entfernen und die daraus entstehenden EDI-Austauschvorgänge in XML- oder ROD-Dokumente transformieren.

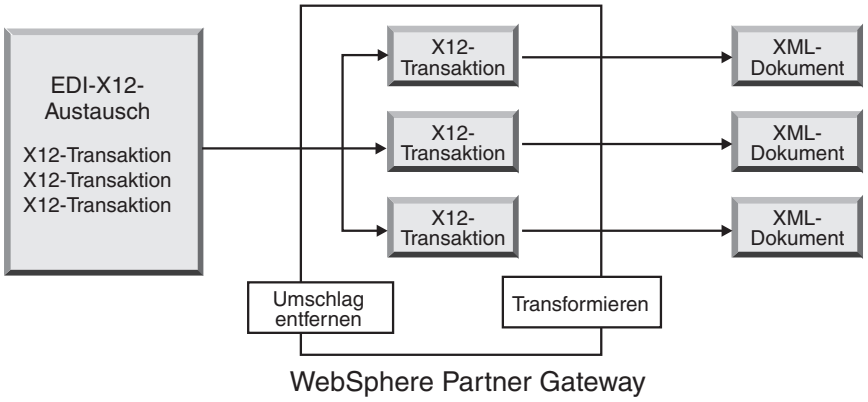

Abbildung 24. Dokumentenfluss: EDI-Austausch zu XML-Dokumenten

Die Transaktion kann in ein einzelnes Dokument transformiert werden, oder, falls die Zuordnungsverkettung zur Erstellung der Zuordnung verwendet wurde, in mehrere Dokumente transformiert werden.

Dokumentenfluss: XML oder ROD zu EDI

WebSphere Partner Gateway kann XML- oder ROD-Dokumente von einem Teilnehmer oder Community Manager empfangen, die Dokumente in EDI-Transaktionen transformieren, die Transaktionen mit einem Umschlag versehen und sie an Community Manager oder einen Teilnehmer senden.

Abb. 25 zeigt XML-Dokumente, die in X12-Transaktionen transformiert und dann mit einem Umschlag versehen werden.

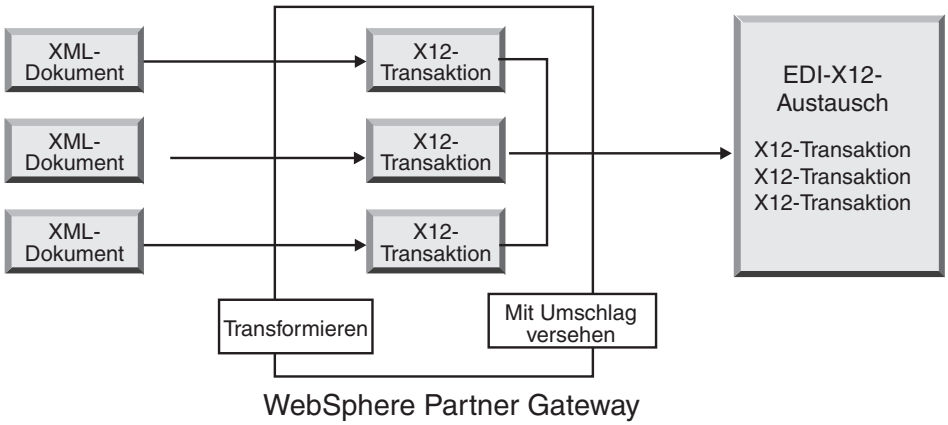

Abbildung 25. Dokumentenfluss: XML-Dokument zu EDI-Austausch

Ein Dokument kann in mehrere Transaktionen transformiert werden, wenn die Zuordnungsverkettung zur Erstellung der Zuordnung verwendet wurde, und die Transaktionen können für verschiedene Austauschvorgänge mit Umschlägen versehen werden. Abb. 26 auf Seite 102 zeigt ein XML-Dokument, das in drei X12-Transaktionen transformiert wird. Zwei der Transaktionen werden mit einem gemeinsamen Umschlag versehen. Die dritte Transaktion wird mit einem separaten Umschlag versehen.

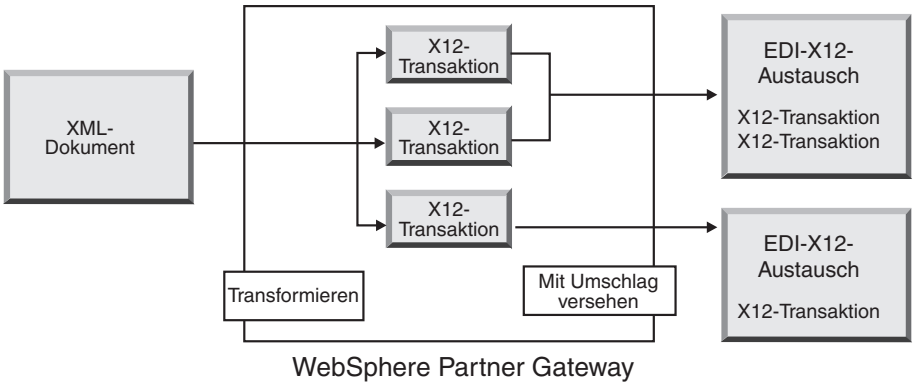

Abbildung 26. Dokumentenfluss: XML-Dokument zu mehreren EDI-Transaktionen

Dokumentenfluss: Mehrere XML- oder ROD-Dokumente zu EDI-Austausch

WebSphere Partner Gateway kann eine Datei, die aus mindestens einem XML- oder ROD-Dokument besteht, von einem Teilnehmer oder Community Manager empfangen, das Dokument bzw. die Dokumente in EDI-Transaktionen transformieren, die EDI-Transaktionen mit mehreren Umschlägen versehen und diese an Community Manager oder einen Teilnehmer senden.

Jedes Dokument kann in eine einzelne Transaktion transformiert werden, oder, falls die Zuordnungsverkettung zur Erstellung der Zuordnung verwendet wurde, in mehrere Transaktionen transformiert werden.

Hinweise:

1. Dokumente, die in einer Datei gesendet werden, müssen vom selben Typ (entweder XML-Dokumente oder ROD-Dokumente) sein, sie dürfen aber nicht gemischt sein.
2. ROD-Dokumente müssen vom selben Typ sein.

Abb. 27 zeigt eine Gruppe von XML-Dokumenten, die aufgeteilt werden, wodurch einzelne XML-Dokumente entstehen. Die XML-Dokumente werden in X12-Transaktionen transformiert und die Transaktionen werden mit Umschlägen versehen.

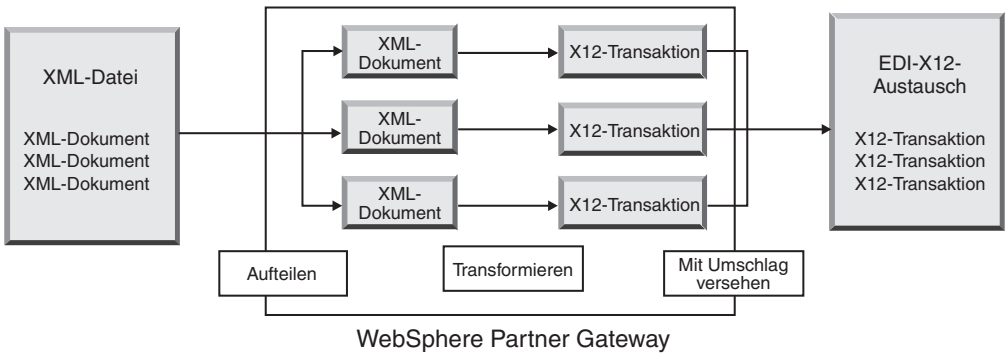

Abbildung 27. Dokumentenfluss: Mehrere XML-Dokumente zu EDI-Austausch

In Abb. 27 auf Seite 102 werden die Dokumente vom XML-Verteilerhandler aufgeteilt und die transformierten Transaktionen zusammen mit einem Umschlag versehen. Für den XML-Verteilerhandler muss die Option BCG_BATCHDOCS auf ON (der Standardwert) gesetzt sein, damit dieses Szenario auftritt. Wenn BCG_BATCHDOCS auf ON gesetzt ist und der Stapelbetrieb des Programms zur Umschlagsgenerierung aktiviert ist, können diese Transaktionen mit demselben EDI-Umschlag versehen werden. Das Attribut für den Stapelbetrieb des Programms zur Umschlagsgenerierung wird in „Stapelbetrieb" auf Seite 109 beschrieben.

Dokumentenfluss: XML zu ROD oder ROD zu XML

WebSphere Partner Gateway kann ein XML- oder ROD-Dokument von einem Teilnehmer oder Community Manager empfangen, das Dokument in einen anderen Typ (XML zu ROD oder ROD zu XML) transformieren und dann das Dokument an den Teilnehmer oder Community Manager senden.

Abb. 28 zeigt eine Reihe von XML-Dokumenten, die in ROD-Dokumente transformiert werden.

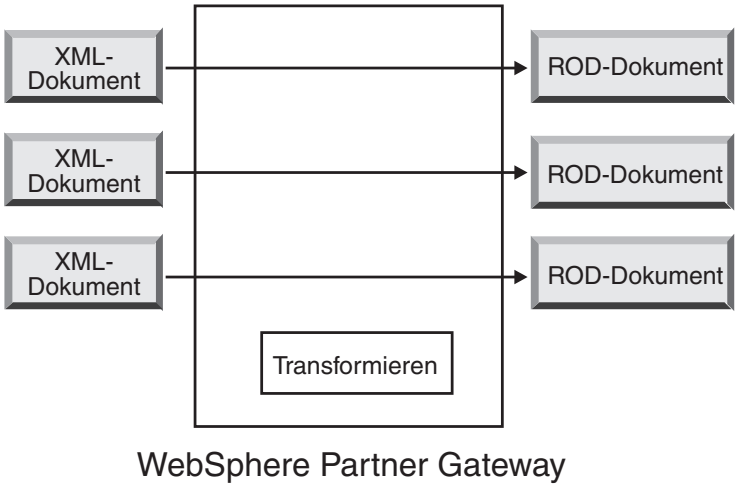

Abbildung 28. Dokumentenfluss: XML-Dokument zu ROD-Dokument

Das Dokument kann in ein einzelnes Dokument transformiert werden, oder, falls die Zuordnungsverkettung zur Erstellung der Zuordnung verwendet wurde, in mehrere Dokumente transformiert werden.

Dokumentenfluss: XML zu XML oder ROD zu ROD

WebSphere Partner Gateway kann ein XML- oder ROD-Dokument von einem Teilnehmer oder Community Manager empfangen, es in ein Dokument desselben Typs (XML zu XML oder ROD zu ROD) transformieren und dann das Dokument an den Teilnehmer oder Community Manager senden.

Abb. 29 auf Seite 104 zeigt XML-Dokumente, die in XML-Dokumente eines anderen Formats transformiert werden.

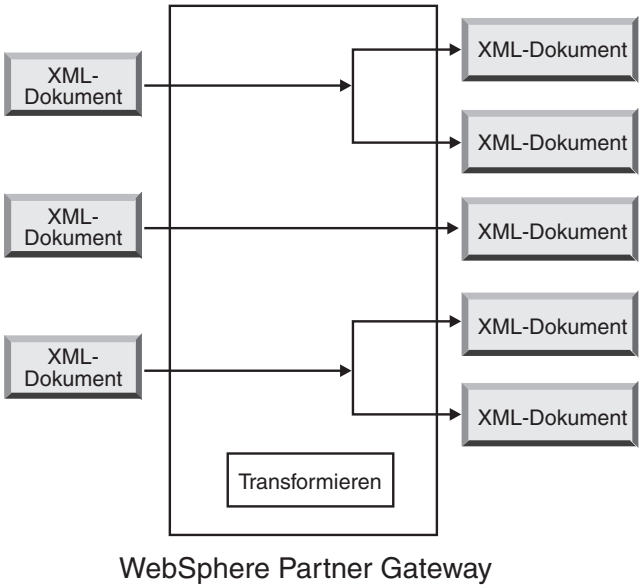

Abbildung 29. Dokumentenfluss: XML-Dokument zu XML-Dokument

Das Dokument kann in ein einzelnes Dokument transformiert werden, oder, falls die Zuordnungsverkettung zur Erstellung der Zuordnung verwendet wurde, in mehrere Dokumente transformiert werden.

Verarbeitung von EDI-Austauschvorgängen

Von einem EDI-Austausch, der auf dem Hub empfangen wird, wird in der Regel der Umschlag entfernt und die einzelnen Transaktionen werden verarbeitet. Oftmals werden Standard-EDI-Transaktionen (wie z. B. X12 850 oder EDIFACT ORDERS, dies stellt eine Bestellung dar) in ein Format transformiert, das von einer Back-End-Anwendung verstanden wird. Darüber hinaus wird häufig eine funktionale Bestätigung an den Teilnehmer gesendet, um anzugeben, dass der Austausch empfangen wurde. Der Austausch von EDI-Austauschvorgängen erfordert daher mehrere Aktionen, wie z. B. **EDI - Umschlag entfernen** und **EDI validieren und EDI konvertieren**. Wenn der Austausch z. B. zwei Transaktionen enthält und keine Bestätigungen erforderlich sind, führt WebSphere Partner Gateway die folgenden Aktionen aus:

1. Entfernt die Umschläge der Austauschvorgänge.

   WebSphere Partner Gateway extrahiert Informationen zum Austausch aus den Umschlagsheader- und Umschlagstrailersegmenten auf den Austausch-, Gruppen- und Transaktionsebenen. Diese Informationen können Folgendes einschließen:

   - Auf der Austauschebene die Geschäfts-IDs der sendenden und empfangenden Teilnehmer, der Nutzungsanzeiger, der angibt, ob der Austausch für eine Produktions- oder Testumgebung bestimmt ist, sowie das Datum und die Uhrzeit, wann der Austausch vorbereitet worden ist
   - Auf der Gruppenebene die Anwendungs-IDs des Absenders und Empfängers sowie das Datum und die Uhrzeit, wann die Gruppe vorbereitet worden ist
   - Auf der Transaktionsebene der Transaktionstyp (wie z. B. X12 850 oder EDIFACT ORDERS)

2. Transformiert die erste Transaktion entsprechend der ihr zugeordneten Zuordnung.
3. Transformiert die zweite Transaktion entsprechend der ihr zugeordneten Zuordnung.
4. Stellt der Back-End-Anwendung die transformierten Dokumente zu.

Ebenso, wenn der Hub ein bzw. mehrere Dokumente sendet, die von der Community Manager-Back-End-Anwendung stammen, werden die Dokumente in Standard-EDI-Transaktionen transformiert. Die entstehenden EDI-Transaktionen werden mit einem Umschlag versehen, bevor Sie an den Teilnehmer gesendet werden. Wie in dem Fall, wenn ein EDI-Austausch empfangen wird, sind mehrere Aktionen erforderlich, um einen EDI-Austausch zu erstellen, ihn mit einem Umschlag zu versehen und zu senden.

Die einzelnen Transaktionen, Gruppen und Austauschvorgänge werden durch Kontrollnummern angegeben. WebSphere Partner Gateway legt diese Nummern fest, wenn ein Austausch stattfindet. Sie können die Kontrollnummern jedoch anpassen, wie in „Kontrollnummern" auf Seite 118 beschrieben.

Die folgende Abbildung zeigt den Gesamtüberblick darüber, wie ein EDI-Austausch in einem AS-Paket von einem Teilnehmer mit dem letztendlichen Ziel gesendet wird, zwei transformierte XML-Dokumente an zwei unterschiedliche Gateways auf dem Community Manager-Back-End-System zuzustellen. In diesem Beispiel werden die 850-Transaktionen in Bestellungen transformiert, die eine Back-End-Anwendung verarbeiten kann. Die 890-Transaktionen werden in Versandaufträge des Warenlagers transformiert, die die Back-End-Anwendung verarbeiten kann.

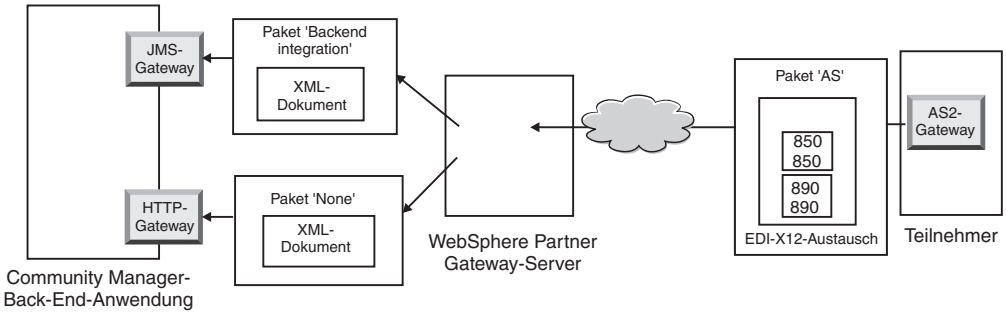

Abbildung 30. Gesamtdokumentenfluss von einem Teilnehmer zu Community Manager

Anstatt nur eine Verbindung vom Teilnehmer zu Community Manager zu erfordern, sind für diesen Austausch drei Verbindungen erforderlich:

- Eine Verbindung vom Teilnehmer zum Hub, um vom Austausch den Umschlag zu entfernen. Da dies ein Zwischenschritt ist (der Umschlag wird vom Austausch entfernt, dem Teilnehmer aber nicht zugestellt), gilt für die Zielseite der Teilnehmerverbindung **N/A** (nicht vorhanden).

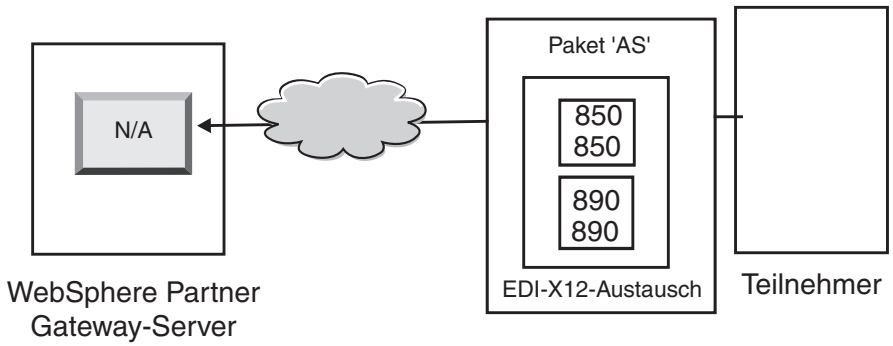

Abbildung 31. Die Verbindung für die Umschlagsentfernung

- Eine Verbindung für die erste Transaktion, die transformiert und dem JMS-Gateway von Community Manager zugestellt werden soll, und eine Verbindung für die zweite Transaktion, die transformiert und dem HTTP-Gateway von Community Manager zugestellt werden soll.

  Für die Transaktionen ist das Quellenpaket nicht zutreffend, da die Transaktionen mit dem ursprünglichen Austausch gekommen sind, dessen Umschlag vom System entfernt worden ist. Für die Quellenseite der Transaktionen sollte daher in der Teilnehmerverbindung **Paket: N/A** angegeben sein.

  Für die Transaktion, die in XML transformiert und über JMS zur Back-End-Anwendung fließen wird, sollte das Zielgateway in der Teilnehmerverbindung dieser Transaktion als das JMS-Gateway von Community Manager angegeben sein. Für die Transaktion, die in XML transformiert wurde und die über HTTP zur Back-End-Anwendung fließen wird, sollte das Zielgateway in der Teilnehmerverbindung dieser Transaktion als das HTTP-Gateway von Community Manager angegeben sein.

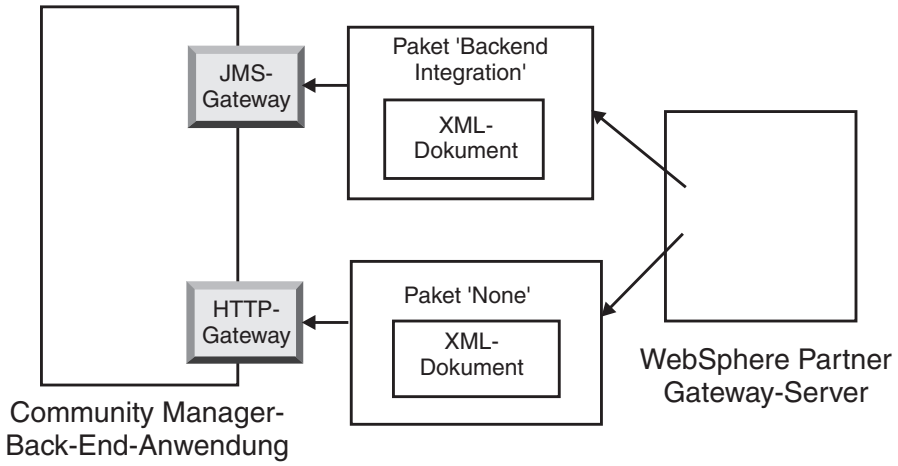

Abbildung 32. Verbindungen für einzelne Transaktionen

Sie können die Dokumentanzeige zum Anzeigen des Austauschs und der einzelnen Transaktionen verwenden, welche in der Dokumentanzeige als *untergeordnete Elemente* des Austauschs betrachtet werden. Sie können mit der Dokumentanzeige die untergeordneten Elemente anzeigen, die einem Quellen- oder Zielaustausch zugeordnet sind, und Sie können die ihnen zugeordneten Ereignisse anzeigen. Die Dokumentanzeige wird im Abschnitt über das Anzeigen von Ereignissen und Dokumenten des Handbuchs *Verwaltung* beschrieben.

Wenn der Absender Bestätigungen anfordert, benötigen Sie zusätzliche Verbindungen:

- Eine Verbindung für jede Bestätigung, die zurück an den Teilnehmer gesendet wird. Die funktionalen Bestätigungen werden vom System generiert und daher sollte für die Quellenseite der Teilnehmerverbindung **Paket: N/A** angegeben sein. Die funktionalen Bestätigungen werden vor ihrer Zustellung mit Umschlägen versehen und daher sollte für die Zielseite der Teilnehmerverbindung **Paket: N/A** angegeben sein. Das Programm zur Umschlagsgenerierung stellt diese Bestätigungen entsprechend einem von Ihnen festgelegten Zeitplan zusammen. Informationen zum Festlegen des Zeitplans finden Sie in „Programm zur Umschlagsgenerierung" auf Seite 108.
- Eine Verbindung, um die Bestätigungen mit einem Umschlag zu versehen, bevor Sie zurück an den Teilnehmer gesendet werden. Der Umschlag wird vom System generiert und daher sollte für die Quellenseite der Teilnehmerverbindung **Paket: N/A** angegeben sein. Für die Zielseite der Teilnehmerverbindung sollte als Zielgateway das Gateway des Teilnehmers, in diesem Fall **Paket: AS**, angegeben sein. Sie können einen Standardumschlag für den EDI-Standard verwenden, oder Sie können Umschläge anpassen. Informationen zum Anpassen von Umschlägen finden Sie in „Umschlagsprofile" auf Seite 110.

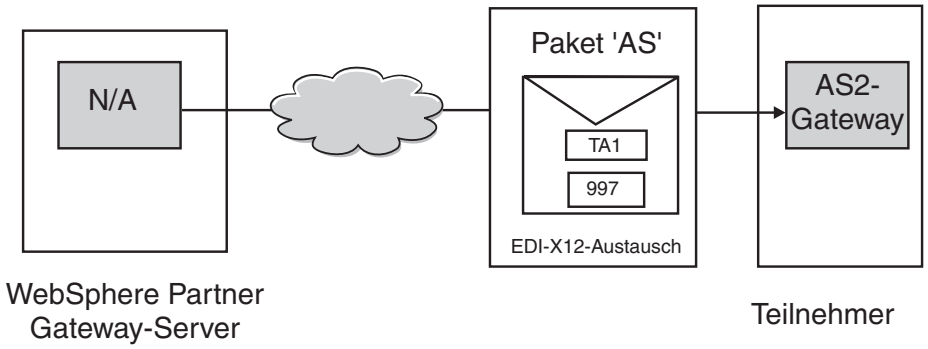

Abbildung 33. Bestätigungen mit Umschlägen versehen und diese an den Absender senden

Verarbeitung von XML- oder ROD-Dokumenten

Ein XML- oder ROD-Dokument wird auf dem Hub als einzelnes Dokument oder als Gruppe von Dokumenten in derselben Datei empfangen. Wenn eine Gruppe von Dokumenten auf dem Hub in derselben Datei empfangen wird, führt WebSphere Partner Gateway die folgenden Aktionen aus:

1. Teilt die Gruppe von Dokumenten in einzelne Dokumente auf.
2. Transformiert jedes Dokument entsprechend der ihm zugeordneten Zuordnung.
3. Wenn die Dokumente in EDI-Transaktionen transformiert werden, versieht es die Transaktionen mit Umschlägen und stellt diese der Back-End-Anwendung zu. Wenn die Dokumente in XML- oder ROD-Dokumente transformiert werden, stellt es die transformierten Dokumente der Back-End-Anwendung zu.

Wenn das XML- oder ROD-Dokument als einzelnes Dokument ankommt, führt WebSphere Partner Gateway die folgenden Aktionen aus:

1. Transformiert das Dokument entsprechend der ihm zugeordneten Zuordnung.
2. Wenn das Dokument in eine EDI-Transaktion transformiert wird, versieht es die Transaktion mit einem Umschlag und stellt es der Back-End-Anwendung zu. Wenn das Dokument in ein anderes XML- oder ROD-Dokument transformiert wird, wird das Dokument der Back-End-Anwendung zugestellt.

Ebenso, wenn der Hub ein bzw. mehrere Dokumente sendet, die von der Community Manager-Back-End-Anwendung stammen, werden die Dokumente in XML- oder ROD-Dokumente transformiert, oder sie werden in EDI-Transaktionen transformiert. Bei EDI-Transaktionen werden die Transaktionen mit einem Umschlag versehen, bevor Sie an den Teilnehmer gesendet werden. Wie in dem Fall, wenn ein EDI-Austausch empfangen wird, sind mehrere Aktionen erforderlich, um das Dokument bzw. die Dokumente zu transformieren, die entstehenden Transaktionen mit einem Umschlag zu versehen und den EDI-Austausch zu senden.

EDI-Umgebung konfigurieren

Wie im vorherigen Abschnitt erwähnt, können Sie viele Attribute angeben, die zum Austausch der EDI-Austauschvorgänge gehören. Sie können z. B. die vom System bereitgestellten Umschlagsprofile ändern, Sie können bestimmte Umschläge definieren, die für bestimmte Verbindungen verwendet werden sollen, Sie können Kontrollnummern festlegen, die den verschiedenen Teilen eines Austauschs zugeordnet sind, und Sie können Verbindungsprofile festlegen, so dass derselbe Austausch in unterschiedlicher Weise zugestellt werden kann. Diese Aufgaben werden in diesem Abschnitt beschrieben.

Programm zur Umschlagsgenerierung

Das Programm zur Umschlagsgenerierung ist die Komponente, die eine Gruppe von Transaktionen zusammenstellt, die an einen Teilnehmer gesendet werden sollen, sie mit einem Umschlag versieht und sie sendet. Sie terminieren das Programm zur Umschlagsgenerierung oder akzeptieren den Standardzeitplan, um WebSphere Partner Gateway anzugeben, wann das Programm zur Umschlagsgenerierung nach zu sendenden Transaktionen suchen soll. Sie können auch die Standardwerte für die Sperrenzeit, das Höchstalter der Warteschlange und Stapelbetrieb aktualisieren.

Anmerkung: Das Konfigurieren des Programms zur Umschlagsgenerierung ist optional. Wenn Sie die Werte für das Programm zur Umschlagsgenerierung nicht ändern, werden die vom System bereitgestellten Werte verwendet.

Sperren

Jede Instanz von Document Manager hat ihr eigenes Programm zur Umschlagsgenerierung. Wenn auf Ihrem System zwei Document Manager installiert sind, verfügen Sie über zwei Programme zur Umschlagsgenerierung. Es ist daher möglich, dass zwei oder mehr Instanzen eines Programms zur Umschlagsgenerierung versuchen, eine Abfrage nach Transaktionen durchzuführen, die darauf warten, mit einem Umschlag versehen zu werden. Sperren werden verwendet, um sicherzustellen, dass eine gegebene Transaktion von genau einem Programm zur Umschlagsgenerierung abgefragt wird. Sperren stellen sicher, dass, wenn mehrere Programme zur Umschlagsgenerierung einbezogen werden, nur ein Programm zur Umschlagsgenerierung eine gegebene Transaktion abfragt und verarbeitet. Die Programme zur Umschlagsgenerierung führen Abfragen gleichzeitig durch, sie arbeiten aber an verschiedenen Transaktionen.

Für die Sperre ist ein Zeitlimit festgelegt worden. Der Standardwert für eine Instanz des Programms zur Umschlagsgenerierung, um die Sperre zu halten, beträgt 240 Sekunden.

Wenn das Programm zur Umschlagsgenerierung auf die Sperre warten muss, wird es in eine Warteschlange gestellt. Das Höchstalter der Warteschlange, d. h. die Dauer, die das Programm zur Umschlagsgenerierung warten sollte, beträgt 740 Sekunden.

In der Regel müssen Sie die Standardwerte für das Sperren nicht ändern.

Stapelbetrieb

Mehrere Dokumente, die in einer Datei ankommen, werden entsprechend dem Verteilerhandler aufgeteilt, den Sie für diesen Dokumenttyp konfiguriert haben. (Das Konfigurieren von Verteilerhandlern, welches zum Definieren von Zielen gehört, wird in „Konfigurationspunkte ändern" auf Seite 52 beschrieben.) Eines der Attribute des Verteilerhandlers ist BCG_BATCHDOCS. Wenn BCG_BATCHDOCS auf ON (den Standardwert) gesetzt ist, fügt der Verteiler den Dokumenten Stapel-IDs hinzu, nachdem die Dokumente aufgeteilt wurden.

Das Programm zur Umschlagsgenerierung verfügt über ein Attribut für den Stapelbetrieb, welches sich auf das Attribut BCG_BATCHDOCS bezieht. Wenn Stapel-IDs den einzelnen Dokumenten zugeordnet worden sind, und Sie den Standardwert (ON) für Stapelbetrieb akzeptieren, stellt das Programm zur Umschlagsgenerierung sicher, dass alle Dokumente, die gemeinsam in derselben Datei ankommen, verarbeitet werden, bevor es diese mit einem Umschlag versieht und sie sendet, damit sichergestellt ist, dass die Transaktionen zusammen mit einem Umschlag versehen werden. Angenommen, es kommen z. B. fünf XML-Dokumente in derselben Datei an. Die XML-Dokumente sollen in EDI-Transaktionen transformiert und demselben Empfänger zugestellt werden. Nachdem nur drei der Dokumente transformiert wurden, beginnt das Programm zur Umschlagsgenerierung damit, seine terminierte Abfrage nach Transaktionen durchzuführen. Wenn der Stapelbetrieb ausgewählt ist, verarbeitet das Programm zur Umschlagsgenerierung die drei bereiten Transaktionen nicht, d. h. es versieht sie nicht mit einem Umschlag. Stattdessen wartet es so lange, bis die Verarbeitung aller fünf Transaktionen beendet wurde, bevor es sie mit einem Umschlag versieht und sie sendet. Die Transaktionen werden mit demselben Umschlag versehen, es sei denn, der gültige EDI-Standard verhindert das.

Die Standardwerte ändern

Führen Sie die folgenden Schritte aus, um beliebige Standardwerte für das Programm zur Umschlagsgenerierung zu ändern:

1. Klicken Sie auf **Hubadmin > Hubkonfiguration > EDI > Programm zur Umschlagsgenerierung**.
2. Klicken Sie auf das Symbol **Bearbeiten**.
3. Geben Sie neue Werte für **Maximale Sperrenzeit (Sekunden)** und **Höchstalter der Warteschlange (Sekunden)** ein, wenn Sie diesen Attributen mehr oder weniger Zeit zuordnen wollen.

   Anmerkung: In der Regel müssen Sie die Standardwerte nicht ändern.
4. Wenn Sie den Stapelbetrieb inaktivieren wollen, entfernen Sie das Häkchen neben **Stapelbetrieb verwenden**.
5. Wenn Sie ändern wollen, wie oft das Programm zur Umschlagsgenerierung eine Überprüfung auf zu sendende Transaktionen durchführt, führen Sie eine der folgenden Aufgabengruppen aus:
   - Um die intervallbasierte Zeitplanung (dies ist die Standardeinstellung) mit Änderung des Zeitraums zu verwenden, geben Sie eine neue Zeit neben **Intervall** ein. Wenn Sie z. B. den Wert in 30 Sekunden ändern, führt das Pro-

gramm zur Umschlagsgenerierung alle 30 Sekunden eine Überprüfung auf Dokumente durch, versieht diese Dokumente mit Umschlägen und sendet sie an den Empfänger.

- Führen Sie die folgenden Aufgaben aus, um die kalenderbasierte Zeitplanung zu verwenden:
  a. Klicken Sie auf **Kalenderbasierte Zeitplanung**.
  b. Wählen Sie den Zeitplanungstyp **Täglicher Zeitplan**, **Wöchentlicher Zeitplan** oder **Angepasster Zeitplan** aus.
     - Wenn Sie **Täglicher Zeitplan** auswählen, dann wählen Sie die Uhrzeit (Stunde und Minute) aus, wann das Programm zur Umschlagsgenerierung eine Überprüfung auf Dokumente durchführen soll.
     - Wenn Sie **Wöchentlicher Zeitplan** auswählen, dann wählen Sie mindestens einen Tag in der Woche zusätzlich zur Uhrzeit aus.
     - Wenn Sie **Angepasster Zeitplan** auswählen, dann wählen Sie die Uhrzeit und schließlich noch **Bereich** oder **Ausgewählte Tage** für die Woche und den Monat aus. Mit **Bereich** geben Sie das Startdatum und das Enddatum an. (Sie können z. B. auf **Mo** und **Fr** klicken, wenn Sie wollen, dass das Programm zur Umschlagsgenerierung nur an Wochentagen zu einer bestimmten Uhrzeit eine Überprüfung auf Dokumente durchführt.) Mit der Option **Ausgewählte Tage** wählen Sie bestimmte Tage in der Woche und im Monat aus.

6. Klicken Sie auf **Speichern**.

Umschlagsprofile

Ein Umschlagsprofil legt die Werte fest, die in bestimmte Elemente des Umschlags gestellt werden. Sie ordnen das Umschlagsprofil den EDI-Transaktionen im Dokumentenflussdefinitions-Attribut **Umschlagsprofil** zu. WebSphere Partner Gateway stellt ein vordefiniertes Umschlagsprofil für jeden unterstützten Standard (X12, EDIFACT oder UCS) bereit. Sie können diese vordefinierten Umschläge direkt verwenden, Sie können sie ändern, oder Sie können sie in neue Umschlagsprofile kopieren. Die Schritte zum Ändern oder Erstellen eines Umschlagsprofils sind in „Die Standardwerte ändern" auf Seite 111 beschrieben.

Die Umschlagsprofile haben für jedes Element im Umschlagsstandard ein Feld. Die Profile stellen konstante oder Literaldaten für das Erstellen von Header- und Trailersegmenten für Transaktionsgruppen, Nachrichten, funktionale Gruppen und Austauschvorgänge bereit. Sie geben nur die Werte an, die ausgefüllt werden müssen und für die keine andere Quelle einen Wert bereitstellt.

Die Feldnamen sind für das problemlose Arbeiten mit Querverweisen entworfen worden. Das Feld UNB03 ist z. B. das dritte Datenelement im UNB-Segment.

Wie in „Umschlagsattribute" beschrieben, haben Attribute, die woanders festgelegt wurden, Vorrang vor den Werten, die Sie im Umschlagsprofil festlegen. Einige von den Attributen können in Attributen oder Zuordnungen überschrieben werden, die sich auf die Dokumentenflussdefinition beziehen.

Umschlagsattribute

Umschlagsattribute können an mehreren unterschiedlichen Punkten während des Konfigurationsprozesses festgelegt werden, und sie können auch in der Transformationszuordnung festgelegt werden, die den Dokumenten zugeordnet ist. Der Zuordnungsexperte des Data Interchange Services-Clients kann z. B. das Merkmal **CtlNumFlag** angeben, wenn er eine Zuordnung definiert. Dieses Merkmal kann auch als Teil des Umschlagsprofils im Feld **Kontrollnummern nach Transaktions-**

IDs festgelegt werden. Jedes Attribut, das in der Transformationszuordnung festgelegt ist, überschreibt die zugehörigen Werte, die in Community Console festgelegt wurden. Wenn z. B. für **CtlNumFlag** in der Transformationszuordnung **N** (nein) festgelegt wurde und Sie den Wert **Y** (ja) im Feld **Kontrollnummern nach Transaktions-IDs** eingeben, wird der Wert **N** verwendet.

Weitere Umschlagsprofile können auf Protokollebene über die Seite **Dokumentenflussdefinitionen verwalten** bzw. über die einem Teilnehmer zugeordnete Seite **B2B-Funktionalität** festgelegt werden, oder sie können als Teil der Verbindung festgelegt werden. Die Rangfolge wird in der folgenden Liste aufgezeigt:

1. Merkmale, die in der Transformationszuordnung festgelegt sind, haben Vorrang vor den zugehörigen Attributen, die in Community Console festgelegt wurden.
2. Attribute, die auf der Verbindungsebene festgelegt sind, haben Vorrang vor denen, die auf der B2B-Funktionalitätsebene festgelegt wurden.
3. Attribute, die auf der B2B-Funktionalitätsebene festgelegt sind, haben Vorrang vor denen, die auf der Ebene der Dokumentenflussdefinitionen festgelegt wurden.
4. Attribute, die an einem beliebigen Ort (entweder in der Transformationszuordnung oder auf der Ebene der Dokumentenflussdefinitionen, der B2B-Funktionalität oder der Verbindung) festgelegt sind, haben Vorrang vor den Werten, die im Umschlagsprofil festgelegt wurden.

Eine Liste der Transformationszuordnungsmerkmale und ihrer zugeordneten Community Console-Attribute finden Sie in „Data Interchange Services-Clientmerkmale" auf Seite 313.

Die Standardwerte ändern

„Attribute für Umschlagsprofil" auf Seite 301 stellt eine Tabelle bereit, die die Standardwerte für jedes EDI-Standardumschlagsattribut zeigt, wenn Sie keinen Wert in das Profil eingeben, oder wenn Sie kein Profil erstellen. Stellen Sie sicher, dass die von Ihnen verwendeten Umschlagsprofile jedes obligatorische Element bereitstellen, das nicht vom System zur Ausführungszeit bereitgestellt wird.

Führen Sie die folgenden Schritte aus, um ein Umschlagsprofil zu konfigurieren:

1. Klicken Sie auf **Hubadmin > Hubkonfiguration > EDI > Umschlagsprofil**.
2. Führen Sie eine der folgenden Schrittegruppen aus:
   - Umschlag erstellen
     a. Klicken Sie auf **Erstellen**.
     b. Geben Sie einen Namen für das Profil ein. Dies ist der Name, der in der Liste **Umschlagsprofile** angezeigt wird.
     c. Geben Sie optional eine Beschreibung des Profils ein.
     d. Klicken Sie auf den EDI-Standard, zu dem der Umschlag gehört. Wenn Sie z. B. Dokumente austauschen, die dem EDI-X12-Standard entsprechen, wählen Sie **X12** aus.
   - Umschlag ändern
     a. Wählen Sie eines der vorhandenen Umschlagsprofile aus, indem Sie auf das Symbol **Details anzeigen** neben dem Namen des Profils klicken.
     b. Klicken Sie auf das Symbol **Bearbeiten**.
3. Die Schaltfläche **Allgemein** ist standardmäßig ausgewählt. Sie können einen Wert für ein beliebiges Feld eingeben mit Ausnahme von ENVTYPE, welcher mit dem Standard vorab ausgefüllt wurde, den Sie in Schritt 2d ausgewählt haben.

Sie können für die folgenden Felder Werte hinzufügen:

- **Länge der Austauschkontrollnummer**. Gibt an, wie viele Zeichen verwendet werden sollten, wenn eine Kontrollnummer einem Austausch im Umschlag zugeordnet wird.
- **Länge der Gruppenkontrollnummer**. Gibt an, wie viele Zeichen verwendet werden sollten, wenn eine Kontrollnummer einer Gruppe im Umschlag zugeordnet wird.
- **Länge der Transaktionskontrollnummer**. Gibt an, wie viele Zeichen verwendet werden sollten, wenn eine Kontrollnummer einer Transaktion im Umschlag zugeordnet wird.
- **Max. Anzahl an Transaktionen**. Gibt die maximale Anzahl Transaktionen an, die in diesem Umschlag zulässig sind.
- **Kontrollnummern nach Transaktions-IDs**. Gibt an, ob Sie die Transaktions-ID als Teil des Schlüssels verwenden wollen, wenn die Gruppennummern in der Datenbank gesucht werden. Ist dies der Fall, werden verschiedene Gruppen von Kontrollnummern für jede Transaktions-ID verwendet.

Die Felder für das Umschlagsprofil **Allgemein** sind in allen drei Standards gleich, außer dass EDIFACT über ein zusätzliches Feld verfügt: **Gruppen für EDI erstellen**.

Wenn Sie Änderungen an der Seite **Allgemein** vorgenommen haben, klicken Sie auf **Speichern**.

4. Um Werte für den Austausch anzugeben, klicken Sie auf **Austausch**. Eine neue Gruppe von Feldern wird auf der Seite angezeigt. Die Felder variieren je nach EDI-Standard. Beachten Sie, dass einige von den Werten schon ausgefüllt sind bzw. während der Ausführung ausgefüllt werden.
   - Für den EDI-X12-Standard können Sie die folgenden Felder ändern:
     - **ISA01: Qualifikationsmerkmal für Autorisierungsinformationen**. Dies ist ein Code für den Informationstyp in ISA02.
     - **ISA02: Autorisierungsinformationen**. Das sind Informationen, die verwendet werden, um den Absender der Austauschdaten noch weiter anzugeben bzw. zu autorisieren.
     - **ISA03: Qualifikationsmerkmal für Sicherheitsinformationen**. Dies ist ein Code für den Informationstyp in ISA04. Gültige Werte:

       00 ISA04 ist nicht aussagekräftig.

       01 ISA04 enthält ein Kennwort.
     - **ISA04: Sicherheitsinformationen**. Das sind Sicherheitsinformationen zu dem Absender oder den Austauschdaten. Der Code in ISA03 definiert den Informationstyp.
     - **ISA11: ID der Austauschstandards**. Das ist ein Code für die Stelle, die den Austausch kontrolliert. Gültige Werte sind **U** (US EDI Community von ASC X12), **TDCC**, und **UCS**.

       Anmerkung: Dieses Attribut wird für X12-Versionen bis 4010 verwendet. In X12 4020 wird das ISA11-Element als Wiederholungstrennzeichen verwendet.
     - **ISA12: ID der Austauschversion**. Das ist die Versionsnummer der Syntax in den Austauschsegmenten und den Steuerungssegmenten der funktionalen Gruppe.
     - **ISA14: Bestätigung angefordert**. Das ist der Code des Absenders für das Anfordern einer Bestätigung. Gültige Werte:

0 Keine Bestätigung anfordern.

1 Bestätigung darüber anfordern, dass ISA- und IEA-Segmente empfangen und erkannt wurden.

– **ISA15: Testanzeiger**. Das ist eine Meldung darüber, dass der Austausch für Testzwecke oder die Produktion ist. Gültige Werte:

T Für Testdaten.

P Für Produktionsdaten.

- Für den UCS-Standard können Sie die folgenden Felder ändern:
  – **BG01: Kommunikations-ID**. Das ist die Kennung des übertragenden Unternehmens.
  – **BG02: Kommunikationskennwort**. Das ist ein vom Empfänger zugeordnetes Kennwort, das von den Teilnehmern als vereinbart verwendet werden soll.
- Für den EDIFACT-Standard können Sie die folgenden Felder ändern:
  – **UNB0101: Syntax-ID**. Das ist die Kennung der Stelle, die die verwendete Syntax kontrolliert. Die kontrollierende Stelle lautet UNO. Die Ebene ist A oder B.
  – **UNB0102: Syntaxversion**. Das ist die Versionsnummer der Syntax, die von der Syntax-ID angegeben wird.
  – **UNB0601: Referenz/Kennwort des Empfängers**. Das ist ein vom Empfänger zugeordnetes Kennwort, das von den Teilnehmern als vereinbart verwendet werden soll.
  – **UNB0602: Qualifikationsmerkmal für Referenz/Kennwort des Empfängers**. Das ist ein Qualifikationsmerkmal für das Kennwort des Empfängers, das von den Teilnehmern als vereinbart verwendet werden soll.
  – **UNB07: Anwendungsreferenz**. Das ist die Kennung des Funktionsbereichs vom Absender, auf die die Austauschnachrichten verweisen.
  – **UNB08: Priorität**. Das ist der Code des Absenders für die Verarbeitungspriorität, wie mit dem Teilnehmer vereinbart. Code A hat die höchste Priorität.
  – **UNB09: Bestätigungsanforderung**. Das ist der Code des Absenders für das Anfordern einer Bestätigung.
  – **UNB10: ID der Kommunikationsvereinbarung**. Das ist der Name oder Code für den Vereinbarungstyp, der für diesen Austausch verwendet wird, wie mit dem Teilnehmer vereinbart.
  – **UNB11: Testanzeiger (Nutzungsanzeiger)**. Das ist eine Meldung darüber, dass der Austausch für Testzwecke ist. 1 gibt einen Testaustausch an.

Wenn Sie Änderungen an der Seite **Austausch** vorgenommen haben, klicken Sie auf **Speichern**.

5. Um Werte für die Gruppen im Austausch anzugeben, klicken Sie auf **Gruppe**. Eine neue Gruppe von Feldern wird angezeigt. Die Felder variieren je nach EDI-Standard.

   Die Felder auf dieser Seite definieren in der Regel den Absender und den Empfänger der Gruppe.

   - Für die EDI-X12- und UCS-Standards können Sie in den folgenden Feldern Werte eingeben:
     – **GS01: ID der funktionalen Gruppe**. Das ist eine Kennung des Transaktionsgruppentyps in der Gruppe.

- **GS02: Anwendungsabsender**. Das ist der Name oder Code für eine bestimmte Abteilung im Unternehmen des Absenders.
- **GS03: Anwendungsempfänger**. Das ist der Name oder Code für die bestimmte Abteilung im Unternehmen des Empfängers, die die Gruppe empfangen soll.
- **GS07: Gruppenstelle**. Das ist ein Code, der mit GS08 verwendet wird, um die Stelle anzugeben, die den Standard kontrolliert.
- **GS08: Gruppenversion**. Das ist ein Code für die Version, das Release und die Branche des Standards.

• Für den EDIFACT-Standard können Sie in den folgenden Feldern Werte eingeben:
- **UNG01: ID der funktionalen Gruppe**. Das ist eine Kennung des Nachrichtentyps in der Gruppe.
- **UNG0201: Anwendungsabsender-ID**. Das ist der Name oder Code für eine bestimmte Abteilung im Unternehmen des Absenders.
- **UNG0202: Qualifikationsmerkmal für Anwendungsabsender-ID**. Das ist das Qualifikationsmerkmal für den Absender-ID-Code. Eine Liste der Qualifikationsmerkmale für den Code finden Sie im Datenelementverzeichnis.
- **UNG0301: Anwendungsempfänger-ID**. Das ist der Name oder Code für die bestimmte Abteilung im Unternehmen des Empfängers, die die Gruppe empfangen soll.
- **UNG0302: Qualifikationsmerkmal für Anwendungsempfänger-ID**. Das ist das Qualifikationsmerkmal für den Empfänger-ID-Code. Eine Liste der Qualifikationsmerkmale für den Code finden Sie im Datenelementverzeichnis.
- **UNG06: Kontrollierende Stelle**. Der Code, der die Stelle angibt, welche die Kontrolle über den Nachrichtentyp in der funktionalen Gruppe hat.
- **UNG0701: Nachrichtenversion**. Das ist die Versionsnummer für den Nachrichtentyp.
- **UNG0702: Nachrichtenrelease**. Das ist die Releasenummer in der Versionsnummer für den Nachrichtentyp.
- **UNG0703: Zugeordnete Assoziation**. Das ist der Code, der von der verantwortlichen Assoziation zugeordnet wurde, der den Nachrichtentyp noch weiter angibt.
- **UNG08: Anwendungskennwort**. Das ist das Kennwort, das von der bestimmten Abteilung im Unternehmen des Empfängers zugeordnet wurde.

Wenn Sie Änderungen an der Seite **Gruppe** vorgenommen haben, klicken Sie auf **Speichern**.

6. Um Werte für Transaktionen in einer Gruppe anzugeben, klicken Sie auf **Transaktion**, oder bei EDIFACT klicken Sie auf **Nachricht**. Eine neue Gruppe von Feldern wird angezeigt. Die Felder variieren je nach EDI-Standard.
   • Für den EDI-X12- oder USC-Standard können Sie einen Wert für **ST03: ID-Zeichenfolge der Implementierungskonvention** eingeben.
   • Für den EDIFACT-Standard können Sie in den folgenden Feldern einen Wert eingeben:
   - **UNH0201: Nachrichtentyp**. Das ist ein Code, der von der kontrollierenden Stelle zugeordnet wurde, um den Nachrichtentyp anzugeben.
   - **UNH0202: Nachrichtenversion**. Das ist die Versionsnummer für den Nachrichtentyp.

- **UNH0203: Nachrichtenrelease**. Das ist die Releasenummer in der Versionsnummer für den Nachrichtentyp.
- **UNH0204: Kontrollierende Stelle**. Das ist ein Code für die Stelle, die den Nachrichtentyp kontrolliert.
- **UNH0205: Von Assoziation zugeordneter Code**. Das ist der Code, der von der verantwortlichen Assoziation zugeordnet wurde, der den Nachrichtentyp noch weiter angibt.
- **UNH03: Referenz für allgemeinen Zugriff**. Das ist der Schlüssel, der auf alle nachfolgenden Datenübertragungen in eine gemeinsame Datei verweist. Teilnehmer können der Verwendung eines Schlüssels zustimmen, der aus Komponenten besteht, aber Unterelementseparatoren können nicht verwendet werden.

Wenn Sie Änderungen an der Seite **Transaktion** vorgenommen haben, klicken Sie auf **Speichern**.

7. Klicken Sie auf **Speichern**.
8. Wiederholen Sie die Schritte 2 auf Seite 111 bis 7 für jedes weitere Umschlagsprofil, das Sie definieren oder ändern wollen.

Nachdem ein Umschlagsprofil definiert ist, wird es in der Liste **Umschlagsprofile** aufgelistet. Sie können das Profil in der Liste auswählen, und klicken Sie dann auf das Symbol **Verwendet von**, um die Verbindungen zu ermitteln, die das Profil verwenden.

Verbindungsprofile

Sie verwenden Verbindungsprofile mit Transaktionen, von denen der Umschlag entfernt wurde, und mit EDI-Austauschvorgängen, die vom Programm zur Umschlaggenerierung erstellt wurden. Bei Transaktionen bestimmt das Verbindungsprofil, wie die Transaktion verarbeitet wird, nachdem ihr Umschlag entfernt wurde. Bei Austauschvorgängen bestimmt das Verbindungsprofil, wie der Austausch zugestellt wird.

Die folgende Tabelle zeigt die Verbindungsprofilattribute, ihre entsprechenden Feldnamen auf der Seite **Details des Verbindungsprofils** und ob sie auf Austauschvorgänge oder Transaktionen angewendet werden:

Tabelle 14. Verbindungsprofilattribute

Attribut	Feldname	EDI-Austausch	EDI-Transaktion
Qualifikationsmerkmal1 für Verbindungsprofil	Qualifikationsmerkmal1	X	
Nutzungsanzeiger für Austausch	EDI-Verwendungstyp		X
Kennung für Absender der Gruppenanwendung	Anwendungsabsender-ID		X
Kennung für Empfänger der Gruppenanwendung	Anwendungsempfänger-ID		X
Kennwort für Gruppenanwendung	Kennwort		X

Transaktionen

Wenn ein EDI-Austausch bei WebSphere Partner Gateway eingeht, besteht die erste Aktion in der Regel darin, vom Austausch den Umschlag zu entfernen, um so die einzelnen Transaktionen zu erhalten. Wenn die Transaktionen erstellt sind, legt die

Aktion zum Umschlag entfernen den **Nutzungsanzeiger für Austausch** und die Gruppeninformationen (**Kennung für Absender der Gruppenanwendung**, **Kennung für Empfänger der Gruppenanwendung** und **Kennwort für Gruppenanwendung**) in den Transaktionsmetadaten fest. Jede Transaktion wird dann erneut von WebSphere Partner Gateway in ihrem eigenen Arbeitsablauf verarbeitet.

Angenommen, Sie verfügen über zwei Transaktionen desselben Typs (z. B. 850), die abhängig von der Gruppe, in der sie sich befinden, oder von den Werten Ihrer Nutzungsanzeiger für Austausch unterschiedlich verarbeitet werden müssen. Wenn der **Nutzungsanzeiger** z. B. Produktion (**P**) lautet, wollen Sie unter Umständen eine Zuordnung (A) verwenden, und wenn der **Nutzungsanzeiger** Test (**T**) lautet, wollen Sie möglicherweise eine zweite Zuordnung (B) verwenden. Zwei ähnliche Verbindungen sind für diese 850-Transaktion erforderlich, der einzige Unterschied besteht darin, dass eine Verbindung Zuordnung A und die andere Verbindung Zuordnung B verwendet.

Da die Transaktionen sich sonst nicht unterscheiden (sie verfügen über Teilnehmer, Paket, Protokoll und Dokumenttyp derselben Quelle und desselben Ziels), benötigt Document Manager eine Möglichkeit, um zu ermitteln, welche Verbindung verwendet werden soll. Er tut dies, indem er das Verbindungsprofilattribut in Übereinstimmung bringt, das Sie in den Transaktionsmetadaten festgelegt haben. Wenn Sie in diesem Beispiel zwei Verbindungsprofile erstellt haben, ein Verbindungsprofil (CPProduction) mit **EDI-Verwendungstyp** auf **P** und das andere Verbindungsprofil (CPTest) mit **EDI-Verwendungstyp** auf **T** gesetzt, bringt Document Manager die Transaktion mit einem **Nutzungsanzeiger** von **P** mit dem CPProduction-Profil in Übereinstimmung. Er weiß dann, dass Zuordnung A zu verwenden ist, um die Transaktion zu konvertieren.

Das Beispiel in diesem Abschnitt hat das Attribut **Nutzungsanzeiger für Austausch** verwendet, aber Sie können auch die Attribute **Kennung für Absender der Gruppenanwendung**, **Kennung für Empfänger der Gruppenanwendung** und **Kennwort für Gruppenanwendung** als Unterscheidungsfaktor für eine Transaktion verwenden.

Austauschvorgänge

Bei Austauschvorgängen verwenden Sie das Attribut **Qualifikationsmerkmal1 für Verbindungsprofil**.

Angenommen, Sie sind z. B. mitten bei der Migration Ihres Unternehmens von der Verwendung eines VAN (Paket **None**) oder des Internets (Paket **AS2**). Sie wollen, dass 840-Transaktionen (Request for Quote) das VAN und 850-Transaktionen (Purchase Order) das Internet verwenden. Sie konfigurieren zwei Teilnehmerverbindungen, die beide denselben Quellenaustausch, aber unterschiedliche Ziele haben (eine Verbindung mit Paket **None** und die andere Verbindung mit Paket **AS2**). Die Verbindungsprofile sind bei der Unterscheidung der zwei Verbindungen hilfreich.

Das Konfigurieren des Verbindungsprofils für Austauschvorgänge schließt mehrere Schritte ein. Die folgenden Schritte würden Sie ausführen, um zwei Verbindungsprofile für das Beispiel zu erstellen:

1. Erstellen Sie zwei Verbindungen für die Transaktionen. Legen Sie das Attribut **Qualifikationsmerkmal1 für Verbindungsprofil** auf der Seite "An" von beiden Verbindungen fest. Der Wert sollte aussagekräftig sein, z. B. `ConNone` und `ConAS2`.
2. Definieren Sie zwei Verbindungsprofile, z. B. `CPNone` und `CPAS2`, legen Sie den Wert **Qualifikationsmerkmal1** für beide so fest, dass sie mit den Attributen

Qualifikationsmerkmal1 für Verbindungsprofil übereinstimmen, die Sie in Schritt 1 auf Seite 116 (`ConNone` und `ConAS2`) festgelegt haben.

3. Erstellen Sie zwei Verbindungen für den Austausch. Jede Verbindung hat dasselbe Quellenpaket **N/A**, aber unterschiedliche Zielpakete (**None** und **AS2**). Für die Teilnehmerverbindung mit dem Verbindungsprofil `ConNone` ist als Zielgateway das FTP-Scripting-Gateway festgelegt, das eine Verbindung zum VAN herstellen kann. Für die Teilnehmerverbindung mit dem Verbindungsprofil `CPAS2` ist als Zielpaket **AS** festgelegt.
4. Ordnen Sie die entsprechenden Verbindungsprofile einander zu.

Das Programm zur Umschlagsgenerierung verwendet das Attribut **Qualifikationsmerkmal1 für Verbindungsprofil** auf der Seite "An" von der Teilnehmerverbindung als Umschlagsunterbrechungspunkt. Daher werden Transaktionen, die unterschiedliche Werte für das Attribut **Qualifikationsmerkmal1 für Verbindungsprofil** haben, mit unterschiedlichen Umschlägen versehen. Wenn Sie unterschiedliche Werte für die Transaktionen festlegen, wird das Programm zur Umschlagsgenerierung die 840- und 850-Transaktionen nie mit einem Umschlag für denselben Austausch versehen.

Wenn Document Manager die Verbindung sucht, werden die zwei möglichen Verbindungen gefunden, aber die Verbindung mit dem übereinstimmenden Verbindungsprofil wird verwendet.

Verbindungsprofile konfigurieren

Das Konfigurieren der Verbindungsprofile ist optional. Wenn Sie für jeden Dokumenttyp nur jeweils eine Verbindung benötigen, dann führen Sie den Austausch für einen Teilnehmer durch. Überspringen Sie diesen Abschnitt.

Gehen Sie wie folgt vor, um ein Verbindungsprofil zu konfigurieren:

1. Klicken Sie auf **Hubadmin > Hubkonfiguration > EDI > Verbindungsprofile**.
2. Klicken Sie auf **Verbindungsprofil erstellen**.
3. Geben Sie auf der Seite **Details des Verbindungsprofils** einen erforderlichen Namen für dieses Verbindungsprofil ein.
4. Geben Sie eine optionale Beschreibung des Profils ein.

   Der Name und die Beschreibung, falls Sie eine Beschreibung eingeben, werden auf der Seite **Liste der Verbindungsprofile** angezeigt.
5. Geben Sie optional einen Wert für **Qualifikationsmerkmal1** zur Angabe des Werts ein, der bestimmt, welche Verbindung für einen EDI-Austausch verwendet wird. Ein Beispiel zur Verwendung von **Qualifikationsmerkmal1** finden Sie in „Austauschvorgänge" auf Seite 116.
6. Geben Sie optional einen Wert für **EDI-Verwendungstyp** ein, um anzugeben, ob dies ein Test-, Produktions- oder Informationsaustausch ist. Ein Beispiel zur Verwendung von **EDI-Verwendungstyp** finden Sie in „Transaktionen" auf Seite 115.
7. Geben Sie optional einen Wert für **Anwendungsabsender-ID** ein, um die Anwendung oder den Unternehmensbereich anzugeben, die bzw. der dem Absender der Gruppe zugeordnet ist.
8. Geben Sie optional einen Wert für **Anwendungsempfänger-ID** ein, um die Anwendung oder den Unternehmensbereich anzugeben, die bzw. der dem Empfänger der Gruppe zugeordnet ist.
9. Geben Sie optional einen Wert für **Kennwort** ein, falls ein Kennwort zwischen dem Anwendungsabsender und dem Anwendungsempfänger erforderlich ist.
10. Klicken Sie auf **Speichern**.

Für die Transaktionen, die Sie in bestimmte Austauschumschläge stellen wollen, können Sie den Attributwert **Qualifikationsmerkmal1 für Verbindungsprofil** angeben, der dem Verbindungsprofil mit demselben Wert für das Attribut **Qualifikationsmerkmal1** entspricht. Das Attribut **Qualifikationsmerkmal1 für Verbindungsprofil** kann auf der Protokollebene einer Dokumentenflussdefinition festgelegt werden. Sie könnten z. B. die Attribute des X12V5R1-Protokolls in der Anzeige **Dokumentenflussdefinitionen verwalten** bearbeiten, um das zu verwendende Verbindungsprofil anzugeben, indem Sie auf den entsprechenden Attributwert **Qualifikationsmerkmal1 für Verbindungsprofil** klicken. Dann, wenn Sie die Austauschverbindung aktiviert haben, ordnen Sie das Verbindungsprofil zu, indem Sie auf die Schaltfläche **Verbindungsprofil** klicken und ein Profil in der Liste auswählen.

Kontrollnummern

Das Programm zur Umschlaggenerierung verwendet Kontrollnummern, um eine eindeutige Nummerierung für Austauschvorgänge, Gruppen und Transaktionen in einem Umschlag bereitzustellen. Kontrollnummern werden für Community Manager und für Teilnehmer erstellt. Wenn der Austausch von Dokumenten stattfindet, werden Kontrollnummern auch für das *Paar* von Teilnehmern generiert.

Für jeden Teilnehmer, der über die EDI-B2B-Funktionalität verfügt, gibt es eine Gruppe von Startinitialisierungswerten für Kontrollnummern. Diese Werte werden verwendet, wenn ein EDI-Austausch das erste Mal erstellt und zwischen einem Teilnehmerpaar gesendet wird. Die Initialisierungswerte werden auf den Teilnehmer angewendet, an den der Austausch gesendet wird. Nachdem ein Dokument von einem Teilnehmer zum anderen gesendet wurde, können die zuletzt verwendeten Nummern auf der Seite **Aktuelle Kontrollnummern** angezeigt werden. Es gibt mehrere Einträge für ein gegebenes Teilnehmerpaar, wenn **Kontrollnummern nach Transaktions-IDs** auf **Y** gesetzt ist. Nachdem ein Eintrag vorhanden ist, werden mit ihm neue Kontrollnummern generiert.

Als Teil der Kontrollnummerninitialisierung können Sie Masken verwenden, um die normale Kontrollnummernerstellung durch das Programm zur Umschlaggenerierung zu ändern. Die Masken werden verwendet, damit die Kontrollnummer entweder auf dem Austausch oder auf der Gruppenkontrollnummer basiert. Die Maskenbeschreibungen folgen. Ersetzen Sie das *n* in der Bearbeitungsmaske mit der Anzahl Byte, die Sie für die Erstellung des Kontrollnummernwerts verwenden wollen. In Tabelle 15 sind die Beschreibungen der verfügbaren Codes enthalten:

Tabelle 15. Kontrollnummernmasken

Code	Kontroll-nummer	Beschreibung
G	Transaktion	Die Transaktionskontrollnummer entspricht der Gruppenkontrollnummer. Es ist nur eine Transaktion für jede Gruppe zulässig.
G*n*	Transaktion	*n* Byte werden von der Gruppenkontrollnummer genommen. Der Rest der Transaktionskontrollnummer wird bis zu ihrer Maximalgröße mit Nullen aufgefüllt. Es ist nur eine Transaktion für jede Gruppe zulässig.
C	Gruppe, Transaktion	Die übrigen Byte im Feld für die Gruppen- oder Transaktionskontrollnummer werden verwendet, um eine Kontrollnummer für diesen Teilnehmer zu verwalten.

Tabelle 15. Kontrollnummernmasken (Forts.)

Code	Kontroll-nummer	Beschreibung
V	Gruppe, Trans-aktion	Ein zunehmender Wert wird verwendet, so dass die erste Gruppe oder Transaktion einen Wert von 1 hat, die zweite einen Wert von 2 usw..
V*n*	Transaktion	Ein zunehmender Wert, der *n* Byte lang ist, wird verwendet, so dass die erste Transaktion einen Wert von 1 hat, die zweite einen Wert von 2 usw..
G*n*C	Transaktion	*n* Byte werden von der Gruppenkontrollnummer genommen und die übrigen Byte im Feld für die Transaktionskontrollnummer werden verwendet, um eine Kontrollnummer zu verwalten. Die Anzahl ausgelassener Stellen bestimmt den Höchstwert der Kontrollnummer. G5C lässt z. B. vier Stellen aus; daher beträgt der Höchstwert 9999. Die Kontroll-nummer springt vom Höchstwert wieder auf 1 zurück.
G*n*V	Transaktion	*n* Byte werden von der Gruppenkontrollnummer genommen. Für die übrigen Byte im Feld für die Transaktionskontrollnummer wird ein zunehmender Wert verwendet, so dass die erste Transaktion einen Wert von 1 hat, die zweite einen Wert von 2 usw..
G*n*V*m*	Transaktion	*n* Byte werden von der Gruppenkontrollnummer genommen. Für die übrigen Byte, bis zu *m* Byte, im Feld für die Transaktionskontrollnummer wird ein zunehmender Wert verwendet, so dass die erste Trans-aktion einen Wert von 1 hat, die zweite einen Wert von 2 usw..
I	Gruppe, Trans-aktion	Die Gruppen- oder Transaktionskontrollnummer sollte der Austauschkontrollnummer gleichen. Für den Aus-tausch ist nur eine Gruppe zulässig und für die Gruppe oder den Austausch ist nur eine Transaktion zulässig.
I*n*	Gruppe, Trans-aktion	*n* Byte werden von der Austauschkontrollnummer genommen. Der Rest des Felds für die Gruppen- oder Transaktionskontrollnummer wird bis zur Maximal-größe mit Nullen aufgefüllt. Für jeden Austausch ist nur eine Gruppe zulässig und für jede Gruppe ist nur eine Transaktion zulässig.
I*n*C	Gruppe, Trans-aktion	*n* Byte werden von der Austauschkontrollnummer genommen. Die übrigen Byte im Feld für die Grup-pen- oder Transaktionskontrollnummer werden ver-wendet, um eine Kontrollnummer zu verwalten. Die Anzahl ausgelassener Stellen bestimmt den Höchst-wert der Kontrollnummer. I5C lässt z. B. vier Stellen aus; daher beträgt der Höchstwert 9999. Die Kontroll-nummer springt vom Höchstwert wieder auf 1 zurück.
I*n*V	Gruppe, Trans-aktion	*n* Byte werden von der Austauschkontrollnummer genommen. Für die übrigen Byte im Feld für die Gruppen- oder Transaktionskontrollnummer wird ein zunehmender Wert verwendet, so dass die erste Gruppe oder Transaktion einen Wert von 1 hat, die zweite einen Wert von 2 usw..

Tabelle 15. Kontrollnummernmasken (Forts.)

Code	Kontroll-nummer	Beschreibung
I*n*V*m*	Transaktion	*n* Byte werden von der Austauschkontrollnummer genommen. Für die übrigen Byte, bis zu *m* Byte, im Feld für die Transaktionskontrollnummer wird ein zunehmender Wert verwendet, so dass die erste Transaktion einen Wert von 1 hat, die zweite einen Wert von 2 usw..
I*n*G*m*	Transaktion	*n* Byte werden von der Austauschkontrollnummer genommen, und ein Maximum von *m* Byte werden von der Gruppenkontrollnummer genommen. Wenn *n* + *m* größer als 9 ist, werden nur 9 - *n* Byte von der Gruppenkontrollnummer genommen. Wenn Sie z. B. I4G6 verwenden, dann werden 4 Byte vom Austausch genommen.
I*n*G*m*C	Transaktion	*n* Byte werden von der Austauschkontrollnummer genommen, und *m* Byte werden von der Gruppenkontrollnummer genommen. Die übrigen Byte im Feld für die Transaktionskontrollnummer werden verwendet, um eine Kontrollnummer zu verwalten. Die Anzahl ausgelassener Stellen bestimmt den Höchstwert der Kontrollnummer. I2G4C lässt z. B. drei Stellen aus; daher beträgt der Höchstwert 999. Die Kontrollnummer springt vom Höchstwert wieder auf 1 zurück.
I*n*G*m*V	Transaktion	*n* Byte werden von der Austauschkontrollnummer genommen, und *m* Byte werden von der Gruppenkontrollnummer genommen. Für die übrigen Byte im Feld für die Transaktionskontrollnummer wird ein zunehmender Wert verwendet, so dass die erste Transaktion einen Wert von 1 hat, die zweite einen Wert von 2 usw..
I*n*G*m*V*o*	Transaktion	*n* Byte werden von der Austauschkontrollnummer genommen, und *m* Byte werden von der Gruppenkontrollnummer genommen. Für die übrigen Byte, bis zu *o* Byte, im Feld für die Transaktionskontrollnummer wird ein zunehmender Wert verwendet, so dass die erste Transaktion einen Wert von 1 hat, die zweite einen Wert von 2 usw..

Initialisierung der Kontrollnummer

Führen Sie die folgenden Schritte aus, um die Kontrollnummern zu konfigurieren, die das Programm zur Umschlaggenerierung verwenden wird:

1. Klicken Sie auf **Hubadmin > Hubkonfiguration > EDI > Initialisierung der Kontrollnummer**.
2. Geben Sie einen Teilnehmernamen ein, und klicken Sie auf **Suchen**, oder klicken Sie auf **Suchen**, ohne einen Namen einzugeben, um alle Teilnehmer anzuzeigen. Wenn Sie **EDI-fähige suchen** auswählen, begrenzen Sie die Suche auf die Teilnehmer, die über EDI-Dokument-B2B-Funktionalität verfügen. Wenn Sie das Häkchen entfernen, durchsuchen Sie alle Teilnehmer.
3. Klicken Sie auf das Symbol **Details anzeigen** neben dem Teilnehmer.

4. Die aktuellen Kontrollnummernzuordnungen des Teilnehmers (sofern vorhanden) werden auf der Seite **Konfigurationsdetails der Kontrollnummer** angezeigt. Klicken Sie auf das Symbol **Bearbeiten**, um die Werte hinzuzufügen oder zu ändern.
5. Geben Sie den Wert neben **Austausch** ein oder ändern Sie ihn, um die Nummer anzugeben, mit der Sie die Kontrollnummerngenerierung für Austauschvorgänge initialisieren wollen.
6. Geben Sie den Wert neben **Gruppen** ein oder ändern Sie ihn, um die Nummer anzugeben, mit der Sie die Kontrollnummerngenerierung für Gruppen initialisieren wollen. Alternativ hierzu können Sie auf **Maske** klicken, und Sie können eine zu verwendende Maske anstelle eines festen Werts eingeben.
7. Geben Sie den Wert neben **Transaktion** ein oder ändern Sie ihn, um die Nummer anzugeben, mit der Sie die Kontrollnummerngenerierung für Transaktionen initialisieren wollen. Alternativ hierzu können Sie auf **Maske** klicken, und Sie können eine zu verwendende Maske anstelle eines festen Werts eingeben.
8. Klicken Sie auf **Speichern**.

Aktuelle Kontrollnummern

Für ein gegebenes Teilnehmerpaar, das bereits über Daten in der Steuertabelle verfügt, können Sie die Kontrollnummerngenerierung ändern. Sie können Folgendes ausführen:

- Setzen Sie die Kontrollnummerngenerierung für das Paar auf einen Anfangsstatus zurück.
- Bearbeiten Sie die Austausch-, Gruppen- oder Transaktionsnummer (oder eine beliebige Kombination dieser Nummern), und speichern Sie diese mit einem neuen Wert.

Anmerkung: Das Zurücksetzen der Kontrollnummerngenerierung bzw. das Bearbeiten einer Gruppe oder Maske sollte mit Vorsicht durchgeführt werden, so dass Probleme mit Nummern in falscher Reihenfolge oder mit duplizierten Kontrollnummern nicht auftreten. Sie könnten eine von diesen Aktionen während der Testphase durchführen oder wenn ein Partner ausdrücklich verschiedene Kontrollnummern anfordert.

Sie verwenden die Funktion **Aktuelle Kontrollnummern**, um zu ermitteln, welchen Teilnehmern Kontrollnummern zugeordnet sind und um zu ermitteln, wie diese Nummern lauten.

1. Klicken Sie auf **Hubadmin > Hubkonfiguration > EDI > Aktuelle Kontrollnummern**.
2. Führen Sie eine der folgenden Schrittegruppen aus:
   - Wenn Sie den aktuellen Status aller Teilnehmer anzeigen wollen, behalten Sie die Auswahl von **Alle Teilnehmer** in den Teilnehmerlisten bei, und klicken Sie auf **Aktuellen Status anzeigen**.
   - Wenn Sie den Status ausgewählter Teilnehmer anzeigen wollen, führen Sie die folgenden Schritte aus:
     a. Geben Sie den Namen der Quellen- und Zielteilnehmer ein, und klicken Sie auf **Suchen**. Wenn Sie die Suchergebnisse auf nur die Teilnehmer beschränken wollen, die EDI-Dokumente austauschen, behalten Sie die Auswahl von **EDI-fähige suchen** bei.
     b. Wählen Sie in den Ergebnislisten mindestens einen Teilnehmer in jeder Liste aus, und klicken Sie auf **Aktuellen Status anzeigen**.

Allgemeine Schritte für das Definieren von Dokumentaustauschvorgängen

Dieser Abschnitt bietet eine Übersicht auf höchster Ebene über die Aufgaben, die Sie ausführen müssen, um den Austausch von Dokumenten für EDI-Austauschvorgänge, die auf dem Hub eingehen, Dokumente oder Transaktionen, die auf dem Hub transformiert werden, sowie für EDI-Austauschvorgänge, die vom Hub gesendet werden, zu erstellen. Die in den folgenden Abschnitten gezeigten Schritte sind allgemein und gelten nur für das Importieren von Zuordnungen und das Konfigurieren von Interaktionen. Die allgemeinen Schritte für das Aktivieren der B2B-Funktionalität für Teilnehmer für alle Dokumentaustauschtypen werden in „B2B-Funktionalität konfigurieren" auf Seite 163 beschrieben. Die allgemeinen Schritte für das Verwalten von Verbindungen für alle Dokumentaustauschtypen wird in Kapitel 12, „Verbindungen verwalten", auf Seite 165 beschrieben. Wenn Sie ein umfassendes Beispiel für einen EDI-Dokumentaustausch vom Importieren der Zuordnungen bis zum Verwalten der Verbindungen sehen wollen, lesen Sie Anhang B, „EDI-Beispiele", auf Seite 211. Der Anhang umfasst die folgenden spezifischen Beispiele:

- „Beispiel: EDI zu ROD" auf Seite 211
- „Beispiel: EDI zu XML" auf Seite 225
- „Beispiel: ROD zu EDI" auf Seite 237
- „Beispiel: XML zu EDI" auf Seite 230

Zuordnungen importieren

Transformationszuordnungen für EDI-, XML- oder ROD-Dokumente können mit dem Data Interchange Services-Clientprogramm erstellt werden. Der Data Interchange Services-Client ist ein Programm, mit dem XML-Schemadokumentdefinitionen, XML-DTD-Dokumentdefinitionen, EDI-Standards, ROD-Dokumentdefinitionen sowie Zuordnungen erstellt und verwaltet werden.

Der Data Interchange Services-Client ist ein separat installiertes Programm, das auf dem WebSphere Partner Gateway-Datenträger enthalten ist, sich aber in der Regel auf einem anderen Computer befindet. Der Zuordnungsexperte von Data Interchange Services erstellt eine Zuordnung, die angibt, wie die Elemente in einem Dokument in die Elemente eines anderen, unterschiedlichen Dokuments versetzt werden. Zusätzlich zu den Anweisungen, die erklären, wie ein Dokument von einem Format in ein anderes konvertiert wird, muss Data Interchange Services auch das Layout oder Format des Quellen- und des Zieldokuments kennen. In Data Interchange Services ist das Layout eines Dokuments eine *Dokumentdefinition*.

Wenn die Transformationszuordnung in WebSphere Partner Gateway importiert ist, werden die Dokumentdefinitionen, die in Data Interchange Services erstellt wurden, als Dokumentenflussdefinitionen (Paket, Protokoll und Dokumentenfluss) auf der Seite **Transformationszuordnung** und **Dokumentenflussdefinitionen verwalten** angezeigt.

Wenn Sie z. B. ein XML-Dokument in eine X12-Transaktion konvertieren, importieren Sie die Zuordnung, die die XML- und X12-Transaktionsdokumentdefinitionen und die Transformation definiert, die durchgeführt werden soll.

Es gibt zwei Methoden für das Empfangen der Zuordnungsdateien von Data Interchange Services. Wenn der Data Interchange Services-Client über eine Direktverbindung zur WebSphere Partner Gateway-Datenbank verfügt, kann der Zuordnungsexperte von Data Interchange Services die Datei direkt in die Datenbank exportieren. Ein wahrscheinlicheres Szenario ist, dass Sie die Dateien per

E-Mail oder als eine FTP-Übertragung empfangen. Wenn die Dateien über FTP zu Ihnen übertragen wurden, beachten Sie, dass sie im binären Format sein müssen.

Wenn ein Fehler während des Exports einer Zuordnung vom Data Interchange Services-Client auftritt, können Sie unter Umständen den Namen der Zuordnung in Community Console sehen. Die Zuordnung kann nicht zum Konvertieren von Dokumenten verwendet werden. Sie müssen den Zuordnungsexperten des Data Interchange Services-Clients über das Exportproblem informieren und den Zuordnungsexperten bitten, die Zuordnung erneut zu exportieren, bevor diese zum Konvertieren von Dokumenten verwendet werden kann.

Führen Sie die folgenden Schritte aus, um eine Zuordnung zu importieren:

1. Öffnen Sie ein Befehlsfenster.
2. Geben Sie den folgenden Befehl bzw. das folgende Script ein:
   - Auf einem UNIX-System:

     ```
     <Produktverz>/bin/bcgDISImport.sh <datenbankbenutzer-ID>
     <kennwort> <steuerzeichenfolge_für_zuordnung>
     ```

   - Auf einem Windows-System:

     ```
     <Produktverz>\bin\bcgDISImport.bat <datenbankbenutzer-ID>
     <kennwort> <steuerzeichenfolge_für_zuordnung>
     ```

     Dabei gilt Folgendes: *<datenbankbenutzer-ID>* und *<kennwort>* sind die Werte, die Sie verwendet haben, als Sie die Datenbank als Teil der WebSphere Partner Gateway-Installation installiert haben. Die *<steuerzeichenfolge_für_zuordnung>* ist der vollständige Pfad der Datei für die Steuerzeichenfolge für Zuordnung, die vom Data Interchange Services-Client exportiert wurde.
3. Prüfen Sie für Transformationszuordnungen, ob die Dokumentenflussdefinition importiert worden ist.
   a. Klicken Sie auf **Hubadmin > Hubkonfiguration > Zuordnungen > Transformationszuordnungen**.
   b. Klicken Sie über die Seite **Transformationszuordnungen** auf das Symbol **Details anzeigen** neben der Zuordnung von Data Interchange Services. Sie werden bemerken, dass die Dokumentenflussdefinitionen für die Quelle und das Ziel angezeigt werden, sie geben das Format an, in dem das Dokument auf dem Hub empfangen wird, und das Format, in dem es vom Hub zugestellt wird.
   c. Klicken Sie auf **Hubadmin > Hubkonfiguration > Dokumentenflussdefinitionen**.
   d. Erweitern Sie die Pakete und Protokolle, die den Dokumentdefinitionen zugeordnet sind, welche auf der Seite **Transformationszuordnungen** angezeigt wurden, um zu überprüfen, ob die Dokumentenflüsse auf der Seite **Dokumentenflussdefinitionen verwalten** angezeigt werden.

Sie können Validierungszuordnungen zusammen mit Transformationszuordnungen verwenden, um zusätzliche EDI-Standardvalidierung einem beliebigen Konvertierungsprozess mit EDI-Standards hinzuzufügen. Validierungszuordnungen geben Ihnen die vollständige Steuerung über die Validierung eines EDI-Dokuments.

Beachten Sie, dass die Transformations- und Validierungszuordnungen, die vom Data Interchange Services-Client exportiert bzw. mit dem Dienstprogramm bcgDISImport importiert wurden, nicht von WebSphere Partner Gateway Community Console heruntergeladen werden können. Der Zuordnungsexperte des Data Interchange Services-Clients verwaltet diese Zuordnungen, indem er eine Verbindung zur WebSphere Partner Gateway-Datenbank über den Data Interchange Services-Client herstellt.

Dokumentenfluss konfigurieren: EDI zu EDI

Dieser Abschnitt beschreibt die nötigen Interaktionen, um einen EDI-Austausch zu empfangen, vom Austausch den Umschlag zu entfernen, eine Transaktion von einem EDI-Format in ein anderes zu transformieren, die Transaktion mit einem Umschlag zu versehen und diese zuzustellen.

1. Prüfen Sie, ob eine Dokumentenflussdefinition für den EDI-Austausch vorhanden ist, der auf dem Hub empfangen wird. Denken Sie daran, dass, nachdem vom Austausch der Umschlag entfernt wurde, der ursprüngliche Umschlag nicht weiter verarbeitet wird. Anders gesagt, es gibt für ihn keinen Zustellpunkt. Daher verwenden Sie das Paket **N/A** für die Zielinteraktion.
   a. Klicken Sie auf **Hubadmin > Hubkonfiguration > Dokumentenflussdefinition**.
   b. Überprüfen Sie, ob eine Dokumentenflussdefinition bereits vorhanden ist. Wenn z. B. ein Teilnehmer einen EDI-Austausch in einem AS-Paket, EDI-X12-Protokoll und ISA-Dokumentenfluss sendet, ist die Definition bereits verfügbar. Ebenso ist eine N/A/EDI-X12/ISA-Dokumentenflussdefinition bereits vorhanden.
   c. Geben Sie für ein beliebiges Attribut einen Wert ein (oder wählen Sie einen in der Liste aus), das Sie dem Profil zuordnen wollen. Wenn Sie z. B. angeben wollen, dass der Umschlag gelöscht werden soll, falls Fehler bei einer der Transaktionen auftreten, klicken Sie auf das Symbol **Attributwerte bearbeiten** neben **Dokumentenfluss**. Wählen Sie in der Zeile **Umschlag bei Fehlern löschen** die Option **Ja** in der Liste aus.
   d. Wenn eine Dokumentenflussdefinition nicht vorhanden ist, erstellen Sie eine, indem Sie das Paket, das Protokoll und den Dokumentenfluss auswählen.
2. Erstellen Sie eine Interaktion für den Austausch.
   a. Klicken Sie auf **Hubadmin > Hubkonfiguration > Dokumentenflussdefinitionen > Interaktionen verwalten**.
   b. Wählen Sie **Interaktion erstellen** aus.
   c. Wählen Sie die Quellen- und Ziel-Dokumentenflussdefinitionen aus. Mit Ausnahme des Pakets, das für das Ziel **N/A** ist, werden die Dokumentenflussdefinitionen identisch sein.
   d. Wählen Sie **EDI - Umschlag entfernen** in der Liste **Aktion** aus.
3. Importieren Sie die Transformationszuordnung, die die Dokumentdefinitionen der EDI-Transaktionen bereitstellt und die beschreibt, wie die Transaktion von einem EDI-Format in ein anderes transformiert wird. Siehe „Zuordnungen importieren” auf Seite 122.

   Wenn der Austausch mehr als eine Transaktion enthält, wiederholen Sie diesen Schritt für jede Transaktion.
4. Wenn Sie Attribute der Dokumentdefinitionen, die der Zuordnung zugeordnet sind, bearbeiten wollen, führen Sie die folgenden Schritte aus:
   a. Klicken Sie auf **Hubadmin > Hubkonfiguration > Dokumentenflussdefinition**.
   b. Klicken Sie auf das Symbol **Attributwerte bearbeiten** neben dem Teilnehmer. Für EDI-Protokolle wird eine lange Liste mit Attributen angezeigt, die Sie festlegen können.

c. Geben Sie für ein beliebiges Attribut einen Wert ein (oder wählen Sie einen in der Liste aus), das Sie dem Protokoll zuordnen wollen.

d. Klicken Sie auf das Symbol **Attributwerte bearbeiten** neben dem Dokumentenfluss. Es wird in der Regel eine kürzere Liste mit Attributen angezeigt als die, die dem Protokoll zugeordnet ist.

e. Geben Sie für ein beliebiges Attribut einen Wert ein (oder wählen Sie einen in der Liste aus), das Sie dem Dokumentenfluss zuordnen wollen. Sie können z. B. die **Validierungszuordnung** ändern, die dem Dokumentenfluss zugeordnet ist.

   Stellen Sie sicher, dass Sie ein Umschlagsprofil für die Transaktion auswählen.

5. Erstellen Sie eine Interaktion für die Zuordnung, die Sie gerade importiert haben.

   a. Klicken Sie auf **Hubadmin > Hubkonfiguration > Dokumentenflussdefinitionen > Interaktionen verwalten**.

   b. Klicken Sie auf **Interaktion erstellen**.

   c. Wählen Sie unter **Quelle** den Dokumentenfluss aus, der der Transaktion zugeordnet ist. Erweitern Sie das Paket und das Protokoll, und wählen Sie den Dokumentenfluss aus. Dies wird normalerweise **N/A** sein, da die Transaktion selbst nicht von einem Teilnehmer stammt, das in der Zuordnung definierte Protokoll, z. B. **X12V4R1**, und das tatsächliche EDI-Dokument, das in der Zuordnung definiert ist, z. B. **850**.

   d. Wählen Sie unter **Ziel** die Dokumentenflussdefinition für das transformierte Dokument aus. Erweitern Sie das Paket und das Protokoll, und wählen Sie den Dokumentenfluss aus. Da die Transaktion mit einem Umschlag versehen wird, und daher nicht direkt einem Teilnehmer zugestellt wird, wird erneut das Paket **N/A** verwendet.

   e. Wählen Sie in der Transformationszuordnungsliste die Zuordnung aus, die die Transformation dieses Dokuments definiert.

   f. Wählen Sie in der Liste **Aktion** die Option **EDI validieren und EDI konvertieren** aus.

6. Prüfen Sie, ob eine Dokumentenflussdefinition für den EDI-Austausch vorhanden ist, der vom Hub gesendet wird, und legen Sie die Attribute fest, die Sie dem Austausch zuordnen wollen.

   a. Klicken Sie auf **Hubadmin > Hubkonfiguration > Dokumentenflussdefinition**.

   b. Überprüfen Sie, ob eine Dokumentenflussdefinition bereits vorhanden ist. Das Quellenpaket wird **N/A** sein und das Protokoll und der Dokumentenfluss stimmen mit dem Protokoll und dem Dokumentenfluss überein, mit denen der Austausch zugestellt wird. Wenn der Austausch z. B. als AS/EDI-X12/ISA zugestellt wird, wird die Quelle N/A/EDI-X12/ISA lauten.

   c. Bearbeiten Sie alle Attribute, die auf den zugestellten Austausch angewendet werden.

   d. Wenn eine Dokumentenflussdefinition nicht vorhanden ist, erstellen Sie eine, indem Sie das Paket, das Protokoll und den Dokumentenfluss auswählen.

7. Erstellen Sie eine Interaktion für den EDI-Austausch, der vom Hub gesendet wird, nachdem die Transaktion transformiert wurde.

   a. Klicken Sie auf **Hubadmin > Hubkonfiguration > Dokumentenflussdefinitionen > Interaktionen verwalten**.

   b. Klicken Sie auf **Interaktion erstellen**.

c. Wählen Sie die Quellen- und Zieldokumente aus. Mit Ausnahme des Pakets, das für das Quellendokument **N/A** ist, werden die Dokumentenflussdefinitionen identisch sein.
d. Wählen Sie **Pass-Through** in der Liste **Aktion** aus.

Zum Hinzufügen einer Bestätigung zum Dokumentenfluss lesen Sie „Bestätigungen konfigurieren" auf Seite 132.

Nachdem Sie die Interaktionen konfiguriert haben, erstellen Sie die B2B-Funktionalität für die Teilnehmer.

- Aktivieren Sie für den Quellenteilnehmer drei Dokumentenflussdefinitionen unter **Quelle festlegen**: eine für den Quellendokumentenfluss, eine für die EDI-Transaktion und eine für den Umschlag.
- Aktivieren Sie für den Zielteilnehmer drei Dokumentenflussdefinitionen unter **Ziel festlegen**: eine für den vom Umschlag entfernten Dokumentenfluss, eine für die transformierte EDI-Transaktion und eine für den EDI-Umschlag.

Die detaillierten Schritte für das Erstellen der B2B-Funktionalität werden in „B2B-Funktionalität konfigurieren" auf Seite 163 beschrieben.

Nachdem Sie die B2B-Funktionalität für die Teilnehmer konfiguriert haben, erstellen Sie Verbindungen. Sie benötigen drei Verbindungen:

- Eine für den Umschlag vom Quellenteilnehmer zum Hub.
- Eine für die Quellen-EDI-Transaktion zur Ziel-EDI-Transaktion.
- Eine für den Umschlag vom Hub zum Zielteilnehmer.

Die detaillierten Schritte für das Erstellen von Verbindungen werden in Kapitel 12, „Verbindungen verwalten", auf Seite 165 beschrieben.

Dokumentenfluss konfigurieren: EDI zu XML oder ROD

Dieser Abschnitt beschreibt die nötigen Interaktionen, um einen EDI-Austausch zu empfangen, vom Austausch den Umschlag zu entfernen, eine Transaktion von einem EDI-Format in ein XML- oder ROD-Dokument zu transformieren und die Transaktion zuzustellen.

Anmerkung: Ein umfassendes Beispiel für den Dokumentenfluss von EDI zu XML finden Sie in „Beispiel: EDI zu XML" auf Seite 225. Ein umfassendes Beispiel für den Dokumentenfluss von EDI zu ROD finden Sie in „Beispiel: EDI zu ROD" auf Seite 211.

1. Prüfen Sie, ob eine Dokumentenflussdefinition für den EDI-Austausch vorhanden ist, der auf dem Hub empfangen wird. Denken Sie daran, dass, nachdem vom Austausch der Umschlag entfernt wurde, der Umschlag nicht weiter verarbeitet wird. Anders gesagt, es gibt für ihn keinen Zustellpunkt. Daher verwenden Sie das Paket **N/A** für die Zielinteraktion.
   a. Klicken Sie auf **Hubadmin > Hubkonfiguration > Dokumentenflussdefinition**.
   b. Überprüfen Sie, ob eine Dokumentenflussdefinition bereits vorhanden ist. Wenn z. B. ein Teilnehmer einen EDI-Austausch in einem AS-Paket, EDI-X12-Protokoll und ISA-Dokumentenfluss sendet, ist die Definition bereits verfügbar. Ebenso ist eine N/A/EDI-X12/ISA-Dokumentenflussdefinition bereits vorhanden.
   c. Wenn eine Dokumentenflussdefinition nicht vorhanden ist, erstellen Sie eine.

2. Erstellen Sie eine Interaktion für den EDI-Austausch, der auf dem Hub empfangen wird.
   a. Klicken Sie auf **Hubadmin > Hubkonfiguration > Dokumentenfluss-definitionen > Interaktionen verwalten**.
   b. Wählen Sie **Interaktion erstellen** aus.
   c. Wählen Sie die Quellen- und Zieldokumente aus. Mit Ausnahme des Pakets, das für das Ziel **N/A** ist, werden die Dokumentenflussdefinitionen identisch sein.
   d. Wählen Sie **EDI - Umschlag entfernen** in der Liste **Aktion** aus.
3. Importieren Sie die Transformationszuordnung, die die Dokumentdefinitionen der EDI-Transaktion und des XML- oder ROD-Dokuments bereitstellt und beschreibt, wie die Transaktion in das XML- oder ROD-Dokument transformiert wird. Siehe „Zuordnungen importieren" auf Seite 122.

   Wenn der Austausch mehr als eine Transaktion enthält, wiederholen Sie diesen Schritt für jede Transaktion.
4. Erstellen Sie eine Interaktion für die Zuordnung, die Sie gerade importiert haben.
   a. Klicken Sie auf **Hubadmin > Hubkonfiguration > Dokumentenfluss-definitionen > Interaktionen verwalten**.
   b. Klicken Sie auf **Interaktion erstellen**.
   c. Wählen Sie unter **Quelle** den Dokumentenfluss aus, der der Transaktion zugeordnet ist. Erweitern Sie das Paket und das Protokoll, und wählen Sie den Dokumentenfluss aus. Dies wird normalerweise **N/A** sein, da die Transaktion selbst nicht von einem Teilnehmer stammt, das in der Zuordnung definierte Protokoll, z. B. **X12V4R1**, und das tatsächliche EDI-Dokument, das in der Zuordnung definiert ist, z. B. **850**.
   d. Wählen Sie unter **Ziel** die Dokumentenflussdefinition für das transformierte (XML- oder ROD-) Dokument aus. Erweitern Sie das Paket und das Protokoll, und wählen Sie den Dokumentenfluss aus.
   e. Wählen Sie in der Transformationszuordnungsliste die Zuordnung aus, die die Transformation dieses Dokuments definiert.
   f. Wählen Sie in der Liste **Aktion** die Option **EDI validieren und EDI konvertieren** aus.

Zum Hinzufügen einer Bestätigung zum Dokumentenfluss lesen Sie „Bestätigungen konfigurieren" auf Seite 132.

Nachdem Sie die Interaktionen konfiguriert haben, erstellen Sie die B2B-Funktionalität für die Teilnehmer.

- Aktivieren Sie für den Quellenteilnehmer zwei Dokumentenflussdefinitionen unter **Quelle festlegen**: eine für den Umschlag und eine für die EDI-Transaktion.
- Aktivieren Sie für den Zielteilnehmer zwei Dokumentenflussdefinitionen unter **Ziel festlegen**: eine für den EDI-Umschlag und eine für das XML- oder ROD-Dokument.

Die detaillierten Schritte für das Erstellen der B2B-Funktionalität werden in „B2B-Funktionalität konfigurieren" auf Seite 163 beschrieben.

Nachdem Sie die B2B-Funktionalität für die Teilnehmer konfiguriert haben, erstellen Sie Verbindungen. Sie benötigen zwei Verbindungen:

- Eine für den Umschlag vom Quellenteilnehmer zum Hub.

- Eine für die Quellen-EDI-Transaktion zum XML- oder ROD-Dokument.

Die detaillierten Schritte für das Erstellen von Verbindungen werden in Kapitel 12, „Verbindungen verwalten", auf Seite 165 beschrieben.

Dokumentenfluss konfigurieren: XML oder ROD zu EDI

Dieser Abschnitt beschreibt die nötigen Interaktionen, um ein XML- oder ROD-Dokument zu empfangen, es in eine EDI-Transaktion zu transformieren, die Transaktion mit einem Umschlag zu versehen und diese zuzustellen.

Anmerkung: Ein umfassendes Beispiel für den Dokumentenfluss von XML zu EDI finden Sie in „Beispiel: XML zu EDI" auf Seite 230. Ein umfassendes Beispiel für den Dokumentenfluss von ROD zu EDI finden Sie in „Beispiel: ROD zu EDI" auf Seite 237.

1. Importieren Sie die Transformationszuordnung, die die Dokumentdefinitionen des XML- oder ROD-Dokuments und der EDI-Transaktion bereitstellt und beschreibt, wie das Dokument in die EDI-Transaktion transformiert wird. Siehe „Zuordnungen importieren" auf Seite 122.
2. Erstellen Sie eine Interaktion für die Zuordnung, die Sie gerade importiert haben.
   a. Klicken Sie auf **Hubadmin > Hubkonfiguration > Dokumentenflussdefinitionen > Interaktionen verwalten**.
   b. Klicken Sie auf **Interaktion erstellen**.
   c. Wählen Sie unter **Quelle** die Dokumentenflussdefinition aus, die dem XML- oder ROD-Dokument zugeordnet ist. Erweitern Sie das Paket und das Protokoll, und wählen Sie den Dokumentenfluss aus.
   d. Wählen Sie unter **Ziel** den Dokumentenfluss aus, der der EDI-Transaktion zugeordnet ist. Erweitern Sie das Paket und das Protokoll, und wählen Sie den Dokumentenfluss aus. Da die Transaktion nicht direkt zugestellt wird, es wird vor der Zustellung mit einem Umschlag versehen, wird **N/A** als Paket aufgelistet.
   e. Wählen Sie in der Transformationszuordnungsliste die Zuordnung aus, die die Transformation dieses Dokuments definiert.
   f. Wählen Sie in der Liste **Aktion** die Option **XML konvertieren und EDI validieren** oder **ROD konvertieren und EDI validieren** aus.
3. Prüfen Sie, ob eine Dokumentenflussdefinition für den EDI-Austausch vorhanden ist, der vom Hub gesendet wird, und legen Sie die Attribute fest, die Sie dem Austausch zuordnen wollen.
   a. Klicken Sie auf **Hubadmin > Hubkonfiguration > Dokumentenflussdefinition**.
   b. Überprüfen Sie, ob eine Dokumentenflussdefinition bereits vorhanden ist. **N/A** sollte als Paket für das Quellendokument verwendet werden (der Austausch wird vom Hub gesendet).
   c. Bearbeiten Sie alle Attribute, die auf den zugestellten Austausch angewendet werden.
   d. Wenn eine Dokumentenflussdefinition nicht vorhanden ist, erstellen Sie eine, indem Sie das Paket, das Protokoll und den Dokumentenfluss auswählen.
4. Erstellen Sie eine Interaktion für den EDI-Austausch, der vom Hub gesendet wird, nachdem das Dokument transformiert wurde.
   a. Klicken Sie auf **Hubadmin > Hubkonfiguration > Dokumentenflussdefinitionen > Interaktionen verwalten**.

b. Klicken Sie auf **Interaktion erstellen**.
c. Wählen Sie die Quellen- und Zieldokumente aus. Die Quellen- und Zieldokumente sind in unterschiedlichen Paketen (das Quellendokument ist in einem Paket **N/A**), aber das Protokoll, z. B. EDI-X12, und der Dokumentenfluss, z. B. ISA, sollten identisch sein.
d. Wählen Sie **Pass-Through** in der Liste **Aktion** aus.

Nachdem Sie die Interaktionen konfiguriert haben, erstellen Sie die B2B-Funktionalität für die Teilnehmer.

- Die Anzahl der Dokumentenflussdefinitionen, die Sie für den Quellenteilnehmer unter **Quelle festlegen** festlegen müssen, variiert je nach Dokumentenflusstyp.
  - Beispiel: Aktivieren Sie für ein XML-Dokument, in dem ICGPO der Dokumentenfluss ist und MX12V3R1 die konvertierte EDI-Transaktion ist, drei Dokumentenflussdefinitionen unter **Quelle festlegen**: eine für das XML-Dokument (ICGPO), eine für die EDI-Transaktion (MX12V3R1) und eine für den Umschlag, der vom Hub gesendet wird.
  - Aktivieren Sie für weitere XML-Dokumente und für ROD-Dokumente zwei Dokumentenflussdefinitionen unter **Quelle festlegen**: eine für das XML- oder ROD-Dokument und eine für den Umschlag, der vom Hub gesendet wird.
- Aktivieren Sie für den Zielteilnehmer zwei Dokumentenflussdefinitionen unter **Ziel festlegen**: eine für die EDI-Transaktion und eine für den EDI-Umschlag, der empfangen wird. Klicken Sie für die EDI-Transaktion auf das Symbol **Attributwerte bearbeiten** neben dem Protokoll, und geben Sie ein Umschlagsprofil an. Sie können auch weitere Attribute angeben.

Die detaillierten Schritte für das Erstellen der B2B-Funktionalität werden in „B2B-Funktionalität konfigurieren" auf Seite 163 beschrieben.

Nachdem Sie die B2B-Funktionalität für die Teilnehmer konfiguriert haben, erstellen Sie Verbindungen. Sie benötigen zwei Verbindungen:

- Eine für das XML- oder ROD-Quellendokument zur EDI-Transaktion.
- Eine für den Umschlag vom Hub zum Teilnehmer.

Die detaillierten Schritte für das Erstellen von Verbindungen werden in Kapitel 12, „Verbindungen verwalten", auf Seite 165 beschrieben.

Dokumentenfluss konfigurieren: Mehrere XML- oder ROD-Dokumente in einer Datei zu EDI

Dieser Abschnitt beschreibt die nötigen Interaktionen, um mehrere XML- oder ROD-Dokumente in einer Datei zu empfangen, die Dokumente in EDI-Transaktionen zu transformieren, die Transaktionen mit einem Umschlag zu versehen und den EDI-Austausch zuzustellen.

1. Importieren Sie die Transformationszuordnung, die die Dokumentdefinitionen der XML- oder ROD-Dokumente und der EDI-Transaktionen bereitstellt und die Transformation beschreibt. Siehe „Zuordnungen importieren" auf Seite 122.
2. Erstellen Sie eine Interaktion für die Quellen- und Zieldokumente.
   a. Klicken Sie auf **Hubadmin > Hubkonfiguration > Dokumentenflussdefinitionen > Interaktionen verwalten**.
   b. Klicken Sie auf **Interaktion erstellen**.
   c. Wählen Sie die Quellen- und Zieldokumente aus, und wählen Sie **XML konvertieren und EDI validieren** oder **ROD konvertieren und EDI validieren** in der Liste **Aktion** aus.

3. Wiederholen Sie Schritt 2 auf Seite 129 für das Quellendokument und jedes Zieldokument, das durch die Transformationszuordnung hergestellt wurde.
4. Prüfen Sie, ob eine Dokumentenflussdefinition für den EDI-Austausch vorhanden ist, der vom Hub gesendet wird, und legen Sie die Attribute fest, die Sie dem Austausch zuordnen wollen.
   a. Klicken Sie auf **Hubadmin > Hubkonfiguration > Dokumentenflussdefinition**.
   b. Überprüfen Sie, ob eine Dokumentenflussdefinition bereits vorhanden ist. Die Quelle wird **N/A** sein und das Protokoll und der Dokumentenfluss stimmen mit dem Protokoll und dem Dokumentenfluss überein, mit denen der Austausch zugestellt wird. Wenn der Austausch z. B. als AS/EDI-X12/ISA zugestellt wird, wird die Quelle N/A/EDI-X12/ISA lauten.
   c. Bearbeiten Sie alle Attribute, die auf den zugestellten Austausch angewendet werden.
   d. Wenn eine Dokumentenflussdefinition nicht vorhanden ist, erstellen Sie eine, indem Sie das Paket, das Protokoll und den Dokumentenfluss auswählen.
5. Erstellen Sie eine Interaktion für den EDI-Austausch, der vom Hub gesendet wird, nachdem die Transaktion transformiert wurde.
   a. Klicken Sie auf **Hubadmin > Hubkonfiguration > Dokumentenflussdefinitionen > Interaktionen verwalten**.
   b. Klicken Sie auf **Interaktion erstellen**.
   c. Wählen Sie die Quellen- und Zieldokumente aus. Die Quellen- und Zieldokumente sind in unterschiedlichen Paketen (das Quellendokument ist in einem Paket **N/A**), aber das Protokoll, z. B. EDI-X12, und der Dokumentenfluss, z. B. ISA, sollten identisch sein.
   d. Wählen Sie **Pass-Through** in der Liste **Aktion** aus.

Nachdem Sie die Interaktionen konfiguriert haben, erstellen Sie die B2B-Funktionalität für die Teilnehmer.

- Die Anzahl der Dokumentenflussdefinitionen, die Sie für den Quellenteilnehmer unter **Quelle festlegen** festlegen müssen, variiert je nach Dokumentenflusstyp.
  - Beispiel: Aktivieren Sie für ein XML-Dokument, in dem ICGPO der Dokumentenfluss ist und MX12V3R1 die konvertierte EDI-Transaktion ist, drei Dokumentenflussdefinitionen unter **Quelle festlegen**: eine für das XML-Dokument (ICGPO), eine für die EDI-Transaktion (MX12V3R1) und eine für den Umschlag, der vom Hub gesendet wird.
  - Aktivieren Sie für weitere XML-Dokumente und für ROD-Dokumente zwei Dokumentenflussdefinitionen unter **Quelle festlegen**: eine für das XML- oder ROD-Dokument und eine für den Umschlag, der vom Hub gesendet wird.

Die detaillierten Schritte für das Erstellen der B2B-Funktionalität werden in „B2B-Funktionalität konfigurieren" auf Seite 163 beschrieben.

Nachdem Sie die B2B-Funktionalität für die Teilnehmer konfiguriert haben, erstellen Sie Verbindungen. Sie benötigen mehrere Verbindungen:

- Eine für jedes XML- oder ROD-Dokument, das in eine EDI-Transaktion transformiert wird.
- Eine für den Umschlag vom Hub zum Teilnehmer.

Die detaillierten Schritte für das Erstellen von Verbindungen werden in Kapitel 12, „Verbindungen verwalten", auf Seite 165 beschrieben.

Dokumentenfluss konfigurieren: XML zu ROD oder ROD zu XML

Dieser Abschnitt beschreibt die nötigen Interaktionen, um ein XML- oder ROD-Dokument zu empfangen, es in den anderen Dokumenttyp (XML zu ROD oder ROD zu XML) zu transformieren und es zuzustellen.

1. Importieren Sie die Transformationszuordnung, die die Dokumentdefinitionen der XML- und ROD-Dokumente bereitstellt und die Transformation der Dokumente beschreibt. Siehe „Zuordnungen importieren" auf Seite 122.
2. Klicken Sie auf **Hubadmin > Hubkonfiguration > Zuordnungen > Transformationszuordnungen**, und klicken Sie auf das Symbol **Details anzeigen** neben der Zuordnung, die Sie gerade importiert haben.
3. Erstellen Sie eine Interaktion für die Zuordnung, die Sie gerade importiert haben.
   a. Klicken Sie auf **Hubadmin > Hubkonfiguration > Dokumentenflussdefinitionen > Interaktionen verwalten**.
   b. Klicken Sie auf **Interaktion erstellen**.
4. Wählen Sie die Quellen- und Zieldokumente aus, und wählen Sie **XML konvertieren und EDI validieren** oder **ROD konvertieren und EDI validieren** in der Liste **Aktion** aus.

Nachdem Sie die Interaktionen konfiguriert haben, erstellen Sie die B2B-Funktionalität für die Teilnehmer.

- Aktivieren Sie für den Quellenteilnehmer Dokumentenflussdefinitionen unter **Quelle festlegen** für das XML- oder ROD-Dokument.
- Aktivieren Sie für den Zielteilnehmer Dokumentenflussdefinitionen unter **Ziel festlegen** für das XML- oder ROD-Dokument.

Die detaillierten Schritte für das Erstellen der B2B-Funktionalität werden in „B2B-Funktionalität konfigurieren" auf Seite 163 beschrieben.

Nachdem Sie die B2B-Funktionalität für die Teilnehmer konfiguriert haben, erstellen Sie Verbindungen. Sie benötigen eine Verbindung für den Dokumentenfluss von XML zu ROD oder für den Dokumentenfluss von ROD zu XML. Die detaillierten Schritte für das Erstellen von Verbindungen werden in Kapitel 12, „Verbindungen verwalten", auf Seite 165 beschrieben.

Dokumentenfluss konfigurieren: XML zu XML oder ROD zu ROD

Dieser Abschnitt beschreibt die nötigen Interaktionen, um ein XML- oder ROD-Dokument zu empfangen, es in ein Dokument desselben Typs (XML zu XML oder ROD zu ROD) zu transformieren und es zuzustellen.

1. Importieren Sie die Transformationszuordnung, die die Dokumentdefinitionen der XML- oder ROD-Dokumente bereitstellt und die Transformation der Dokumente beschreibt. Siehe „Zuordnungen importieren" auf Seite 122.
2. Klicken Sie auf **Hubadmin > Hubkonfiguration > Zuordnungen > Transformationszuordnungen**, und klicken Sie auf das Symbol **Details anzeigen** neben der Zuordnung, die Sie gerade importiert haben.
3. Erstellen Sie eine Interaktion für die Zuordnung, die Sie gerade importiert haben.
   a. Klicken Sie auf **Hubadmin > Hubkonfiguration > Dokumentenflussdefinitionen > Interaktionen verwalten**.
   b. Klicken Sie auf **Interaktion erstellen**.

c. Wählen Sie die Quellen- und Zieldokumente aus.
d. Wählen Sie **XML konvertieren und EDI validieren** oder **ROD konvertieren und EDI validieren** in der Liste **Aktion** aus.

Nachdem Sie die Interaktionen konfiguriert haben, erstellen Sie die B2B-Funktionalität für die Teilnehmer.

- Aktivieren Sie für den Quellenteilnehmer eine Dokumentenflussdefinition unter **Quelle festlegen** für das XML- oder ROD-Dokument.
- Aktivieren Sie für den Zielteilnehmer eine Dokumentenflussdefinition unter **Ziel festlegen** für das XML- oder ROD-Dokument.

Die detaillierten Schritte für das Erstellen der B2B-Funktionalität werden in „B2B-Funktionalität konfigurieren" auf Seite 163 beschrieben.

Nachdem Sie die B2B-Funktionalität für die Teilnehmer konfiguriert haben, erstellen Sie Verbindungen. Sie benötigen eine Verbindung für den Dokumentenfluss von XML zu XML oder für den Dokumentenfluss von ROD zu ROD. Die detaillierten Schritte für das Erstellen von Verbindungen werden in Kapitel 12, „Verbindungen verwalten", auf Seite 165 beschrieben.

Bestätigungen konfigurieren

Dieser Abschnitt beschreibt, wie Sie Interaktionen installieren, um dem Absender des Dokuments Bestätigungen für den Austausch oder den Transaktionsempfang zu senden.

Funktionale Bestätigungen

Zuordnungen der funktionalen Bestätigungen werden verwendet, um die Generierung von funktionalen Bestätigungen bereitzustellen, wenn auf EDI-Dokumente geantwortet wird, die von einem Teilnehmer empfangen wurden. WebSphere Partner Gateway stellt eine Gruppe von Zuordnungen der funktionalen Bestätigungen bereit, die die häufig verwendeten funktionalen EDI-Bestätigungen herstellen. Der Zuordnungsexperte kann auch FA- und Validierungszuordnungen erstellen, in diesem Fall würden die Zuordnungen in WebSphere Partner Gateway hochgeladen werden.

Anmerkung: Eine Zuordnung der funktionalen Bestätigungen sollte nur erstellt werden, wenn eine angepasste funktionale Bestätigung erforderlich ist.

Neben den Zuordnungen der funktionalen Bestätigungen, die mit WebSphere Partner Gateway bereitgestellt werden, wird das Protokoll &FUNC_ACK_METADATA_DICTIONARY und das zugehörige &FUNC_ACK_META zur Verfügung gestellt. Sie werden unter **Paket:None** auf der Seite **Dokumentenflussdefinitionen** aufgelistet. &FUNC_ACK_META ist die Quellendokumentdefinition für alle Zuordnungen der funktionalen Bestätigungen. Diese Zuordnung stellt die Struktur der funktionalen Bestätigung bereit. Eine funktionale Bestätigung fließt zu Teilnehmern und die Zuordnung der funktionalen Bestätigungen teilt dem System mit, wie die Bestätigung generiert werden soll. Der Name der Quellendokumentdefinition kann nicht geändert werden. Der Zuordnungsexperte des Data Interchange Services-Clients kann eine Zuordnung der funktionalen Bestätigungen ohne diese Dokumentdefinition in Ihrer Datenbank nicht erstellen.

Die Zieldokumentdefinition in einer Zuordnung der funktionalen Bestätigungen beschreibt das Layout der funktionalen Bestätigung. Sie muss eine EDI-Dokumentdefinition mit einem der folgenden Namen sein: 997, 999 oder CONTRL.

Die folgenden Zuordnungen der funktionalen Bestätigungen werden mit WebSphere Partner Gateway installiert und auf der Seite **Dokumentenfluss-definitionen verwalten** unter **Paket: N/A** angezeigt:

Tabelle 16. Vom System bereitgestellte Zuordnungen der funktionalen Bestätigungen

Protokoll	Dokumentenfluss	Beschreibung
&DTCTL21	CONTRL	Funktionale Bestätigung CONTRL – UN/EDIFACT Version 2 Release 1 (D94B)
&DTCTL	CONTRL	Funktionale Bestätigung CONTRL – UN/EDIFACT vor D94B
&DT99933	999	Funktionale Bestätigung 999 – UCS Version 3 Release 3
&DT99737	997	Funktionale Bestätigung 997 – X12 Version 3 Release 7
&DT99735	997	Funktionale Bestätigung 997 – X12 Version 3 Release 5
&DT99724	997	Funktionale Bestätigung 997 – X12 Version 2 Release 4

Darüber hinaus werden das Protokoll &X44TA1 und ein zugeordneter TA1-Dokumentenfluss unter **Paket: N/A** aufgelistet. Diese Zuordnung wird verwendet, um eine TA1 zu generieren. TA1 ist eine funktionale Bestätigung, die für eingehende X12-Austauschvorgänge generiert wird.

Das Protokoll &WDIEVAL und ein zugeordnetes X12ENV wird auch unter **Paket: N/A** bereitgestellt.

Genau wie EDI-Transaktionen werden auch funktionale Bestätigungen vor ihrer Zustellung stets in einen EDI-Austausch gestellt.

TA1-Bestätigungen

TA1 ist ein EDI-Segment, das eine X12-Austauschbestätigung bereitstellt. Es bestätigt den Empfang und die syntaktische Korrektheit eines X12-Austauschheader- und -trailerpaares (ISA und IEA). Der Absender kann TA1 vom Empfänger anfordern, indem er das Element 14 des ISA-Austauschkontrollheaders mit **1** festlegt. Die Austauschkontrollnummer von TA1 wird mit einem zuvor übertragenen X12-Austausch mit derselben Kontrollnummer in Übereinstimmung gebracht, um den Bestätigungsprozess abzuschließen.

Genau wie EDI-Transaktionen und funktionale Bestätigungen werden auch TA1s vor ihrer Zustellung stets in einen EDI-Austausch gestellt.

Dem Dokumentenfluss eine Bestätigung hinzufügen

Führen Sie die folgenden Schritte aus, um einem Dokumentenfluss eine Bestätigung hinzuzufügen:

1. Wenn die Zuordnung der funktionalen Bestätigungen nicht von WebSphere Partner Gateway bereitgestellt wird, importieren Sie die Zuordnung vom Data Interchange Services-Client. Siehe „Zuordnungen importieren" auf Seite 122.
2. Ordnen Sie die Zuordnung der funktionalen Bestätigungen einer Dokumentenflussdefinition zu:
   a. Klicken Sie auf **Hubadmin > Hubkonfiguration > Zuordnungen > EDI FA-Zuordnungen**.

b. Klicken Sie auf das Symbol **Details anzeigen** neben der Zuordnung.
c. Klicken Sie auf das Symbol **Erweitern** neben einem Paket, um es einzeln auf die gewünschte Ebene zu erweitern, erweitern Sie z. B. die Ordner **Paket** und **Protokoll**, und wählen Sie die Transaktion aus.
d. Klicken Sie auf **Speichern**.

3. Erstellen Sie eine Interaktion für die Zuordnung, die Sie gerade importiert haben.
   a. Klicken Sie auf **Hubadmin > Hubkonfiguration > Dokumentenflussdefinition > Interaktionen verwalten**.
   b. Klicken Sie auf **Interaktion erstellen**.
   c. Wählen Sie unter **Quelle** den Dokumentenfluss aus, der der funktionalen Bestätigung zugeordnet ist. Erweitern Sie das Paket und das Protokoll, und wählen Sie den Dokumentenfluss aus.
   d. Wählen Sie unter **Ziel** dieselben Werte aus.
   e. Wählen Sie in der Liste **Aktion** die Option **Pass-Through** aus.
4. Prüfen Sie, ob eine Dokumentenflussdefinition für den EDI-Austausch vorhanden ist, der vom Hub gesendet wird, und legen Sie die Attribute fest, die Sie dem Austausch zuordnen wollen.
   a. Klicken Sie auf **Hubadmin > Hubkonfiguration > Dokumentenflussdefinition**.
   b. Überprüfen Sie, ob eine Dokumentenflussdefinition bereits vorhanden ist. Die Quelle wird **N/A** sein und das Protokoll und der Dokumentenfluss stimmen mit dem Protokoll und dem Dokumentenfluss überein, mit denen der Austausch zugestellt wird. Wenn der Austausch z. B. als AS/EDI-X12/ISA zugestellt wird, wird die Quelle N/A/EDI-X12/ISA lauten.
   c. Bearbeiten Sie alle Attribute, die auf den zugestellten Austausch angewendet werden.
   d. Wenn eine Dokumentenflussdefinition nicht vorhanden ist, erstellen Sie eine, indem Sie das Paket, das Protokoll und den Dokumentenfluss auswählen.
5. Erstellen Sie eine Interaktion für den EDI-Austausch, der vom Hub gesendet wird, nachdem das Dokument transformiert wurde.
   a. Klicken Sie auf **Hubadmin > Hubkonfiguration > Dokumentenflussdefinitionen > Interaktionen verwalten**.
   b. Klicken Sie auf **Interaktion erstellen**.
   c. Wählen Sie die Quellen- und Zieldokumente aus.
   d. Wählen Sie **Pass-Through** in der Liste **Aktion** aus.

Nachdem Sie die Interaktionen konfiguriert haben, erstellen Sie die B2B-Funktionalität für die Teilnehmer. Beachten Sie, dass der Zielteilnehmer in einer Übertragung der funktionalen Bestätigung der Quellenteilnehmer des ursprünglichen EDI-Dokuments ist.

- Aktivieren Sie für den Quellenteilnehmer Dokumentenflussdefinitionen unter **Quelle festlegen** für die funktionale Bestätigung. Aktivieren Sie außerdem eine Dokumentenflussdefinition für den Umschlag, der vom Hub gesendet wird.
- Aktivieren Sie für den Zielteilnehmer eine Dokumentenflussdefinition unter **Ziel festlegen** für die funktionale Bestätigung. Aktivieren Sie außerdem eine Dokumentenflussdefinition für den EDI-Umschlag, der empfangen wird.

  Klicken Sie für die funktionale Bestätigung auf das Symbol **Attributwerte bearbeiten** neben dem Protokoll, und geben Sie ein Umschlagsprofil an.

Die detaillierten Schritte für das Erstellen der B2B-Funktionalität werden in „B2B-Funktionalität konfigurieren" auf Seite 163 beschrieben.

Nachdem Sie die B2B-Funktionalität für die Teilnehmer konfiguriert haben, erstellen Sie Verbindungen. Sie benötigen zwei Verbindungen:

- Eine für die funktionale Bestätigung.
- Eine für den Umschlag vom Hub zum Teilnehmer.

Die detaillierten Schritte für das Erstellen von Verbindungen werden in Kapitel 12, „Verbindungen verwalten", auf Seite 165 beschrieben.

EDI-Austauschvorgänge und -Transaktionen anzeigen

Wie zuvor in diesem Kapitel erwähnt, verwenden Sie die Dokumentanzeige, um Informationen zu EDI-Austauschvorgängen und EDI-Transaktionen anzuzeigen, die einen Dokumentenfluss ausmachen. Sie können unformatierte Dokumente und zugeordnete Dokumentverarbeitungsdetails und Ereignisse mit Hilfe von bestimmten Suchkriterien anzeigen. Diese Informationen sind nützlich, wenn Sie zu ermitteln versuchen, ob ein EDI-Austausch erfolgreich zugestellt wurde bzw. worin die Ursache eines Fehlers besteht.

Klicken Sie auf **Anzeigen > Dokumentanzeige**, um die Dokumentanzeige anzuzeigen. Informationen zur Verwendung der Dokumentanzeige finden Sie im Handbuch *Verwaltung*.

Kapitel 9. Das Community Manager-Profil und B2B-Funktionalität erstellen

Nachdem Sie den Hub konfiguriert haben, einschließlich dem Einrichten der Ziele sowie dem Definieren der Dokumentenflussdefinitionen und Interaktionen, können Sie nun Community Manager für Ihre Hub-Community erstellen. Sie erstellen dann die B2B-Funktionalität von Community Manager. Nachdem Sie Teilnehmer erstellt haben (wie in Kapitel 11, „Teilnehmer und ihre B2B-Funktionalität erstellen", auf Seite 161 beschrieben), aktivieren Sie die tatsächlichen Verbindungen zwischen Community Manager und Teilnehmern, so dass Dokumente ausgetauscht werden können.

Dieses Kapitel behandelt die folgenden Themen:

- „Das Community Manager-Profil erstellen"
- „B2B-Funktionalität konfigurieren" auf Seite 139

Das Community Manager-Profil erstellen

Community Manager ist in der Regel das Unternehmen, das Eigner des WebSphere Partner Gateway-Servers ist und das den Server verwendet, um mit Teilnehmern zu kommunizieren. Außerdem wird Community Manager als ein Teilnehmer des Hubs betrachtet und verfügt als solcher über ein Profil, Gateways und B2B-Funktionalität.

Führen Sie die folgenden Schritte aus, um das Community Manager-Profil zu erstellen:

1. Klicken Sie auf **Kontenadmin > Profile > Community-Teilnehmer**.
2. Klicken Sie auf **Erstellen**.
3. Geben Sie in **Anmeldename des Unternehmens** den Namen ein, den Community Manager im Unternehmensfeld beim Anmelden am Hub verwendet. Sie könnten z. B. `Manager` eingeben.
4. Geben Sie in **Anzeigename des Teilnehmers** den Firmennamen oder einen anderen beschreibenden Namen für Community Manager ein. Dies ist der Name, der in der Liste **Teilnehmersuche** angezeigt wird.
5. Wählen Sie in der Liste **Teilnehmertyp** den Eintrag **Community Manager** aus.

   Anmerkung: WebSphere Partner Gateway unterstützt nur einen Community Manager und nur einen Community Operator. Community Operator wird automatisch erstellt, wenn Sie WebSphere Partner Gateway installieren.
6. Wählen Sie den Status für Community Manager aus. Sie wollen wahrscheinlich den Standardwert **Aktiviert** verwenden.
7. Geben Sie optional den Firmentyp in das Feld **Lieferantentyp** ein.
8. Geben Sie optional die Website von Community Manager ein.
9. Klicken Sie auf **Neu** unterhalb von **Geschäfts-ID**.
10. Geben Sie einen Typ aus der Liste an, und geben Sie die entsprechende Kennung ein. WebSphere Partner Gateway verwendet die von Ihnen hier eingegebene Nummer, um Dokumente zu Community Manager und von Community Manager weiterzuleiten.

Beachten Sie die folgenden Richtlinien, wenn Sie die Kennung eingeben:

a. DUNS-Nummern müssen neun Ziffern umfassen.
b. DUNS+4 müssen über 13 Ziffern verfügen.
c. Unformatierte ID-Nummern akzeptieren bis zu 60 alphanumerische Zeichen und Sonderzeichen.

Anmerkung: Sie können Community Manager mehr als eine Geschäfts-ID zuordnen. In einigen Fällen ist mehr als eine Geschäfts-ID erforderlich. Wenn z. B. der Hub EDI-X12- und EDIFACT-Dokumente sendet und empfängt, verwendet er sowohl DUNS- als auch unformatierte IDs während des Dokumentenaustauschs.

Sowohl Community Manager als auch die Teilnehmer, die an diesen Dokumentenflusstypen beteiligt sind, sollten jeweils über eine DUNS-ID und eine unformatierte ID verfügen. Die unformatierte ID wird verwendet, um EDI-IDs darzustellen, die über eine Kennung und ein Qualifikationsmerkmal verfügen. Angenommen, das EDI-Qualifikationsmerkmal lautet z. B. ″ZZ″ und die EDI-Kennung lautet ″810810810″. Dann könnte die unformatierte ID wie folgt angegeben werden: ZZ-810810810.

11. Geben Sie optional eine IP-Adresse für Community Manager ein, indem Sie die folgenden Schritte ausführen:
    a. Klicken Sie unter **IP-Adresse** auf **Neu**.
    b. Geben Sie den Gateway-Typ an.
    c. Geben Sie die IP-Adresse von Community Manager ein.
12. Klicken Sie auf **Speichern**.
13. Ihnen wird ein Kennwort übermittelt, das Community Manager verwenden wird, um sich beim Hub anzumelden. Notieren Sie sich dieses Kennwort. Stellen Sie es dem Community Manager-Administrator zur Verfügung.

    Anmerkung: Wenn Sie das Community Manager-Profil erstellen, erstellen Sie in Wirklichkeit den Administrator für Community Manager. Administratoren können dann einzelne Benutzer innerhalb ihrer Organisationen erstellen, oder Sie können als Hubadmin die Benutzer für die Teilnehmer erstellen.

Nachdem Sie ein Profil für Community Manager erstellt haben, erstellen Sie die Gateways, mit denen der Hub Dokumente an Community Manager senden wird. Lesen Sie die folgenden Abschnitte über das Konfigurieren der Gateways für Community Manager.

- „HTTP-Gateway konfigurieren” auf Seite 144
- „HTTPS-Gateway konfigurieren” auf Seite 145
- „JMS-Gateway konfigurieren” auf Seite 149
- „Dateiverzeichnisgateway konfigurieren” auf Seite 151

Nachdem Sie die Gateways für Community Manager konfiguriert haben, konfigurieren Sie die B2B-Funktionalität von Community Manager.

B2B-Funktionalität konfigurieren

Community Manager verfügt über B2B-Funktionalität, die die Dokumenttypen definiert, die Community Manager senden und empfangen kann.

Sie verwenden die Funktion **B2B-Funktionalität**, um die B2B-Funktionalität von Community Manager einer Dokumentenflussdefinition zuzuordnen.

Verwenden Sie die folgende Prozedur, um die B2B-Funktionalität von Community Manager zu konfigurieren.

1. Klicken Sie auf **Kontenadmin > Profile > Community-Teilnehmer**.
2. Geben Sie Suchkriterien ein, und klicken Sie auf **Suchen**, oder klicken Sie auf **Suchen**, ohne Suchkriterien einzugeben, um eine Liste aller Teilnehmer anzuzeigen.
3. Klicken Sie auf das Symbol **Details anzeigen** neben Community Manager.
4. Klicken Sie auf **B2B-Funktionalität**. Die Seite **B2B-Funktionalität** wird angezeigt. Auf der Seite werden rechts die Pakete, Protokolle und Dokumentenflüsse angezeigt, die vom System als Dokumentenflussdefinitionen unterstützt werden.
5. Klicken Sie auf das Symbol **Rolle ist nicht aktiv** unter der Spalte **Quelle festlegen** für die Pakete auf der rechten Seite, die Dokumente enthalten, welche Community Manager an Teilnehmer senden wird.
6. Wählen Sie **Ziel festlegen**, damit Sie dieselben Dokumente von Teilnehmern empfangen. Community Console zeigt ein Häkchen an, wenn die Dokumentenflussdefinition aktiviert ist.

   Anmerkung: Die Auswahl von **Quelle festlegen** ist für alle Aktionen in einem Zweiwege-PIP gleich, ungeachtet der Tatsache, dass die Anforderung von einem der Teilnehmer und die entsprechende Bestätigung von einem anderen stammt. Dies gilt auch für **Ziel festlegen**.
7. Klicken Sie auf das Symbol **Erweitern** auf der Ebene **Paket**, um einen einzelnen Knoten auf die entsprechende Ebene der Dokumentenflussdefinition zu erweitern, oder wählen Sie eine Nummer zwischen **0-4** oder **Alle** aus, um alle angezeigten Dokumentenflussdefinitionen zur ausgewählten Ebene zu erweitern.
8. Wählen Sie erneut **Quelle festlegen**, **Ziel festlegen** oder beide Rollen für die unteren Ebenen von **Protokoll** und **Dokumentenfluss** für jede Dokumentenflussdefinition aus, die Ihr System unterstützt.

   Wenn eine Definition auf der Ebene **Dokumentenfluss** aktiviert ist, werden die Definitionen **Aktion** und **Aktivität**, sofern vorhanden, automatisch aktiviert.
9. Klicken Sie optional auf **Aktiviert** in der Spalte **Aktiviert**, um eine Dokumentenflussdefinition offline zu setzen. (Wenn Sie **Quelle festlegen** oder **Ziel festlegen** auswählen, ist der Eintrag automatisch aktiviert.) Klicken Sie auf **Inaktiviert**, um die Definition online zu setzen.

   Wenn ein Paket inaktiviert ist, sind alle Dokumentenflussdefinitionen der unteren Ebene im selben Knoten ebenfalls inaktiviert, ungeachtet dessen, ob sie individuell aktiviert waren.

Wenn eine Dokumentenflussdefinition der unteren Ebene inaktiviert wird, bleiben alle Definitionen der höheren Ebenen im selben Kontext aktiviert. Wenn eine Dokumentenflussdefinition inaktiviert wird, funktionieren alle zuvor vorhandenen Verbindungen und Attribute weiterhin. Die inaktivierte Dokumentenflussdefinition schränkt lediglich die Erstellung neuer Verbindungen ein.

10. Klicken Sie auf das Symbol **Bearbeiten**, um beliebige Attribute eines Protokolls, Pakets, Dokumentenflusses, einer Aktivität oder eines Signals zu bearbeiten. Anschließend werden die Einstellungen für die Attribute angezeigt (sofern Attribute vorhanden sind). Sie können die Attribute modifizieren, indem Sie einen Wert eingeben oder einen Wert in der Spalte **Aktualisieren** auswählen und dann auf **Speichern** klicken.

    Wie schon in Schritt 10 auf Seite 137 erwähnt, können Community Manager mehrere Geschäfts-IDs zugeordnet sein und in manchen Fällen ist dies sogar erforderlich. Wenn der Teilnehmer nur ein Format der ID empfangen darf, müssen Sie den entsprechenden Wert für die ID auswählen. Gehen Sie wie folgt vor, um die ID auszuwählen:

    a. Klicken Sie auf das Symbol **Bearbeiten** neben **None**.

       Sie sehen, dass das Attribut (**AS-Geschäfts-ID**) dem Paket **None** zugeordnet ist.

    b. Wählen Sie in der Liste **Aktualisieren** die **AS-Geschäfts-ID** mit dem Format aus, welches Ihr Teilnehmer akzeptieren kann.

    c. Klicken Sie auf **Speichern**.

    Anmerkung: Wenn Sie das Attribut auf der Seite **B2B-Funktionalität** festlegen, wird es auf alle Austauschvorgänge angewendet, die von Community Manager und dem Paket **None** stammen. Um die Auswahl für eine bestimmte Verbindung spezifischer zu gestalten, können Sie den Wert auf der Verbindungsebene festlegen oder den hier festgelegten Wert überschreiben. Lesen Sie hierzu „Teilnehmerverbindungen aktivieren” auf Seite 165.

Kapitel 10. Gateways erstellen

Nachdem Sie die Teilnehmer erstellt haben, definieren Sie Gateways für die Teilnehmer. Gateways definieren Einstiegspunkte in das System des Teilnehmers.

Dieses Kapitel behandelt die folgenden Themen:

- „Übersicht"
- „Globale Transportwerte konfigurieren" auf Seite 142
- „Forward Proxy konfigurieren" auf Seite 143
- „HTTP-Gateway konfigurieren" auf Seite 144
- „HTTPS-Gateway konfigurieren" auf Seite 145
- „FTP-Gateway konfigurieren" auf Seite 147
- „SMTP-Gateway konfigurieren" auf Seite 148
- „JMS-Gateway konfigurieren" auf Seite 149
- „Dateiverzeichnisgateway konfigurieren" auf Seite 151
- „FTPS-Gateway konfigurieren" auf Seite 152
- „FTP-Scripting-Gateway konfigurieren" auf Seite 154
- „Handler konfigurieren" auf Seite 158
- „Gateway für benutzerdefinierten Transport konfigurieren" auf Seite 158
- „Standardgateway angeben" auf Seite 159

Übersicht

WebSphere Partner Gateway verwendet Gateways, um Dokumente an ihr ordnungsgemäßes Ziel weiterzuleiten. Der Empfänger kann ein Community-Teilnehmer oder Community Manager sein.

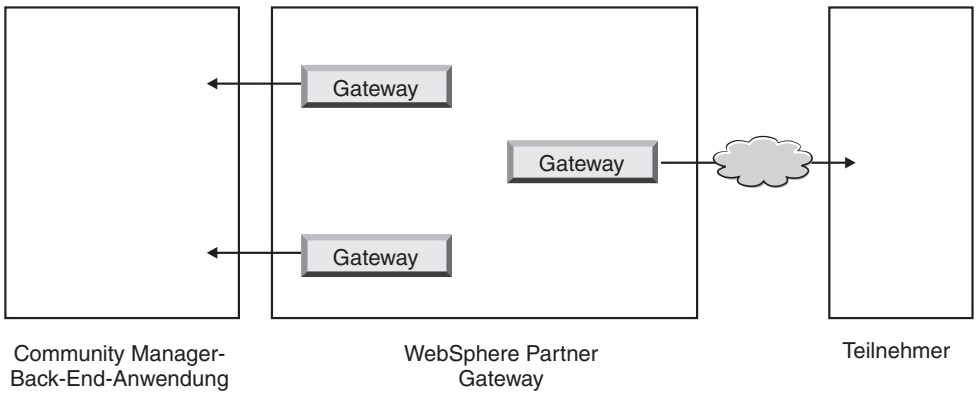

Abbildung 34. Gateways zu Community Manager und Teilnehmern

Das Ausgangstransportprotokoll bestimmt, welche Informationen während der Gatewaykonfiguration verwendet werden.

Die folgenden Transporte werden standardmäßig für Teilnehmergateways unterstützt:

- HTTP/1.1

- HTTPS/1.0
- HTTPS/1.1
- FTP
- FTPS
- JMS
- SMTP

  Anmerkung: Sie können ein SMTP-Gateway nur für Teilnehmer definieren, nicht für Community Manager.
- Dateiverzeichnis
- FTP-Scripting

Sie können auch einen benutzerdefinierten Transport angeben, das Sie während der Gateway-Erstellung hochladen.

Als Hubadmin können Sie die Gateways für Ihre Teilnehmer konfigurieren bzw. die Teilnehmer können diese Aufgabe selbst ausführen. In diesem Kapitel erfahren Sie, wie Sie diese Aufgabe für die Teilnehmer ausführen.

Globale Transportwerte konfigurieren

Sie legen globale Transportattribute fest, die auf alle FTP-Scripting-Gateways angewendet werden. Wenn Sie keine FTP-Scripting-Gateways definieren, können Sie diesen Abschnitt überspringen.

Der FTP-Scripting-Transport verwendet einen Sperrmechanismus, der verhindert, dass mehr als eine FTP-Scripting-Instanz gleichzeitig auf dasselbe Gateway zugreift. Standardwerte werden für Folgendes bereitgestellt: wie lange eine Gatewayinstanz wartet, um die Sperre zu erhalten, und wie oft es versucht, die Sperre abzurufen, falls diese verwendet wird. Sie können diese Standardwerte verwenden bzw. diese ändern.

1. Klicken Sie auf **Kontenadmin > Profile > Community-Teilnehmer**.
2. Klicken Sie auf **Gateways**.
3. Wählen Sie **Globale Transportattribute** in der Liste **Gateway** aus.

   Wenn Sie entweder **Maximale Sperrenzeit (Sekunden)** oder **Höchstalter der Warteschlange (Sekunden)** aktualisiert haben, als Sie die globalen Transportwerte während der Erstellung der Ziele angegeben haben, werden diese aktualisierten Werte hier wiedergegeben.
4. Wenn die Standardwerte für Ihre Konfiguration geeignet sind, klicken Sie auf **Abbrechen**. Andernfalls fahren Sie mit den übrigen Schritten in diesem Abschnitt fort.
5. Klicken Sie auf das Symbol **Bearbeiten** neben **FTP-Scripting-Transport**.
6. Um mindestens einen Wert zu ändern, geben Sie den neuen Wert ein. Sie können Folgendes ändern:
   - **Wiederholungszähler für Sperren**. Gibt an, wie oft das Gateway versucht, eine Sperre zu erhalten, wenn die Sperre gerade verwendet wird. Der Standardwert ist 3.
   - **Wiederholungsintervall für Sperren (Sekunden)**. Gibt an, wie viel Zeit zwischen den Versuchen, eine Sperre zu erhalten, verstreichen wird. Der Standardwert ist 260 Sekunden.

- **Maximale Sperrenzeit (Sekunden)**. Gibt an, wie lange das Gateway die Sperre beibehalten kann. Der Standardwert ist 240 Sekunden, es sei denn, Sie haben ihn geändert, als Sie die Ziele erstellt haben.
- **Höchstalter der Warteschlange (Sekunden)**. Gibt an, wie lange das Ziel in einer Warteschlange warten wird, um die Sperre zu erhalten. Der Standardwert ist 740 Sekunden, es sei denn, Sie haben ihn geändert, als Sie die Ziele erstellt haben.

7. Klicken Sie auf **Speichern**.

Forward Proxy konfigurieren

Für die HTTP- und HTTPS-Transporte können Sie eine Forward Proxy-Unterstützung konfigurieren, so dass Dokumente über einen konfigurierten Proxy-Server gesendet werden. Sie können mit WebSphere Partner Gateway die folgenden Unterstützungstypen konfigurieren:

- Proxy-Unterstützung über HTTP
- Proxy-Unterstützung über HTTPS
- Proxy-Unterstützung über HTTPS mit Authentifizierung
- Proxy-Unterstützung über SOCKS

Nachdem Sie einen Forward Proxy konfiguriert haben, können Sie ihn global für den Transport einrichten, indem Sie ihn zum Standardgateway machen, z. B. dass alle HTTP-Gateways den Forward Proxy verwenden.

Führen Sie die folgenden Schritte aus, um einen Forward Proxy zu konfigurieren:

1. Klicken Sie auf **Kontenadmin > Profile > Community-Teilnehmer**.
2. Klicken Sie auf **Gateways**.
3. Klicken Sie auf **Forward Proxy-Unterstützung**.
4. Klicken Sie auf der Seite **Forward Proxy-Liste** auf **Erstellen**.
5. Geben Sie einen Namen für den Proxy-Server ein.
6. Geben Sie optional eine Beschreibung des Proxy-Servers ein.
7. Wählen Sie den Transporttyp in der Liste aus.

   Anmerkung: Die verfügbaren Transporte sind HTTP und HTTPS.
8. Geben Sie die folgenden Informationen ein. Geben Sie entweder Proxy-Host und Proxy-Port *oder* Socks-Proxy-Host und Socks-Proxy-Port ein.
   - Geben Sie für **Proxy-Host** den zu verwendenden Proxy-Server ein, z. B. http://proxy.abc.com.
   - Geben Sie für **Proxy-Port** die Portnummer ein.
   - Wenn der Proxy-Server einen Benutzername und ein Kennwort erfordert, geben Sie diese in die Felder **Benutzername** und **Kennwort** ein.
   - Geben Sie für **Socks-Proxy-Host** den zu verwendenden Socks-Proxy-Server ein.
   - Geben Sie für **Socks-Proxy-Port** die Portnummer ein.
9. Wählen Sie das Markierungsfeld aus, wenn Sie diesen Proxy-Server als Standard-Proxy-Server verwenden wollen, der von jedem Teilnehmer mit Proxy-Unterstützung verwendet werden kann.
10. Klicken Sie auf **Speichern**.

HTTP-Gateway konfigurieren

Sie konfigurieren ein HTTP-Gateway so, dass Dokumente vom Hub an die IP-Adresse Ihres Teilnehmers gesendet werden können. Wenn Sie ein HTTP-Gateway konfigurieren, können Sie auch angeben, dass Dokumente über einen konfigurierten Proxy-Server gesendet werden.

Verwenden Sie die folgende Prozedur, um mit dem Erstellungsprozess für einen HTTP-Gateway zu beginnen.

1. Klicken Sie auf **Kontenadmin > Profile > Community-Teilnehmer**.
2. Geben Sie Suchkriterien ein, und klicken Sie auf **Suchen**, oder klicken Sie auf **Suchen**, ohne Suchkriterien einzugeben, um eine Liste aller Teilnehmer anzuzeigen.
3. Klicken Sie auf das Symbol **Details anzeigen**, um das Profil des Teilnehmers anzuzeigen.
4. Klicken Sie auf **Gateways**.
5. Klicken Sie auf **Erstellen**.

Gateway-Details

Führen Sie über die Seite **Gateway-Liste** die folgenden Schritte aus:

1. Geben Sie einen Namen ein, um das Gateway anzugeben. Dies ist ein erforderliches Feld. Dies ist der Name, der in der Liste mit Gateways angezeigt wird.
2. Geben Sie optional den Status des Gateways an. **Aktiviert** ist die Standardeinstellung. Ein aktiviertes Gateway ist für das Senden von Dokumenten bereit. Ein inaktiviertes Gateway kann keine Dokumente senden.
3. Geben Sie optional an, ob das Gateway online oder offline ist. Die Standardeinstellung ist **Online**.
4. Geben Sie optional eine Beschreibung für das Gateway ein.

Gatewaykonfiguration

Führen Sie die folgenden Schritte im Abschnitt **Gatewaykonfiguration** der Seite aus:

1. Wählen Sie **HTTP/1.1** in der Liste **Transport** aus.
2. Wählen Sie optional einen zu verwendenden Proxy-Server aus. Die **Forward Proxy-Liste** schließt alle Proxy-Server ein, die Sie erstellt haben, einschließlich dem Standard-Proxy-Server. Der Standardwert für dieses Feld ist **Standardmäßigen Forward Proxy verwenden**. Wenn Sie wollen, dass der ausgewählte Teilnehmer einen anderen Proxy-Server verwendet, wählen Sie diesen Server in der Liste aus. Wenn Sie diese Funktion nicht mit dem ausgewählten Teilnehmer verwenden wollen, wählen Sie **Keinen Forward Proxy verwenden** aus.
3. Geben Sie in das Feld **Adresse** die URI ein, der das Dokument zugestellt werden soll. Dieses Feld ist erforderlich.

   Das Format lautet: http://*<servername>*:*<optionaler_port>*/*<pfad>*

   Beispiel für dieses Format:

   ```
   http://weitererserver.ibm.com:57080/bcgreceiver/Receiver
   ```

   Wenn Sie ein Gateway für die Verwendung durch einen Web-Service konfigurieren, geben Sie den privaten URL an, der vom Web-Service-Provider bereitgestellt wird. Dort wird WebSphere Partner Gateway den Web-Service aufrufen, wenn er als Proxy-Server für den Web-Service-Provider agiert.

4. Geben Sie optional einen Benutzernamen und ein Kennwort ein, wenn ein Benutzername und ein Kennwort für den Zugriff auf den HTTP-Server erforderlich sind.
5. Geben Sie in das Feld **Wiederholungszahl** die Anzahl Versuche ein, die das Gateway unternehmen soll, um ein Dokument zu senden, bevor es fehlschlägt. Der Standardwert ist 3.
6. Geben Sie in das Feld **Wiederholungsintervall** die Zeit ein, die das Gateway warten soll, bevor es versucht, das Dokument erneut zu senden. Der Standardwert ist 300 Sekunden.
7. Geben Sie in das Feld **Anzahl Threads** die Anzahl Dokumente ein, die gleichzeitig verarbeitet werden können. Der Standardwert ist 3.
8. Wählen Sie im Feld **Client-IP prüfen** die Option **Ja** aus, wenn Sie wollen, dass die IP-Adresse des Absenders geprüft wird, bevor das Dokument verarbeitet wird. Wählen Sie andernfalls **Nein** aus. Die Standardeinstellung ist **Nein**.
9. Wählen Sie im Feld **Autom. Warteschlange** die Option **Ja** aus, wenn Sie wollen, dass das Gateway (automatisch) offline gehen soll, wenn ein Übermittlungsfehler auftritt, weil die Anzahl Wiederholungen aufgebraucht ist. Wählen Sie andernfalls **Nein** aus. Die Standardeinstellung ist **Nein**.

   Wenn Sie **Autom. Warteschlange** auswählen, bleiben alle Dokumente so lange in der Warteschlange, bis das Gateway wieder manuell online gestellt wird.
10. Geben Sie in das Feld **Verbindungszeitlimit** die Anzahl Sekunden ein, die ein Socket ohne Datenverkehr geöffnet bleibt. Der Standardwert ist 120 Sekunden.
11. Wenn Sie den Vorverarbeitungs- oder den Nachverarbeitungsschritt für das Gateway konfigurieren wollen, fahren Sie mit „Handler konfigurieren” auf Seite 158 fort. Ansonsten klicken Sie auf **Speichern**.

HTTPS-Gateway konfigurieren

Sie konfigurieren ein HTTPS-Gateway so, dass Dokumente vom Hub an die IP-Adresse Ihres Teilnehmers gesendet werden können. Wenn Sie ein HTTPS-Gateway konfigurieren, können Sie auch angeben, dass Dokumente über einen konfigurierten Proxy-Server gesendet werden.

Verwenden Sie die folgende Prozedur, um HTTPS-Gateways zu erstellen.

1. Klicken Sie auf **Kontenadmin > Profile > Community-Teilnehmer**.
2. Geben Sie Suchkriterien ein, und klicken Sie auf **Suchen**, oder klicken Sie auf **Suchen**, ohne Suchkriterien einzugeben, um eine Liste aller Teilnehmer anzuzeigen.
3. Klicken Sie auf das Symbol **Details anzeigen**, um das Profil des Teilnehmers anzuzeigen.
4. Klicken Sie auf **Gateways**.
5. Klicken Sie auf **Erstellen**.

Gateway-Details

Führen Sie über die Seite **Gateway-Liste** die folgenden Schritte aus:

1. Geben Sie einen Namen ein, um das Gateway anzugeben. Dies ist ein erforderliches Feld.
2. Geben Sie optional den Status des Gateways an. **Aktiviert** ist die Standardeinstellung. Ein aktiviertes Gateway ist für das Senden von Dokumenten bereit. Ein inaktiviertes Gateway kann keine Dokumente senden.

3. Geben Sie optional an, ob das Gateway online oder offline ist. Die Standardeinstellung ist **Online**.
4. Geben Sie optional eine Beschreibung für das Gateway ein.

Gatewaykonfiguration

Führen Sie die folgenden Schritte im Abschnitt **Gatewaykonfiguration** der Seite aus:

1. Wählen Sie **HTTPS/1.0** oder **HTTPS/1.1** in der Liste **Transport** aus.
2. Wählen Sie optional einen zu verwendenden Proxy-Server aus. Die **Forward Proxy-Liste** schließt alle Proxy-Server ein, die Sie erstellt haben, einschließlich dem Standard-Proxy-Server. Der Standardwert für dieses Feld ist **Standardmäßigen Forward Proxy verwenden**. Wenn Sie wollen, dass der ausgewählte Teilnehmer einen anderen Proxy-Server verwendet, wählen Sie diesen Server in der Liste aus. Wenn Sie diese Funktion nicht mit dem ausgewählten Teilnehmer verwenden wollen, wählen Sie **Keinen Forward Proxy verwenden** aus.
3. Geben Sie in das Feld **Adresse** die URI ein, der das Dokument zugestellt werden soll. Dieses Feld ist erforderlich.

   Das Format lautet: https://*<servername>*:*<optionaler_port>*/*<pfad>*

   Beispiel:

   ```
   https://weitererserver.ibm.com:57443/bcgreceiver/Receiver
   ```
4. Geben Sie optional einen Benutzernamen und ein Kennwort ein, wenn ein Benutzername und ein Kennwort für den Zugriff auf den HTTPS-Server erforderlich sind.
5. Geben Sie in das Feld **Wiederholungszahl** die Anzahl Versuche ein, die das Gateway unternehmen soll, um ein Dokument zu senden, bevor es fehlschlägt. Der Standardwert ist 3.
6. Geben Sie in das Feld **Wiederholungsintervall** die Zeit ein, die das Gateway warten soll, bevor es versucht, das Dokument erneut zu senden. Der Standardwert ist 300 Sekunden.
7. Geben Sie in das Feld **Anzahl Threads** die Anzahl Dokumente ein, die gleichzeitig verarbeitet werden können. Der Standardwert ist 3.
8. Wählen Sie im Feld **Client-IP prüfen** die Option **Ja** aus, wenn Sie wollen, dass die IP-Adresse des Absenders geprüft wird, bevor das Dokument verarbeitet wird. Wählen Sie andernfalls **Nein** aus. Die Standardeinstellung ist **Nein**.
9. Wählen Sie im Feld **Client-SSL-Zertifikat prüfen** die Option **Ja** aus, wenn Sie wollen, dass das digitale Zertifikat des sendenden Partners mit der dem Dokument zugeordneten Geschäfts-ID geprüft wird. Die Standardeinstellung ist **Nein**.
10. Wählen Sie im Feld **Autom. Warteschlange** die Option **Ja** aus, wenn Sie wollen, dass das Gateway (automatisch) offline gehen soll, wenn ein Übermittlungsfehler auftritt, weil die Anzahl Wiederholungen aufgebraucht ist. Wählen Sie andernfalls **Nein** aus. Die Standardeinstellung ist **Nein**.

    Wenn Sie **Autom. Warteschlange** auswählen, bleiben alle Dokumente so lange in der Warteschlange, bis das Gateway wieder manuell online gestellt wird.
11. Geben Sie in das Feld **Verbindungszeitlimit** die Anzahl Sekunden ein, die ein Socket ohne Datenverkehr geöffnet bleibt. Der Standardwert ist 120 Sekunden.
12. Wenn Sie den Vorverarbeitungs- oder den Nachverarbeitungsschritt für das Gateway konfigurieren wollen, fahren Sie mit „Handler konfigurieren" auf Seite 158 fort. Ansonsten klicken Sie auf **Speichern**.

FTP-Gateway konfigurieren

Verwenden Sie die folgende Prozedur, um um ein FTP-Gateway zu erstellen.

1. Klicken Sie auf **Kontenadmin > Profile > Community-Teilnehmer**.
2. Geben Sie Suchkriterien ein, und klicken Sie auf **Suchen**, oder klicken Sie auf **Suchen**, ohne Suchkriterien einzugeben, um eine Liste aller Teilnehmer anzuzeigen.
3. Klicken Sie auf das Symbol **Details anzeigen**, um das Profil des Teilnehmers anzuzeigen.
4. Klicken Sie auf **Gateways**.
5. Klicken Sie auf **Erstellen**.

Gateway-Details

Führen Sie über die Seite **Gateway-Details** die folgenden Schritte aus:

1. Geben Sie einen Namen ein, um das Gateway anzugeben. Dies ist ein erforderliches Feld.
2. Geben Sie optional den Status des Gateways an. **Aktiviert** ist die Standardeinstellung. Ein aktiviertes Gateway ist für das Senden von Dokumenten bereit. Ein inaktiviertes Gateway kann keine Dokumente senden.
3. Geben Sie optional an, ob das Gateway online oder offline ist. Die Standardeinstellung ist **Online**.
4. Geben Sie optional eine Beschreibung für das Gateway ein.

Gatewaykonfiguration

Führen Sie die folgenden Schritte im Abschnitt **Gatewaykonfiguration** der Seite aus:

1. Wählen Sie **FTP** in der Liste **Transport** aus.
2. Geben Sie in das Feld **Adresse** die URI ein, der das Dokument zugestellt werden soll. Dieses Feld ist erforderlich.

   Das Format lautet: ftp://<*ftp-servername*>: <*portnr*>

   Beispiel:

   ```
   ftp://ftpserver1.ibm.com:2115
   ```

   Wenn Sie keine Portnummer eingeben, wird der Standard-FTP-Port verwendet.
3. Geben Sie optional einen Benutzernamen und ein Kennwort ein, wenn ein Benutzername und ein Kennwort für den Zugriff auf den FTP-Server erforderlich sind.
4. Geben Sie in das Feld **Wiederholungszahl** die Anzahl Versuche ein, die das Gateway unternehmen soll, um ein Dokument zu senden, bevor es fehlschlägt. Der Standardwert ist 3.
5. Geben Sie in das Feld **Wiederholungsintervall** die Zeit ein, die das Gateway warten soll, bevor es versucht, das Dokument erneut zu senden. Der Standardwert ist 300 Sekunden.
6. Geben Sie in das Feld **Anzahl Threads** die Anzahl Dokumente ein, die gleichzeitig verarbeitet werden können. Der Standardwert ist 3.
7. Wählen Sie im Feld **Client-IP prüfen** die Option **Ja** aus, wenn Sie wollen, dass die IP-Adresse des Absenders geprüft wird, bevor das Dokument verarbeitet wird. Wählen Sie andernfalls **Nein** aus. Die Standardeinstellung ist **Nein**.
8. Wählen Sie im Feld **Autom. Warteschlange** die Option **Ja** aus, wenn Sie wollen, dass das Gateway (automatisch) offline gehen soll, wenn ein

Übermittlungsfehler auftritt, weil die Anzahl Wiederholungen aufgebraucht ist. Wählen Sie andernfalls **Nein** aus. Die Standardeinstellung ist **Nein**.

Wenn Sie **Autom. Warteschlange** auswählen, bleiben alle Dokumente so lange in der Warteschlange, bis das Gateway wieder manuell online gestellt wird.

9. Geben Sie in das Feld **Verbindungszeitlimit** die Anzahl Sekunden ein, die ein Socket ohne Datenverkehr geöffnet bleibt. Der Standardwert ist 120 Sekunden.
10. Behalten Sie die Auswahl des Felds **Eindeutigen Dateinamen verwenden** bei, wenn Sie wollen, dass das Dokument seinen ursprünglichen Namen hat, wenn es an sein Ziel gesendet wird. Andernfalls klicken Sie auf das Feld, um das Häkchen zu entfernen, in diesem Fall wird WebSphere Partner Gateway der Datei einen Namen zuordnen.
11. Wenn Sie den Vorverarbeitungs- oder den Nachverarbeitungsschritt für das Gateway konfigurieren wollen, fahren Sie mit „Handler konfigurieren" auf Seite 158 fort. Ansonsten klicken Sie auf **Speichern**.

SMTP-Gateway konfigurieren

Verwenden Sie die folgende Prozedur, um um ein SMTP-Gateway zu erstellen.

1. Klicken Sie auf **Kontenadmin > Profile > Community-Teilnehmer**.
2. Geben Sie Suchkriterien ein, und klicken Sie auf **Suchen**, oder klicken Sie auf **Suchen**, ohne Suchkriterien einzugeben, um eine Liste aller Teilnehmer anzuzeigen.
3. Klicken Sie auf das Symbol **Details anzeigen**, um das Profil des Teilnehmers anzuzeigen.
4. Klicken Sie auf **Gateways**.
5. Klicken Sie auf **Erstellen**.

Gateway-Details

Führen Sie über die Seite **Gateway-Liste** die folgenden Schritte aus:

1. Geben Sie einen Namen ein, um das Gateway anzugeben. Dies ist ein erforderliches Feld.
2. Geben Sie optional den Status des Gateways an. **Aktiviert** ist die Standardeinstellung. Ein aktiviertes Gateway ist für das Senden von Dokumenten bereit. Ein inaktiviertes Gateway kann keine Dokumente senden.
3. Geben Sie optional an, ob das Gateway online oder offline ist. Die Standardeinstellung ist **Online**.
4. Geben Sie optional eine Beschreibung für das Gateway ein.

Gatewaykonfiguration

Führen Sie die folgenden Schritte im Abschnitt **Gatewaykonfiguration** der Seite aus:

1. Wählen Sie **SMTP** in der Liste **Transport** aus.
2. Geben Sie in das Feld **Adresse** die URI ein, der das Dokument zugestellt werden soll. Dieses Feld ist erforderlich.

   Das Format lautet: mailto:<*benutzer@servername*>

   Beispiel:

   ```
   mailto:admin@weitererserver.ibm.com
   ```
3. Geben Sie optional einen Benutzernamen und ein Kennwort ein, wenn ein Benutzername und ein Kennwort für den Zugriff auf den SMTP-Server erforderlich sind.

4. Geben Sie in das Feld **Wiederholungszahl** die Anzahl Versuche ein, die das Gateway unternehmen soll, um ein Dokument zu senden, bevor es fehlschlägt. Der Standardwert ist 3.
5. Geben Sie in das Feld **Wiederholungsintervall** die Zeit ein, die das Gateway warten soll, bevor es versucht, das Dokument erneut zu senden. Der Standardwert ist 300 Sekunden.
6. Geben Sie in das Feld **Anzahl Threads** die Anzahl Dokumente ein, die gleichzeitig verarbeitet werden können. Der Standardwert ist 3.
7. Wählen Sie im Feld **Client-IP prüfen** die Option **Ja** aus, wenn Sie wollen, dass die IP-Adresse des Absenders geprüft wird, bevor das Dokument verarbeitet wird. Wählen Sie andernfalls **Nein** aus. Die Standardeinstellung ist **Nein**.
8. Wählen Sie im Feld **Autom. Warteschlange** die Option **Ja** aus, wenn Sie wollen, dass das Gateway (automatisch) offline gehen soll, wenn ein Übermittlungsfehler auftritt, weil die Anzahl Wiederholungen aufgebraucht ist. Wählen Sie andernfalls **Nein** aus. Die Standardeinstellung ist **Nein**.

   Wenn Sie **Autom. Warteschlange** auswählen, bleiben alle Dokumente so lange in der Warteschlange, bis das Gateway wieder manuell online gestellt wird.
9. Geben Sie im Feld **Authentifizierung erforderlich** an, ob ein Benutzername und ein Kennwort mit dem Dokument bereitgestellt werden. Die Standardeinstellung ist **Nein**.
10. Wenn Sie den Vorverarbeitungs- oder den Nachverarbeitungsschritt für das Gateway konfigurieren wollen, fahren Sie mit „Handler konfigurieren" auf Seite 158 fort. Ansonsten klicken Sie auf **Speichern**.

JMS-Gateway konfigurieren

Verwenden Sie die folgende Prozedur, um JMS-Gateways zu erstellen.

1. Klicken Sie auf **Kontenadmin > Profile > Community-Teilnehmer**.
2. Geben Sie Suchkriterien ein, und klicken Sie auf **Suchen**, oder klicken Sie auf **Suchen**, ohne Suchkriterien einzugeben, um eine Liste aller Teilnehmer anzuzeigen.
3. Klicken Sie auf das Symbol **Details anzeigen**, um das Profil des Teilnehmers anzuzeigen.
4. Klicken Sie auf **Gateways**.
5. Klicken Sie auf **Erstellen**.

Gateway-Details

Führen Sie über die Seite **Gateway-Liste** die folgenden Schritte aus:

1. Geben Sie einen Namen ein, um das Gateway anzugeben. Dies ist ein erforderliches Feld.
2. Geben Sie optional den Status des Gateways an. **Aktiviert** ist die Standardeinstellung. Ein aktiviertes Gateway ist für das Senden von Dokumenten bereit. Ein inaktiviertes Gateway kann keine Dokumente senden.
3. Geben Sie optional an, ob das Gateway online oder offline ist. Die Standardeinstellung ist **Online**.
4. Geben Sie optional eine Beschreibung für das Gateway ein.

Gatewaykonfiguration

Führen Sie die folgenden Schritte im Abschnitt **Gatewaykonfiguration** der Seite aus:

1. Wählen Sie **JMS** in der Liste **Transport** aus.

2. Geben Sie in das Feld **Adresse** die URI ein, der das Dokument zugestellt werden soll. Dieses Feld ist erforderlich.

   Für WebSphere MQ-JMS lautet das Format der Ziel-URI wie folgt:

   `file:///<benutzerdefinierter_MQ_JNDI_bindings_pfad>`

   Beispiel:

   `file:///opt/JNDI-Directory`

   Das Verzeichnis enthält die ".bindings"-Datei für die dateibasierte JNDI. Diese Datei gibt WebSphere Partner Gateway an, wie das Dokument an sein beabsichtigtes Ziel weitergeleitet wird.

   - Für ein internes JMS-Gateway, das ist das Gateway zu Ihrem Back-End-System, sollte dies mit dem Wert übereinstimmen, den Sie eingegeben haben (der Dateisystempfad zur `.bindungs`-Datei), als Sie WebSphere Partner Gateway für JMS konfiguriert haben (Schritt 5 auf Seite 25). Sie können den Unterordner für den JMS-Kontext auch als Teil des JMS-Provider-URLs angeben.

     Sie würden z. B. ohne den JMS-Kontext `c:/temp/JMS` eingeben. Mit dem JMS-Kontext würden Sie `c:/temp/JMS/JMS` eingeben.
   - Für Teilnehmergateways stellt der Teilnehmer wahrscheinlich die ".bindings"-Datei bereit.

   Dieses Feld ist erforderlich.
3. Geben Sie optional einen Benutzernamen und ein Kennwort ein, wenn ein Benutzername und ein Kennwort für den Zugriff auf die JMS-Warteschlange erforderlich sind.
4. Geben Sie in das Feld **Wiederholungszahl** die Anzahl Versuche ein, die das Gateway unternehmen soll, um ein Dokument zu senden, bevor es fehlschlägt. Der Standardwert ist 3.
5. Geben Sie in das Feld **Wiederholungsintervall** die Zeit ein, die das Gateway warten soll, bevor es versucht, das Dokument erneut zu senden. Der Standardwert ist 300 Sekunden.
6. Geben Sie in das Feld **Anzahl Threads** die Anzahl Dokumente ein, die gleichzeitig verarbeitet werden können. Der Standardwert ist 3.
7. Wählen Sie im Feld **Client-IP prüfen** die Option **Ja** aus, wenn Sie wollen, dass die IP-Adresse des Absenders geprüft wird, bevor das Dokument verarbeitet wird. Wählen Sie andernfalls **Nein** aus. Die Standardeinstellung ist **Nein**.
8. Wählen Sie im Feld **Autom. Warteschlange** die Option **Ja** aus, wenn Sie wollen, dass das Gateway (automatisch) offline gehen soll, wenn ein Übermittlungsfehler auftritt, weil die Anzahl Wiederholungen aufgebraucht ist. Wählen Sie andernfalls **Nein** aus. Die Standardeinstellung ist **Nein**.

   Wenn Sie **Autom. Warteschlange** auswählen, bleiben alle Dokumente so lange in der Warteschlange, bis das Gateway wieder manuell online gestellt wird.
9. Geben Sie im Feld **Authentifizierung erforderlich** an, ob ein Benutzername und ein Kennwort mit dem Dokument bereitgestellt werden. Die Standardeinstellung ist **Nein**.
10. Geben Sie im Feld **JMS-Factory-Name** den Namen der Java-Klasse ein, den der JMS-Provider verwendet, um eine Verbindung zur JMS-Warteschlange herzustellen. Dieses Feld ist erforderlich.

    Für interne JMS-Gateways sollte dieser Name mit dem Namen übereinstimmen, den Sie mit dem Befehl `define qcf` angegeben haben, als Sie die `.bindungs`-Datei erstellt haben (Schritt 4 auf Seite 27).

    Wenn Sie den Unterordner für den JMS-Kontext in Schritt 2 eingegeben haben, geben Sie hier nur den Factory-Namen ein, z. B. `Hub`. Wenn Sie den Unter-

ordner für den JMS-Kontext nicht im Feld **Adresse** eingegeben haben, geben Sie den Unterordner vor dem Factory-Namen ein, z. B. `JMS/Hub`.

11. Geben Sie im Feld **JMS-Nachrichtenklasse** die Nachrichtenklasse ein. Zu den Auswahlmöglichkeiten gehören alle gültigen JMS-Nachrichtenklassen, wie z. B. TextMessage oder BytesMessage. Dieses Feld ist erforderlich.
12. Geben Sie in das Feld **JMS-Nachrichtentyp** den Nachrichtentyp ein. Dies ist ein optionales Feld.
13. Geben Sie in das Feld **Provider-URL-Pakete** den Namen der Klassen (oder JAR-Datei) ein, mit denen Java den JMS-Kontext-URL versteht. Dieses Feld ist optional. Wenn Sie keinen Wert angeben, wird der Dateisystempfad zur ″.bindings″-Datei verwendet.
14. Geben Sie in das Feld **JMS-Warteschlangenname** den Namen der JMS-Warteschlange ein, an die Dokumente gesendet werden. Dieses Feld ist erforderlich.

    Für interne JMS-Gateways sollte dieser Name mit dem Namen übereinstimmen, den Sie mit dem Befehl `define q` angegeben haben, als Sie die `.bindungs`-Datei erstellt haben (Schritt 4 auf Seite 27).

    Wenn Sie den Unterordner für den JMS-Kontext in Schritt 2 auf Seite 150 eingegeben haben, geben Sie hier nur den Namen der Warteschlange ein, z. B. `outQ`. Wenn Sie den Unterordner für den JMS-Kontext nicht im Feld **JMS-Provider-URL** eingegeben haben, geben Sie den Unterordner vor dem Namen der Warteschlange ein, z. B. `JMS/outQ`.
15. Geben Sie in das Feld **JMS-JNDI-Factory-Name** den Factory-Namen ein, der für den Verbindungsaufbau zum Namensservice verwendet wird. Dieses Feld ist erforderlich. Sie werden wahrscheinlich den Wert `com.sun.jndi.fscontext.RefFSContextFactory` verwenden, wenn Sie Ihre JMS-Konfiguration, wie in „Den Hub für das JMS-Transportprotokoll konfigurieren” auf Seite 25 beschrieben, einrichten.
16. Wenn Sie den Vorverarbeitungs- oder den Nachverarbeitungsschritt für das Gateway konfigurieren wollen, fahren Sie mit „Handler konfigurieren” auf Seite 158 fort. Ansonsten klicken Sie auf **Speichern**.

Dateiverzeichnisgateway konfigurieren

Verwenden Sie die folgende Prozedur, um Dateiverzeichnisgateways zu erstellen.

1. Klicken Sie auf **Kontenadmin > Profile > Community-Teilnehmer**.
2. Geben Sie Suchkriterien ein, und klicken Sie auf **Suchen**, oder klicken Sie auf **Suchen**, ohne Suchkriterien einzugeben, um eine Liste aller Teilnehmer anzuzeigen.
3. Klicken Sie auf das Symbol **Details anzeigen**, um das Profil des Teilnehmers anzuzeigen.
4. Klicken Sie auf **Gateways**.
5. Klicken Sie auf **Erstellen**.

Gateway-Details

Führen Sie über die Seite **Gateway-Liste** die folgenden Schritte aus:

1. Geben Sie einen Namen ein, um das Gateway anzugeben. Dies ist ein erforderliches Feld.
2. Geben Sie optional den Status des Gateways an. **Aktiviert** ist die Standardeinstellung. Ein aktiviertes Gateway ist für das Senden von Dokumenten bereit. Ein inaktiviertes Gateway kann keine Dokumente senden.

3. Geben Sie optional an, ob das Gateway online oder offline ist. Die Standardeinstellung ist **Online**.
4. Geben Sie optional eine Beschreibung für das Gateway ein.

Gatewaykonfiguration

Führen Sie die folgenden Schritte im Abschnitt **Gatewaykonfiguration** der Seite aus:

1. Wählen Sie **Dateiverzeichnis** in der Liste **Transport** aus.
2. Geben Sie in das Feld **Adresse** die URI ein, der das Dokument zugestellt werden soll. Dieses Feld ist erforderlich.

   Das Format für UNIX-Systeme und für Windows-Systeme, bei denen sich das Dateiverzeichnis auf demselben Laufwerk befindet wie die WebSphere Partner Gateway-Installation, lautet: file:///<*pfad_zu_zielverzeichnis*>

   Beispiel:

   ```
   file:///lokalesdateiverz
   ```

   Dabei steht *lokalesdateiverz* für ein Verzeichnis im Stammverzeichnis.

   Für Windows-Systeme, bei denen sich das Dateiverzeichnis nicht auf dem Laufwerk mit WebSphere Partner Gateway befindet, lautet das Format: file:///<*laufwerkbuchstabe*>:/<*pfad*>
3. Geben Sie in das Feld **Wiederholungszahl** die Anzahl Versuche ein, die das Gateway unternehmen soll, um ein Dokument zu senden, bevor es fehlschlägt. Der Standardwert ist 3.
4. Geben Sie in das Feld **Wiederholungsintervall** die Zeit ein, die das Gateway warten soll, bevor es versucht, das Dokument erneut zu senden. Der Standardwert ist 300 Sekunden.
5. Geben Sie in das Feld **Anzahl Threads** die Anzahl Dokumente ein, die gleichzeitig verarbeitet werden sollen. Der Standardwert ist 3.
6. Wählen Sie im Feld **Client-IP prüfen** die Option **Ja** aus, wenn Sie wollen, dass die IP-Adresse des Absenders geprüft wird, bevor das Dokument verarbeitet wird. Wählen Sie andernfalls **Nein** aus. Die Standardeinstellung ist **Nein**.
7. Wählen Sie im Feld **Autom. Warteschlange** die Option **Ja** aus, wenn Sie wollen, dass das Gateway (automatisch) offline gehen soll, wenn ein Übermittlungsfehler auftritt, weil die Anzahl Wiederholungen aufgebraucht ist. Wählen Sie andernfalls **Nein** aus. Die Standardeinstellung ist **Nein**.

   Wenn Sie **Autom. Warteschlange** auswählen, bleiben alle Dokumente so lange in der Warteschlange, bis das Gateway wieder manuell online gestellt wird.
8. Behalten Sie die Auswahl des Felds **Eindeutigen Dateinamen verwenden** bei, wenn Sie wollen, dass das Dokument seinen ursprünglichen Namen hat, wenn es an sein Ziel gesendet wird. Andernfalls klicken Sie auf das Feld, um das Häkchen zu entfernen, in diesem Fall wird WebSphere Partner Gateway der Datei einen Namen zuordnen.
9. Wenn Sie den Vorverarbeitungs- oder den Nachverarbeitungsschritt für das Gateway konfigurieren wollen, fahren Sie mit „Handler konfigurieren" auf Seite 158 fort. Ansonsten klicken Sie auf **Speichern**.

FTPS-Gateway konfigurieren

Verwenden Sie die folgende Prozedur, um FTPS-Gateways zu erstellen.

1. Klicken Sie auf **Kontenadmin > Profile > Community-Teilnehmer**.

2. Geben Sie Suchkriterien ein, und klicken Sie auf **Suchen**, oder klicken Sie auf **Suchen**, ohne Suchkriterien einzugeben, um eine Liste aller Teilnehmer anzuzeigen.
3. Klicken Sie auf das Symbol **Details anzeigen**, um das Profil des Teilnehmers anzuzeigen.
4. Klicken Sie auf **Gateways**.
5. Klicken Sie auf **Erstellen**.

Gateway-Details

Führen Sie über die Seite **Gateway-Liste** die folgenden Schritte aus:

1. Geben Sie einen Namen ein, um das Gateway anzugeben. Dies ist ein erforderliches Feld.
2. Geben Sie optional den Status des Gateways an. **Aktiviert** ist die Standardeinstellung. Ein aktiviertes Gateway ist für das Senden von Dokumenten bereit. Ein inaktiviertes Gateway kann keine Dokumente senden.
3. Geben Sie optional an, ob das Gateway online oder offline ist. Die Standardeinstellung ist **Online**.
4. Geben Sie optional eine Beschreibung für das Gateway ein.

Gatewaykonfiguration

Führen Sie die folgenden Schritte im Abschnitt **Gatewaykonfiguration** der Seite aus:

1. Wählen Sie **FTPS** in der Liste **Transport** aus.
2. Geben Sie in das Feld **Adresse** die URI ein, der das Dokument zugestellt werden soll. Dieses Feld ist erforderlich.

   Das Format lautet: ftp://<*ftp-servername*>: <*portnr*>

   Beispiel:

   ```
   ftp://ftpserver1.ibm.com:2115
   ```

   Wenn Sie keine Portnummer eingeben, wird der Standard-FTP-Port verwendet.
3. Geben Sie optional einen Benutzernamen und ein Kennwort ein, wenn ein Benutzername und ein Kennwort für den Zugriff auf den FTPS-Server erforderlich sind.
4. Geben Sie in das Feld **Wiederholungszahl** die Anzahl Versuche ein, die das Gateway unternehmen soll, um ein Dokument zu senden, bevor es fehlschlägt. Der Standardwert ist 3.
5. Geben Sie in das Feld **Wiederholungsintervall** die Zeit ein, die das Gateway warten soll, bevor es versucht, das Dokument erneut zu senden. Der Standardwert ist 300 Sekunden.
6. Geben Sie in das Feld **Anzahl Threads** die Anzahl Dokumente ein, die gleichzeitig verarbeitet werden sollen. Der Standardwert ist 3.
7. Wählen Sie im Feld **Client-IP prüfen** die Option **Ja** aus, wenn Sie wollen, dass die IP-Adresse des Absenders geprüft wird, bevor das Dokument verarbeitet wird. Wählen Sie andernfalls **Nein** aus. Die Standardeinstellung ist **Nein**.
8. Wählen Sie im Feld **Autom. Warteschlange** die Option **Ja** aus, wenn Sie wollen, dass das Gateway (automatisch) offline gehen soll, wenn ein Übermittlungsfehler auftritt, weil die Anzahl Wiederholungen aufgebraucht ist. Wählen Sie andernfalls **Nein** aus. Die Standardeinstellung ist **Nein**.

   Wenn Sie **Autom. Warteschlange** auswählen, bleiben alle Dokumente so lange in der Warteschlange, bis das Gateway wieder manuell online gestellt wird.

9. Geben Sie in das Feld **Verbindungszeitlimit** die Anzahl Sekunden ein, die ein Socket ohne Datenverkehr geöffnet bleibt. Der Standardwert ist 120 Sekunden.
10. Behalten Sie die Auswahl des Felds **Eindeutigen Dateinamen verwenden** bei, wenn Sie wollen, dass das Dokument seinen ursprünglichen Namen hat, wenn es an sein Ziel gesendet wird. Andernfalls klicken Sie auf das Feld, um das Häkchen zu entfernen, in diesem Fall wird WebSphere Partner Gateway der Datei einen Namen zuordnen.
11. Wenn Sie den Vorverarbeitungs- oder den Nachverarbeitungsschritt für das Gateway konfigurieren wollen, fahren Sie mit „Handler konfigurieren" auf Seite 158 fort. Ansonsten klicken Sie auf **Speichern**.

FTP-Scripting-Gateway konfigurieren

Ein FTP-Scripting-Gateway wird entsprechend dem von Ihnen festgelegten Zeitplan ausgeführt. Das Verhalten eines FTP-Scripting-Gateways wird von einem FTP-Befehlsscript geregelt.

Das FTP-Script erstellen

Um ein FTP-Scripting-Gateway zu verwenden, erstellen Sie eine Datei mit allen erforderlichen FTP-Befehlen, die von Ihrem FTP-Server akzeptiert werden können.

1. Erstellen Sie ein Script für die Gateways, um die Aktionen anzugeben, die Sie ausführen wollen. Das folgende Script ist ein Beispiel für das Herstellen einer Verbindung zu dem angegebenen FTP-Server (mit dem angegebenen Namen und Kennwort), für das Wechseln zum angegebenen Verzeichnis auf dem FTP-Server und für das Senden aller Dateien zu dem angegebenen Verzeichnis auf dem Server:

```
open %BCGSERVERIP% %BCGUSERID% %BCGPASSWORD% %BCGOPTIONx%
cd %BCGOPTIONx%
          mput *
          quit
```

   Die Platzhalter (z. B. %BCGSERVERIP%) werden ersetzt, wenn das Gateway aktiviert wird durch die Werte, die Sie eingeben, wenn Sie eine bestimmte Instanz eines FTP-Scripting-Gateways erstellen, wie in der folgenden Tabelle gezeigt wird:

Tabelle 17. Zuordnung der Scriptparameter zu den Feldeinträgen für das FTP-Scripting-Gateway

Scriptparameter	Feldeintrag für das FTP-Scripting-Gateway
%BCGSERVERIP%	Server-IP
%BCGUSERID%	Benutzer-ID
%BCGPASSWORD%	Kennwort
%BCGOPTIONx%	Option*x* unter **Benutzerdefinierte Attribute**

   Sie können über bis zu 10 benutzerdefinierte Optionen verfügen.
2. Speichern Sie die Datei.

FTP-Scriptbefehle

Sie können die folgenden Befehle verwenden, wenn Sie das Script erstellen:

- ascii, binary, passive

  Diese Befehle werden nicht an den FTP-Server gesendet. Sie ändern den Modus für die Übertragung (ascii, binary oder passive) zum FTP-Server.

- cd

  Dieser Befehl wechselt zum angegebenen Verzeichnis.
- delete

  Dieser Befehl entfernt eine Datei vom FTP-Server.
- mkdir

  Dieser Befehl erstellt ein Verzeichnis auf dem FTP-Server.
- mput

  Dieser Befehl verfügt über ein einzelnes Argument, das mindestens eine Datei angibt, die auf das ferne System übertragen werden soll. Dieses Argument kann die Standardplatzhalterzeichen ('*' und '?') enthalten, um mehrere Dateien anzugeben.
- open

  Dieser Befehl verwendet drei Parameter: die IP-Adresse des FTP-Servers, den Benutzernamen und ein Kennwort. Diese Parameter stimmen mit den Variablen %BCGSERVERIP%, %BCGUSERID% und %BCGPASSWORD% überein.

  Die erste Zeile Ihres FTP-Scripting-Gateway-Scripts sollte daher wie folgt lauten:

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

  Dieser Befehl beendet eine vorhandene Verbindung zu einem FTP-Server.
- quote

  Dieser Befehl gibt an, dass alles nach dem Befehl `QUOTE` an das ferne System als Befehl gesendet werden soll. Dies ermöglicht Ihnen, Befehle an einen fernen FTP-Server zu senden, die möglicherweise nicht im Standard-FTP-Protokoll definiert sind.
- rmdir

  Dieser Befehl entfernt ein Verzeichnis vom FTP-Server.
- site

  Dieser Befehl kann verwendet werden, um sitespezifische Befehle auf dem fernen System abzusetzen. Das ferne System bestimmt, ob der Inhalt dieses Befehls gültig ist.

FTP-Scripting-Gateways

Wenn Sie FTP-Scripting-Gateways verwenden, führen Sie die folgenden Aufgaben aus:

Verwenden Sie die folgende Prozedur, um FTP-Scripting-Gateways zu erstellen.

1. Klicken Sie auf **Kontenadmin > Profile > Community-Teilnehmer**.
2. Geben Sie Suchkriterien ein, und klicken Sie auf **Suchen**, oder klicken Sie auf **Suchen**, ohne Suchkriterien einzugeben, um eine Liste aller Teilnehmer anzuzeigen.
3. Klicken Sie auf das Symbol **Details anzeigen**, um das Profil des Teilnehmers anzuzeigen.
4. Klicken Sie auf **Gateways**.
5. Klicken Sie auf **Erstellen**.

Gateway-Details

Führen Sie über die Seite **Gateway-Liste** die folgenden Schritte aus:

1. Geben Sie einen Namen ein, um das Gateway anzugeben. Dies ist ein erforderliches Feld.
2. Geben Sie optional den Status des Gateways an. **Aktiviert** ist die Standardeinstellung. Ein aktiviertes Gateway ist für das Senden von Dokumenten bereit. Ein inaktiviertes Gateway kann keine Dokumente senden.
3. Geben Sie optional an, ob das Gateway online oder offline ist. Die Standardeinstellung ist **Online**.
4. Geben Sie optional eine Beschreibung für das Gateway ein.

Gatewaykonfiguration

Führen Sie die folgenden Schritte im Abschnitt **Gatewaykonfiguration** der Seite aus:

1. Wählen Sie **FTP-Scripting** in der Liste **Transport** aus.
2. Geben Sie die IP-Adresse des FTP-Servers ein, zu dem Sie Dokumente senden. Der Wert, den Sie hier eingeben, wird %BCGSERVERIP% ersetzen, wenn das FTP-Script ausgeführt wird.
3. Geben Sie die Benutzer-ID und das Kennwort ein, die für den Zugriff auf den FTP-Server erforderlich sind. Die Werte, die Sie hier eingeben, werden %BCGUSERID% und %BCGPASSWORD% ersetzen, wenn das FTP-Script ausgeführt wird.
4. Wenn das Ziel sich im gesicherten Modus befindet, verwenden Sie die Standardeinstellung **Ja** für **FTPS-Modus**. Andernfalls klicken Sie auf **Nein**.
5. Laden Sie die Scriptdatei hoch, indem Sie die folgenden Schritte befolgen:
   a. Klicken Sie auf **Scriptdatei hochladen**.
   b. Geben Sie den Namen der Datei ein, die das Script für die Verarbeitung von Dokumenten enthält, oder navigieren Sie mit **Durchsuchen** zu der Datei.
   c. Klicken Sie auf **Datei laden**, um die Scriptdatei in das Textfeld **Momentan geladene Scriptdatei** zu laden.
   d. Wenn es sich um die gewünschte Scriptdatei handelt, klicken Sie auf **Speichern**.
   e. Klicken Sie auf **Fenster schließen**.
6. Geben Sie in das Feld **Wiederholungszahl** die Anzahl Versuche ein, die das Gateway unternehmen soll, um ein Dokument zu senden, bevor es fehlschlägt. Der Standardwert ist 3.
7. Geben Sie in das Feld **Wiederholungsintervall** die Zeit ein, die das Gateway warten soll, bevor es versucht, das Dokument erneut zu senden. Der Standardwert ist 300 Sekunden.
8. Geben Sie für **Verbindungszeitlimit** die Anzahl Sekunden ein, die ein Socket ohne Datenverkehr geöffnet bleibt. Der Standardwert ist 120 Sekunden.
9. Geben Sie im Feld **Benutzer sperren** an, ob das Gateway eine Sperre anfordern wird, so dass keine anderen Instanzen eines FTP-Scripting-Gateways gleichzeitig auf dasselbe FTP-Serververzeichnis zugreifen können.

Anmerkung: Die Werte für **Attribute des globalen FTP-Scripting** sind bereits ausgefüllt und Sie können diese über diese Seite nicht bearbeiten. Verwenden Sie die Seite **Globale Transportattribute**, um diese Werte zu ändern, wie in „Globale Transportwerte konfigurieren” auf Seite 142 beschrieben.

Benutzerdefinierte Attribute

Wenn Sie zusätzliche Attribute angeben wollen, führen Sie die folgenden Schritte aus. Der Wert, den Sie für die Option eingeben, wird %BCGOPTION*x*% ersetzen, wenn das FTP-Script ausgeführt wird (dabei entspricht *x* der Optionsnummer).

1. Klicken Sie auf **Neu**.
2. Geben Sie einen Wert neben **Option 1** ein.
3. Wenn Sie zusätzliche Attribute anzugeben haben, klicken Sie wieder auf **Neu**, und geben Sie einen Wert ein.
4. Wiederholen Sie Schritt 3 so oft wie nötig, um alle Attribute zu definieren.

Angenommen, Ihr FTP-Script sieht z. B. wie folgt aus:

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

%BCGOPTION% wäre in diesem Fall ein Verzeichnisname.

Zeitplan

Führen Sie die folgenden Schritte über den Abschnitt **Zeitplan** der Seite aus:

1. Geben Sie an, ob Sie intervallbasierte Zeitplanung oder kalenderbasierte Zeitplanung verwenden wollen.
   - Wenn Sie **Intervallbasierte Zeitplanung** auswählen, dann wählen Sie die Anzahl Sekunden aus, die verstreichen sollen, bevor das Gateway abgefragt wird, oder akzeptieren Sie den Standardwert.
   - Wenn Sie **Kalenderbasierte Zeitplanung** auswählen, dann wählen Sie den Zeitplanungstyp (**Täglicher Zeitplan**, **Wöchentlicher Zeitplan** oder **Angepasster Zeitplan**) aus.
     - Wenn Sie **Täglicher Zeitplan** auswählen, dann geben Sie die Uhrzeit ein, wann das Gateway abgefragt werden soll.
     - Wenn Sie **Wöchentlicher Zeitplan** auswählen, dann wählen Sie mindestens einen Tag in der Woche zusätzlich zur Uhrzeit aus.
     - Wenn Sie **Angepasster Zeitplan** auswählen, dann wählen Sie die Uhrzeit und schließlich noch **Bereich** oder **Ausgewählte Tage** für die Woche und den Monat aus. Mit **Bereich** geben Sie das Startdatum und das Enddatum an. (Klicken Sie z. B. auf **Mo** und **Fr**, wenn Sie wollen, dass der Server nur an Wochentagen zu einer bestimmten Uhrzeit abgefragt wird.) Mit der Option **Ausgewählte Tage** wählen Sie bestimmte Tage in der Woche und im Monat aus.
2. Wenn Sie den Vorverarbeitungs- oder den Nachverarbeitungsschritt für das Gateway konfigurieren wollen, fahren Sie mit „Handler konfigurieren” auf Seite 158 fort. Ansonsten klicken Sie auf **Speichern**.

Handler konfigurieren

Wie in Kapitel 1, „Einführung" beschrieben, können Sie zwei Verarbeitungspunkte für ein Gateway modifizieren: die Vorverarbeitung und die Nachverarbeitung.

Für den Vorverarbeitungs- oder Nachverarbeitungsschritt werden standardmäßig keine Handler bereitgestellt, und daher sind auch standardmäßig keine Handler in der **Verfügbarkeitsliste** aufgelistet. Wenn Sie einen Handler hochgeladen haben, können Sie ihn auswählen und in die **Konfigurationsliste** versetzen.

Um einen benutzerdefinierten Handler auf diese Konfigurationspunkte anzuwenden, müssen Sie zuerst den Handler hochladen, wie in „Benutzerdefinierte Handler hochladen" auf Seite 40 beschrieben. (Wählen Sie **Gateway** anstelle von **Ziel** für Schritt 2 auf Seite 40 aus). Führen Sie dann die folgenden Schritte aus:

1. Wählen Sie **Vorverarbeitung** oder **Nachverarbeitung** in der Liste **Konfigurationspunkt-Handler** aus.
2. Wählen Sie den Handler in der **Verfügbarkeitsliste** aus, und klicken Sie auf **Hinzufügen**.
3. Wenn Sie die Attribute des Handlers ändern wollen, wählen Sie ihn in der **Konfigurationsliste** aus, und klicken Sie auf **Konfigurieren**. Eine Liste mit Attributen, die geändert werden können, wird angezeigt. Nehmen Sie die notwendigen Änderungen vor, und klicken Sie auf **Festlegen**.
4. Klicken Sie auf **Speichern**.

Sie können die **Konfigurationsliste** wie folgt noch weiter ändern:

- Entfernen Sie einen Handler, indem Sie den Handler in der **Konfigurationsliste** auswählen, und klicken Sie auf **Entfernen**. Der Handler wird in die **Verfügbarkeitsliste** versetzt.
- Ändern Sie die Reihenfolge, in der der Handler verarbeitet wird, indem Sie den Handler auswählen und auf **Nach oben** oder **Nach unten** klicken.

Gateway für benutzerdefinierten Transport konfigurieren

Wenn Sie einen benutzerdefinierten Transport hochladen wollen, führen Sie die folgenden Schritte aus.

1. Klicken Sie auf **Kontenadmin > Profile > Community-Teilnehmer**.
2. Klicken Sie auf **Gateways**.
3. Klicken Sie auf **Transporttypen verwalten**.
4. Geben Sie den Namen einer XML-Datei ein, die den Transport definiert oder verwenden Sie **Durchsuchen**, um zur Datei zu navigieren.
5. Verwenden Sie die Standardeinstellung **Ja** für **In Datenbank festschreiben**. Wählen Sie **Nein** aus, wenn Sie diesen Transport testen, bevor Sie ihn in Produktion nehmen.
6. Geben Sie an, ob diese Datei eine Datei mit demselben Namen ersetzen soll, die sich schon in der Datenbank befindet.
7. Klicken Sie auf **Hochladen**.

Anmerkung: Sie können von der Seite **Transporttypen verwalten** auch einen benutzerdefinierten Transporttyp löschen. Sie können keinen Transport löschen, der von WebSphere Partner Gateway bereitgestellt wurde. Ebenfalls können Sie keinen benutzerdefinierten Transport löschen, nachdem er zum Erstellen eines Gateways verwendet wurde.

8. Klicken Sie auf **Erstellen**.
9. Geben Sie einen Namen ein, um das Gateway anzugeben. Dies ist ein erforderliches Feld.
10. Geben Sie optional den Status des Gateways an. **Aktiviert** ist die Standardeinstellung. Ein aktiviertes Gateway ist für das Senden von Dokumenten bereit. Ein inaktiviertes Gateway kann keine Dokumente senden.
11. Geben Sie optional an, ob das Gateway online oder offline ist. Die Standardeinstellung ist **Online**.
12. Geben Sie optional eine Beschreibung für das Gateway ein.
13. Füllen Sie die Felder aus, die für jeden benutzerdefinierten Transport eindeutig sind, und klicken Sie auf **Speichern**.

Standardgateway angeben

Nachdem Sie Gateways für Community Manager oder den Teilnehmer erstellt haben, wählen Sie eines der Gateways als Standardgateway.

1. Klicken Sie auf **Kontenadmin > Profile > Community-Teilnehmer**.
2. Geben Sie Suchkriterien ein, und klicken Sie auf **Suchen**, oder klicken Sie auf **Suchen**, ohne Suchkriterien einzugeben, um eine Liste aller Teilnehmer anzuzeigen.
3. Klicken Sie auf das Symbol **Details anzeigen**, um das Profil des Teilnehmers anzuzeigen.
4. Klicken Sie auf **Gateways**.
5. Klicken Sie auf **Standardgateways anzeigen**.

   Eine Liste mit Gateways, die für den Teilnehmer definiert sind, wird angezeigt.
6. Wählen Sie in der Liste **Produktion** das Gateway aus, das für diesen Teilnehmer der Standard sein wird. Sie können auch Standardgateways für andere Gateway-Typen, wie z. B. **Test**, festlegen.
7. Klicken Sie auf **Speichern**.

Kapitel 11. Teilnehmer und ihre B2B-Funktionalität erstellen

Für jeden Teilnehmer, mit dem Sie Dokumente austauschen werden, erstellen Sie ein Teilnehmerprofil. Dann legen Sie die B2B-Funktionalität der Teilnehmer fest bzw. die Teilnehmer können diesen Schritt selbst ausführen.

Dieses Kapitel behandelt die folgenden Themen:

- „Teilnehmerprofile erstellen"
- „B2B-Funktionalität konfigurieren" auf Seite 163

Teilnehmerprofile erstellen

Zum Erstellen eines Teilnehmers müssen Sie mindestens die folgenden Informationen zum Teilnehmer kennen:

- Die IP-Adresse des Teilnehmers
- Die Geschäfts-ID, die der Teilnehmer verwendet. Diese kann wie folgt lauten:
  - **DUNS**. Dies ist die Dun & Bradstreet-Standardnummer, die einer Firma zugeordnet ist.
  - **DUNS+4**. Dies ist eine erweiterte Version der DUNS-Nummer.
  - **Unformatiert**. Dies kann eine beliebige Nummer sein, die der Teilnehmer auswählt, um mit ihr die Firma anzugeben.

Befolgen Sie für jeden Teilnehmer, den Sie der Hub-Community hinzufügen wollen, diese Prozedur:

1. Klicken Sie auf **Kontenadmin > Profile > Community-Teilnehmer**.
2. Klicken Sie auf **Erstellen**.
3. Geben Sie in **Anmeldename des Unternehmens** den Namen ein, den der Teilnehmer im Unternehmensfeld beim Anmelden am Hub verwendet.
4. Geben Sie in **Anzeigename des Teilnehmers** den Firmennamen oder einen anderen beschreibenden Namen für den Teilnehmer ein. Dies ist der Name, der in der Liste **Teilnehmersuche** angezeigt wird.
5. Wählen Sie den Teilnehmertyp aus. Da WebSphere Partner Gateway nur über einen Community Manager und einen Community Operator verfügen kann, ist Ihre Wahl auf **Community-Teilnehmer** beschränkt.
6. Wählen Sie den Status für den Teilnehmer aus. Wenn Sie einen Teilnehmer erstellen, sollten Sie den Standardwert **Aktiviert** verwenden.
7. Geben Sie optional den Firmentyp in das Feld **Lieferantentyp** ein.
8. Geben Sie optional die Website des Teilnehmers ein.
9. Klicken Sie auf **Neu** unterhalb von **Geschäfts-ID**.
10. Geben Sie einen Typ aus der Liste an, und geben Sie die entsprechende Kennung ein. WebSphere Partner Gateway verwendet die von Ihnen hier eingegebene Nummer, um das Dokument zum Teilnehmer und vom Teilnehmer weiterzuleiten.

    Beachten Sie die folgenden Richtlinien, wenn Sie die Kennung eingeben:

    a. DUNS-Nummern müssen neun Ziffern umfassen.

    b. DUNS+4 müssen über 13 Ziffern verfügen.

c. Unformatierte ID-Nummern akzeptieren bis zu 60 alphanumerische Zeichen und Sonderzeichen.

Anmerkung: Sie können einem Teilnehmer mehr als eine Geschäfts-ID zuordnen. In einigen Fällen ist mehr als eine Geschäfts-ID erforderlich. Wenn z. B. der Hub EDI-X12- und EDIFACT-Dokumente sendet und empfängt, verwendet er sowohl DUNS- als auch unformatierte IDs während des Dokumentenaustauschs.

Sowohl Community Manager als auch die Teilnehmer, die an diesen Dokumentenflusstypen beteiligt sind, sollten jeweils über eine DUNS-ID und eine unformatierte ID verfügen. Die unformatierte ID wird verwendet, um EDI-IDs darzustellen, die über eine Kennung und ein Qualifikationsmerkmal verfügen. Angenommen, das EDI-Qualifikationsmerkmal lautet z. B. ″ZZ″ und die EDI-Kennung lautet ″810810810″. Dann könnte die unformatierte ID wie folgt angegeben werden: ZZ-810810810.

11. Geben Sie optional eine IP-Adresse für den Teilnehmer ein, indem Sie die folgenden Schritte ausführen:
    a. Klicken Sie unter **IP-Adresse** auf **Neu**.
    b. Geben Sie den Gateway-Typ an.
    c. Geben Sie die IP-Adresse des Teilnehmers ein.
12. Klicken Sie auf **Speichern**.
13. Ihnen wird ein Kennwort übermittelt, das der Teilnehmer verwenden wird, um sich beim Hub anzumelden. Notieren Sie sich dieses Kennwort. Stellen Sie es dem Administrator des Teilnehmers zur Verfügung.

Wenn Sie einen Teilnehmer erstellen, erstellen Sie in Wirklichkeit den Administrator für diesen Teilnehmer. Administratoren können dann einzelne Benutzer innerhalb ihrer Organisationen erstellen, oder Sie können als Hubadmin die Benutzer für die Teilnehmer erstellen.

Nachdem Sie ein Profil für einen Teilnehmer erstellt haben, erstellen Sie die Gateways, mit denen der Hub Dokumente an den Teilnehmer senden wird. Lesen Sie die folgenden Abschnitte über das Konfigurieren der Gateways für Teilnehmer.

- „Globale Transportwerte konfigurieren” auf Seite 142

  Anmerkung: Diese Werte gehören nur zum FTP-Scripting-Gateway.
- „HTTP-Gateway konfigurieren” auf Seite 144
- „HTTPS-Gateway konfigurieren” auf Seite 145
- „FTP-Gateway konfigurieren” auf Seite 147
- „SMTP-Gateway konfigurieren” auf Seite 148
- „JMS-Gateway konfigurieren” auf Seite 149
- „Dateiverzeichnisgateway konfigurieren” auf Seite 151
- „FTPS-Gateway konfigurieren” auf Seite 152
- „FTP-Scripting-Gateway konfigurieren” auf Seite 154

B2B-Funktionalität konfigurieren

Jeder Teilnehmer verfügt über B2B-Funktionalität, die die Dokumenttypen definiert, die der Teilnehmer senden und empfangen kann.

Als Hubadmin können Sie die B2B-Funktionalität Ihrer Teilnehmer konfigurieren bzw. die Teilnehmer können diese Aufgabe selbst ausführen. In diesem Kapitel erfahren Sie, wie Sie diese Aufgabe für die Teilnehmer ausführen.

Sie verwenden die B2B-Funktionalitätsfunktion, um die B2B-Funktionalität eines Teilnehmers einer Dokumentenflussdefinition zuzuordnen.

Verwenden Sie die folgende Prozedur, um die B2B-Funktionalität jedes Teilnehmers zu konfigurieren.

1. Klicken Sie auf **Kontenadmin > Profile > Community-Teilnehmer**.
2. Geben Sie Suchkriterien ein, und klicken Sie auf **Suchen**, oder klicken Sie auf **Suchen**, ohne Suchkriterien einzugeben, um eine Liste aller Teilnehmer anzuzeigen.
3. Klicken Sie auf das Symbol **Details anzeigen**, um das Profil des Teilnehmers anzuzeigen.
4. Klicken Sie auf **B2B-Funktionalität**. Die Seite **B2B-Funktionalität** wird angezeigt. Auf der Seite werden rechts die Pakete, Protokolle und Dokumente angezeigt, die vom System als Dokumentenflussdefinitionen unterstützt werden.
5. Klicken Sie auf das Symbol **Rolle ist nicht aktiv** unter der Spalte **Quelle festlegen** für die Pakete auf der rechten Seite, die Dokumente enthalten, welche die Teilnehmer an Community Manager senden werden.
6. Wählen Sie sowohl **Quelle festlegen** als auch **Ziel festlegen** aus, wenn die Teilnehmer dieselben Dokumente senden und empfangen werden. Die Konsole zeigt ein Häkchen an, wenn die Dokumentenflussdefinition aktiviert ist.

   Anmerkung: Die Auswahl von **Quelle festlegen** ist für alle Aktionen in einem Zweiwege-PIP gleich, ungeachtet der Tatsache, dass die Anforderung von einem der Teilnehmer und die entsprechende Bestätigung von einem anderen stammt. Dies gilt auch für **Ziel festlegen**.
7. Klicken Sie auf das Symbol **Erweitern** auf der Ebene **Paket**, um einen einzelnen Knoten auf die entsprechende Ebene der Dokumentenflussdefinition zu erweitern, oder wählen Sie eine Nummer zwischen **0-4** oder **Alle** aus, um alle angezeigten Dokumentenflussdefinitionen zur ausgewählten Ebene zu erweitern.
8. Wählen Sie erneut **Quelle festlegen**, **Ziel festlegen** oder beide Rollen für die unteren Ebenen von **Protokoll** und **Dokumentenfluss** für jede Dokumentenflussdefinition aus, die Ihr System unterstützt.

   Wenn eine Definition auf der Ebene **Dokumentenfluss** aktiviert ist, werden die Definitionen **Aktion** und **Aktivität**, sofern vorhanden, automatisch aktiviert.

9. Klicken Sie optional auf **Aktiviert** in der Spalte **Aktiviert**, um eine Dokumentenflussdefinition offline zu setzen. (Wenn Sie **Quelle festlegen** oder **Ziel festlegen** auswählen, ist der Eintrag automatisch aktiviert.) Klicken Sie auf **Inaktiviert**, um die Definition online zu setzen.

   Wenn ein Paket inaktiviert ist, sind alle Dokumentenflussdefinitionen der unteren Ebene im selben Knoten ebenfalls inaktiviert, ungeachtet dessen, ob sie individuell aktiviert waren. Wenn eine Dokumentenflussdefinition der unteren Ebene inaktiviert wird, bleiben alle Definitionen der höheren Ebenen im selben Kontext aktiviert. Wenn eine Dokumentenflussdefinition inaktiviert wird, funktionieren alle zuvor vorhandenen Verbindungen und Attribute weiterhin. Die inaktivierte Dokumentenflussdefinition schränkt lediglich die Erstellung neuer Verbindungen ein.
10. Klicken Sie optional auf das Symbol **Bearbeiten**, wenn Sie beliebige Attribute eines Protokolls, Pakets, Dokumentenflusses, einer Aktivität oder eines Signals bearbeiten wollen. Anschließend werden die Einstellungen für die Attribute angezeigt (sofern Attribute vorhanden sind). Sie können die Attribute modifizieren, indem Sie einen Wert eingeben oder einen Wert in der Spalte **Aktualisieren** auswählen und dann auf **Speichern** klicken.

Kapitel 12. Verbindungen verwalten

Nachdem Sie die B2B-Funktionalität von Teilnehmern erstellt haben, erstellen Sie Verbindungen zwischen Community Manager und Teilnehmern. Dieses Kapitel behandelt die folgenden Themen:

- „Übersicht"
- „Teilnehmerverbindungen aktivieren"
- „Attribute angeben oder ändern" auf Seite 166

Übersicht

Sie konfigurieren eine Verbindung zwischen Teilnehmern für jeden Dokumenttyp, der ausgetauscht wird. Sie könnten z. B. über mehrere Verbindungen von Community Manager zum selben Teilnehmer verfügen, da das Paket, das Protokoll, der Dokumentenfluss, die Aktion oder die Zuordnung möglicherweise verschieden sind.

Wenn Sie Verbindungen aktivieren, können Sie Attribute für den Quellen- oder Zielteilnehmer angeben. Jedes Attribut, das Sie auf der Verbindungsebene festgelegt haben, hat Vorrang vor Attributen, die Sie auf der B2B-Funktionalitätsebene für einen bestimmten Teilnehmer oder auf der Dokumentenflussdefinitions-Ebene festgelegt haben.

Sie verfügen bei EDI-, XML- und ROD-Dokumenten über mehrere Verbindungen für jeden Austausch, wenn der Austausch das Versehen mit einem Umschlag oder eine Transformation miteinbezieht. Sie können für diese Dokumenttypen noch weitere Verbindungen definieren, indem Sie von einer Gruppe mit Profilen auswählen, die der Verbindung zugeordnet sind. Weitere Details finden Sie in „Verbindungsprofile" auf Seite 115.

Teilnehmerverbindungen aktivieren

Teilnehmerverbindungen enthalten die Informationen, die für den ordnungsgemäßen Austausch jedes Dokumentenflusses nötig sind. Ein Dokument kann nicht weitergeleitet werden, es sei denn, es ist eine Verbindung zwischen Community Manager und einem seiner Teilnehmer vorhanden.

Das System erstellt automatisch Verbindungen zwischen Community Manager und Teilnehmern auf der Basis ihrer B2B-Funktionalität.

Sie suchen nach diesen Verbindungen und aktivieren diese dann.

Wenn Sie eine Quelle oder ein Ziel auswählen, beachten Sie die folgenden Richtlinien:

- Die Quelle und das Ziel müssen eindeutig sein.
- Mischen Sie kein Produktionsgateway mit einem Testgateway, wenn Sie Quelle und Ziel auswählen, ansonsten tritt ein Fehler auf.
- Sowohl die Quelle als auch das Ziel müssen Produktions- oder Testgateways sein.

Verwenden Sie die folgende Prozedur, um eine grundlegende Suche nach Verbindungen auszuführen und dann die Verbindungen zu aktivieren.

1. Klicken Sie auf **Kontenadmin > Teilnehmerverbindungen**. Die Seite **Verbindungen verwalten** wird angezeigt.
2. Wählen Sie unter **Quelle** eine Quelle aus. Wenn Sie z. B. einen Austausch konfigurieren, der von Community Manager stammt, wählen Sie **Community Manager** aus.
3. Wählen Sie unter **Ziel** ein Ziel aus. Wenn Sie z. B. einen Austausch konfigurieren, der von einem Teilnehmer empfangen wird, wählen Sie diesen Teilnehmer aus.

   Anmerkung: Wenn Sie eine neue Verbindung erstellen, müssen die Quelle und das Ziel eindeutig sein.
4. Klicken Sie auf **Suchen**, um die Verbindungen zu suchen, die mit Ihren Kriterien übereinstimmen.

   Anmerkung: Sie können auch die Seite **Erweiterte Suche** verwenden, wenn Sie detailliertere Suchkriterien eingeben wollen.
5. Klicken Sie auf **Aktivieren**, um eine Verbindung zu aktivieren. Die Seite **Verbindungen verwalten** wird erneut angezeigt, diesmal ist die Verbindung grün hervorgehoben. Diese Seite zeigt das Paket, das Protokoll und den Dokumentenfluss für die Quelle und das Ziel an. Sie stellt auch Schaltflächen bereit, auf die Sie klicken können, um den Status und die Parameter der Partnerverbindung anzuzeigen und zu ändern.
6. Informationen dazu, wie Sie Attribute für die Quelle oder das Ziel angeben, oder wie Sie ein Verbindungsprofil auswählen, finden Sie in „Attribute angeben oder ändern".

Aktivieren Sie bei einer Doppelaktions-PIP die Verbindung in beide Richtungen, um die zweite Aktion des PIP zu unterstützen. Um dies durchzuführen, definieren Sie die Quelle und das Ziel der zweiten Aktion als das Gegenüber der Quelle und des Ziels von der ersten Aktion.

Stellen Sie bei EDI-, XML- oder ROD-Dokumenten, für die Sie mehr als eine Interaktion definiert haben, sicher, dass Sie alle Verbindungen aktivieren, die den Interaktionen zugeordnet sind.

Attribute angeben oder ändern

Wenn Sie die Verbindung aktivieren, können Sie Attribute festlegen oder zuvor definierte Attribute ändern. Gehen Sie wie folgt vor, um die Attribute für diese Verbindung anzugeben oder zu ändern:

1. Klicken Sie auf **Attribute**, um die Attributwerte anzuzeigen oder zu ändern.

   Angenommen, dass Community Manager z. B. ein Dokument im Paket **None** an einen Teilnehmer sendet. Dann empfängt der Teilnehmer das Dokument in einem AS-Paket. Es ist möglich, dass Community Manager mehr als eine Geschäfts-ID zugeordnet ist. Gehen Sie wie folgt vor, um WebSphere Partner Gateway anzugeben, welche ID verwendet werden soll:

   a. Klicken Sie auf **Attribute** auf der Seite **Quelle** der Verbindung.
   b. Wenn die Seite **Verbindungsattribute** angezeigt wird, erweitern Sie den Ordner **None**.

c. Wählen Sie in der Liste **Aktualisieren** die AS-ID aus, die Sie dem Teilnehmer senden wollen.
d. Klicken Sie auf **Speichern**.

Anmerkung: Wenn Sie vorher eine AS-ID angegeben haben (z. B. auf der Seite **B2B-Funktionalität**), wird der hier eingegebene Wert den früheren Wert überschreiben.

Ein weiteres Beispiel für das Konfigurieren von Attributen ist, einen Wert für die MDN-Adresse einzugeben, wenn Sie von einem Teilnehmer Dokumente in AS-Paketen empfangen. Die Adresse gibt an, wohin die MDN zugestellt wird.

2. Klicken Sie auf **Aktionen**, wenn Sie eine Aktion oder eine Transformationszuordnung, die dieser Verbindung zugeordnet ist, anzeigen oder ändern wollen. Jeder Wert, den Sie hier ändern, überschreibt alle anderen Werte, die Sie für die Aktion oder Zuordnung festgelegt haben.
3. Klicken Sie auf **Gateways**, wenn Sie das Quellen- oder Zielgateway anzeigen oder ändern wollen.
4. Wenn die Schaltfläche **Verbindungsprofil hinzufügen** und die Liste **Aktive Profile** angezeigt werden, können Sie diese Verbindung einem bestimmten Profil zuordnen, das Sie vorher definiert haben.

Die Attribute, das Sie auf der Verbindungsebene festgelegt haben, haben Vorrang vor jeglichen Attributen, die Sie auf der Protokoll- oder auf der Dokumentenflussebene festgelegt haben.

Kapitel 13. Sicherheit für Eingangs- und Ausgangsaustauschvorgänge konfigurieren

Sie können mit WebSphere Partner Gateway mehrere Zertifikatstypen für Eingangs- und Ausgangstransaktionen installieren und verwenden. Dieses Kapitel behandelt die folgenden Themen:

- „Begriffe und Konzepte für Sicherheit"
- „SSL-Zertifikate erstellen und installieren" auf Seite 173
- „Unterschriftszertifikate erstellen und installieren" auf Seite 181
- „Verschlüsselungszertifikate erstellen und installieren" auf Seite 183
- „Eingangs-SSL für Konsole und Empfänger konfigurieren" auf Seite 186
- „Übersicht über Zertifikate" auf Seite 187

Begriffe und Konzepte für Sicherheit

Dieser Abschnitt bietet eine allgemeine Übersicht über die Sicherheitstypen, die zum Generieren und Hochladen von Zertifikaten verwendeten Tools und die Datensammlungstypen, die von WebSphere Partner Gateway installiert wurden.

In WebSphere Partner Gateway verwendete Sicherheitsmechanismen und Protokolle

Dieser Abschnitt stellt Informationen zu SSL, digitalen Unterschriften und Verschlüsselung bereit.

SSL

WebSphere Partner Gateway kann SSL verwenden, um eingehende und ausgehende Dokumente zu schützen. Ein eingehendes Dokument ist ein Dokument, das an den Hub gesendet wird. Ein ausgehendes Dokument ist ein Dokument, das vom Hub gesendet wird.

SSL ist ein häufig verwendetes Protokoll für das Verwalten der Sicherheit über das Internet. SSL bietet sichere Verbindungen, indem zwei Anwendungen, die über eine Netzverbindung miteinander verbunden sind, in die Lage versetzt werden, die Identität des anderen zu authentifizieren, und um die Vertraulichkeit der Daten und Datenintegrität sicherzustellen.

Eine HTTP-basierte SSL-Verbindung wird immer vom Client initiiert, der einen URL mit https:// am Anfang, anstelle von http:// am Anfang verwendet. Eine SSL-Verbindung beginnt mit einem Handshake. Während dieses Stadiums tauschen die Anwendungen digitale Zertifikate aus, sie verständigen sich über die zu verwendenden Verschlüsselungsalgorithmen und generieren Chiffrierschlüssel, die für den verbleibenden Teil der Sitzung verwendet werden.

Hinweise:

1. WebSphere Partner Gateway unterstützt die RC2- und TripleDES-Algorithmen. Der RC5-Algorithmus wird aber nicht unterstützt. Wenn Sie den RC5-Algorithmus in früheren Versionen verwendet haben, wechseln Sie zu einem der unterstützten Algorithmen.

2. WebSphere Partner Gateway unterstützt außerdem die AES- und DES-Algorithmen. Sie können diese Algorithmen in der Datei `bcg.properties` oder mit der SecurityService-API festlegen. Informationen zur Datei `bcg.properties` finden Sie im Handbuch *Verwaltung*. Weitere Informationen zu SecurityService finden Sie im Handbuch *Programmer Guide*.

Das SSL-Protokoll bietet die folgenden Sicherheitsfunktionen:

- Serverauthentifizierung. Dies bedeutet, dass der Server sein digitales Zertifikat verwendet, um sich bei Clients zu authentifizieren.
- Clientauthentifizierung. Dies ist ein optionaler Schritt, bei dem Clients sich möglicherweise beim Server authentifizieren müssen, indem sie ihre eigenen digitalen Zertifikate bereitstellen.

Digitale Unterschrift

Die digitale Unterzeichnung ist der Mechanismus, um die Unbestreitbarkeit sicherzustellen. Die Unbestreitbarkeit bedeutet, dass ein Teilnehmer nicht bestreiten kann, eine Nachricht verfasst und gesendet zu haben. Es wird ferner sichergestellt, dass der Teilnehmer den Empfang einer Nachricht nicht bestreiten kann.

Eine digitale Unterschrift ermöglicht dem Verfasser, eine Nachricht zu unterzeichnen, so dass der Verfasser als die Person bestätigt wird, die die Nachricht tatsächlich gesendet hat. Außerdem wird sichergestellt, dass die Nachricht seit ihrer Unterzeichnung nicht geändert worden ist.

WebSphere Partner Gateway unterstützt freigegebene PKCS#7 SignedData-Formate für die digitale Unterschrift gemäß den Geschäftsprotokollen.

Verschlüsselung

WebSphere Partner Gateway verwendet ein verschlüsseltes System, das als Verschlüsselung mit öffentlichem Schlüssel bekannt ist, um die Kommunikation zwischen Teilnehmern und dem Hub zu schützen. Die Verschlüsselung mit öffentlichem Schlüssel verwendet ein mathematisch zusammengehöriges Schlüsselpaar. Ein Dokument, das mit dem ersten Schlüssel verschlüsselt ist, muss mit dem zweiten Schlüssel entschlüsselt werden, und ein Dokument, das mit dem zweiten Schlüssel verschlüsselt ist, muss mit dem ersten Schlüssel entschlüsselt werden.

Jeder Teilnehmer an einem System mit öffentlichen Schlüsseln verfügt über ein Schlüsselpaar. Einer der Schlüssel wird geheim gehalten; dies ist der private Schlüssel. Der andere Schlüssel wird an jeden Interessierten verteilt; dies ist der öffentliche Schlüssel. WebSphere Partner Gateway verwendet den öffentlichen Schlüssel eines Teilnehmers, um ein Dokument zu verschlüsseln. Der private Schlüssel wird zum Entschlüsseln des Dokuments verwendet.

Das Dienstprogramm iKeyman

Wie in den nachfolgenden Abschnitten beschrieben, verwenden Sie IBM Key Management Tool (iKeyman), um Schlüsseldatenbanken, öffentliche und private Schlüsselpaare sowie Zertifikatsanforderungen zu erstellen. Sie können iKeyman auch verwenden, um selbst unterzeichnete Zertifikate zu erstellen. Das Dienstprogramm iKeyman befindet sich im Verzeichnis `/<Produktverz>/was/bin`, das WebSphere Partner Gateway während der Installation erstellt.

Sie können mit iKeyman auch eine Anforderung für ein Zertifikat von einer Zertifizierungsstelle (CA - Certifying Authority) generieren.

Community Console

Sie installieren mit Community Console alle erforderlichen Client-, Unterschrifts- und Verschlüsselungszertifikate für den WebSphere Partner Gateway-Speicher. Sie können mit Community Console auch die Zertifikate Root und Intermediate der Zertifizierungsstelle installieren.

Anmerkung: Wenn das Zertifikat eines Teilnehmers abläuft, liegt es im Zuständigkeitsbereich des Teilnehmers, sich ein neues Zertifikat zu besorgen. Die Alertfunktion von Community Console schließt Zertifikatsablaufalerts für Zertifikate mit ein, die in WebSphere Partner Gateway gespeichert sind.

Keystores und Truststores

Wenn Sie WebSphere Partner Gateway installieren, werden ein Keystore und ein Truststore für den Empfänger und die Konsole installiert.

- Ein Keystore ist eine Datei, die Ihre öffentlichen und privaten Schlüssel enthält.
- Ein Truststore ist eine Schlüsseldatei, die die öffentlichen Schlüssel für die selbst unterzeichneten Zertifikate und CA-Zertifikate Ihrer Teilnehmer enthält. Der öffentliche Schlüssel wird als ein Unterzeichnerzertifikat gespeichert. Bei kommerziellen Zertifizierungsstellen (CA) wird das CA-Rootzertifikat hinzugefügt. Die Truststore-Datei kann eine mehr der Öffentlichkeit zugängliche Schlüsseldatei sein, die alle vertrauenswürdigen Zertifikate enthält.

Standardmäßig werden die zwei Keystores und die zwei Truststores im Verzeichnis `<Produktverz>/common/security/keystore` erstellt. Sie heißen wie folgt:

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

Das Standardkennwort ändern

Das Standardkennwort für den Zugriff auf alle vier Speicher ist **WebAS**. Der eingebettete WebSphere Application Server wird so konfiguriert, dass er diese vier Speicher verwendet. Sie können mit dem Dienstprogramm iKeyman das Kennwort ändern. Alternativ hierzu können Sie auch den folgenden UNIX-Befehl verwenden, um das Kennwort der Keystore-Datei zu ändern:

```
/<Produktverz>/console/was/java/bin/keytool
 -storepasswd -new $NEW_PASSWORD$ -keystore $KEYSTORE_LOCATION$
 -storepass $CURRENT_PASSWORD$ -storetype JKS
```

Wenn die Keystore-Kennwörter geändert werden, muss jede WebSphere Application Server-Instanzkonfiguration ebenfalls geändert werden. Dies kann mit Hilfe des Scripts `bcgChgPassword.jacl` geschehen. Navigieren Sie für die Konsolinstanz zum folgenden Verzeichnis:

```
/<Produktverz>/bin
```

Setzen Sie den folgenden Befehl ab:

```
./bcgwsadmin.sh -f /<Produktverz>/scripts/
bcgChgPassword.jacl -conntype NONE
```

Wiederholen Sie diesen Befehl für die WebSphere Application Server-Instanzen des Empfängers und von Document Manager.

Anmerkung: Verwenden Sie für Windows-Installationen `bcgwsadmin.bat` anstelle von `./bcgwsadmin.sh`.

Sie werden aufgefordert, das neue Kennwort einzugeben.

Abgelaufenes Zertifikat ersetzen

Wenn ein Zertifikat in einem Truststore abgelaufen ist, müssen Sie, um es zu ersetzen, ein neues Zertifikat hinzufügen, indem Sie die folgende Prozedur verwenden:

1. Starten Sie iKeyman, falls es nicht bereits ausgeführt wird.
2. Öffnen Sie die Truststore-Datei.
3. Geben Sie das Kennwort ein, und klicken Sie auf **OK**.
4. Wählen Sie **Signer Certificates** aus dem Menü aus.
5. Klicken Sie auf **Add**.
6. Klicken Sie auf **Data type**, und wählen Sie einen Datentyp, wie z. B. Base64-verschlüsselte ASCII-Daten, aus.

   Dieser Datentyp muss mit dem Datentyp des importierenden Zertifikats übereinstimmen.
7. Geben Sie einen Zertifikatsdateinamen und seine Position für das digitale CA-Rootzertifikat ein, oder klicken Sie auf **Browse**, um den Namen und die Position auszuwählen.
8. Klicken Sie auf **OK**.
9. Geben Sie eine Bezeichnung für das importierende Zertifikat ein.
10. Klicken Sie auf **OK**.

Zertifikatketten

Eine Zertifikatkette besteht aus einem Zertifikat eines Teilnehmers und beliebigen Zertifikaten, die zur Authentifizierung des Zertifikats eines Teilnehmers verwendet werden. Wenn z. B. eine Zertifizierungsstelle (CA) verwendet wurde, um das Zertifikat eines Teilnehmers zu erstellen, könnte die Zertifizierungsstelle selbst von einer anderen Zertifizierungsstelle zertifiziert worden sein. Die Anerkennungskette beginnt bei der *Stamm*zertifizierungsstelle, dem Trust Anchor (Vertrauensanker). Das digitale Zertifikat der Stammzertifizierungsstelle ist selbst unterzeichnet, d. h. die Zertifizierungsstelle verwendet ihren eigenen privaten Schlüssel, um das digitale Zertifikat zu unterzeichnen. Alle Zertifikate zwischen dem Trust Anchor (Vertrauensanker) und dem Zertifikat des Teilnehmers (dem Zielzertifikat) sind *Intermediate*-Zertifikate.

Bei jedem von einer Zertifizierungsstelle ausgegebenem Zertifikat müssen alle Zertifikate in der Kette hinzugefügt werden. Es müssen z. B. in einer Zertifikatkette, in der A (der Vertrauensanker) der Ausgeber von B ist und B der Ausgeber von C (dem Zielzertifikat) ist, die Zertifikate A und B als Zertifikate der Zertifizierungsstelle hochgeladen werden.

WebSphere Partner Gateway behandelt alle selbst unterzeichneten Zertifikate als Vertrauensanker. Das selbst unterzeichnete Zertifikat kann von einer Zertifizierungsstelle ausgegeben sein oder es kann ein selbst unterzeichnetes Zertifikat sein, das von dem Teilnehmer generiert wurde.

Primäre und sekundäre Zertifikate

Sie können mehr als ein Zertifikat eines bestimmten Typs erstellen und eines zum primären Zertifikat und eines zum sekundären Zertifikat bestimmen. Wenn das primäre Zertifikat abgelaufen ist oder andernfalls nicht verwendet werden kann, wechselt WebSphere Partner Gateway zum sekundären Zertifikat. Sie geben in Community Console an, welches Zertifikat das primäre und welches das sekundäre ist.

Die Möglichkeit primäre und sekundäre Zertifikate bereitzustellen, ist für die folgenden Zertifikate verfügbar:

- Verschlüsselungszertifikat eines Teilnehmers
- Signaturzertifikat des Hub-Operators
- SSL-Clientzertifikat des Hub-Operators

Die Verschlüsselungsstufe ändern

Beachten Sie die folgenden wichtigen Einschränkungen bei der Verwendung von Verschlüsselungszertifikaten. Java Runtime Environment (JRE), die mit WebSphere Partner Gateway geliefert wird, erzwingt Einschränkungen bezüglich der Verschlüsselungsalgorithmen und maximal verschlüsselten Stufen, die zur Verwendung verfügbar sind. Eine eingeschränkte Richtlinie gibt z. B. Begrenzungen bei der zulässigen Länge und folglich die Stufe der Verschlüsselungsschlüssel an. Diese Einschränkungen werden in Dateien mit dem Namen *JRE-Standortrichtliniendateien* (Jurisdiction Policy Files) angegeben. Die maximal zulässige Länge ist 2048 Byte. Wenn Sie Zertifikate mit einer Schlüsselgröße von größer als 2048 Byte unterstützen wollen, verwenden Sie die uneingeschränkte bzw. nicht begrenzte Stufenversion der Standortrichtliniendateien. Sie können angeben, dass Sie eine stärkere, uneingeschränkte Richtlinie verwenden wollen, indem Sie neue Richtliniendateien in ein Unterverzeichnis der installierten JRE installieren. Es gibt außerdem Verschlüsselungseinschränkungen für symmetrische Schlüsselalgorithmen, wie z. B. DES3. Wenn Sie einen stärkeren symmetrischen Schlüsselalgorithmus benötigen, das Ersetzen der Standortrichtliniendateien entfernt auch die Einschränkungen für die symmetrischen Schlüssel.

Führen Sie die folgenden Schritte aus, um uneingeschränkte Standortrichtliniendateien in WebSphere Partner Gateway zu installieren:

1. Laden Sie die Standortrichtliniendateien mit uneingeschränkter Stufe über den Link **IBM SDK Policy files** von der folgenden Website herunter: http://www.ibm.com/developerworks/java/jdk/security/142/.
2. Dekomprimieren Sie die heruntergeladene Datei in einen temporären Ordner.
3. Kopieren Sie `local_policy.jar` und `US_export_policy.jar` von dem temporären Ordner.
4. Wechseln Sie in den Ordner `<Produktverz>\was\java\jre\lib\security`.
5. Benennen Sie die vorhandenen Dateien `local_policy.jar` und `US_export_policy.jar` in `local_policy.jar.bak` und `US_export_policy.jar.bak` um.
6. Fügen Sie die JAR-Dateien, die Sie in Schritt 3 kopiert haben, in den Ordner `<Produktverz>\was\java\jre\lib\security` ein.
7. Starten Sie den Server erneut.

Diese Schritte gelten für alle konfigurierten WebSphere Application Server-Instanzen.

SSL-Zertifikate erstellen und installieren

Die folgenden Abschnitte beschreiben, wie Sie SSL-Zertifikate zur Verwendung mit WebSphere Partner Gateway erstellen und installieren. Außerdem ist eine Übersicht des SSL-Handshake-Prozesses enthalten. Wenn Ihre Community SSL nicht verwendet, benötigen weder Sie noch Ihre Teilnehmer ein eingehendes oder ausgehendes SSL-Zertifikat.

SSL-Handshake

Jede SSL-Sitzung beginnt mit einem Handshake.

Wenn ein Client (der Teilnehmer oder Community Manager) einen Nachrichtenaustausch initiiert, treten folgende Schritte auf:

1. Der Client sendet eine Clientnachricht ″hello″, die die verschlüsselten Funktionen des Clients (sortiert in der vom Client bevorzugten Reihenfolge) auflistet, wie z. B. die Version von SSL, die vom Client unterstützten Cipher Suites und die vom Client unterstützten Datenkomprimierungsmethoden. Die Nachricht enthält außerdem eine 28-Byte-Zufallszahl.
2. Der Server antwortet mit einer Servernachricht ″hello done″ (erledigt), die die verschlüsselte Methode (Cipher Suite) und die vom Server ausgewählte Datenkomprimierungsmethode, die Sitzungs-ID und eine weitere Zufallszahl enthält.

   Anmerkung: Der Client und der Server müssen mindestens eine gemeinsame Cipher Suite unterstützen, ansonsten schlägt der Handshake fehl. Der Server wählt im Allgemeinen die stärkste gemeinsame Cipher Suite aus.
3. Der Server sendet sein digitales Zertifikat.

   Serverauthentifizierung geschieht in diesem Schritt.
4. Der Server sendet eine Nachricht ″digital certificate request″ (Anforderung für digitales Zertifikat). In der Nachricht ″digital certificate request″ sendet der Server eine Liste mit den unterstützten digitalen Zertifikattypen und die definierten Namen von akzeptablen Zertifizierungsstellen.
5. Der Server sendet eine Servernachricht ″hello done″ und wartet auf die Clientantwort.
6. Nach Empfang der Servernachricht ″hello done″ prüft der Client die Gültigkeit des digitalen Zertifikats vom Server und überprüft, ob die Serverparameter für ″hello″ akzeptabel sind.
7. Wenn der Server ein digitales Zertifikat vom Client angefordert hat, sendet der Client ein digitales Zertifikat oder falls kein passendes digitales Zertifikat verfügbar ist, sendet der Client einen Alert ″no digital certificate″ (kein digitales Zertifikat). Dieser Alert ist nur eine Warnung, aber die Serveranwendung kann in der Sitzung fehlschlagen, wenn die Clientauthentifizierung obligatorisch ist.
8. Der Client sendet eine Nachricht ″client key exchange″ (Clientschlüsselaustausch). Diese Nachricht enthält einen geheimen Pre-Master-Secret-Wert (Pre-Master Secret), eine 46-Byte-Zufallszahl, die bei der Generierung der symmetrischen Verschlüsselungsschlüssel und der MAC-Schlüssel (MAC - Message Authentication Code - Nachrichtenauthentifizierungscode) verwendet wird, welche mit dem öffentlichen Schlüssel des Servers verschlüsselt sind.
9. Wenn der Client ein digitales Zertifikat an den Server sendet, sendet der Client eine Nachricht ″digital certificate verify″ (digitales Zertifikat prüfen), die mit dem privaten Schlüssel des Clients unterzeichnet ist. Indem der Server die Unterschrift dieser Nachricht prüft, kann er explizit das Eigentumsrecht des digitalen Zertifikats vom Client prüfen.

   Anmerkung: Ein zusätzlicher Prozess, um das digitale Zertifikat vom Server zu prüfen, ist nicht notwendig. Wenn der Server nicht über den privaten Schlüssel verfügt, der zum digitalen Zertifikat gehört, kann er den Pre-Master Secret nicht entschlüsseln und die richtigen Schlüssel für den symmetrischen Verschlüsselungsalgorithmus nicht erstellen und der Handshake schlägt fehl.

10. Der Client verwendet eine Reihe von verschlüsselten Operationen, um den geheimen Pre-Master-Secret-Wert in einen geheimen Master-Secret-Wert zu konvertieren, von dem alles Schlüsselmaterial abgeleitet wird, das zur Verschlüsselung und Nachrichtenauthentifizierung erforderlich ist. Der Client sendet dann eine Nachricht ″change cipher spec″ (Verschlüsselungsspezifikation ändern), damit der Server zur neu festgelegten Cipher Suite wechselt. Die nächste vom Client gesendete Nachricht ″finished″ (fertig) ist die erste Nachricht, die mit dieser Verschlüsselungsmethode und den Verschlüsselungsschlüsseln verschlüsselt ist.
11. Der Server antwortet mit einer Nachricht ″change cipher spec″ und einer eigenen Nachricht ″finished″.

Die Clientauthentifizierung erfordert die Schritte 4 auf Seite 174, 7 auf Seite 174 und 9 auf Seite 174.

Der SSL-Handshake wird beendet und die verschlüsselten Anwendungsdaten können gesendet werden.

Eingehende SSL-Zertifikate

Dieser Abschnitt beschreibt, wie Sie die Serverauthentifizierung und die Clientauthentifizierung für eingehende Verbindungsanforderungen von Teilnehmern konfigurieren.

Serverauthentifizierung

WebSphere Application Server verwendet das SSL-Zertifikat, wenn er Verbindungsanforderungen von Teilnehmern über SSL empfängt. Es ist das Zertifikat, das der Empfänger präsentiert, um dem Teilnehmer den Hub anzugeben. Dieses Serverzertifikat kann selbst unterzeichnet oder von einer Zertifizierungsstelle (CA) unterzeichnet sein. In den meisten Fällen verwenden Sie ein CA-Zertifikat, um die Sicherheit zu erhöhen. Sie könnten ein selbst unterzeichnetes Zertifikat in einer Testumgebung verwenden. Verwenden Sie iKeyman, um ein Zertifikat und ein Schlüsselpaar zu generieren. Weitere Informationen entnehmen Sie der von IBM verfügbaren Dokumentation zur Verwendung von iKeyman.

Nachdem Sie das Zertifikat und das Schlüsselpaar generiert haben, verwenden Sie das Zertifikat für den eingehenden SSL-Datenverkehr aller Teilnehmer. Wenn Sie über mehrere Empfänger oder Konsolen verfügen, kopieren Sie den generierten Keystore auf jede Instanz. Wenn das Zertifikat selbst unterzeichnet ist, stellen Sie dieses Zertifikat den Teilnehmern zur Verfügung. Um dieses Zertifikat zu erhalten, extrahieren Sie mit iKeyman das öffentliche Zertifikat in eine Datei.

Selbst unterzeichnetes Zertifikat verwenden: Wenn Sie selbst unterzeichnete Serverzertifikate verwenden, führen Sie die folgende Prozedur aus.

1. Starten Sie das Dienstprogramm iKeyman, welches sich in `/<Produktverz>/was/bin` befindet. Wenn Sie iKeyman zum ersten Mal verwenden, löschen Sie das Zertifikat “dummy”, das sich im Keystore befindet.
2. Generieren Sie mit iKeyman ein selbst unterzeichnetes Zertifikat und ein Schlüsselpaar für den Keystore des Empfängers bzw. der Konsole.
3. Extrahieren Sie mit iKeyman das Zertifikat in eine Datei, das Ihren öffentlichen Schlüssel enthalten wird.

   Speichern Sie den Keystore in einer JKS-, PKCS12- oder JCEK-Datei.
4. Installieren Sie die Datei in den Keystore des Empfängers bzw. der Konsole, für den sie erstellt worden ist.

5. Verteilen Sie das Zertifikat an Ihre Teilnehmer. Die bevorzugte Verteilungsmethode ist das Senden des Zertifikats in einer kennwortgeschützten komprimierten Datei per E-Mail. Ihre Teilnehmer müssen sich an Sie wenden und das Kennwort für die komprimierte Datei anfordern.

Von Zertifizierungsstelle generiertes Zertifikat verwenden: Wenn Sie ein von einer Zertifizierungsstelle (CA) unterzeichnetes Zertifikat verwenden, führen Sie die folgende Prozedur aus.

1. Starten Sie das Dienstprogramm iKeyman, welches sich im Verzeichnis `/<Produktverz>/was/bin` befindet.
2. Generieren Sie mit iKeyman eine Zertifikatsanforderung und ein Schlüsselpaar für den Empfänger.
3. Übergeben Sie eine Zertifikatsunterzeichungsanforderung (CSR - Certificate Signing Request) an eine Zertifizierungsstelle.
4. Wenn Sie das unterzeichnete Zertifikat von der Zertifizierungsstelle empfangen, stellen Sie das unterzeichnete Zertifikat mit iKeyman in den Keystore.
5. Verteilen Sie das CA-Zertifikat an alle Teilnehmer.

Clientauthentifizierung

Wenn Sie Teilnehmer authentifizieren wollen, die Dokumente senden, führen Sie die Schritte in diesem Abschnitt aus.

Das Clientzertifikat installieren: Verwenden Sie für die Clientauthentifizierung die folgende Prozedur:

1. Rufen Sie das Zertifikat Ihres Teilnehmers ab.
2. Installieren Sie das Zertifikat bzw. die Zertifikate mit iKeyman in den Truststore.
3. Stellen Sie die zugehörige Zertifizierungsstelle bzw. die zugehörigen Zertifizierungsstellen in den zugehörigen Keystore.

Anmerkung: Wenn Sie mehrere Teilnehmer Ihrer Hub-Community hinzufügen, können Sie mit iKeyman ihre Zertifikate dem Truststore hinzufügen. Wenn ein Teilnehmer die Community verlässt, können Sie mit iKeyman die Zertifikate des Teilnehmers aus dem Truststore entfernen.

Clientauthentifizierung konfigurieren: Nachdem Sie das Zertifikat bzw. die Zertifikate installiert haben, konfigurieren Sie WebSphere Application Server für die Verwendung der Clientauthentifizierung, indem Sie das Dienstprogrammscript **bcgClientAuth.jacl** ausführen.

1. Navigieren Sie zum folgenden Verzeichnis: `/<Produktverz>/bin`
2. Zum Aktivieren der Clientauthentifizierung rufen Sie das Script wie folgt auf:

```
./bcgwsadmin.sh -f /<Produktverz>/scripts/bcgClientAuth.jacl
   -conntype NONE set
```

   Anmerkung: Zum Inaktivieren der Clientauthentifizierung rufen Sie das Script wie folgt auf:

```
./bcgwsadmin.sh -f /<Produktverz>/receiver/scripts/bcgClientAuth.jacl
  -conntype NONE clear
```

Sie müssen den Server `bcgreceiver` erneut starten, damit diese Änderungen wirksam werden.

Das Clientzertifikat prüfen: Es gibt eine Zusatzfunktion, die mit der SSL-Clientauthentifizierung verwendet werden kann. Diese Funktion wird über Community Console aktiviert. Für HTTPS überprüft WebSphere Partner Gateway Zertifikate

anhand der Geschäfts-IDs in den eingehenden Dokumenten. Zur Verwendung dieser Funktion erstellen Sie das Teilnehmerprofil, importieren das Clientzertifikat und markieren es als SSL.

1. Importieren Sie das Clientzertifikat.
   a. Klicken Sie auf **Kontenadmin > Profile > Community-Teilnehmer**, und suchen Sie nach dem Profil des Teilnehmers.
   b. Klicken Sie auf **Zertifikate**.
   c. Klicken Sie auf **Zertifikat laden**.
   d. Wählen Sie **SSL-Client** als Zertifikattyp aus.
   e. Geben Sie eine Beschreibung des Zertifikats ein, welches erforderlich ist.
   f. Ändern Sie den Status in **Aktiviert**.
   g. Klicken Sie auf **Durchsuchen**, und navigieren Sie zum Verzeichnis, in dem Sie das Zertifikat gespeichert haben.
   h. Wählen Sie das Zertifikat aus, und klicken Sie auf **Öffnen**.
   i. Wenn Sie einen anderen Gateway-Typ als **Produktion** (die Standardeinstellung) auswählen wollen, wählen Sie ihn in der Liste aus.
   j. Klicken Sie auf **Hochladen** und dann auf **Speichern**.
2. Aktualisieren Sie das Clientgateway.
   a. Klicken Sie auf **Kontenadmin > Profile > Community-Teilnehmer**, und suchen Sie nach dem Profil des Teilnehmers.
   b. Klicken Sie auf **Gateways**.
   c. Wählen Sie das HTTPS-Gateway aus, das Sie vorher erstellt haben. Wenn Sie das HTTPS-Gateway noch nicht erstellt haben, lesen Sie „HTTPS-Gateway konfigurieren" auf Seite 145.
   d. Klicken Sie auf das Symbol **Bearbeiten**, um das Gateway zu bearbeiten.
   e. Wählen Sie **Ja** für **Client-SSL-Zertifikat prüfen** aus.
   f. Klicken Sie auf **Speichern**.

Ausgehende SSL-Zertifikate

Wenn Ihre Community SSL nicht verwendet, benötigen Sie kein eingehendes oder ausgehendes SSL-Zertifikat.

Serverauthentifizierung

Wenn SSL zum Senden der ausgehenden Dokumente an Ihre Teilnehmer verwendet wird, fordert WebSphere Partner Gateway ein serverseitiges Zertifikat von den Teilnehmern an. Dasselbe CA-Zertifikat kann für mehrere Teilnehmer verwendet werden. Das Zertifikat muss in X.509-DER-Format sein.

Anmerkung: Sie können das Format mit dem Dienstprogramm iKeyman konvertieren. Befolgen Sie diese Schritte, um das Format zu konvertieren:

1. Starten Sie das Dienstprogramm iKeyman.
2. Erstellen Sie einen neuen leeren Keystore, oder öffnen Sie einen vorhandenen Keystore.
3. Wählen Sie in **Key Database Content** die Option **Signer Certificates** aus.
4. Fügen Sie das ARM-Zertifikat mit der Option **Add** hinzu.
5. Extrahieren Sie dasselbe Zertifikat als Binary-DER-Daten mit der Option **Extract**.
6. Schließen Sie das Dienstprogramm iKeyman.

Installieren Sie das selbst unterzeichnete Zertifikat des Teilnehmers in das Profil des Hub-Operators. Wenn das Zertifikat von einer Zertifizierungsstelle unterzeich-

net wurde und das Rootzertifikat der Zertifizierungsstelle und alle anderen Zertifikate, die Teil der Zertifikatkette sind, noch nicht im Profil des Hub-Operators installiert sind, installieren Sie die Zertifikate jetzt im Profil des Hub-Operators.

1. Klicken Sie auf **Zertifikate**.
2. Klicken Sie auf **Zertifikat laden**.
3. Wählen Sie **Root und Intermediate** als Zertifikattyp aus.
4. Geben Sie eine Beschreibung des Zertifikats ein, welches erforderlich ist.
5. Ändern Sie den Status in **Aktiviert**.
6. Klicken Sie auf **Durchsuchen**, und navigieren Sie zum Verzeichnis, in dem Sie das Zertifikat gespeichert haben.
7. Wählen Sie das Zertifikat aus, und klicken Sie auf **Öffnen**.
8. Klicken Sie auf **Hochladen** und dann auf **Speichern**.

Anmerkung: Sie müssen die vorherigen Schritte nicht ausführen, wenn das Zertifikat der Zertifizierungsstelle bereits installiert ist.

Clientauthentifizierung

Wenn SSL-Clientauthentifizierung erforderlich ist, wird der Teilnehmer seinerseits ein Zertifikat vom Hub anfordern. Importieren Sie mit Community Console Ihr Zertifikat in WebSphere Partner Gateway. Sie können das Zertifikat mit iKeyman generieren. Wenn das Zertifikat ein selbst unterzeichnetes Zertifikat ist, muss es dem Teilnehmer zur Verfügung gestellt werden. Wenn es ein CA-unterzeichnetes Zertifikat ist, muss das CA-Rootzertifikat den Teilnehmern gegeben werden, so dass sie es ihren vertrauenswürdigen Zertifikaten hinzufügen können.

Sie können über mehr als ein SSL-Zertifikat verfügen. Eines ist das primäre Zertifikat, welches standardmäßig verwendet wird. Das andere Zertifikat ist das sekundäre Zertifikat, welches verwendet wird, wenn das primäre Zertifikat abgelaufen ist oder andernfalls nicht verwendet werden kann.

Selbst unterzeichnetes Zertifikat verwenden: Wenn Sie ein selbst unterzeichnetes Zertifikat verwenden, führen Sie die folgende Prozedur aus.

1. Starten Sie das Dienstprogramm iKeyman.
2. Verwenden Sie iKeyman, um ein selbst unterzeichnetes Zertifikat und ein Schlüsselpaar zu generieren.
3. Extrahieren Sie mit iKeyman das Zertifikat in eine Datei, das Ihren öffentlichen Schlüssel enthalten wird.
4. Verteilen Sie das Zertifikat an Ihre Teilnehmer. Die bevorzugte Verteilungsmethode ist das Senden des Zertifikats in einer kennwortgeschützten komprimierten Datei per E-Mail. Ihre Teilnehmer müssen sich an Sie wenden und das Kennwort für die komprimierte Datei anfordern.
5. Verwenden Sie iKeyman, um das selbst unterzeichnete Zertifikat und das private Schlüsselpaar in Form einer PKCS12-Datei zu exportieren.
6. Installieren Sie das selbst unterzeichnete Zertifikat und den Schlüssel über Community Console.
   a. Klicken Sie auf **Kontenadmin > Profile > Zertifikate**, um die Seite **Zertifikatliste** anzuzeigen.

      Stellen Sie sicher, dass Sie an Community Console als Hub-Operator angemeldet sind.
   b. Klicken Sie auf **PKCS12 laden**.

Anmerkung: Die PKCS12-Datei, die hochgeladen wird, sollte nur einen privaten Schlüssel und das zugeordnete Zertifikat enthalten.

c. Wählen Sie **SSL-Client** als Zertifikattyp aus.
d. Geben Sie eine Beschreibung des Zertifikats ein, welches erforderlich ist.
e. Ändern Sie den Status in **Aktiviert**.
f. Klicken Sie auf **Durchsuchen**, und navigieren Sie zum Verzeichnis, in dem Sie das Zertifikat gespeichert haben.
g. Wählen Sie das Zertifikat aus, und klicken Sie auf **Öffnen**.
h. Geben Sie das Kennwort ein.
i. Wenn Sie einen anderen Gateway-Typ als **Produktion** (die Standardeinstellung) auswählen wollen, wählen Sie ihn in der Liste aus.
j. Wenn Sie über zwei SSL-Zertifikate verfügen, geben Sie an, welches von ihnen das primäre bzw. das sekundäre Zertifikat ist, indem Sie **Primär** oder **Sekundär** in der Liste **Zertifikatverwendung** auswählen.
k. Klicken Sie auf **Hochladen** und dann auf **Speichern**.

Wenn Sie primäre und sekundäre Zertifikate für die SSL-Clientauthentifizierung und die digitale Unterschrift hochladen, und Sie die primären Zertifikate als zwei separate Einträge hochladen, stellen Sie sicher, dass die entsprechenden sekundären Zertifikate als zwei unterschiedliche Einträge hochgeladen werden.

Von Zertifizierungsstelle unterzeichnetes Zertifikat verwenden: Wenn Sie ein von einer Zertifizierungsstelle unterzeichnetes Zertifikat verwenden, führen Sie die folgende Prozedur aus:

1. Generieren Sie mit iKeyman eine Zertifikatsanforderung und ein Schlüsselpaar für den Empfänger.
2. Übergeben Sie eine Zertifikatsunterzeichungsanforderung (CSR - Certificate Signing Request) an eine Zertifizierungsstelle.
3. Wenn Sie das unterzeichnete Zertifikat von der Zertifizierungsstelle empfangen, stellen Sie das unterzeichnete Zertifikat mit iKeyman in den Keystore.
4. Verteilen Sie das unterzeichnende CA-Zertifikat an alle Teilnehmer.

Zertifikatswiderrufsliste hinzufügen

WebSphere Partner Gateway enthält eine CRL-Funktion (CRL - Certificate Revocation List - Zertifikatswiderrufsliste). Die CRL, die von einer Zertifizierungsstelle herausgegeben wird, gibt Teilnehmer an, die Zertifikate vor ihrem terminierten Ablaufdatum widerrufen haben. Teilnehmern mit widerrufenen Zertifikaten wird der Zugriff auf WebSphere Partner Gateway verweigert. Jedes widerrufene Zertifikat wird in einer CRL durch seine fortlaufende Zertifikatsnummer angegeben. Document Manager durchsucht die CRL alle 60 Sekunden und lehnt ein Zertifikat ab, wenn es in der CRL-Liste enthalten ist.

CRLs werden an der folgenden Position gespeichert: `/<gemeinsames_datenverzeichnis>/security/crl`. WebSphere Partner Gateway verwendet die Einstellung `bcg.CRLDir` in der Datei `bcg.properties`, um die Position des CRL-Verzeichnisses anzugeben.

Erstellen Sie eine `.crl`-Datei, die die widerrufenen Zertifikate enthält, und stellen Sie diese in das CRL-Verzeichnis.

In der Datei `bcg.properties` würden Sie z. B. die folgende Einstellung verwenden:

```
bcg.CRLDir=/<gemeinsames_datenverzeichnis>/security/crl
```

Zugriff auf CRL-Verteilungspunkte aktivieren

Zertifizierungsstellen verwalten und aktualisieren die Zertifikatswiderrufslisten (CRLs). Diese Zertifikatswiderrufslisten werden normalerweise an einem CRL-Verteilungspunkt gespeichert. Zertifikatswiderrufslisten werden während der Widerrufsüberprüfungen für die Zertifikate verwendet, um zu ermitteln, ob das Zertifikat widerrufen wurde.

Das Script `bcgSetCRLDP.jacl` kann verwendet werden, um die CRL-Verteilungspunktüberprüfung zu aktivieren bzw. zu inaktivieren, wenn die Widerrufsüberprüfung ausgeführt wird. Falls Sie auf die CRL-Verteilungspunkte zugreifen müssen, wenn die Widerrufsüberprüfung eines Zertifikats ausgeführt wird, aktivieren Sie die Verwendung von CRL-Verteilungspunkten. Wenn die Zertifikate, die Sie installiert haben, eine CRL DP-Erweiterung enthalten, können Sie die Verwendung von CRL-Verteilungspunkten aktivieren, so dass auf die Verteilungspunkte zugegriffen wird, wenn die Widerrufsüberprüfung ausgeführt wird. Wenn Sie alle erforderlichen Zertifikatswiderrufslisten in das Verzeichnis heruntergeladen haben, das in `bcg.properties` für das Merkmal `bcg.CRLDir` festgelegt ist, wollen Sie unter Umständen die Verwendung von CRL-Verteilungspunkten nicht aktivieren. Falls die aktuellen Zertifikatswiderrufslisten sehr wahrscheinlich nicht im Verzeichnis `bcg.CRLDir` verfügbar sind, sollten Sie die Verwendung von CRL-Verteilungspunkten aktivieren.

Die CRL-Verteilungspunkte, auf die über HTTP und LDAP zugegriffen werden kann, werden unterstützt. Sie können auch Proxy-Server für den Zugriff auf die CRL-Verteilungspunkte konfigurieren.

Anmerkung: Verwenden Sie für Windows-Installationen `bcgwsadmin.bat` anstelle von `./bcgwsadmin.sh` in den Befehlen, die in diesem Abschnitt aufgelistet werden.

Führen Sie den folgenden Befehl vom Verzeichnis *<Produktverz>*`/bin` aus, um die Verwendung von CRL-Verteilungspunkten zu aktivieren:

```
./bcgwsadmin.sh -f <Produktverz>/scripts/bcgSetCRLDP.jacl install
 <knotenname> <servername> CRLDP
```

Dabei gilt Folgendes:

<serverstammverzeichnis>
: Das Stammverzeichnis des Servers, z. B. `/opt/ibm/receiver/was/profiles/bcgreceiver`.

<servername>
: Kann `bcgdocmgr`, `bcgreceiver` oder `bcgconsole` sein. Der Befehl muss vom entsprechenden *<serverstammverzeichnis>* ausgeführt werden.

Führen Sie den folgenden Befehl vom Verzeichnis *<Produktverz>*`/bin` aus, um die Verwendung von CRL-Verteilungspunkten zu inaktivieren:

```
./bcgwsadmin.sh -f <Produktverz>/scripts/bcgSetCRLDP.jacl uninstall
 <knotenname> <servername> CRLDP
```

Führen Sie den folgenden Befehl vom Verzeichnis *<Produktverz>*`/bin` aus, um die Verwendung von CRL-Verteilungspunkten mit einem Proxy-Server zu aktivieren:

```
./bcgwsadmin.sh -f <Produktverz>/scripts/bcgSetCRLDP.jacl install
 <knotenname> <servername> CRLDP <proxy-host> <proxy-port>
```

Führen Sie den folgenden Befehl vom Verzeichnis <*Produktverz*>/bin aus, um anzugeben, dass Sie keinen Proxy-Server verwenden wollen:

```
./bcgwsadmin.sh -f <Produktverz>/scripts/bcgSetCRLDP.jacl
 uninstall <knotenname> <servername> PROXY
```

Wenn Sie einen Empfängerbenutzerexit verwenden, und wenn der Benutzerexit die SecurityService-API verwendet, können die obigen Einstellungen auch auf den Server bcgreceiver angewendet werden. Zum Ausführen der obigen Befehle für den Empfänger, ersetzen Sie bcgdocmgr durch bcgreceiver.

Unterschriftszertifikate erstellen und installieren

Dieser Abschnitt beschreibt Unterschriftszertifikate, die für die Unbestreitbarkeit und für die Prüfung des Unterzeichners verwendet werden.

Eingehendes Unterschriftszertifikat

Document Manager verwendet das unterzeichnete Zertifikat des Teilnehmers, um die Unterschrift des Absenders zu prüfen, wenn Sie Dokumente empfangen. Die Teilnehmer senden ihre selbst unterzeichneten Unterschriftszertifikate in X.509-DER-Format an Sie. Sie installieren Ihrerseits die Zertifikate der Teilnehmer über Community Console in dem Profil des jeweiligen Teilnehmers.

Verwenden Sie die folgende Prozedur, um das Zertifikat zu installieren.

1. Empfangen Sie das X.509-Unterschriftszertifikat des Teilnehmers im DER-Format.
2. Installieren Sie das Zertifikat über Community Console im Profil des Teilnehmers.
   a. Klicken Sie auf **Kontenadmin > Profile > Community-Teilnehmer**, und suchen Sie nach dem Profil des Teilnehmers.
   b. Klicken Sie auf **Zertifikate**.
   c. Klicken Sie auf **Zertifikat laden**.
   d. Wählen Sie **Digitale Unterschrift** als Zertifikattyp aus.
   e. Geben Sie eine Beschreibung des Zertifikats ein, welches erforderlich ist.
   f. Ändern Sie den Status in **Aktiviert**.
   g. Klicken Sie auf **Durchsuchen**, und navigieren Sie zum Verzeichnis, in dem Sie das Zertifikat gespeichert haben.
   h. Wählen Sie das Zertifikat aus, und klicken Sie auf **Öffnen**.
   i. Klicken Sie auf **Hochladen** und dann auf **Speichern**.
3. Wenn das Zertifikat von einer Zertifizierungsstelle unterzeichnet wurde und das Rootzertifikat der Zertifizierungsstelle und alle anderen Zertifikate, die Teil der Zertifikatkette sind, noch nicht im Profil des Hub-Operators installiert sind, installieren Sie die Zertifikate jetzt.
   a. Klicken Sie auf **Kontenadmin > Profile > Zertifikate**, um die Seite **Zertifikatliste** anzuzeigen.

      Stellen Sie sicher, dass Sie an Community Console als Hub-Operator angemeldet sind, und installieren Sie das Zertifikat in Ihrem eigenen Profil.
   b. Klicken Sie auf **Zertifikat laden**.
   c. Wählen Sie **Root und Intermediate** aus.
   d. Geben Sie eine Beschreibung des Zertifikats ein, welches erforderlich ist.
   e. Ändern Sie den Status in **Aktiviert**.

f. Klicken Sie auf **Durchsuchen**, und navigieren Sie zum Verzeichnis, in dem Sie das Zertifikat gespeichert haben.

g. Wählen Sie das Zertifikat aus, und klicken Sie auf **Öffnen**.

h. Klicken Sie auf **Hochladen** und dann auf **Speichern**.

Anmerkung: Sie müssen den vorherigen Schritt nicht ausführen, wenn das CA-Zertifikat bereits installiert ist.

4. Aktivieren Sie das Unterzeichnen auf der Ebene für Pakete (höchste Ebene), Teilnehmer oder Verbindungen (unterste Ebene). Ihre Einstellung kann andere Einstellungen auf der Verbindungsebene überschreiben. Die Verbindungszusammenfassung informiert Sie darüber, ob ein erforderliches Attribut fehlt.

   Zum Ändern der Attribute von z. B. einer Teilnehmerverbindung klicken Sie auf **Kontenadmin > Teilnehmerverbindungen**, und wählen Sie dann die Teilnehmer aus. Klicken Sie auf **Attribute**, und bearbeiten Sie dann das Attribut. Beispiel: **AS unterzeichnet**.

Ausgehendes Unterschriftszertifikat

Document Manager verwendet dieses Zertifikat, wenn er ausgehende, unterzeichnete Dokumente an Teilnehmer sendet. Dasselbe Zertifikat und derselbe Schlüssel werden für alle Ports und Protokolle verwendet.

Sie können über mehr als ein Zertifikat für digitale Unterschrift verfügen. Eines ist das primäre Zertifikat, welches standardmäßig verwendet wird. Das andere Zertifikat ist das sekundäre Zertifikat, welches verwendet wird, wenn das primäre Zertifikat abgelaufen ist oder andernfalls nicht verwendet werden kann.

Selbst unterzeichnetes Zertifikat verwenden

Wenn Sie ein selbst unterzeichnetes Zertifikat verwenden, führen Sie die folgende Prozedur aus.

1. Starten Sie das Dienstprogramm iKeyman.
2. Verwenden Sie iKeyman, um ein selbst unterzeichnetes Zertifikat und ein Schlüsselpaar zu generieren.
3. Extrahieren Sie mit iKeyman das Zertifikat in eine Datei, das Ihren öffentlichen Schlüssel enthalten wird.
4. Verteilen Sie das Zertifikat an Ihre Teilnehmer. Die bevorzugte Verteilungsmethode ist das Senden des Zertifikats in einer kennwortgeschützten komprimierten Datei per E-Mail. Ihre Teilnehmer müssen sich an Sie wenden und das Kennwort für die komprimierte Datei anfordern.
5. Verwenden Sie iKeyman, um das selbst unterzeichnete Zertifikat und das private Schlüsselpaar in Form einer PKCS12-Datei zu exportieren.
6. Installieren Sie das selbst unterzeichnete Zertifikat und das private Schlüsselpaar in Form einer PKCS12-Datei über Community Console.
   a. Klicken Sie auf **Kontenadmin > Profile > Zertifikate**, um die Seite **Zertifikatliste** anzuzeigen.

      Stellen Sie sicher, dass Sie an Community Console als Hub-Operator angemeldet sind.

   b. Klicken Sie auf **PKCS12 laden**.

      Hinweise:

      1) Die PKCS12-Datei, die hochgeladen wird, sollte nur einen privaten Schlüssel und das zugeordnete Zertifikat enthalten.

2) Sie können das Zertifikat und den privaten Schlüssel auch als ein DER-verschlüsseltes Zertifikat und einen PKCS#8-codierten privaten Schlüssel hochladen.

c. Wählen Sie **Digitale Unterschrift** als Zertifikattyp aus.

d. Geben Sie eine Beschreibung des Zertifikats ein, welches erforderlich ist.

e. Ändern Sie den Status in **Aktiviert**.

f. Klicken Sie auf **Durchsuchen**, und navigieren Sie zum Verzeichnis, in dem Sie das Zertifikat gespeichert haben.

g. Wählen Sie das Zertifikat aus, und klicken Sie auf **Öffnen**.

h. Geben Sie ein Kennwort ein.

i. Wenn Sie über zwei Zertifikate für digitale Unterschrift verfügen, geben Sie an, welches von ihnen das primäre bzw. das sekundäre Zertifikat ist, indem Sie **Primär** oder **Sekundär** in der Liste **Zertifikatverwendung** auswählen.

j. Klicken Sie auf **Hochladen** und dann auf **Speichern**.

7. Wiederholen Sie Schritt 6 auf Seite 182, wenn der Teilnehmer über ein zweites Unterschriftszertifikat verfügt.

Wenn Sie primäre und sekundäre Zertifikate für die SSL-Clientauthentifizierung und die digitale Unterschrift hochladen, und Sie die primären Zertifikate als zwei separate Einträge hochladen, stellen Sie sicher, dass die entsprechenden sekundären Zertifikate als zwei unterschiedliche Einträge hochgeladen werden.

Von Zertifizierungsstelle unterzeichnetes Zertifikat verwenden

Wenn Sie ein von einer Zertifizierungsstelle unterzeichnetes Zertifikat verwenden, führen Sie die folgende Prozedur aus:

1. Starten Sie das Dienstprogramm iKeyman.
2. Generieren Sie mit iKeyman eine Zertifikatsanforderung und ein Schlüsselpaar für den Empfänger.
3. Übergeben Sie eine Zertifikatsunterzeichungsanforderung (CSR - Certificate Signing Request) an eine Zertifizierungsstelle.
4. Wenn Sie das unterzeichnete Zertifikat von der Zertifizierungsstelle empfangen, stellen Sie das unterzeichnete Zertifikat mit iKeyman in den Keystore.
5. Verteilen Sie das unterzeichnende CA-Zertifikat an alle Teilnehmer.

Verschlüsselungszertifikate erstellen und installieren

Dieser Abschnitt beschreibt Verschlüsselungszertifikate.

Eingehendes Verschlüsselungszertifikat

Dieses Zertifikat wird vom Hub verwendet, um verschlüsselte Dateien zu entschlüsseln, die von Teilnehmern empfangen wurden. Der Hub verwendet Ihren privaten Schlüssel, um die Dokumente zu entschlüsseln. Die Verschlüsselung wird verwendet, um zu verhindern, dass Dritte neben dem Absender und dem beabsichtigten Empfänger Transitdokumente anzeigen können.

Beachten Sie, dass die folgende wichtige Einschränkung beim Empfangen von verschlüsselten AS2-Nachrichten von Teilnehmern. Wenn ein Teilnehmer eine verschlüsselte AS2-Nachricht sendet, aber das falsche Zertifikat verwendet, schlägt die Entschlüsselung fehl. Es wird jedoch keine MDN an den Teilnehmer zurückgegeben, um den Fehler anzugeben. Damit Ihr Teilnehmer in dieser Situation MDNs empfängt, erstellen Sie eine Verbindung zum Teilnehmer mit der folgenden Dokumentenflussdefinition:

- Paket: **AS**
- Protokoll: **Binary**
- Dokumentenfluss: **Binary**

Selbst unterzeichnetes Zertifikat verwenden

Wenn Sie ein selbst unterzeichnetes Zertifikat verwenden, führen Sie die folgende Prozedur aus.

1. Starten Sie das Dienstprogramm iKeyman.
2. Verwenden Sie iKeyman, um ein selbst unterzeichnetes Zertifikat und ein Schlüsselpaar zu generieren.
3. Extrahieren Sie mit iKeyman das Zertifikat in eine Datei, das Ihren öffentlichen Schlüssel enthalten wird.
4. Verteilen Sie das Zertifikat an Ihre Teilnehmer. Sie müssen die Datei in ihr B2B-Produkt importieren, um diese als Verschlüsselungszertifikat zu verwenden. Geben Sie ihnen den Rat, es zu verwenden, wenn sie verschlüsselte Dateien an Community Manager senden wollen. Wenn Ihr Zertifikat CA-unterzeichnet ist, stellen Sie das CA-Zertifikat ebenfalls zur Verfügung.
5. Verwenden Sie iKeyman, um das selbst unterzeichnete Zertifikat und das private Schlüsselpaar in Form einer PKCS12-Datei zu speichern.
6. Installieren Sie das selbst unterzeichnete Zertifikat und das private Schlüsselpaar in Form einer PKCS12-Datei über Community Console.
   a. Klicken Sie auf **Kontenadmin > Profile > Zertifikate**, um die Seite **Zertifikatliste** anzuzeigen.

      Stellen Sie sicher, dass Sie an Community Console als Hub-Operator angemeldet sind.
   b. Klicken Sie auf **PKCS12 laden**.

      Hinweise:

      1) Die PKCS12-Datei, die hochgeladen wird, sollte nur einen privaten Schlüssel und das zugeordnete Zertifikat enthalten.
      2) Sie können das Zertifikat und den privaten Schlüssel auch als ein DER-verschlüsseltes Zertifikat und einen PKCS#8-codierten privaten Schlüssel hochladen.
   c. Wählen Sie **Verschlüsselung** als Zertifikattyp aus.
   d. Geben Sie eine Beschreibung des Zertifikats ein, welches erforderlich ist.
   e. Ändern Sie den Status in **Aktiviert**.
   f. Klicken Sie auf **Durchsuchen**, und navigieren Sie zum Verzeichnis, in dem Sie das Zertifikat gespeichert haben.
   g. Wählen Sie das Zertifikat aus, und klicken Sie auf **Öffnen**.
   h. Geben Sie ein Kennwort ein.
   i. Klicken Sie auf **Hochladen** und dann auf **Speichern**.
7. Aktivieren Sie die Verschlüsselung auf der Ebene für Pakete (höchste Ebene), Teilnehmer oder Verbindungen (unterste Ebene). Ihre Einstellung kann andere Einstellungen auf der Verbindungsebene überschreiben. Die Verbindungszusammenfassung informiert Sie darüber, ob ein erforderliches Attribut fehlt.

   Zum Ändern der Attribute von z. B. einer Teilnehmerverbindung klicken Sie auf **Kontenadmin > Teilnehmerverbindungen**, und wählen Sie dann die Teilnehmer aus. Klicken Sie auf **Attribute**, und bearbeiten Sie dann das Attribut. Beispiel: **AS verschlüsselt**.

Von Zertifizierungsstelle signiertes Zertifikat verwenden

Wenn Sie ein von einer Zertifizierungsstelle unterzeichnetes Zertifikat verwenden, führen Sie die folgende Prozedur aus:

1. Starten Sie das Dienstprogramm iKeyman.
2. Generieren Sie mit iKeyman eine Zertifikatsanforderung und ein Schlüsselpaar für den Empfänger.
3. Übergeben Sie eine Zertifikatsunterzeichungsanforderung (CSR - Certificate Signing Request) an eine Zertifizierungsstelle.
4. Wenn Sie das unterzeichnete Zertifikat von der Zertifizierungsstelle empfangen, stellen Sie das unterzeichnete Zertifikat mit iKeyman in den Keystore.
5. Verteilen Sie das unterzeichnende CA-Zertifikat an alle Teilnehmer.

Ausgehendes Verschlüsselungszertifikat

Das ausgehende Verschlüsselungszertifikat wird verwendet, wenn der Hub verschlüsselte Dokumente an Teilnehmer sendet. WebSphere Partner Gateway verschlüsselt Dokumente mit den öffentlichen Schlüsseln der Teilnehmer und die Teilnehmer entschlüsseln die Dokumente mit ihren privaten Schlüsseln.

Der Teilnehmer kann mehr als ein Verschlüsselungszertifikat haben. Eines ist das primäre Zertifikat, welches standardmäßig verwendet wird. Das andere Zertifikat ist das sekundäre Zertifikat, welches verwendet wird, wenn das primäre Zertifikat abgelaufen ist oder andernfalls nicht verwendet werden kann.

1. Rufen Sie das Verschlüsselungszertifikat des Teilnehmers ab. Das Zertifikat muss in X.509-DER-Format sein. Beachten Sie, dass WebSphere Partner Gateway nur X5.09-Zertifikate unterstützt.
2. Installieren Sie das Zertifikat über Community Console im Profil des Teilnehmers.
   a. Klicken Sie auf **Kontenadmin > Profile > Community-Teilnehmer**, und suchen Sie nach dem Profil des Teilnehmers.
   b. Klicken Sie auf **Zertifikate**.
   c. Klicken Sie auf **Zertifikat laden**.
   d. Wählen Sie **Verschlüsselung** als Zertifikattyp aus.
   e. Geben Sie eine Beschreibung des Zertifikats ein, welches erforderlich ist.
   f. Ändern Sie den Status in **Aktiviert**.
   g. Klicken Sie auf **Durchsuchen**, und navigieren Sie zum Verzeichnis, in dem Sie das Zertifikat gespeichert haben.
   h. Wählen Sie das Zertifikat aus, und klicken Sie auf **Öffnen**.
   i. Wenn der Teilnehmer über zwei Verschlüsselungszertifikate verfügt, geben Sie an, welches von ihnen das primäre bzw. das sekundäre Zertifikat ist, indem Sie **Primär** oder **Sekundär** in der Liste **Zertifikatverwendung** auswählen.
   j. Klicken Sie auf **Hochladen** und dann auf **Speichern**.
3. Wiederholen Sie Schritt 2, wenn der Teilnehmer über ein zweites Verschlüsselungszertifikat verfügt.
4. Wenn das Zertifikat von einer Zertifizierungsstelle unterzeichnet wurde und das Rootzertifikat der Zertifizierungsstelle und alle anderen Zertifikate, die Teil der Zertifikatkette sind, noch nicht im Profil des Hub-Operators installiert sind, installieren Sie die Zertifikate jetzt.
   a. Klicken Sie auf **Kontenadmin > Profile > Zertifikate**, um die Seite **Zertifikatliste** anzuzeigen.

Stellen Sie sicher, dass Sie an Community Console als Hub-Operator angemeldet sind, und installieren Sie das Zertifikat in Ihrem eigenen Profil.

b. Klicken Sie auf **Zertifikat laden**.
c. Wählen Sie **Root und Intermediate** aus.
d. Geben Sie eine Beschreibung des Zertifikats ein, welches erforderlich ist.
e. Ändern Sie den Status in **Aktiviert**.
f. Klicken Sie auf **Durchsuchen**, und navigieren Sie zum Verzeichnis, in dem Sie das Zertifikat gespeichert haben.
g. Wählen Sie das Zertifikat aus, und klicken Sie auf **Öffnen**.
h. Klicken Sie auf **Hochladen** und dann auf **Speichern**.

Anmerkung: Sie müssen den vorherigen Schritt nicht ausführen, wenn das CA-Zertifikat bereits installiert ist.

5. Aktivieren Sie die Verschlüsselung auf der Ebene für Pakete (höchste Ebene), Teilnehmer oder Verbindungen (unterste Ebene). Ihre Einstellung kann andere Einstellungen auf der Verbindungsebene überschreiben. Die Verbindungszusammenfassung informiert Sie darüber, ob ein erforderliches Attribut fehlt.

   Zum Ändern der Attribute von z. B. einer Teilnehmerverbindung klicken Sie auf **Kontenadmin > Teilnehmerverbindungen**, und wählen Sie dann die Teilnehmer aus. Klicken Sie auf **Attribute**, und bearbeiten Sie dann das Attribut. Beispiel: **AS verschlüsselt**.

Wenn die Fehlernachricht `No valid encryption certificate found` (Kein gültiges Verschlüsselungszertifikat wurde gefunden) angezeigt wird, ist weder das primäre noch das sekundäre Zertifikat gültig. Die Zertifikate sind unter Umständen abgelaufen oder sie wurden widerrufen. Wenn die Zertifikate abgelaufen sind oder widerrufen wurden, ist das entsprechende Ereignis (`Certificate revoked or expired`) auch in der Ereignisanzeige sichtbar. Beachten Sie, dass diese zwei Ereignisse möglicherweise durch andere Ereignisse getrennt wurden. Klicken Sie auf **Anzeigen > Ereignisanzeige**, um die Ereignisanzeige anzuzeigen.

Eingangs-SSL für Konsole und Empfänger konfigurieren

Die WebSphere Partner Gateway-Keystores sind in WebSphere Application Server vorkonfiguriert. Dieser Abschnitt gilt nur, wenn Sie verschiedene Keystores verwenden.

Verwenden Sie die folgende Prozedur, um SSL für die Konsole und den Empfänger in WebSphere Partner Gateway zu konfigurieren.

1. Rufen Sie die folgenden Informationen ab.
   - Die vollständigen Pfadnamen der Schlüsseldatei und der Anerkennungsdatei für z. B. den Empfänger:
     <Produktverz>/common/security/keystore/receiver.jks und
     <Produktverz>/common/security/keystore/receiverTrust.jks

     Sie müssen diese Namen korrekt eingeben. In der UNIX-Umgebung muss bei diesen Namen die Groß-/Kleinschreibung beachtet werden.
   - Die neuen Kennwörter für jede Datei.
   - Das Format jeder Datei. Dieses muss aus einem der folgenden Werte ausgewählt werden: JKS, JCEK oder PKCS12. Geben Sie diesen Wert in Großbuchstaben genau wie angezeigt ein.
   - Der Pfad zur Scriptdatei namens `bcgssl.jacl`.

2. Öffnen Sie ein Community Console-Fenster, und wechseln Sie in das Verzeichnis /<*Produktverz*>/bin. Der Server muss zum Ändern der Kennwörter nicht aktiv sein.
3. Geben Sie den folgenden Befehl ein, und ersetzen Sie die Werte, die in <> eingeschlossen sind. Alle Werte müssen eingegeben werden.

```
./bcgwsadmin.sh -f /<Produktverz>/
scripts/bcgssl.jacl -conntype NONE install
<schlüsseldatei_pfadname>
<schlüsseldatei_kennwort> <schlüsseldatei_format> <trust-datei_pfadname>
<trust-dateikennwort> <trust-dateiformat>
```

4. Starten Sie den Server. Wenn der Start des Servers fehlschlägt, könnte es an einem Fehler bei der Ausführung von bcgssl.jacl liegen. Wenn Sie einen Fehler machen, können Sie das Script erneut ausführen, um ihn zu beheben.
5. Wenn Sie bcgClientAuth.jacl verwendet haben, um das SSL-Merkmal **clientAuthentication** zu konfigurieren, setzen Sie es nach Verwendung von bcgssl.jacl zurück. Dies liegt daran, dass bcgssl.jacl jeden Wert, der für **clientAuthentication** gesetzt worden ist, mit dem Wert **false** überschreibt.

Anmerkung: Wiederholen Sie diese Schritte für die Konsole, und ersetzen Sie **receiver** durch **console** im Pfadnamen.

Übersicht über Zertifikate

Tabelle 18 fasst die Art und Weise zusammen, wie Zertifikate in WebSphere Partner Gateway verwendet werden. Zertifikatspositionen werden in runden Klammern "( )" angezeigt.

Tabelle 18. Übersichtsdaten zu Zertifikaten

Nachrichten-übermittlung-smethode (siehe Hinweis 1)	Hub-Operator-zertifikat	Zertifikat und Zertifizierungs-stelle vom Teil-nehmer erhalten	Zertifizierungs-stelle (siehe Hinweis 2)	Teilnehmer ein Zertifikat geben (siehe Hinweis 3)	Kommentare
Eingangs-SSL	Auf WebSphere Application Ser-ver-seitigem SSL installieren. (In den WebSphere Application Ser-ver-Keystore stel-len.)	N/V	Wird nur benö-tigt, wenn die Clientauthenti-fizierung verwendet wird. (Zertifizierungs-stelle oder selbst unterzeichnetes Zertifikat in den WebSphere Application Ser-ver-Truststore stellen.)	Hub-Operator-zertifikat, falls selbst unterzeich-net, oder das CA-Rootzertifikat, falls es von der Zertifizierungs-stelle authen-tifiziert ist.	
Ausgangs-SSL	Wenn die Clientauthentifi-zierung verwen-det wird. (WebSphere Part-ner Gateway)	Teilnehmerserver-seitiges Zertifikat oder CA-Rootzertifikat, falls es von der Zertifizierungs-stelle authenti-fiziert ist.	WebSphere Part-ner Gateway	Hub-Operator-zertifikat, falls selbst unterzeich-net, oder öffentli-cher Schlüssel, falls es von einem Dritthersteller unterzeichnet ist.	
Eingangs-verschlüsselung	Privater Schlüssel (WebSphere Part-ner Gateway)	N/V	N/V	Hub-Operator-zertifikat	Für Entschlüsse-lung der Nach-richt

Tabelle 18. Übersichtsdaten zu Zertifikaten (Forts.)

Nachrichten-übermittlungs-methode (siehe Hinweis 1)	Hub-Operator-zertifikat	Zertifikat und Zertifizierungs-stelle vom Teil-nehmer erhalten	Zertifizierungs-stelle (siehe Hinweis 2)	Teilnehmer ein Zertifikat geben (siehe Hinweis 3)	Kommentare
Eingangsunter-schrift	N/V	Zertifikat zum Prüfen des Zertifikats, das für die digitale Unterschrift verwendet wird. (WebSphere Partner Gateway)	WebSphere Partner Gateway	N/V	Für Prüfung und Unbestreitbarkeit
Ausgangs-verschlüsselung	N/V	Das Zertifikat verwenden, das vom Teilnehmer erhalten wurde. (Zertifikat ist im Profil des Teilnehmers installiert.)	Zertifizierungs-stelle für Clientzertifikat, falls nicht selbst unterzeichnet.	N/V	Für Verschlüsselung von ausgehenden Nachrichten
Ausgangsunter-schrift	Privater Schlüssel (WebSphere Partner Gateway)	N/V	N/V	Optional, hängt vom Partner ab; WebSphere Partner Gateway öffentlichen Schlüssel geben.	
Zertifikat für DUNS-Prüfung	N/V	In Teilnehmer-profil laden.	Dasselbe Zertifikat (wie das in der linken Spalte) in das Hub-Operatorprofil als das CA-Zertifikat laden.		Prüft, ob dieses Zertifikat für diese DUNS-ID ist, wenn die SSL-Überprüfung fertig ist.

Hinweise:

1. Eine eingehende Nachricht ist eine Nachricht, die in WebSphere Partner Gateway von einem Teilnehmer eingeht. Eine ausgehende Nachricht ist eine Nachricht, die von WebSphere Partner Gateway zu einem Teilnehmer ausgeht.
2. Wenn das Zertifikat von einer Zertifizierungsstelle ausgegeben ist, muss die ausgebende Zertifizierungsstelle abgerufen und gespeichert werden. Dies gilt für das Hub-Operatorzertifikat oder das Zertifikat des Teilnehmers.
3. Wenn ein privater Schlüssel mit einbezogen wird, entspricht dieses Zertifikat dem privaten Schlüssel.

Kapitel 14. Die Konfiguration fertig stellen

Dieses Kapitel beschreibt zusätzliche Aufgaben, die Sie ausführen können, um den Hub zu konfigurieren. Es behandelt die folgenden Themen:

- „Die Verwendung von APIs aktivieren"
- „Die für Ereignisse verwendeten Warteschlangen angeben"
- „Alertfähige Ereignisse angeben" auf Seite 191
- „Benutzerdefinierten Transport aktualisieren" auf Seite 191

Die Verwendung von APIs aktivieren

WebSphere Partner Gateway stellt eine Gruppe von APIs bereit, mit denen auf bestimmte Funktionen zugegriffen werden kann, die üblicherweise in Community Console ausgeführt werden. Diese APIs werden im Handbuch *Programmer Guide* beschrieben.

Verwenden Sie diese Prozedur, um die Verwendung der XML-basierten APIs zu aktivieren, so dass Teilnehmer API-Aufrufe auf dem WebSphere Partner Gateway-Server durchführen können:

1. Klicken Sie im Hauptmenü auf **Systemverwaltung > Funktionsverwaltung > Administrations-API**.
2. Klicken Sie auf das Symbol **Bearbeiten** neben **Die XML-basierte API aktivieren**.
3. Wählen Sie das Markierungsfeld aus, um die Verwendung der XML-basierten API zu aktivieren.
4. Klicken Sie auf **Speichern**.

Die für Ereignisse verwendeten Warteschlangen angeben

Sie können den Hub konfigurieren, um einer externen Warteschlange Ereignisse zuzustellen, die unter Verwendung der JMS-Konfiguration konfiguriert wurde.

Die Standard-JMS-Konfiguration wird eingerichtet, wenn Sie den Hub installieren. Sie können einige dieser Werte auf der Seite **Merkmale für Ereignisveröffentlichung** sehen. Wenn Sie keinen Wert in den Feldern **Provider-URL-Pakete** oder **JMS-Provider-URL** bereitstellen, werden die Standardwerte verwendet, die sich im Abschnitt für MQ-Merkmale der Datei `bcg.properties` befinden. Diese Standardwerte verwenden die JMS-Bindungen, die während der Installation generiert wurden. Wenn Sie die Standardwerte nehmen, verwenden die JMS-Bindungen Port 9999 auf dem MQ-Server, den Sie während der Installation benannt haben.

Um auf eine andere Gruppe von JMS-Bindungen zu zeigen, ändern Sie **Provider-URL-Pakete** so, dass auf ein Verzeichnis gezeigt wird, in dem eine JMS-Bindungsdatei enthalten ist, die Sie selbst vorbereitet haben. Ändern Sie auch den Namen für die **Warteschlangenverbindungsfactory** und den **Namen der Warteschlange** so, dass sie mit den Namen übereinstimmen, die Sie in Ihren JMS-Bindungen ausgewählt haben. Sie würden so vorgehen, wenn Sie die Ereignisse in einer Warteschlange auf einem anderen MQ-Server veröffentlichen wollen als demjenigen, den Sie während der Installation angegeben haben.

Gehen Sie wie folgt vor, um anzugeben, wohin die Ereignisse übermittelt werden sollten:

1. Klicken Sie im Hauptmenü auf **Systemverwaltung > Ereignisverarbeitung > Informationen zur Ereignisübermittlung**.
2. Klicken Sie auf das Symbol **Bearbeiten** neben **Ereigniszustellung aktivieren**.
3. Wählen Sie das Markierungsfeld **Ereigniszustellung aktivieren** aus, um die Ereignisveröffentlichung zu aktivieren.
4. Wenn die Standardwerte für Ihre Installation korrekt sind, verändern Sie diese nicht. Die Standardwerte unterstützen die Ereignisübermittlung an die Warteschlange namens **DeliveryQ**, die vom JMS-Server bereitgestellt wird, welchen Sie während der Installation konfiguriert haben.

   Wenn Sie ändern wollen, wohin Ereignisse übermittelt werden, aktualisieren Sie die Felder. Verwenden Sie die folgenden Informationen als Referenz:

   - Geben Sie Werte für **Benutzer-ID** und **Kennwort** ein, wenn eine Benutzer-ID und ein Kennwort für den Zugriff auf die Warteschlange erforderlich sind.
   - Geben Sie für **JMS-Warteschlangenfactory-Name** den Namen der JMS-Warteschlangenverbindungsfactory von der JMS-Datei `.bindings` ein, die Sie verwenden.

     Anmerkung: In einigen Windows-Versionen vor XP müssen Sie unter Umständen den Standardwert des Felds **JMS-Warteschlangenfactory-Name** ändern, wenn Sie die Standardfunktion für Ereigniszustellung verwenden wollen. Sie müssen den Wert für **JMS-Warteschlangenfactory-Name** von `WBIC/QCF` in `WBIC\\QCF` ändern.
   - Geben Sie für **JMS-Nachrichtentyp** den Nachrichtentyp ein, der übermittelt wird. Die Auswahlmöglichkeiten sind hier **byte** oder **text**.
   - Geben Sie für **JMS-Warteschlangenname** den Namen der JMS-Warteschlange ein, in der die Ereignisse veröffentlicht werden. Diese Warteschlange muss bereits in der JMS-Datei `.bindings` definiert sein, die Sie in WebSphere MQ verwenden.

     Anmerkung: In einigen Windows-Versionen vor XP müssen Sie unter Umständen den Standardwert des Felds **JMS-Warteschlangenname** ändern, wenn Sie die Standardfunktion für Ereigniszustellung verwenden wollen. Sie müssen den Wert für **JMS-Warteschlangenname** von `WBIC/DeliveryQ` in `WBIC\\DeliveryQ` ändern.
   - Geben Sie für **JNDI-Factory-Name** den Namen ein, der für den Zugriff auf die `.bindings`-Datei verwendet wird. Der Standardwert bietet Zugriff auf die Standardbindung im Dateisystem.
   - Geben Sie für **Provider-URL-Pakete** eine URL-Adresse ein, die Zugriff auf die JMS-Bindungsdatei bietet. Diese URL-Adresse muss dem JNDI-Factory-Name entsprechen. Dieses Feld ist optional und, wenn es leer ist, wird die Standarddateisystemposition für JMS-Bindungen verwendet.
   - Geben Sie für **Nachrichtenzeichensatz** den Zeichensatz ein, der zum Erstellen der Bytenachricht in der JMS-Warteschlange verwendet werden soll. Der Standardwert ist UTF-8. Dieses Feld ist nur für Bytenachrichten relevant.
   - Geben Sie für **JMS-Provider-URL** die URL-Adresse des JMS-Providers ein. Dieses Feld ist optional und, wenn es leer ist, wird der Standard-JMS-Provider verwendet, der bei der Installation angegeben wurde.
5. Klicken Sie auf **Speichern**.

Alertfähige Ereignisse angeben

Wenn ein Ereignis in WebSphere Partner Gateway auftritt, wird ein Ereigniscode generiert. Mit der Seite **Ereigniscodes** können Sie den alertfähigen Status des Ereigniscodes festlegen. Wenn ein Ereignis als alertfähig festgelegt wurde, wird das Ereignis in der Liste **Ereignisname** der Seite **Alert** angezeigt. Sie können dann einen Alert für das Ereignis festlegen.

Gehen Sie wie folgt vor, um anzugeben, welche Ereignisse alertfähig sein sollten:

1. Klicken Sie auf **Hubadmin > Hubkonfiguration > Ereigniscodes**.
   Die Seite **Ereigniscodes** wird angezeigt.
2. Gehen Sie für jedes Ereignis, das Sie alertfähig machen wollen, wie folgt vor:
   a. Klicken Sie auf das Symbol **Details anzeigen** neben dem Ereigniscode. Die Seite **Ereigniscodedetails** wird angezeigt.
   b. Wählen Sie **Alertfähig?** aus.
   c. Klicken Sie auf **Speichern**.

Benutzerdefinierten Transport aktualisieren

Wie in Kapitel 5, „Ziele definieren" und Kapitel 10, „Gateways erstellen", auf Seite 141 beschrieben, können Sie eine XML-Datei hochladen, die einen benutzerdefinierten Transport beschreibt. Sie können mit **Transporttypen verwalten** die Datei hochladen. Nachdem Sie die XML-Datei hochgeladen haben, ist der Transport zur Verwendung verfügbar, wenn Sie ein Ziel oder Gateway definieren.

Die XML-Datei, die den benutzerdefinierten Transport beschreibt, schließt die Attribute für den Transport mit ein. Diese Attribute werden im Abschnitt **Angepasste Transportattribute** auf der Ziel- oder Gateway-Seite angezeigt, wenn Sie einen benutzerdefinierten Transport angeben. Ein benutzerdefinierter Transport für ein Gateway könnte z. B. das Attribut **GatewayRetryCount** mit einschließen.

Der Autor der XML-Datei, die den Transport beschreibt, kann die Attribute aktualisieren, indem er die Attribute hinzufügt, löscht oder ändert. Wenn die XML-Datei geändert wurde, laden Sie mit **Transporttypen verwalten** erneut die Datei hoch. Jede Änderung an den Attributen wird auf der Gateway- oder Zielseite wiedergegeben.

Anhang A. Grundlegende Beispiele

Dieser Anhang enthält Beispiele für das Konfigurieren des Hubs. Er behandelt die folgenden Themen:

- „Basiskonfiguration – EDI-Pass-Through-Dokumente austauschen"
- „Basiskonfiguration - Sicherheit für eingehende und ausgehende Dokumente konfigurieren" auf Seite 199
- „Die Basiskonfiguration erweitern" auf Seite 205

Ein separater Anhang enthält Beispiele für das Austauschen von EDI-Austauschvorgängen, welche das Entfernen von Umschlägen, das Transformieren, das Versehen mit Umschlägen und das Übertragen von funktionalen Bestätigungen einschließen. Siehe Anhang B, „EDI-Beispiele", auf Seite 211.

Diese Beispiele sollen Ihnen eine schnelle Übersicht über die Schritte geben, die zum Konfigurieren eines Systems erforderlich sind. Wenn Sie diese Beispiele verwenden, um Ihr System zu konfigurieren, ändern Sie die spezifischen Informationen, z. B. die Namen und Geschäfts-IDs, um sie Ihren Geschäftsbedürfnissen anzupassen.

Basiskonfiguration – EDI-Pass-Through-Dokumente austauschen

In diesem Beispiel ist die Hubkonfiguration relativ einfach gehalten: Es sind zwei Ziele definiert (eines für Dokumente, die beim Hub von einem Teilnehmer eingehen, und eines für Dokumente, die beim Hub vom Community Manager-Back-End-System eingehen). Die Austauschvorgänge, die in diesem Beispiel konfiguriert werden, verwenden die Dokumentenflussdefinitionen, die von WebSphere Partner Gateway zur Verfügung gestellt werden. Aus diesem Grund müssen Sie nur Interaktionen auf der Basis dieser Dokumentenflüsse erstellen. In diesem Beispiel wird kein kundenspezifisches XML verwendet.

Dieses Beispiel zeigt einen Austausch zwischen einer Back-End-Anwendung von Community Manager und einem Community-Teilnehmer (Partner Zwei).

Den Hub konfigurieren

Der erste Schritt in der Konfiguration des Hubs besteht darin, die zwei Ziele zu erstellen.

- Ein HTTP-Ziel (namens "HttpZiel") zum Empfangen von Dokumenten über HTTP (von `Partner Zwei`), die an das Back-End-System von Community Manager gesendet werden sollen.
- Ein Dateiverzeichnisziel (namens "Dateisystemziel") zum Abrufen der Dokumente vom Dateisystem (vom Back-End-System von Community Manager), die an `Partner Zwei` gesendet werden sollen.

Die Ziele definieren

Gehen Sie wie folgt vor, um ein Ziel für den Empfang von Dokumenten über HTTP zu erstellen:

1. Klicken Sie auf **Hubadmin > Hubkonfiguration > Ziele**.
2. Klicken Sie auf **Ziel erstellen**.
3. Geben Sie als **Zielname** den Namen `HttpZiel` ein.

4. Wählen Sie in der Liste **Transport** die Option **HTTP/S** aus.
5. Verwenden Sie als Gateway-Typ den Standardwert **Produktion**.
6. Geben Sie als URI Folgendes ein: **/bcgreceiver/submit**
7. Klicken Sie auf **Speichern**.

Erstellen Sie dann ein Ziel, um ein Verzeichnis im Dateisystem abzufragen. Durch das Erstellen des Ziels wird automatisch ein neues Verzeichnis im Dateisystem erstellt.

Gehen Sie wie folgt vor, um das Dateisystemziel zu erstellen:

1. Klicken Sie auf **Hubadmin > Hubkonfiguration > Ziele**.
2. Klicken Sie auf **Ziel erstellen**.
3. Geben Sie `Dateisystemziel` als Zielname ein.
4. Wählen Sie in der Liste **Transport** die Option **Dateiverzeichnis** aus.
5. Verwenden Sie als Standardgateway-Typ den Standardwert **Produktion**.
6. Geben Sie als Dokumentstammverzeichnispfad das Folgende ein: `\temp\Dateisystemziel`

   Anmerkung: Dadurch wird ein Verzeichnis `Dateisystemziel` innerhalb des temporären Verzeichnisses erstellt. Stellen Sie sicher, dass ein Verzeichnis **temp** im Dateisystem vorhanden ist.
7. Klicken Sie auf **Speichern**.

Dokumentenflüsse und Interaktionen definieren

In diesem Beispiel konfigurieren Sie den Austausch von Dokumenten, die dem EDI-X12-Standard entsprechen. In diesem Beispiel werden die Dokumente einfach durch den Hub weitergeleitet. Vom EDI-Austausch wird kein Umschlag entfernt und es tritt auch keine Transformation auf. Beispiele für das Entfernen von Umschlägen eines Austauschs, dem Transformieren der Transaktionen und dem Senden von Bestätigungen finden Sie in Anhang B, „EDI-Beispiele", auf Seite 211.

In diesem Abschnitt werden die folgenden Austauschvorgänge beschrieben:

- Ein EDI-X12-Dokument ohne Paket von Community Manager an `Partner Zwei` senden.
- Ein EDI-X12-Dokument im AS2-Paket von `Partner Zwei` an Community Manager senden.

Aufgrund der einbezogenen Pakete und Protokolle muss keine neue Dokumentenflussdefinition erstellt werden. Die Pakete, Protokolle und Dokumentenflüsse sind im System vordefiniert.

Sie müssen allerdings Interaktionen auf der Basis dieser vordefinierten Dokumentenflüsse definieren.

Erstellen Sie die erste Interaktion, in der die Quelle ein ISA-formatiertes Dokument ist, das dem EDI-X12-Standard ohne Paket entspricht, und das Ziel ein ISA-formatiertes Dokument ist, das dem EDI-X12-Standard mit AS2-Paket entspricht.

1. Klicken Sie auf **Hubadmin > Hubkonfiguration > Dokumentenflussdefinition**.
2. Klicken Sie auf **Interaktionen verwalten** und dann auf **Interaktion erstellen**.
3. Erweitern Sie in der Spalte **Quelle** Folgendes:
   a. **Paket: None**

b. **Protokoll: EDI-X12**

4. Klicken Sie auf **Dokumentenfluss: ISA**.
5. Erweitern Sie in der Spalte **Ziel** Folgendes:
   a. **Paket: AS**
   b. **Protokoll: EDI-X12**
6. Klicken Sie auf **Dokumentenfluss: ISA**.
7. Wählen Sie in der Liste **Aktion** die Option **Pass-Through** aus.
8. Klicken Sie auf **Speichern**.

Erstellen Sie eine zweite Interaktion, in der das Quellenformat ein ISA-formatiertes Dokument ist, das dem EDI-X12-Standard mit AS-Paket entspricht, und das Zielformat ein ISA-formatiertes Dokument ist, das dem EDI-X12-Standard ohne Paket entspricht:

1. Klicken Sie auf **Interaktion erstellen**.
2. Erweitern Sie in der Spalte **Quelle** Folgendes:
   a. **Paket:AS**
   b. **Protokoll: EDI-X12**
3. Klicken Sie auf **Dokumentenfluss: ISA**.
4. Erweitern Sie in der Spalte **Ziel** Folgendes:
   a. **Paket:None**
   b. **Protokoll: EDI-X12**
5. Klicken Sie auf **Dokumentenfluss:ISA**.
6. Wählen Sie in der Liste **Aktion** die Option **Pass-Through** aus.
7. Klicken Sie auf **Speichern**.

Teilnehmer und Teilnehmerverbindungen erstellen

In diesem Beispiel wird ein externer Teilnehmer zusätzlich zu Community Manager erstellt. Die Gateways für die Teilnehmer umfassen Standardtransporte. Es sind keine Konfigurationspunkte für die Gateways definiert.

Die Teilnehmer erstellen

Erstellen Sie zwei neue Teilnehmer. Gehen Sie wie folgt vor, um Community Manager zu definieren:

1. Klicken Sie auf **Kontenadmin** vom Hauptmenü. Die Seite **Teilnehmersuche** ist die Standardanzeige.
2. Klicken Sie auf **Erstellen**.
3. Geben Sie als **Anmeldename des Unternehmens** Folgendes ein: **CommMan**.
4. Geben Sie als **Anzeigename des Teilnehmers** Folgendes ein: **Comm Man**.
5. Wählen Sie als **Teilnehmertyp** Folgendes aus: **Community Manager**.
6. Klicken Sie auf **Neu** unterhalb von **Geschäfts-ID**.
7. Behalten Sie für **Typ** den Eintrag **DUNS** bei, und geben Sie einen Kennungswert **123456789** ein.

   Anmerkung: An dieser Stelle und im ganzen Handbuch sind die verwendeten DUNS-Nummern, nur als Beispiele zu verstehen.
8. Klicken Sie auf **Neu** unterhalb von **Geschäfts-ID**.
9. Wählen Sie **Unformatiert** aus, und geben Sie einen Kennungswert von **12-3456789** ein.
10. Klicken Sie auf **Speichern**.

Gehen Sie wie folgt vor, um **Partner Zwei** zu definieren:

1. Klicken Sie auf **Kontenadmin > Profile > Community-Teilnehmer**.
2. Klicken Sie auf **Erstellen**.
3. Geben Sie als **Anmeldename des Unternehmens** Folgendes ein: **partnerZwei**.
4. Geben Sie als **Anzeigename des Teilnehmers** Folgendes ein: **Partner Zwei**.
5. Wählen Sie als **Teilnehmertyp** Folgendes aus: **Community-Teilnehmer**.
6. Klicken Sie auf **Neu** unterhalb von **Geschäfts-ID**.
7. Behalten Sie für **Typ** den Eintrag **DUNS** bei, und geben Sie als Kennung **987654321** ein.
8. Klicken Sie auf **Neu** unterhalb von **Geschäfts-ID**.
9. Wählen Sie **Unformatiert** aus, und geben Sie einen Kennungswert von **98-7654321** ein.
10. Klicken Sie auf **Speichern**.

Jetzt haben Sie sowohl Community Manager als auch `Partner Zwei` für den Hub definiert.

Zu den nächsten Schritten gehört nun das Konfigurieren von Gateways für Community Manager und `Partner Zwei`.

Die Gateways erstellen

Bevor Sie ein Dateiverzeichnisgateway für Community Manager erstellen, müssen Sie die Verzeichnisstruktur erstellen, die von diesem Gateway verwendet wird. Erstellen Sie ein neues Verzeichnis **Dateisystemgateway** auf dem Stammlaufwerk. In diesem Verzeichnis speichert Community Manager Dateien, die von Teilnehmern empfangen wurden.

In dem Fall von Community Manager stellt das Gateway den Einstiegspunkt in das Back-End-System dar.

Gehen Sie wie folgt vor, um ein Gateway für Community Manager zu erstellen:

1. Klicken Sie auf **Kontenadmin > Profile > Community-Teilnehmer**.
2. Klicken Sie auf **Suchen**.
3. Wählen Sie **Comm Man** aus, indem Sie auf das Symbol **Details anzeigen** klicken.
4. Klicken Sie auf **Gateways** in der horizontalen Navigationsleiste.
5. Klicken Sie auf **Erstellen**.
6. Geben Sie als **Gateway-Name** Folgendes ein: **Dateisystemgateway**.
7. Wählen Sie als **Transport** die Option **Dateiverzeichnis** aus.
8. Geben Sie als **Adresse** Folgendes ein: **file://C:\Dateisystemgateway**
9. Klicken Sie auf **Speichern**.

Legen Sie nun dieses neu erstellte Gateway als das Standardgateway für Community Manager fest.

1. Klicken Sie auf **Liste**, um alle Gateways anzuzeigen, die für Community Manager konfiguriert sind.
2. Klicken Sie auf **Standardgateways anzeigen**.
3. Wählen Sie in der Liste **Produktion** den Eintrag **Dateisystemgateway** aus.
4. Klicken Sie auf **Speichern**.

Erstellen Sie ein Gateway für **Partner Zwei**.

1. Klicken Sie auf **Kontenadmin > Profile > Community-Teilnehmer**.
2. Klicken Sie auf **Suchen**, und wählen Sie dann `Partner Zwei` aus, indem Sie auf das Symbol **Details anzeigen** klicken.
3. Klicken Sie auf **Gateways** in der horizontalen Navigationsleiste.
4. Klicken Sie auf **Erstellen**.
5. Geben Sie als **Gateway-Name** Folgendes ein: **HttpGateway**.
6. Wählen Sie als **Transport** die Option **HTTP/1.1** aus.
7. Geben Sie als **Adresse** Folgendes ein: **http://<***IP-adresse***>:80/input/AS2**. Dabei steht <*IP-adresse*> für den Computer von **Partner Zwei**.
8. Geben Sie als **Benutzername** Folgendes ein: **Comm Man**.
9. Geben Sie als **Kennwort** Folgendes ein: **commMan**.
10. Klicken Sie auf **Speichern**.

Beachten Sie, dass in diesem Beispiel davon ausgegangen wird, dass Teilnehmer, die sich am System von **Partner Zwei** anmelden wollen, einen Benutzernamen und ein Kennwort benötigen.

Für diesen Teilnehmer müssen Sie auch einen Standardgateway definieren.

1. Klicken Sie auf **Liste** und dann auf **Standardgateways anzeigen**.
2. Wählen Sie in der Liste **Produktion** den Eintrag **HttpGateway** aus.
3. Klicken Sie auf **Speichern**.

B2B-Funktionalität konfigurieren

Definieren Sie als Nächstes die B2B-Funktionalität für Community Manager.

1. Klicken Sie im Hauptmenü auf **Kontenadmin > Profile > Community-Teilnehmer**.
2. Klicken Sie auf **Suchen**.
3. Wählen Sie **Comm Man** aus, indem Sie auf das Symbol **Details anzeigen** klicken.
4. Klicken Sie auf **B2B-Funktionalität** in der horizontalen Navigationsleiste.
5. Legen Sie die Quelle und das Ziel für das **Paket: None**, das **Protokoll: EDI-X12** und den **Dokumentenfluss: ISA** fest, indem Sie die folgenden Schritte ausführen:
   a. Klicken Sie auf das Symbol **Rolle ist nicht aktiv** unter **Quelle festlegen** für **Paket: None**.
   b. Klicken Sie auf das Symbol **Rolle ist nicht aktiv** unter **Ziel festlegen** für **Paket: None**.
   c. Klicken Sie auf das Symbol **Erweitern** neben **Paket: None**.
   d. Klicken Sie auf das Symbol **Rolle ist nicht aktiv** für **Protokoll: EDI-X12 (ALL)** für die Quelle und das Ziel.
   e. Klicken Sie auf das Symbol **Erweitern** neben **Protokoll: EDI-X12 (ALL)**.
   f. Klicken Sie auf das Symbol **Rolle ist nicht aktiv** für **Dokumentenfluss: ISA** für die Quelle und das Ziel.

Legen Sie dann die B2B-Funktionalität für **Partner Zwei** fest.

1. Klicken Sie im Hauptmenü auf **Kontenadmin > Profile > Community-Teilnehmer**.
2. Klicken Sie auf **Suchen**.

3. Wählen Sie **Partner Zwei** aus, indem Sie auf das Symbol **Details anzeigen** klicken.
4. Klicken Sie auf **B2B-Funktionalität** in der horizontalen Navigationsleiste.
5. Wählen Sie **Quelle festlegen** und **Ziel festlegen** für das **Paket: AS**, das **Protokoll: EDI-X12** und den **Dokumentenfluss: ISA** aus, indem Sie die folgenden Schritte ausführen:
   a. Klicken Sie auf das Symbol **Rolle ist nicht aktiv** unter **Quelle festlegen** für **Paket: AS**.
   b. Klicken Sie auf das Symbol **Rolle ist nicht aktiv** unter **Ziel festlegen** für **Paket: AS**.
   c. Klicken Sie auf das Symbol **Erweitern** neben **Paket: AS**.
   d. Klicken Sie auf das Symbol **Rolle ist nicht aktiv** für **Protokoll: EDI-X12 (ALL)** für die Quelle und das Ziel.
   e. Klicken Sie auf das Symbol **Erweitern** neben **Protokoll: EDI-X12 (ALL)**.
   f. Klicken Sie auf das Symbol **Rolle ist nicht aktiv** für **Dokumentenfluss: ISA** für die Quelle und das Ziel.

Teilnehmerverbindungen definieren

Definieren Sie die Teilnehmerverbindung für EDI-Dokumente ohne Paket, die von Community Manager eingehen und **Partner Zwei** zugestellt werden sollen.

1. Klicken Sie auf **Kontenadmin > Teilnehmerverbindungen**.
2. Wählen Sie in der Liste **Quelle** den Eintrag **Comm Man** aus.
3. Wählen Sie in der Liste **Ziel** den Eintrag **Partner Zwei** aus.
4. Klicken Sie auf **Suchen**.
5. Klicken Sie auf **Aktivieren** für die Verbindung mit den folgenden Zusatzinformationen:
   a. **Quelle**
      1) Paket: **None (N/A)**
      2) Protokoll: **EDI-X12 (ALL)**
      3) Dokumentenfluss: **ISA(ALL)**
   b. **Ziel**
      1) Paket: **AS (N/A)**
      2) Protokoll: **EDI-X12 (ALL)**
      3) Dokumentenfluss: **ISA(ALL)**

Definieren Sie als Nächstes die Verbindung für EDI-Dokumente im AS2-Paket, die von **Partner Zwei** eingehen und Community Manager ohne Paket zugestellt werden sollen. Dies ähnelt sehr der Verbindung, die Sie im vorherigen Abschnitt definiert haben, außer dass Sie auch noch AS2-Attribute konfigurieren.

1. Klicken Sie auf **Kontenadmin > Teilnehmerverbindungen**.
2. Wählen Sie in der Liste **Quelle** den Eintrag **Partner Zwei** aus.
3. Wählen Sie in der Liste **Ziel** den Eintrag **Comm Man** aus.
4. Klicken Sie auf **Suchen**.
5. Klicken Sie auf **Aktivieren** für die Verbindung mit den folgenden Zusatzinformationen:
   a. **Quelle**
      1) Paket: **AS (N/A)**
      2) Protokoll: **EDI-X12 (ALL)**
      3) Dokumentenfluss: **ISA(ALL)**

b. **Ziel**
   1) Paket: **None (N/A)**
   2) Protokoll: **EDI-X12 (ALL)**
   3) Dokumentenfluss: **ISA(ALL)**

Wählen Sie als Nächstes **Attribute** neben dem Kästchen **Paket: AS (N/A)** für **Partner Zwei** aus.

1. Bearbeiten Sie die Attribute von **Paket: AS (N/A)**, indem Sie auf der Seite abwärts blättern, und klicken Sie auf das Symbol **Erweitern** neben **Paket: AS (N/A)**.
2. Geben Sie einen Wert für **AS-MDN-E-Mail-Adresse** (AS1) ein. Dies kann eine beliebige gültige E-Mail-Adresse sein.
3. Geben Sie einen Wert für **AS-MDN-HTTP-URL-Adresse** (AS2) ein. Dieser sollte wie folgt eingegeben werden: **http://<***IP-adresse***>:57080/bcgreceiver/submit**. Dabei steht <*IP-adresse*> für den Hub.
4. Klicken Sie auf **Speichern**.

Basiskonfiguration - Sicherheit für eingehende und ausgehende Dokumente konfigurieren

In diesem Abschnitt erfahren Sie, wie die folgenden Sicherheitstypen der Basiskonfiguration hinzugefügt werden:

- SSL-Serverauthentifizierung (SSL - Secure Socket Layers)
- Verschlüsselung
- Digitale Unterschriften

SSL-Authentifizierung für Eingangsdokumente konfigurieren

In diesem Abschnitt konfigurieren Sie die Serverauthentifizierung mit iKeyman, so dass **Partner Zwei** AS2-Dokumente über HTTPS senden kann.

Führen Sie die folgenden Schritte aus, um die Serverauthentifizierung zu konfigurieren:

1. Initiieren Sie die Anwendung iKeyman, indem Sie die Datei `ikeyman.bat` vom Verzeichnis `/<Produktverz>/was/bin` öffnen.
2. Öffnen Sie den Standard-Keystore des Empfängers, `receiver.jks`. Wählen Sie in der Menüleiste **Key Database File Open** aus. Bei einer Standardinstallation befindet sich `receiver.jks` im folgenden Verzeichnis: <*Produktverz*>/common/security/keystore
3. Wenn Sie dazu aufgefordert werden, geben Sie das Standardkennwort für `receiver.jks` ein. Dieses Kennwort lautet **WebAS**.
4. Wenn Sie `receiver.jks` zum ersten Mal öffnen, löschen Sie das Zertifikat "Dummy".

Der nächste Schritt besteht darin, ein neues selbst unterzeichnetes Zertifikat zu erstellen. Durch die Erstellung eines selbst unterzeichneten persönlichen Zertifikats werden ein privater Schlüssel und ein öffentlicher Schlüssel in der Server-Keystore-Datei erstellt.

Gehen Sie wie folgt vor, um ein neues selbst unterzeichnetes Zertifikat zu erstellen:

1. Klicken Sie auf **New Self Signed**.

2. Geben Sie dem Zertifikat eine Schlüsselbezeichnung, mit der das Zertifikat innerhalb des Keystores eindeutig gekennzeichnet ist. Verwenden Sie die Bezeichnung **selfSignedCert** .
3. Geben Sie den allgemeinen Namen des Servers ein. Dies ist die primäre, universelle Identität für das Zertifikat. Sie sollte den Teilnehmer, den sie darstellt, eindeutig kennzeichnen.
4. Geben Sie den Namen Ihres Unternehmens ein.
5. Akzeptieren Sie alle übrigen Standardeinstellungen, und klicken Sie auf **OK**.

Angenommen, dass **Partner Zwei** eine EDI-Nachricht über AS2 mit HTTPS senden will. **Partner Zwei** muss auf das öffentliche Zertifikat verweisen, welches bei der Erstellung des selbst unterzeichneten Zertifikats mit erstellt wurde, um dies auszuführen.

Um **Partner Zwei** für die Verwendung des öffentlichen Zertifikats zu aktivieren, exportieren Sie das öffentliche Zertifikat wie folgt aus der Server-Keystore-Datei:

1. Wählen Sie das neu erstellte selbst unterzeichnete Zertifikat vom Dienstprogramm IBM Key Management (iKeyman) aus.
2. Klicken Sie auf **Extract Certificate**.
3. Ändern Sie den Datentyp in **Binary DER data**.
4. Stellen Sie den Dateinamen **commManOeffentlich** bereit, und klicken Sie auf **OK**.

Verwenden Sie iKeyman dann, um das selbst unterzeichnete Zertifikat und das private Schlüsselpaar in Form einer PKCS12-Datei zu exportieren. Diese PCKS12-Datei wird zur Verschlüsselung verwendet, dies wird in einem späteren Abschnitt beschrieben.

Gehen Sie wie folgt vor, um das selbst unterzeichnete Zertifikat und das private Schlüsselpaar zu exportieren:

1. Klicken Sie auf **Export/Import**.
2. Ändern Sie den Schlüsseldateityp in **PKCS12**.
3. Stellen Sie den Dateinamen **commManPrivat** bereit, und klicken Sie auf **OK**.
4. Geben Sie ein Kennwort ein, um die PKCS12-Zieldatei zu schützen. Bestätigen Sie das Kennwort, und klicken Sie auf **OK**.

Anmerkung: Stoppen und starten Sie den Empfänger erneut, damit diese Änderungen wirksam werden.

Das eingegebene Kennwort wird später verwendet, wenn Sie dieses private Zertifikat in den Hub importieren.

Partner Zwei muss auch einige Konfigurationsschritte ausführen, hierzu gehören das Importieren des Zertifikats und das Ändern der Adresse, an die die AS2-Dokumente gesendet werden. **Partner Zwei** muss z. B. die Adresse wie folgt ändern:

`https://<IP-adresse>:57443/bcgreceiver/submit`

Dabei steht *<IP-adresse>* für den Hub.

Das selbst unterzeichnete Zertifikat, das im Standard-Keystore des Empfängers platziert wurde, wird **Partner Zwei** jetzt immer dann angezeigt, wenn **Partner Zwei** ein Dokument über HTTPS sendet.

Um die entgegengesetzte Situation zu konfigurieren, muss **Partner Zwei** für den Hub einen SSL-Schlüssel in Form einer .der-Datei (in diesem Fall `partnerZweiSSL-.der`) bereitstellen. Falls nötig, muss **Partner Zwei** die Konfiguration auch so ändern, dass das Empfangen von Dokumenten über den HTTPS-Transport zugelassen wird.

Laden Sie die Datei `partnerZweiSSL.der` von **Partner Zwei** in das Profil des Hub-Operators als Rootzertifikat. Ein Rootzertifikat ist ein Zertifikat, das von einer Zertifizierungsstelle (CA - Certifying Authority) ausgestellt wird, die für das Einrichten einer Zertifikatkette verwendet wird. In diesem Beispiel hat **Partner Zwei** das Zertifikat generiert, welches als Rootzertifikat geladen wurde, um den Hub in die Lage zu versetzen, den Sender zu erkennen und ihm zu vertrauen.

Laden Sie `partnerZweiSSL.der` in den Hub:

1. Klicken Sie im Hauptmenü auf **Kontenadmin > Profile > Community-Teilnehmer**.
2. Klicken Sie auf **Suchen**.
3. Wählen Sie **Hub-Operator** aus, indem Sie das Symbol **Details anzeigen** auswählen.
4. Klicken Sie auf **Zertifikate** und dann auf **Zertifikat laden**.
5. Setzen Sie den **Zertifikatstyp** auf **Root und Intermediate**.
6. Ändern Sie die Beschreibung in **Partner Zwei SSL-Zertifikat**.
7. Setzen Sie den **Status** auf **Aktiviert**.
8. Klicken Sie auf **Durchsuchen**, und navigieren Sie zum Verzeichnis, in dem Sie die Datei `partnerZweiSSL.der` gespeichert haben.
9. Wählen Sie das Zertifikat aus, und klicken Sie auf **Öffnen**.
10. Klicken Sie auf **Hochladen** und dann auf **Speichern**.

Ändern Sie das Gateway von **Partner Zwei** so, dass es HTTPS verwendet.

1. Klicken Sie auf **Kontenadmin > Profile > Community-Teilnehmer** in der horizontalen Navigationsleiste.
2. Klicken Sie auf **Suchen**, und wählen Sie `Partner Zwei` aus, indem Sie auf das Symbol **Details anzeigen** klicken.
3. Klicken Sie auf **Gateways** in der horizontalen Navigationsleiste. Wählen Sie als Nächstes **HttpGateway** aus, indem Sie auf das Symbol **Details anzeigen** klicken.
4. Bearbeiten Sie es, indem Sie auf Symbol **Bearbeiten** klicken.
5. Ändern Sie den Transportwert in **HTTPS/1.1**.
6. Ändern Sie den Wert der Adresse wie folgt: **https://<***IP-adresse***>:443/input/AS2**. Dabei steht <*IP-adresse*> für das System von **Partner Zwei**.
7. Alle anderen Werte können unverändert bleiben. Klicken Sie auf **Speichern**.

Verschlüsselung konfigurieren

Dieser Abschnitt enthält die Schritte zum Konfigurieren der Verschlüsselung.

Partner Zwei muss alle nötigen Konfigurationsschritte ausführen, z. B. das Importieren des öffentlichen Zertifikats und des selbst unterzeichneten Zertifikats, und die Verschlüsselung von Dokumenten konfigurieren, die zum Hub gesendet werden.

WebSphere Partner Gateway verwendet seinen privaten Schlüssel zum Entschlüsseln von Dokumenten. Um dem Hub dies zu ermöglichen, laden Sie zuerst den privaten Schlüssel, den Sie aus dem selbst unterzeichneten Zertifikat extrahiert haben, in Community Console. Führen Sie diese Aufgabe aus, wenn Sie als Hub-Operator an Community Console angemeldet sind, und installieren Sie das Zertifikat in Ihrem eigenen Profil.

Gehen Sie wie folgt vor, um die PKCS12-Datei zu laden:

1. Klicken Sie auf **Kontenadmin > Profile > Community-Teilnehmer** in der horizontalen Navigationsleiste.
2. Klicken Sie auf **Suchen**.
3. Wählen Sie **Hub-Operator** aus, indem Sie auf das Symbol **Details anzeigen** klicken.
4. Klicken Sie auf **Zertifikate** und dann auf **PKCS12 laden**.
5. Wählen Sie das Markierungsfeld links von **Verschlüsselung** aus.
6. Ändern Sie die Beschreibung in **CommManPrivat**.
7. Wählen Sie **Aktiviert** aus.
8. Klicken Sie auf **Durchsuchen**, und navigieren Sie zum Verzeichnis, in dem die PKCS12-Datei `commMannPrivat.p12` gespeichert ist.
9. Wählen Sie die Datei aus, und klicken Sie auf **Öffnen**.
10. Geben Sie das Kennwort ein, das für die PKCS12-Datei bereitgestellt wurde.
11. Übernehmen Sie den Gateway-Typ **Produktion**.
12. Klicken Sie auf **Hochladen** und dann auf **Speichern**.

Das beendet die Konfiguration, die erforderlich ist, damit ein Teilnehmer verschlüsselte Transaktionen über HTTPS an den Hub senden kann.

Im folgenden Abschnitt wird die vorherige Prozedur umgekehrt; nun sendet der Hub eine verschlüsselte EDI-Transaktion über HTTPS.

Partner Zwei muss ein Schlüsselpaar zur Dokumententschlüsselung generieren (in diesem Beispiel die Datei `partnerZweiEntschlüsseln.der`) und sollte das öffentliche Zertifikat für den Hub verfügbar machen.

Wie bereits erwähnt, wird der öffentliche Schlüssel vom Hub verwendet, wenn Transaktionen verschlüsselt werden, die an den Teilnehmer gesendet werden sollen. Damit dies geschehen kann, laden Sie das öffentliche Zertifikat in den Hub.

1. Klicken Sie im Hauptmenü auf **Kontenadmin > Profile > Community-Teilnehmer**.
2. Klicken Sie auf **Suchen**.
3. Wählen Sie **Partner Zwei** aus, indem Sie auf das Symbol **Details anzeigen** klicken.
4. Klicken Sie auf **Zertifikate** in der horizontalen Navigationsleiste.
5. Klicken Sie auf **Zertifikat laden**.
6. Wählen Sie das Markierungsfeld neben **Verschlüsselung** aus.
7. Ändern Sie die Beschreibung in **Partner Zwei verschlüsseln**.
8. Setzen Sie den Status auf **Aktiviert**.
9. Klicken Sie auf **Durchsuchen**.
10. Navigieren Sie zum Verzeichnis, in dem das Entschlüsselungszertifikat `partnerZweiEntschlüsselt.der` gespeichert ist.

11. Wählen Sie das Zertifikat aus, und klicken Sie auf **Öffnen**.
12. Übernehmen Sie den Gateway-Typ **Produktion**.
13. Klicken Sie auf **Hochladen** und dann auf **Speichern**.

Der letzte Schritt in der Hubkonfiguration zum Senden von verschlüsselten Nachrichten über HTTPS mit AS2 besteht darin, die Teilnehmerverbindung zu ändern, die zwischen Community Manager und **Partner Zwei** vorhanden ist.

Gehen Sie wie folgt vor, um die Teilnehmerverbindung über Community Console zu modifizieren:

1. Klicken Sie auf **Kontenadmin > Teilnehmerverbindungen** in der horizontalen Navigationsleiste.
2. Wählen Sie in der Liste **Quelle** den Eintrag **Comm Man** aus.
3. Wählen Sie in der Liste **Ziel** den Eintrag **Partner Zwei** aus.
4. Klicken Sie auf **Suchen**.
5. Klicken Sie für das Ziel auf die Schaltfläche **Attribute**.
6. Beachten Sie in der **Verbindungszusammenfassung**, dass das Attribut **AS verschlüsselt** den aktuellen Wert **Nein** hat. Bearbeiten Sie diesen Wert, indem Sie auf das Symbol **Erweitern** neben **Paket: AS (N/A)** klicken.

   Anmerkung: Sie müssen auf der Seite abwärts blättern, damit diese Option angezeigt wird.
7. Aktualisieren Sie in der Liste das Attribut **AS verschlüsselt** in **Ja**, und klicken Sie auf **Speichern**.

Dokumentunterzeichnung konfigurieren

Wenn Sie eine Transaktion oder Nachricht digital unterzeichnen, verwendet WebSphere Partner Gateway Ihren privaten Schlüssel, um die Unterschrift zu erstellen und zu unterzeichnen. Ihr Partner, der diese Nachricht empfängt, verwendet Ihren öffentlichen Schlüssel, um die Unterschrift zu prüfen. Aus diesem Grund verwendet WebSphere Partner Gateway digitale Unterschriften.

Dieser Abschnitt stellt die Schritte bereit, die erforderlich sind, um sowohl den Hub als auch einen Teilnehmer zur Verwendung für digitale Unterschriften zu konfigurieren.

Partner Zwei muss die nötigen Konfigurationsschritte ausführen (z. B. das Erstellen eines selbst unterzeichneten Dokuments, das in diesem Beispiel `partnerZweiUnterzeichnend.der` genannt wurde) und die Unterzeichnung von Dokumenten konfigurieren. **Partner Zwei** muss `partnerZweiUnterzeichnend.der` für den Hub verfügbar machen.

Gehen Sie wie folgt vor, um das digitale Zertifikat in den Hub zu laden:

1. Klicken Sie auf **Kontenadmin > Profile > Community-Teilnehmer** in der horizontalen Navigationsleiste.
2. Klicken Sie auf **Suchen**.
3. Wählen Sie **Partner Zwei** aus, indem Sie auf das Symbol **Details anzeigen** klicken.
4. Wählen Sie **Zertifikate** in der horizontalen Navigationsleiste aus.
5. Klicken Sie auf **Zertifikat laden**.
6. Wählen Sie das Markierungsfeld neben **Digitale Unterschrift** aus.

7. Ändern Sie die Beschreibung in **CommMan unterzeichnend**.
8. Setzen Sie den **Status** auf **Aktiviert**.
9. Klicken Sie auf **Durchsuchen**.
10. Navigieren Sie zum Verzeichnis, in dem das digitales Zertifikat `partnerZweiUnterzeichnend.der` gespeichert ist, wählen Sie das Zertifikat aus, und klicken Sie auf **Öffnen**.
11. Klicken Sie auf **Hochladen** und dann auf **Speichern**.

Damit ist die Anfangskonfiguration für digitale Unterschriften abgeschlossen.

Der Teilnehmer verwendet das öffentliche Zertifikat, um unterzeichnete, an den Hub gesendete Transaktionen zu authentifizieren.

Der Hub verwendet den privaten Schlüssel, um ausgehende Transaktionen, die an den Teilnehmer gesendet wurden, digital zu unterzeichnen. Zuerst aktivieren Sie den privaten Schlüssel für die digitale Unterschrift.

Gehen Sie wie folgt vor, um den privaten Schlüssel für die digitale Unterschrift zu aktivieren:

1. Klicken Sie auf **Kontenadmin > Profile > Zertifikate** in der horizontalen Navigationsleiste.
2. Klicken Sie auf das Symbol **Details anzeigen** neben **Hub-Operator**.
3. Klicken Sie auf das Symbol **Details anzeigen** neben **CommManPrivat**.

   Anmerkung: Dies war das private Zertifikat, das Sie zuvor in den Hub geladen haben.
4. Klicken Sie auf das Symbol **Bearbeiten**.
5. Wählen Sie das Markierungsfeld neben **Digitale Unterschrift** aus.

   Anmerkung: Wenn mehr als ein Zertifikat für digitale Unterschrift verfügbar ist, würden Sie auswählen, welches das primäre bzw. das sekundäre Zertifikat ist, indem Sie **Primär** oder **Sekundär** in der Liste **Zertifikatverwendung** auswählen.
6. Klicken Sie auf **Speichern**.

Als Nächstes ändern Sie die Attribute der vorhandenen Teilnehmerverbindung zwischen Community Manager und **Partner Zwei**, um unterzeichnete AS2-Transaktionen zu unterstützen.

Gehen Sie wie folgt vor, um die Attribute der Teilnehmerverbindung zu ändern:

1. Klicken Sie auf **Kontenadmin > Teilnehmerverbindungen** in der horizontalen Navigationsleiste.
2. Wählen Sie **Comm Man** in der Liste **Quelle** aus.
3. Wählen Sie **Partner Zwei** in der Liste **Ziel** aus.
4. Klicken Sie auf **Suchen**.
5. Klicken Sie für **Partner Zwei** auf die Schaltfläche **Attribute**.
6. Bearbeiten Sie das Attribut **AS unterzeichnet**, indem Sie auf das Symbol **Erweitern** neben **Paket: AS (N/A)** klicken.
7. Wählen Sie **Ja** in der Liste **AS unterzeichnet** aus.
8. Klicken Sie auf **Speichern**.

Damit ist die Konfiguration abgeschlossen, die zum Senden einer unterzeichneten AS2-Transaktion von WebSphere Partner Gateway an den Teilnehmer erforderlich ist.

Die Basiskonfiguration erweitern

Dieser Abschnitt zeigt Ihnen, wie Sie die in diesem Anhang beschriebene Basiskonfiguration modifizieren können. Dieser Abschnitt beschreibt unter Verwendung derselben, zuvor beschriebenen Partner und Konfiguration (einen Community Manager namens **Com Man** mit der DUNS-ID **123456789** und einem Dateiverzeichnisgateway und einem Teilnehmer namens **PartnerZwei** mit der DUNS-ID **987654321** und einem HTTP-Gateway) wie die Unterstützung für Folgendes hinzugefügt wird:

- Den FTP-Transport
- Angepasste XML-Dokumente
- Binärdateien (ohne Paket)

FTP-Ziel erstellen

Das FTP-Ziel empfängt Dateien und übergibt sie zur Verarbeitung an Document Manager. Wie in „Den FTP-Server für das Empfangen von Dokumenten konfigurieren" auf Seite 21 beschrieben, müssen Sie, bevor Sie ein FTP-Ziel erstellen können, einen FTP-Server installieren, und Sie müssen ein FTP-Verzeichnis erstellt und Ihren FTP-Server konfiguriert haben.

In diesem Beispiel wird davon ausgegangen, dass der FTP-Server für **Partner Zwei** konfiguriert wurde, und dass das Stammverzeichnis `c:/ftproot` lautet.

1. Klicken Sie auf **Hubadmin > Hubkonfiguration > Ziele**.
2. Klicken Sie auf **Ziel erstellen**.
3. Geben Sie die folgenden Informationen ein:
   a. Zielname: **FTP_Receiver**
   b. Transport: **FTP-Verzeichnis**
   c. FTP-Stammverzeichnis: **C:/ftproot**
4. Klicken Sie auf **Speichern**.

Den Hub zum Empfangen von Binärdateien konfigurieren

Dieser Abschnitt behandelt die erforderlichen Schritte, um den Hub zum Empfangen von Binärdokumenten zu konfigurieren, die **Partner Zwei** an Community Manager senden will.

Interaktion für Binärdokumente erstellen

Standardmäßig stellt WebSphere Partner Gateway vier Interaktionen bereit, die binäre Dokumente einschließen. Es stellt jedoch keine Interaktion für Binärdokumente im Paket **None** bereit, die an einen Teilnehmer mit dem Dokument im Paket **None** gehen. In diesem Abschnitt erstellen Sie die erforderliche Interaktion, damit Binärdokumente durch das System weitergeleitet werden können.

1. Klicken Sie auf **Hubadmin > Hubkonfiguration > Dokumentenflussdefinition**.
2. Klicken Sie auf **Interaktionen verwalten**.
3. Klicken Sie auf **Interaktion erstellen**.
4. Wählen Sie in der Liste **Quelle** Folgendes aus: **Paket: None Protokoll: Binary (1.0) Dokumentenfluss: Binary (1.0)**.

5. Wählen Sie in der Liste **Ziel** Folgendes aus: **Paket: None Protokoll: Binary (1.0) Dokumentenfluss: Binary (1.0)**.
6. Wählen Sie in der Liste **Aktion** die Option **Pass-Through** aus.
7. Klicken Sie auf **Speichern**.

Die B2B-Funktionalität für Community Manager aktualisieren

Dieser Abschnitt zeigt, wie Sie Community Manager so konfigurieren, dass er Binärdokumente akzeptieren kann.

1. Klicken Sie auf **Kontenadmin > Profile > Community-Teilnehmer**.
2. Klicken Sie auf **Suchen**.
3. Klicken Sie auf das Symbol **Details anzeigen** neben **Comm Man**.
4. Klicken Sie auf **B2B-Funktionalität**.
5. Klicken Sie zum Aktivieren auf das Symbol **Rolle ist nicht aktiv** unter **Ziel festlegen** für **Paket: None**.
6. Klicken Sie auf das Symbol **Erweitern** neben **Paket: None**.
7. Klicken Sie auf das Symbol **Rolle ist nicht aktiv** für **Protokoll: Binary (1.0)** unter **Ziel festlegen**.
8. Klicken Sie auf das Symbol **Erweitern** neben **Protokoll: Binary (1.0)**.
9. Klicken Sie schließlich auf das Symbol **Rolle ist nicht aktiv** für **Dokumentenfluss: Binary (1.0)** unter **Ziel festlegen**.

Die B2B-Funktionalität für "Partner Zwei" aktualisieren

Dieser Abschnitt zeigt, wie Sie **Partner Zwei** so konfigurieren, dass er Binärdokumente senden kann.

1. Klicken Sie auf **Kontenadmin > Profile > Community-Teilnehmer**.
2. Klicken Sie auf **Suchen**.
3. Klicken Sie auf das Symbol **Details anzeigen** neben **Partner Zwei**.
4. Klicken Sie auf **B2B-Funktionalität**.
5. Klicken Sie zum Aktivieren auf das Symbol **Rolle ist nicht aktiv** unter **Quelle festlegen** für **Paket: None**.
6. Klicken Sie auf das Symbol **Erweitern** neben **Paket: None**.
7. Klicken Sie auf das Symbol **Rolle ist nicht aktiv** für **Protokoll: Binary (1.0)** unter **Quelle festlegen**.
8. Klicken Sie auf das Symbol **Erweitern** neben **Protokoll: Binary (1.0)**.
9. Klicken Sie schließlich auf das Symbol **Rolle ist nicht aktiv** für **Dokumentenfluss: Binary (1.0)** unter **Quelle festlegen**.

Neue Teilnehmerverbindung erstellen

Dieser Abschnitt zeigt, wie Sie eine neue Teilnehmerverbindung zwischen Community Manager und **Partner Zwei** für Binärdokumente konfigurieren können.

1. Klicken Sie auf **Kontenadmin > Teilnehmerverbindungen**.
2. Wählen Sie **Partner Zwei** in der Liste **Quelle** aus.
3. Wählen Sie **Comm Man** in der Liste **Ziel** aus.
4. Klicken Sie auf **Suchen**.
5. Suchen Sie die Verbindung **None (N/A), Binary (1.0), Binary (1.0)** zu **None (N/A), Binary (1.0), Binary (1.0)**, und klicken Sie auf **Aktivieren**, um sie zu aktivieren.

Den Hub für angepasste XML-Dokumente konfigurieren

Wie in „Angepasste XML-Dokumente” auf Seite 89 beschrieben, müssen Sie den Hub konfigurieren, damit er angepasste XML-Dateien weiterleiten kann.Dieser Abschnitt behandelt die erforderlichen Schritte, um Document Manager zum Weiterleiten der folgenden XML-Dokumente zu konfigurieren:

```
<?xml version="1.0" encoding="UTF-8"?>
       <!DOCTYPE Tester>
         <Tester>
        <From>987654321</From>
       <To>123456789</To>
   </Tester>
```

Document Manager gibt mit **RootTag** den Typ des XML-Dokuments an. Dann extrahiert er die Werte aus den **From**- und **To**-Tags, um die Namen von **Absenderteilnehmer** und **Zielteilnehmer** anzugeben.

Das Protokolldefinitionsformat für angepasstes XML erstellen

Der erste Schritt besteht darin, ein neues Protokoll für das angepasste XML zu erstellen, das Sie austauschen werden.

1. Klicken Sie auf **Hubadmin > Hubkonfiguration > Dokumentenflussdefinition**.
2. Klicken Sie auf **Dokumentenflussdefinition erstellen**.
3. Wählen Sie **Protokoll** in der Liste **Dokumentenflusstyp** aus.
4. Geben Sie die folgenden Informationen ein:
   a. Code: **CustomXML**
   b. Version: **1.0**
   c. Beschreibung: **CustomXML**
5. Setzen Sie **Dokumentebene** auf **Nein**.
6. Setzen Sie **Status** auf **Aktiviert**.
7. Setzen Sie **Sichtbarkeit: Community Operator** auf **Ja**.
8. Setzen Sie **Sichtbarkeit: Community Manager** auf **Ja**.
9. Setzen Sie **Sichtbarkeit: Community-Teilnehmer** auf **Ja**.
10. Wählen Sie Folgendes aus:
    a. Paket: **AS**
    b. Paket: **None**
    c. Paket: **Backend Integration**.
11. Klicken Sie auf **Speichern**.

Die Dokumentendefinition ″Tester_XML″ erstellen

Der zweite Schritt besteht darin, eine Dokumentenflussdefinition für das neue Protokoll zu erstellen.

1. Klicken Sie auf **Hubadmin > Hubkonfiguration > Dokumentenflussdefinition**.
2. Klicken Sie auf **Dokumentenflussdefinition erstellen**.
3. Wählen Sie **Dokumentenfluss** in der Liste **Dokumentenflusstyp** aus.
4. Geben Sie die folgenden Informationen ein:
   a. Code: **XML_Tester**
   b. Version: **1.0**
   c. Beschreibung: **XML_Tester**
5. Setzen Sie **Dokumentebene** auf **Ja**.

6. Setzen Sie **Status** auf **Aktiviert**.
7. Setzen Sie **Sichtbarkeit: Community Operator** auf **Ja**.
8. Setzen Sie **Sichtbarkeit: Community Manager** auf **Ja**.
9. Setzen Sie **Sichtbarkeit: Community-Teilnehmer** auf **Ja**.
10. Klicken Sie auf das Symbol **Erweitern** neben **Paket: AS**, und wählen Sie **Protokoll: CustomXML** aus.
11. Klicken Sie auf das Symbol **Erweitern** neben **Paket: None**, und wählen Sie **Protokoll: CustomXML** aus.
12. Klicken Sie auf das Symbol **Erweitern** neben **Paket: Backend Integration**, und wählen Sie **Protokoll: CustomXML** aus.
13. Klicken Sie auf **Speichern**.

Das XML-Format ″Tester_XML″ erstellen

Schließlich erstellen Sie das XML-Format, das dem neuen Protokoll zugeordnet ist.

1. Klicken Sie auf **Hubadmin > Hubkonfiguration > XML-Formate**.
2. Klicken Sie auf **XML-Format erstellen**.
3. Wählen Sie **CustomXML 1.0** in der Liste **Routing-Format** aus.
4. Wählen Sie **XML** in der Liste **Dateityp** aus.
5. Wählen Sie **Root-Tag** in der Liste **Kennungstyp** aus, und geben Sie als Wert **Tester** ein.
6. Wählen Sie **Elementpfad** in der Liste **Quellengeschäfts-ID** aus, und geben Sie als Wert **/Tester/From** ein.
7. Wählen Sie **Elementpfad** in der Liste **Zielgeschäfts-ID** aus, und geben Sie als Wert **/Tester/To** ein.
8. Wählen Sie **Konstante** in der Liste **Quellendokumentenfluss** aus, und geben Sie als Wert **XML_Tester** ein.
9. Wählen Sie **Konstante** in der Liste **Quellendokumentenflussversion** aus, und geben Sie als Wert **1.0** ein.
10. Klicken Sie auf **Speichern**.

Interaktion für XML-Dokumente von ″XML_Tester″ erstellen

Sie verfügen nun über ein neues Protokoll und einen Dokumentenfluss, mit dem Sie eine Interaktion definieren können.

1. Klicken Sie auf **Hubadmin > Hubkonfiguration > Dokumentenflussdefinition**.
2. Klicken Sie auf **Interaktionen verwalten**.
3. Klicken Sie auf **Interaktion erstellen**.
4. Wählen Sie in der Liste **Quelle** Folgendes aus:
   a. Paket: **None**
   b. Protokoll: **CustomXML (1.0)**
   c. Dokumentenfluss: **XML_Tester (1.0)**.
5. Wählen Sie in der Liste **Ziel** Folgendes aus:
   a. Paket: **None**
   b. Protokoll: **CustomXML (1.0)**
   c. Dokumentenfluss: **XML_Tester (1.0)**.
6. Wählen Sie in der Liste **Aktion** die Option **Pass-Through** aus.
7. Klicken Sie auf **Speichern**.

Die B2B-Funktionalität für Community Manager aktualisieren

Um den Austausch des angepassten XML-Dokuments zu aktivieren, müssen Sie die B2B-Funktionalität der Teilnehmer aktualisieren.

1. Klicken Sie auf **Kontenadmin > Profile > Community-Teilnehmer**.
2. Klicken Sie auf **Suchen**.
3. Klicken Sie auf das Symbol **Details anzeigen** neben **Comm Man**.
4. Klicken Sie auf **B2B-Funktionalität**.
5. Klicken Sie zum Aktivieren auf das Symbol **Rolle ist nicht aktiv** unter **Ziel festlegen** für **Paket: None**.
6. Klicken Sie auf das Symbol **Erweitern** neben **Paket: None**.
7. Klicken Sie auf das Symbol **Rolle ist nicht aktiv** für **Protokoll: CustomXML (1.0)** unter **Ziel festlegen**.
8. Klicken Sie auf das Symbol **Erweitern** neben **Protokoll: CustomXML (1.0)**.
9. Klicken Sie schließlich auf das Symbol **Rolle ist nicht aktiv** für **Dokumentenfluss: XML_Tester (1.0)** unter **Ziel festlegen**.

Die B2B-Funktionalität für "partnerZwei" aktualisieren

Sie aktualisieren die B2B-Funktionalität von **Partner Zwei**, um den Austausch des neuen angepassten XML-Formats zu ermöglichen.

1. Klicken Sie auf **Kontenadmin > Profile > Community-Teilnehmer**.
2. Klicken Sie auf **Suchen**.
3. Klicken Sie auf das Symbol **Details anzeigen** neben **Partner Zwei**.
4. Klicken Sie auf **B2B-Funktionalität**.
5. Klicken Sie zum Aktivieren auf das Symbol **Rolle ist nicht aktiv** unter **Quelle festlegen** für **Paket: None**.
6. Klicken Sie auf das Symbol **Erweitern** neben **Paket: None**.
7. Klicken Sie auf das Symbol **Rolle ist nicht aktiv** für **Protokoll: CustomXML (1.0)** unter **Quelle festlegen**.
8. Klicken Sie auf das Symbol **Erweitern** neben **Protokoll: CustomXML (1.0)**.
9. Klicken Sie schließlich auf das Symbol **Rolle ist nicht aktiv** für **Dokumentenfluss: XML_Tester (1.0)** unter **Quelle festlegen**.

Neue Teilnehmerverbindung erstellen

Erstellen Sie schließlich eine neue Teilnehmerverbindung.

1. Klicken Sie auf **Kontenadmin > Teilnehmerverbindungen**.
2. Wählen Sie **Partner Zwei** in der Liste **Quelle** aus.
3. Wählen Sie **Comm Man** in der Liste **Ziel** aus.
4. Klicken Sie auf **Suchen**.
5. Suchen Sie die Verbindung **None (N/A), CustomXML (1.0), XML_Tester (1.0)** zu **None (N/A), CustomXML(1.0), XML_Tester (1.0)**, und klicken Sie zum Aktivieren auf **Aktivieren**.

Anhang B. EDI-Beispiele

Dieser Anhang enthält Beispiele für das Senden und Empfangen von EDI-Austauschvorgängen und deren Transformation in und von XML-Dokumenten und satzorientierten Datendokumenten (ROD).

Die Beispiele in diesem Anhang unterscheiden sich von denen in Anhang A, „Grundlegende Beispiele", auf Seite 193. Für die Beispiele in diesem Anhang werden neue Ziele, Gateways und Profile erstellt.

Anmerkung: Ein Beispiel eines EDI-Austauschs, der durch den Hub ohne Entfernen von Umschlägen oder Transformation weitergeleitet wird, finden Sie in Anhang A, „Grundlegende Beispiele".

Jedes dieser vier Beispiele ist in sich abgeschlossen. Wenn Sie z. B. dem Beispiel für EDI zu XML folgen, werden Sie alle Schritte vom Erstellen der Ziele bis zum Aktivieren von Verbindungen für dieses Beispiel finden.

Dieser Anhang behandelt die folgenden Themen:

- „Beispiel: EDI zu ROD"
- „Beispiel: EDI zu XML" auf Seite 225
- „Beispiel: XML zu EDI" auf Seite 230
- „Beispiel: ROD zu EDI" auf Seite 237

Diese Beispiele sollen Ihnen eine schnelle Übersicht über die Schritte geben, die zum Konfigurieren eines Systems erforderlich sind. Wenn Sie diese Beispiele verwenden, um Ihr System zu konfigurieren, ändern Sie die spezifischen Informationen, z. B. die Namen und Geschäfts-IDs, um sie Ihren Geschäftsbedürfnissen anzupassen.

Beispiel: EDI zu ROD

Dieser Abschnitt enthält ein Beispiel für das Senden einer EDI-Transaktion in einem Umschlag an den Hub, auf dem sie in ein satzorientiertes Datendokument (ROD-Dokument) transformiert und an Community Manager gesendet wird.

Umschlag vom EDI-Austausch entfernen und EDI-Austausch transformieren

In diesem Beispiel wird davon ausgegangen, dass der Zuordnungsexperte von Data Interchange Services eine Transformationszuordnung erstellt hat, die eine EDI-850-Standardtransaktion, welche mit dem Wörterbuch X12V5R1 definiert ist und der Version 5010 von X12 entspricht, nimmt und diese in ein ROD-Dokument transformiert, das von der Back-End-Anwendung von Community Manager verarbeitet wird. In diesem Beispiel heißt die Zuordnung S_DT_EDI_TO_ROD.eif.

Der Zuordnungsexperte von Data Interchange Services kann die Transformationszuordnung direkt in die WebSphere Partner Gateway-Datenbank exportieren. Alternativ hierzu kann der Zuordnungsexperte von Data Interchange Services Ihnen die Datei senden, in dem Fall verwenden Sie das Dienstprogramm bcgDISImport, um die Datei in WebSphere Partner Gateway zu importieren. Dieser Anhang geht vom zweiten Szenario aus.

Die Transformationszuordnung importieren

Dieser Abschnitt beschreibt die Schritte, die Sie beim Importieren einer Transformationszuordnung ausführen, die die EDI-Eingabe nimmt und diese in ein ROD-Format transformiert. Beim Importieren der Transformationszuordnung können Sie auch die Dokumentdefinition importieren, die der Zuordnung zugeordnet ist.

Bevor Sie die Transformationszuordnung importieren können, muss der Zuordnungsexperte von Data Interchange Services Ihnen diese zusenden. Diese Gruppe von Schritten geht davon aus, dass sich die Datei `S_DT_EDI_TO_ROD.eif` auf Ihrem System befindet.

1. Öffnen Sie ein Befehlsfenster.
2. Geben Sie den folgenden Befehl bzw. das folgende Script ein:
   - Auf einem UNIX-System:

     ```
     <Produktverz>/bin/bcgDISImport.sh <datenbankbenutzer-ID>
     <kennwort> S_DT_EDI_TO_ROD.eif
     ```

   - Auf einem Windows-System:

     ```
     <Produktverz>\bin\bcgDISImport.bat <datenbankbenutzer-ID>
     <kennwort> S_DT_EDI_TO_ROD.eif
     ```

     Dabei gilt Folgendes: *<datenbankbenutzer-ID>* und *<kennwort>* sind die Werte, die Sie verwendet haben, als Sie die Datenbank als Teil der WebSphere Partner Gateway-Installation installiert haben.

Die Transformationszuordnung und Dokumentenflussdefinitionen prüfen

Führen Sie die folgenden Schritte aus, um zu prüfen, ob die Transformationszuordnungen und Dokumentdefinitionen, die Sie importiert haben, in Community Console verfügbar sind:

1. Klicken Sie auf **Hubadmin > Hubkonfiguration > Zuordnungen > Transformationszuordnungen**.

   Die Zuordnung S_DT_EDI_TO_ROD wird angezeigt.
2. Klicken Sie auf das Symbol **Details anzeigen** neben der Zuordnung.

   Die Dokumentenflussdefinitionen, denen diese Zuordnung zugeordnet ist:

Tabelle 19. Dokumentenflussdefinition, die der Zuordnung zugeordnet ist

Quelle	Ziel
Paket: N/A Protokoll: X12V5R1 (ALL) Dokumentenfluss: 850 (ALL)	Paket: None Protokoll: DEMO850CL_DICTIONARY (ALL) Dokumentenfluss: DEMO850CLSUW (ALL)

Die Zuordnung S_DT_EDI_TO_ROD wurde definiert, um eine X12-850-Transaktion zu nehmen, die mit dem X12V5R1-Standard konform ist, und sie in ein angepasstes Protokoll (DEMO850CL_DICTIONARY) und einen Dokumentenfluss (DEMO850CLSUW) transformiert.

Das Ziel konfigurieren

In diesem Abschnitt erstellen Sie ein Dateisystemverzeichnisziel für den Hub:

1. Klicken Sie auf **Hubadmin > Hubkonfiguration > Ziele**, und klicken Sie dann auf **Ziel erstellen**.
2. Geben Sie als **Zielname** den Namen `EDIDateiziel` ein.
3. Wählen Sie in der Liste **Transport** die Option **Dateiverzeichnis** aus.
4. Geben Sie als Stammverzeichnispfad **/Data/Manager/editarget** ein.

5. Klicken Sie auf **Speichern**.

Der Community-Teilnehmer sendet den EDI-Austausch an dieses Ziel.

Die Interaktionen erstellen

Sie erstellen zwei Interaktionen: eine für den EDI-Umschlag und eine für die Transaktion im EDI-Umschlag.

Erstellen Sie eine Interaktion, die den EDI-Umschlag darstellt.

1. Klicken Sie auf **Hubadmin > Hubkonfiguration > Dokumentenfluss-definition**.
2. Klicken Sie auf **Interaktionen verwalten** und dann auf **Interaktion erstellen**.
3. Erweitern Sie unter **Quelle** den Eintrag **Paket: None** und **Protokoll: EDI-X12**, und wählen Sie **Dokumentenfluss: ISA** aus.
4. Erweitern Sie unter **Ziel** den Eintrag **Paket: N/A** und **Protokoll: EDI-X12**, und wählen Sie **Dokumentenfluss: ISA** aus.
5. Wählen Sie in der Liste **Aktion** die Option **EDI - Umschlag entfernen** aus.

   Anmerkung: In dieser Interaktion findet keine Transformation statt. Vom EDI-Austausch wird der Umschlag entfernt, wodurch die einzelne Transaktion (850) entsteht. Sie benötigen daher keine Transformationszuordnung für diese Interaktion.
6. Klicken Sie auf **Speichern**.

Erstellen Sie eine Interaktion, die über eine Quelle verfügt, die die 850-Transaktion darstellt, und ein Ziel, das das transformierte Dokument darstellt.

1. Klicken Sie auf **Hubadmin > Hubkonfiguration > Dokumentenfluss-definition**.
2. Klicken Sie auf **Interaktionen verwalten** und dann auf **Interaktion erstellen**.
3. Erweitern Sie unter **Quelle** den Eintrag **Paket: N/A** und **Protokoll: X12V5R1**, und wählen Sie **Dokumentenfluss: 850** aus.
4. Erweitern Sie unter **Ziel** den Eintrag **Paket: None** und **Protokoll: DEMO850CL_DICTIONARY**, und wählen Sie **Dokumentenfluss: DEMO850CLSUW** aus.
5. Wählen Sie in der Liste **Transformationszuordnung** den Eintrag **S_DT_EDI-_TO_ROD** aus.
6. Wählen Sie in der Liste **Aktion** die Option **EDI validieren und EDI konvertieren** aus.
7. Klicken Sie auf **Speichern**.

Diese Interaktion stellt die Transformation einer EDI-X12-850-Standardtransaktion in ein anderes Format dar, und daher müssen Sie eine Transformationszuordnung auswählen.

Die Teilnehmer erstellen

Sie haben für dieses Beispiel zwei Teilnehmer: Community Manager (Manager) und einen Teilnehmer (TP1).

Erstellen Sie das Profil **Community Manager**:

1. Klicken Sie auf **Kontenadmin > Profile > Community-Teilnehmer**, und klicken Sie auf **Erstellen**.
2. Geben Sie als **Anmeldename des Unternehmens** Folgendes ein: **ComManager**.

3. Geben Sie als **Anzeigename des Teilnehmers** Folgendes ein: **Manager**.
4. Wählen Sie als **Teilnehmertyp** Folgendes aus: **Community Manager**.
5. Klicken Sie auf **Neu** für die Geschäfts-ID, und geben Sie `000000000` als unformatierte ID ein.

   Anmerkung: Stellen Sie sicher, dass Sie **Unformatiert** und nicht **DUNS** ausgewählt haben.
6. Klicken Sie erneut auf **Neu** für die Geschäfts-ID, und geben Sie `01-000000000` als unformatierte ID ein.
7. Klicken Sie auf **Speichern**.

Erstellen Sie den zweiten Teilnehmer:

1. Klicken Sie auf **Kontenadmin > Profile > Community-Teilnehmer**, und klicken Sie auf **Erstellen**.
2. Geben Sie als **Anmeldename des Unternehmens** Folgendes ein: **TP1**.
3. Geben Sie als **Anzeigename des Teilnehmers** Folgendes ein, **TP1**.
4. Wählen Sie als **Teilnehmertyp** Folgendes aus: **Community-Teilnehmer**.
5. Klicken Sie auf **Neu** für die Geschäfts-ID, und geben Sie `000000001` als unformatierte ID ein.

   Anmerkung: Stellen Sie sicher, dass Sie **Unformatiert** und nicht **DUNS** ausgewählt haben.
6. Klicken Sie erneut auf **Neu** für die Geschäfts-ID, und geben Sie `01-000000001` als unformatierte ID ein.
7. Klicken Sie auf **Speichern**.

Die Gateways erstellen

Erstellen Sie Dateiverzeichnisgateways für beide Teilnehmer im Beispiel. Erstellen Sie zuerst ein Gateway für den Manager.

1. Klicken Sie auf **Kontenadmin > Profile > Community-Teilnehmer**, und klicken Sie auf **Suchen**.
2. Klicken Sie auf das Symbol **Details anzeigen** neben dem Profil **Manager**.
3. Klicken Sie auf **Gateways** und dann auf **Erstellen**.
4. Geben Sie die folgenden Werte für das Gateway ein. Denken Sie daran, dass das Dateiverzeichnis (der vollständige Pfad) schon auf Ihrem Dateisystem vorhanden sein muss.
   a. Geben Sie als Name **Managerdateigateway** ein.
   b. Wählen Sie in der Liste **Transport** die Option **Dateiverzeichnis** aus.
   c. Geben Sie als **Adresse** Folgendes ein: **file:///Data/Manager/filegateway**
   d. Klicken Sie auf **Speichern**.
5. Klicken Sie auf **Liste**, um alle Gateways für Community Manager aufzulisten.
6. Klicken Sie auf **Standardgateways anzeigen**.
7. Wählen Sie in der Liste **Produktion** das Gateway aus, das Sie in Schritt 4 erstellt haben.
8. Klicken Sie auf **Speichern**.

Erstellen Sie als Nächstes ein Gateway für den Teilnehmer.

1. Klicken Sie auf **Kontenadmin > Profile > Community-Teilnehmer**, und klicken Sie auf **Suchen**.

2. Wählen Sie den anderen Teilnehmer aus, den Sie für dieses Beispiel erstellt haben, indem Sie auf das Symbol **Details anzeigen** neben **TP1** klicken.
3. Klicken Sie auf **Gateways** und dann auf **Erstellen**.
4. Geben Sie die folgenden Werte für das Gateway ein. Denken Sie daran, dass das Dateiverzeichnis (der vollständige Pfad) schon vorhanden sein muss.
   a. Geben Sie als Name **TP1Dateigateway** ein.
   b. Wählen Sie in der Liste **Transport** die Option **Dateiverzeichnis** aus.
   c. Geben Sie als **Adresse** Folgendes ein: **file:///Data/TP1/filegateway**
   d. Klicken Sie auf **Speichern**.
5. Klicken Sie auf **Liste**, um alle Gateways für den Teilnehmer aufzulisten.
6. Klicken Sie auf **Standardgateways anzeigen**.
7. Wählen Sie in der Liste **Produktion** das Gateway aus, das Sie in Schritt 4 erstellt haben.
8. Klicken Sie auf **Speichern**.

B2B-Funktionalität konfigurieren

Aktivieren Sie die B2B-Funktionalität der zwei Teilnehmer in diesem Austausch. In diesem Beispiel stammt der EDI-Austausch vom Community-Teilnehmer (TP1) und wird Community Manager zugestellt.

1. Klicken Sie auf **Kontenadmin > Profile > Community-Teilnehmer**, und klicken Sie auf **Suchen**.
2. Klicken Sie auf das Symbol **Details anzeigen** für den Quellenteilnehmer dieses Beispiels (**TP1**).
3. Klicken Sie auf **B2B-Funktionalität**.
4. Aktivieren Sie zwei Funktionalitätsgruppen für den Quellenteilnehmer.
   a. Aktivieren Sie zuerst die Dokumentenflussdefinition, die den EDI-Umschlag darstellt:
      1) Klicken Sie zum Aktivieren auf das Symbol **Rolle ist nicht aktiv** unter **Quelle festlegen** für **Paket: None**.
      2) Erweitern Sie **Paket: None**.
      3) Klicken Sie auf das Symbol **Rolle ist nicht aktiv** unter **Quelle festlegen** für **Protokoll: EDI-X12 (ALL)**.
      4) Erweitern Sie **Protokoll: EDI-X12 (ALL)**.
      5) Klicken Sie auf das Symbol **Rolle ist nicht aktiv** unter **Quelle festlegen** für **Dokumentenfluss: ISA (ALL)**.
   b. Aktivieren Sie danach die Dokumentenflussdefinition, die die 850-Transaktion darstellt:
      1) Klicken Sie zum Aktivieren auf das Symbol **Rolle ist nicht aktiv** unter **Quelle festlegen** für **Paket: N/A**.
      2) Erweitern Sie **Paket: N/A**.
      3) Klicken Sie auf das Symbol **Rolle ist nicht aktiv** unter **Quelle festlegen** für **Protokoll: X12V5R1 (ALL)**.
      4) Erweitern Sie **Protokoll: X12V5R1 (ALL)**.
      5) Klicken Sie auf das Symbol **Rolle ist nicht aktiv** unter **Quelle festlegen** für **Dokumentenfluss: 850**.
5. Klicken Sie auf **Kontenadmin > Profile > Community-Teilnehmer**, und klicken Sie auf **Suchen**.
6. Klicken Sie auf das Symbol **Details anzeigen** für den Zielteilnehmer dieses Beispiels (**Manager**).

7. Klicken Sie auf **B2B-Funktionalität**.
8. Aktivieren Sie zwei Funktionalitätsgruppen für den Zielteilnehmer.
   a. Aktivieren Sie zuerst die Dokumentenflussdefinition, die den Umschlag darstellt:
      1) Klicken Sie zum Aktivieren auf das Symbol **Rolle ist nicht aktiv** unter **Ziel festlegen** für **Paket: N/A**.
      2) Erweitern Sie **Paket: N/A**.
      3) Klicken Sie auf das Symbol **Rolle ist nicht aktiv** unter **Ziel festlegen** für **Protokoll: EDI-X12 (ALL)**.
      4) Erweitern Sie **Protokoll: EDI-X12 (ALL)**.
      5) Klicken Sie auf das Symbol **Rolle ist nicht aktiv** unter **Ziel festlegen** für **Dokumentenfluss: ISA (ALL)**.
   b. Aktivieren Sie als Nächstes die Dokumentenflussdefinition, die das transformierte Dokument darstellt:
      1) Klicken Sie zum Aktivieren auf das Symbol **Rolle ist nicht aktiv** unter **Ziel festlegen** für **Paket: None**.
      2) Erweitern Sie **Paket: None**.
      3) Klicken Sie auf das Symbol **Rolle ist nicht aktiv** unter **Ziel festlegen** für **Protokoll: DEMO850CL_DICTIONARY (ALL)**.
      4) Erweitern Sie **Protokoll: DEMO850CL_DICTIONARY (ALL)**.
      5) Klicken Sie auf das Symbol **Rolle ist nicht aktiv** unter **Ziel festlegen** für **Dokumentenfluss: DEMO850CLSUW (ALL)**.

Die Verbindungen aktivieren

Gehen Sie wie folgt vor, um die Verbindungen zu aktivieren:

1. Klicken Sie auf **Kontenadmin > Teilnehmerverbindungen**.
2. Wählen Sie **TP1** in der Liste **Quelle** aus.
3. Wählen Sie **Manager** in der Liste **Ziel** aus.
4. Klicken Sie auf **Suchen**.
5. Klicken Sie auf **Aktivieren** für die Verbindung, die den Umschlag darstellt:

Tabelle 20. Verbindung für Umschlag

Quelle	Ziel
Paket: None (N/A) Protokoll: EDI-X12 (ALL) Dokumentenfluss: ISA (ALL)	Paket: N/A (N/A) Protokoll: EDI-X12 (ALL) Dokumentenfluss: ISA (ALL)

6. Klicken Sie auf **Aktivieren** für die Verbindung, die die 850-Transaktion darstellt, zum transformierten Dokument:

Tabelle 21. Verbindung für EDI-Transaktion zu ROD-Dokument

Quelle	Ziel
Paket: N/A (N/A) Protokoll: X12V5R1 Dokumentenfluss: 850 (ALL)	Paket: None (N/A) Protokoll: DEMO850CL_DICTIONARY (ALL) Dokumentenfluss: DEMO850CLSUW (ALL)

Attribute hinzufügen

Legen Sie das Attribut fest, das Dokumente mit doppelten IDs zulässt:

1. Klicken Sie auf **Hubadmin > Hubkonfiguration > Dokumentenflussdefinition**.

2. Klicken Sie auf das Symbol **Erweitern** neben **Paket: None**.
3. Klicken Sie auf das Symbol **Attributwerte bearbeiten** neben **Protokoll: EDI-X12**.
4. Blättern Sie auf der Seite bis zum Abschnitt **Attribute für Dokumentenflusskontexte** vor. Wählen Sie in der Zeile **Dokumente mit doppelten Dokument-IDs zulassen** die Option **Ja** in der Liste aus.
5. Klicken Sie auf **Speichern**.

Wenn an dieser Stelle TP1 einen EDI-Austausch mit einer 850-Transaktion an Community Manager gesendet hat, würde vom EDI-Austausch der Umschlag entfernt werden, wodurch eine 850-Transaktion entstände. Die 850-Transaktion würde dann in den Dokumenttyp DEMO850CLSUW transformiert werden und das transformierte Dokument würde an das Gateway von Community Manager gesendet werden.

Dem Austausch TA1 hinzufügen

In X12 ist TA1 ein optionales Segment, mit dem der Empfang eines Austauschs bestätigt werden kann. Der Absender kann TA1 vom Empfänger anfordern, indem er das Element 14 des ISA-Austauschkontrollheaders mit **1** festlegt. Mit dem Attribut **TA1-Anforderung zulassen** können Sie in WebSphere Partner Gateway steuern, ob TA1 gesendet wird, wenn der Absender dies anfordert.

Die Zuordnung &WDI_TA1_ACK wird während der Installation von WebSphere Partner Gateway installiert, so dass Sie diese nicht importieren müssen.

Die Assoziationen erstellen

Führen Sie die folgenden Schritte aus, um die Zuordnung einer Dokumentenflussdefinition zuzuordnen:

1. Klicken Sie auf **Hubadmin > Hubkonfiguration > Zuordnungen > EDI FA-Zuordnungen**.

   Die Zuordnung &WDI_TA1_ACK wird angezeigt.
2. Klicken Sie auf das Symbol **Details anzeigen** neben der Zuordnung.

   Es werden Informationen zur Zuordnung wie auch ein Ordner für jeden Pakettyp, der auf dem System verfügbar ist, angezeigt.
3. Erstellen Sie die Assoziation zur Dokumentenflussdefinition, indem Sie diese Schritte ausführen:
   a. Wählen Sie das Markierungsfeld neben **Paket: None** aus, und erweitern Sie den Ordner.
   b. Wählen Sie das Markierungsfeld neben **Protokoll: EDI-X12 (ALL)** aus, und erweitern Sie den Ordner.
   c. Wählen Sie das Markierungsfeld neben **Dokumentenfluss: ISA (ALL)** aus.
   d. Klicken Sie auf **Speichern**.

Sie haben eine Assoziation zwischen der Zuordnung &WDI_TA1_ACK1 und der Dokumentenflussdefinition für den Umschlag erstellt.

Interaktionen erstellen

Erstellen Sie eine Interaktion, die die TA1-Transaktion darstellt.

1. Klicken Sie auf **Hubadmin > Hubkonfiguration > Dokumentenflussdefinition**.
2. Klicken Sie auf **Interaktionen verwalten** und dann auf **Interaktion erstellen**.

3. Erweitern Sie unter **Quelle** den Eintrag **Paket: N/A** und **Protokoll: &X44TA1**, und wählen Sie **Dokumentenfluss: TA1** aus.
4. Erweitern Sie unter **Ziel** den Eintrag **Paket: N/A** und **Protokoll: &X44TA1**, und wählen Sie **Dokumentenfluss: TA1** aus.
5. Wählen Sie in der Liste **Aktion** die Option **Pass-Through** aus.
6. Klicken Sie auf **Speichern**.

Erstellen Sie eine Interaktion mit einer Quelle, die den EDI-Umschlag darstellt, in dem TA1 enthalten sein wird.

1. Klicken Sie auf **Hubadmin > Hubkonfiguration > Dokumentenfluss-definition**.
2. Klicken Sie auf **Interaktionen verwalten** und dann auf **Interaktion erstellen**.
3. Erweitern Sie unter **Quelle** den Eintrag **Paket: N/A** und **Protokoll: EDI-X12**, und wählen Sie **Dokumentenfluss: ISA** aus.
4. Erweitern Sie unter **Ziel** den Eintrag **Paket: None** und **Protokoll: EDI-X12**, und wählen Sie **Dokumentenfluss: ISA** aus.
5. Wählen Sie in der Liste **Aktion** die Option **Pass-Through** aus.
6. Klicken Sie auf **Speichern**.

B2B-Funktionalität aktivieren

Fügen Sie als Nächstes die neu erstellten Interaktionen der B2B-Funktionalität von den Teilnehmern hinzu.

1. Klicken Sie auf **Kontenadmin > Profile > Community-Teilnehmer**, und klicken Sie auf **Suchen**.
2. Klicken Sie auf das Symbol **Details anzeigen** für den Quellenteilnehmer dieses Beispiels (**Manager**).

   Anmerkung: Denken Sie daran, dass die TA1 vom Teilnehmer, der das ROD-Dokument empfängt, zum Teilnehmer fließt, der sie gesendet hat. In diesem Beispiel ist der Manager die Quelle der TA1 und der Teilnehmer TP1 ist das Ziel.
3. Klicken Sie auf **B2B-Funktionalität**.
4. Aktivieren Sie zwei Funktionalitätsgruppen für den Quellenteilnehmer.
   a. Aktivieren Sie zuerst die Funktion für die TA1.
      1) Klicken Sie zum Aktivieren auf das Symbol **Rolle ist nicht aktiv** unter **Quelle festlegen** für **Paket: N/A**.
      2) Erweitern Sie **Paket: N/A**.
      3) Klicken Sie auf das Symbol **Rolle ist nicht aktiv** unter **Quelle festlegen** für **Protokoll: &X44TA1**.
      4) Erweitern Sie **Protokoll: &X44TA1**.
      5) Klicken Sie auf das Symbol **Rolle ist nicht aktiv** unter **Quelle festlegen** für **Dokumentenfluss: TA1 (ALL)**.
   b. Aktivieren Sie als Nächstes die Funktion für den Umschlag:
      1) Klicken Sie zum Aktivieren auf das Symbol **Rolle ist nicht aktiv** unter **Quelle festlegen** für **Paket: N/A**.
      2) Erweitern Sie **Paket: N/A**.
      3) Klicken Sie auf das Symbol **Rolle ist nicht aktiv** unter **Quelle festlegen** für **Protokoll: EDI-X12**.
      4) Erweitern Sie **Protokoll: EDI-X12 (ALL)**.

5) Klicken Sie auf das Symbol **Rolle ist nicht aktiv** unter **Quelle festlegen** für **Dokumentenfluss: ISA (ALL)**.

5. Klicken Sie auf **Kontenadmin > Profile > Community-Teilnehmer**, und klicken Sie auf **Suchen**.
6. Klicken Sie auf das Symbol **Details anzeigen** für den Zielteilnehmer dieses Beispiels (**TP1**).
7. Klicken Sie auf **B2B-Funktionalität**.
8. Aktivieren Sie zwei Funktionalitätsgruppen für den Zielteilnehmer.
   a. Aktivieren Sie zuerst die Dokumentenflussdefinition, die die TA1 darstellt:
      1) Klicken Sie zum Aktivieren auf das Symbol **Rolle ist nicht aktiv** unter **Ziel festlegen** für **Paket: N/A**.
      2) Erweitern Sie **Paket: N/A**.
      3) Klicken Sie auf das Symbol **Rolle ist nicht aktiv** unter **Ziel festlegen** für **Protokoll: &X44TA1 (ALL)**.
      4) Erweitern Sie **Protokoll: &X44TA1 (ALL)**.
      5) Klicken Sie auf das Symbol **Rolle ist nicht aktiv** unter **Ziel festlegen** für **Dokumentenfluss: TA1 (ALL)**.
   b. Aktivieren Sie als Nächstes die Dokumentenflussdefinition, die den EDI-Umschlag darstellt:
      1) Klicken Sie zum Aktivieren auf das Symbol **Rolle ist nicht aktiv** unter **Ziel festlegen** für **Paket: None**.
      2) Erweitern Sie **Paket: None**.
      3) Klicken Sie auf das Symbol **Rolle ist nicht aktiv** unter **Ziel festlegen** für **Protokoll: EDI-X12 (ALL)**.
      4) Erweitern Sie **Protokoll: EDI-X12 (ALL)**.
      5) Klicken Sie auf das Symbol **Rolle ist nicht aktiv** unter **Ziel festlegen** für **Dokumentenfluss: ISA (ALL)**.

Das Umschlagsprofil erstellen

Sie erstellen als Nächstes das Profil für den Umschlag, der die TA1 enthalten wird:

1. Klicken Sie auf **Hubadmin > Hubkonfiguration > EDI > Umschlagsprofil**.
2. Klicken Sie auf **Erstellen**.
3. Geben Sie den Namen des Profils ein: **UmschProf1**.
4. Wählen Sie in der Liste **EDI-Standard** die Option **X12** aus.
5. Die Schaltfläche **Allgemein** ist standardmäßig ausgewählt. Geben Sie die folgenden Werte für die allgemeinen Attribute des Umschlags ein:
   - INTCTLLEN: **9**
   - GRPCTLLEN: **9**
   - TRXCTLLEN: **9**
   - MAXDOCS: **1000**
6. Klicken Sie auf die Schaltfläche **Austausch**, und geben Sie die folgenden Werte für die Austauschattribute ein:
   - ISA01: **01**
   - ISA02: **ISA0000002**
   - ISA03: **02**
   - ISA04: **ISA0000004**
   - ISA11: \
   - ISA12: **00501**
   - ISA15: **T**
7. Klicken Sie auf **Speichern**.

Teilnehmerverbindungen aktivieren

Gehen Sie wie folgt vor, um die Verbindungen zu aktivieren:

1. Klicken Sie auf **Kontenadmin > Teilnehmerverbindungen**.
2. Wählen Sie **Manager** in der Liste **Quelle** aus.
3. Wählen Sie **TP1** in der Liste **Ziel** aus.
4. Klicken Sie auf **Suchen**.
5. Aktivieren Sie die Verbindung, die die TA1 darstellt.

Tabelle 22. TA1-Verbindung

Quelle	Ziel
Paket: N/A (N/A) Protokoll: &X44TA1 (ALL) Dokumentenfluss: TA1 (ALL)	Paket: N/A (N/A) Protokoll: &X44TA1 (ALL) Dokumentenfluss: TA1 (ALL)

6. Aktivieren Sie die Verbindung, die den Umschlag darstellt:

Tabelle 23. Verbindung für Umschlag

Quelle	Ziel
Paket: N/A (N/A) Protokoll: EDI-X12 (ALL) Dokumentenfluss: ISA (ALL)	Paket: None (N/A) Protokoll: EDI-X12 (ALL) Dokumentenfluss: ISA (ALL)

Die Attribute konfigurieren

Gehen Sie wie folgt vor, um Attribute für das Umschlagsprofil anzugeben:

1. Klicken Sie auf **Kontenadmin > Profile > Community-Teilnehmer**, und klicken Sie auf **Suchen**.
2. Wählen Sie **TP1** in der Liste aus.
3. Klicken Sie auf **B2B-Funktionalität**.
4. Klicken Sie auf das Symbol **Erweitern** neben **Paket: None**.
5. Klicken Sie auf das Symbol **Bearbeiten** neben **Protokoll: EDI-X12 (ALL)**.
6. Wählen Sie in der Zeile **TA1-Anforderung zulassen** die Option **Ja** aus.
7. Klicken Sie auf **Speichern**.
8. Klicken Sie erneut auf **B2B-Funktionalität**.
9. Klicken Sie auf das Symbol **Erweitern** neben **Paket: N/A**.
10. Klicken Sie auf das Symbol **Bearbeiten** neben **Protokoll: &X44TA1 (ALL)**.
11. Geben Sie die folgenden Attribute an:
    a. Wählen Sie in der Zeile **Umschlagsprofil** den Eintrag **UmschProf1** in der Liste aus.
    b. Geben Sie in der Zeile **Qualifikationsmerkmal für Austausch** den Wert **01** ein.
    c. Geben Sie in der Zeile **Kennung für Austausch** den Wert **000000001** ein.
    d. Geben Sie in der Zeile **Nutzungsanzeiger für Austausch** den Buchstaben **T** ein.
12. Klicken Sie auf **Speichern**.

Mit dieser Aufgabenabfolge haben Sie dem Austausch eine TA1-Bestätigung hinzugefügt. Wenn der Austausch empfangen wird, sendet WebSphere Partner Gateway eine TA1 zurück an den Absender (TP1). Die TA1 wird in einem Umschlag gesendet, der sich nach dem Umschlagsprofil **UmschProf1** richtet.

FA-Zuordnung hinzufügen

Dieser Abschnitt beschreibt, wie Sie eine funktionale Standardbestätigung (997) dem in „Beispiel: EDI zu ROD" auf Seite 211 beschriebenen Dokumentenfluss hinzufügen. Die funktionale Bestätigung bietet dem Absender die Bestätigung, dass die Transaktion empfangen worden ist.

Anmerkung: Dieses Beispiel ähnelt „Dem Austausch TA1 hinzufügen" auf Seite 217. Es bezieht sich jedoch nicht direkt auf das Beispiel. Stattdessen baut es auf den Aufgaben auf, die Sie in „Beispiel: EDI zu ROD" auf Seite 211 ausgeführt haben.

WebSphere Partner Gateway enthält eine Gruppe vorinstallierter Namen für Zuordnungen der funktionalen Bestätigungen, die mit $DT_FA beginnen. Diesem folgt der Name für die funktionale Bestätigungsnachricht sowie die Version und das Release der Nachricht. Version 2 Release 4 der funktionalen Bestätigungsnachricht 997 heißt dementsprechend $DT_997V2R4. Eine Liste mit Zuordnungen, die WebSphere Partner Gateway bereitstellt, finden Sie in „Funktionale Bestätigungen" auf Seite 132.

Die Assoziationen erstellen

Führen Sie die folgenden Schritte aus, um die Zuordnung einer Dokumentenflussdefinition zuzuordnen:

1. Klicken Sie auf **Hubadmin > Hubkonfiguration > Zuordnungen > EDI FA-Zuordnungen**.

   Die Zuordnung &DT_FA997V2R4 wird angezeigt.
2. Klicken Sie auf das Symbol **Details anzeigen** neben der Zuordnung.

   Es werden Informationen zur Zuordnung wie auch ein Ordner für jeden Pakettyp, der auf dem System verfügbar ist, angezeigt.
3. Erstellen Sie die Assoziation zur Dokumentenflussdefinition, indem Sie diese Schritte ausführen:
   a. Wählen Sie das Markierungsfeld neben **Paket: N/V** aus, und erweitern Sie den Ordner.
   b. Wählen Sie das Markierungsfeld neben **Protokoll: X12V5R1** aus, und erweitern Sie den Ordner.
   c. Wählen Sie das Markierungsfeld neben **Dokumentenfluss: 850** aus.
   d. Klicken Sie auf **Speichern**.

Sie haben diese Zuordnung für funktionale Bestätigungen 997 dem X12-Protokoll hinzugefügt.

Interaktionen erstellen

Erstellen Sie eine Interaktion, die die Bestätigung 997 darstellt.

1. Klicken Sie auf **Hubadmin > Hubkonfiguration > Dokumentenflussdefinition**.
2. Klicken Sie auf **Interaktionen verwalten** und dann auf **Interaktion erstellen**.
3. Erweitern Sie unter **Quelle** den Eintrag **Paket: N/A** und **Protokoll: &DT99724**, und wählen Sie **Dokumentenfluss: 997** aus.

4. Erweitern Sie unter **Ziel** den Eintrag **Paket: N/A** und **Protokoll: &DT99724**, und wählen Sie **Dokumentenfluss: 997** aus.
5. Wählen Sie in der Liste **Aktion** die Option **Pass-Through** aus.
6. Klicken Sie auf **Speichern**.

Erstellen Sie eine Interaktion, die den Umschlag darstellt.

1. Klicken Sie auf **Hubadmin > Hubkonfiguration > Dokumentenfluss-definition**.
2. Klicken Sie auf **Interaktionen verwalten** und dann auf **Interaktion erstellen**.
3. Erweitern Sie den Eintrag **Paket: N/A** und **Protokoll: EDI-X12**, und wählen Sie **Dokumentenfluss: ISA** aus.
4. Erweitern Sie den Eintrag **Paket: None** und **Protokoll: EDI-X12**, und wählen Sie **Dokumentenfluss: ISA** aus.
5. Wählen Sie in der Liste **Aktion** die Option **Pass-Through** aus.
6. Klicken Sie auf **Speichern**.

B2B-Funktionalität aktivieren

Fügen Sie als Nächstes die neu erstellten Interaktionen der B2B-Funktionalität von den Teilnehmern hinzu.

1. Klicken Sie auf **Kontenadmin > Profile > Community-Teilnehmer**, und klicken Sie auf **Suchen**.
2. Klicken Sie auf das Symbol **Details anzeigen** für den Quellenteilnehmer dieses Beispiels (**Manager**).

   Anmerkung: Denken Sie daran, dass die funktionale Bestätigung vom Teilnehmer, der das ROD-Dokument empfängt, zum Teilnehmer fließt, der sie gesendet hat. In diesem Beispiel ist der Manager die Quelle der funktionalen Bestätigung und der Teilnehmer TP1 ist das Ziel.
3. Klicken Sie auf **B2B-Funktionalität**.
4. Aktivieren Sie zwei Funktionalitätsgruppen für den Quellenteilnehmer.
   a. Aktivieren Sie zuerst die Funktion für die funktionale Bestätigung.
      1) Klicken Sie zum Aktivieren auf das Symbol **Rolle ist nicht aktiv** unter **Quelle festlegen** für **Paket: N/A**.
      2) Erweitern Sie **Paket: N/A**.
      3) Klicken Sie auf das Symbol **Rolle ist nicht aktiv** unter **Quelle festlegen** für **Protokoll: &DT99724**.
      4) Erweitern Sie **Protokoll: &DT99724**.
      5) Klicken Sie auf das Symbol **Rolle ist nicht aktiv** unter **Quelle festlegen** für **Dokumentenfluss: 997 (ALL)**.
   b. Aktivieren Sie als Nächstes die Funktion für den Umschlag:
      1) Klicken Sie zum Aktivieren auf das Symbol **Rolle ist nicht aktiv** unter **Quelle festlegen** für **Paket: N/A**.
      2) Erweitern Sie **Paket: N/A**.
      3) Klicken Sie auf das Symbol **Rolle ist nicht aktiv** unter **Quelle festlegen** für **Protokoll: EDI-X12**.
      4) Erweitern Sie **Protokoll: EDI-X12 (ALL)**.
      5) Klicken Sie auf das Symbol **Rolle ist nicht aktiv** unter **Quelle festlegen** für **Dokumentenfluss: ISA (ALL)**.
5. Klicken Sie auf **Kontenadmin > Profile > Community-Teilnehmer**, und klicken Sie auf **Suchen**.

6. Klicken Sie auf das Symbol **Details anzeigen** für den Zielteilnehmer dieses Beispiels (**TP1**).
7. Klicken Sie auf **B2B-Funktionalität**.
8. Aktivieren Sie zwei Funktionalitätsgruppen für den Zielteilnehmer.
   a. Aktivieren Sie zuerst die Dokumentenflussdefinition, die funktionale Bestätigung 997 darstellt:
      1) Klicken Sie zum Aktivieren auf das Symbol **Rolle ist nicht aktiv** unter **Ziel festlegen** für **Paket: N/A**.
      2) Erweitern Sie **Paket: N/A**.
      3) Klicken Sie auf das Symbol **Rolle ist nicht aktiv** unter **Ziel festlegen** für **Protokoll: &DT99724 (ALL)**.
      4) Erweitern Sie **Protokoll: &DT99724 (ALL)**.
      5) Klicken Sie auf das Symbol **Rolle ist nicht aktiv** unter **Ziel festlegen** für **Dokumentenfluss: 997 (ALL)**.
   b. Aktivieren Sie als Nächstes die Dokumentenflussdefinition, die den EDI-Umschlag darstellt:
      1) Klicken Sie zum Aktivieren auf das Symbol **Rolle ist nicht aktiv** unter **Ziel festlegen** für **Paket: None**.
      2) Erweitern Sie **Paket: None**.
      3) Klicken Sie auf das Symbol **Rolle ist nicht aktiv** unter **Ziel festlegen** für **Protokoll: EDI-X12 (ALL)**.
      4) Erweitern Sie **Protokoll: EDI-X12 (ALL)**.
      5) Klicken Sie auf das Symbol **Rolle ist nicht aktiv** unter **Ziel festlegen** für **Dokumentenfluss: ISA (ALL)**.

Das Umschlagsprofil erstellen

Sie erstellen als Nächstes das Profil für den Umschlag, der die funktionale Bestätigung 997 enthalten wird: Eine funktionale Bestätigung muss, wie eine Transaktion, mit einem Umschlag versehen werden, bevor sie gesendet werden kann.

1. Klicken Sie auf **Hubadmin > Hubkonfiguration > EDI > Umschlagsprofil**.
2. Klicken Sie auf **Erstellen**.
3. Geben Sie den Namen des Profils ein: **UmschProf1**.
4. Wählen Sie in der Liste **EDI-Standard** die Option **X12** aus.
5. Die Schaltfläche **Allgemein** ist standardmäßig ausgewählt. Geben Sie die folgenden Werte für die allgemeinen Attribute des Umschlags ein:
   - INTCTLLEN: **9**
   - GRPCTLLEN: **9**
   - TRXCTLLEN: **9**
   - MAXDOCS: **1000**
6. Klicken Sie auf die Schaltfläche **Austausch**, und geben Sie die folgenden Werte für die Austauschattribute ein:
   - ISA01: **01**
   - ISA02: **ISA0000002**
   - ISA03: **02**
   - ISA04: **ISA0000004**
   - ISA11: \
   - ISA12: **00501**
   - ISA15: **T**
7. Klicken Sie auf **Speichern**.

Teilnehmerverbindungen aktivieren

Gehen Sie wie folgt vor, um die Verbindungen zu aktivieren:

1. Klicken Sie auf **Kontenadmin > Teilnehmerverbindungen**.
2. Wählen Sie **Manager** in der Liste **Quelle** aus.
3. Wählen Sie **TP1** in der Liste **Ziel** aus.
4. Klicken Sie auf **Suchen**.
5. Klicken Sie auf **Aktivieren** für die Verbindung, die die funktionale Bestätigung 997 darstellt:

Tabelle 24. Verbindung für funktionale Bestätigung

Quelle	Ziel
Paket: N/A (N/A) Protokoll: &DT99724 (ALL) Dokumentenfluss: 997 (ALL)	Paket: N/A (N/A) Protokoll: &DT99724 (ALL) Dokumentenfluss: 997 (ALL)

6. Klicken Sie auf **Aktivieren** für die Verbindung, die den EDI-Umschlag darstellt, der an den Absender des Austauschs zurückgesendet wird:

Tabelle 25. Verbindung für Umschlag

Quelle	Ziel
Paket: N/A (N/A) Protokoll: EDI-X12 (ALL) Dokumentenfluss: ISA (ALL)	Paket: None (N/A) Protokoll: EDI-X12 (ALL) Dokumentenfluss: ISA (ALL)

Attribute konfigurieren

Geben Sie zuerst an, welche FA-Zuordnung verwendet werden soll:

1. Klicken Sie auf **Kontenadmin > Profile > Community-Teilnehmer**, und klicken Sie auf **Suchen**.
2. Wählen Sie **TP1** in der Liste aus.
3. Klicken Sie auf **B2B-Funktionalität**.
4. Klicken Sie auf das Symbol **Erweitern** neben **Paket: N/A**.
5. Klicken Sie auf das Symbol **Bearbeiten** neben **Protokoll: X12V5R1 (ALL)**.
6. Wählen Sie in der Zeile **FA-Zuordnung** die Option **&DT_FA997V2R4** aus.
7. Klicken Sie erneut auf **B2B-Funktionalität**.
8. Klicken Sie auf das Symbol **Erweitern** neben **Paket: N/A**.
9. Klicken Sie auf das Symbol **Bearbeiten** neben **Protokoll: &DT99724 (ALL)**.
10. Geben Sie die folgenden Attribute an:
    a. Wählen Sie in der Zeile **Umschlagsprofil** den Eintrag **UmschProf1** in der Liste aus.
    b. Geben Sie in der Zeile **Qualifikationsmerkmal für Austausch** den Wert **01** ein.
    c. Geben Sie in der Zeile **Kennung für Austausch** den Wert **000000001** ein.
    d. Geben Sie in der Zeile **Nutzungsanzeiger für Austausch** den Buchstaben **T** ein.
11. Klicken Sie auf **Speichern**.

Mit dieser Aufgabenabfolge haben Sie eine funktionale Bestätigung EDI-X12 997 dem Austausch hinzugefügt, so dass, wenn Community Manager das Dokument empfängt, er die funktionale Bestätigung 997 an den Absender (TP1) zurücksendet. Die Bestätigung 997 wird in einem Umschlag gesendet, der sich nach dem Umschlagsprofil **UmschProf1** richtet.

Beispiel: EDI zu XML

Dieser Abschnitt enthält ein Beispiel für das Senden einer EDI-Transaktion in einem Umschlag an den Hub, auf dem sie in ein XML-Dokument transformiert und an Community Manager gesendet wird.

In diesem Beispiel wird davon ausgegangen, dass der Zuordnungsexperte von Data Interchange Services eine Transformationszuordnung erstellt hat, die eine EDI-879-Standardtransaktion (die mit dem Wörterbuch X12V5R1 definiert ist und der Version 5010 von X12 entspricht) nimmt und diese in ein XML-Dokument transformiert, das von der Back-End-Anwendung von Community Manager verarbeitet wird. In diesem Beispiel heißt die Zuordnung S_DT_EDI_TO_XML.eif.

Der Zuordnungsexperte von Data Interchange Services kann die Transformationszuordnung direkt in die WebSphere Partner Gateway-Datenbank exportieren. Alternativ hierzu kann der Zuordnungsexperte von Data Interchange Services Ihnen die Datei senden, in dem Fall verwenden Sie das Dienstprogramm bcgDISImport, um die Datei in WebSphere Partner Gateway zu importieren. Dieser Anhang geht vom zweiten Szenario aus.

Die Transformationszuordnung importieren

Dieser Abschnitt beschreibt die Schritte, die Sie beim Importieren einer Transformationszuordnung ausführen, die die EDI-Eingabe nimmt und diese in ein XML-Format transformiert. Beim Importieren der Transformationszuordnung können Sie auch die Dokumentdefinition importieren, die der Zuordnung zugeordnet ist.

Bevor Sie die Transformationszuordnung importieren können, muss der Zuordnungsexperte von Data Interchange Services Ihnen diese zusenden. Diese Gruppe von Schritten geht davon aus, dass sich die Datei `S_DT_EDI_TO_XML.eif` auf Ihrem System befindet.

1. Öffnen Sie ein Befehlsfenster.
2. Geben Sie den folgenden Befehl bzw. das folgende Script ein:
   - Auf einem UNIX-System:

     ```
     <Produktverz>/bin/bcgDISImport.sh <datenbankbenutzer-ID>
      <kennwort> S_DT_EDI_TO_XML.eif
     ```

   - Auf einem Windows-System:

     ```
     <Produktverz>\bin\bcgDISImport.bat <datenbankbenutzer-ID>
      <kennwort> S_DT_EDI_TO_XML.eif
     ```

     Dabei gilt Folgendes: *<datenbankbenutzer-ID>* und *<kennwort>* sind die Werte, die Sie verwendet haben, als Sie die Datenbank als Teil der WebSphere Partner Gateway-Installation installiert haben.

Die Transformationszuordnung und Dokumentenflussdefinitionen prüfen

Führen Sie die folgenden Schritte aus, um zu prüfen, ob die Transformationszuordnungen und Dokumentdefinitionen, die Sie importiert haben, in Community Console verfügbar sind:

1. Klicken Sie auf **Hubadmin > Hubkonfiguration > Zuordnungen > Transformationszuordnungen**.

   Die Zuordnung S_DT_EDI_TO_XML wird angezeigt.
2. Klicken Sie auf das Symbol **Details anzeigen** neben der Zuordnung.

Die Dokumentenflussdefinitionen, denen diese Zuordnung zugeordnet ist:

Tabelle 26. Dokumentenflussdefinition, die der Zuordnung zugeordnet ist

Quelle	Ziel
Paket: N/A Protokoll: X12V5R1 Dokumentenfluss: 879 (ALL)	Paket: None Protokoll: FVT-XML-TEST (ALL) Dokumentenfluss: WWRE_ITEMCREATIONINTERNAL (ALL)

Die Zuordnung S_DT_EDI_TO_XML wurde definiert, um eine X12-879-Transaktion zu nehmen, die mit dem X12V4R1-Standard konform ist, und sie in ein angepasstes Protokoll transformiert.

Das Ziel konfigurieren

In diesem Abschnitt erstellen Sie ein Dateisystemverzeichnisziel für den Hub:

1. Klicken Sie auf **Hubadmin > Hubkonfiguration > Ziele**, und klicken Sie dann auf **Ziel erstellen**.
2. Geben Sie als **Zielname** den Namen `EDIDateiziel` ein.
3. Wählen Sie in der Liste **Transport** die Option **Dateiverzeichnis** aus.
4. Geben Sie als Stammverzeichnispfad **/Data/Manager/editarget** ein.
5. Klicken Sie auf **Speichern**.

Der Community-Teilnehmer sendet den EDI-Austausch an dieses Ziel.

Die Interaktionen erstellen

Sie erstellen zwei Interaktionen: eine für den EDI-Umschlag und eine für die Transaktion im EDI-Umschlag.

Erstellen Sie eine Interaktion, die den EDI-Umschlag darstellt.

1. Klicken Sie auf **Hubadmin > Hubkonfiguration > Dokumentenflussdefinition**.
2. Klicken Sie auf **Interaktionen verwalten** und dann auf **Interaktion erstellen**.
3. Erweitern Sie den Eintrag **Paket: None** und **Protokoll: EDI-X12**, und wählen Sie **Dokumentenfluss: ISA** aus.
4. Erweitern Sie den Eintrag **Paket: N/A** und **Protokoll: EDI-X12**, und wählen Sie **Dokumentenfluss: ISA** aus.
5. Wählen Sie in der Liste **Aktion** die Option **EDI - Umschlag entfernen** aus.

   Anmerkung: In dieser Interaktion findet keine Transformation statt. Vom EDI-Austausch wird der Umschlag entfernt, wodurch die einzelne Transaktion (879) entsteht. Sie benötigen daher keine Transformationszuordnung für diese Interaktion.
6. Klicken Sie auf **Speichern**.

Erstellen Sie eine Interaktion, die über eine Quelle verfügt, die die 879-Transaktion darstellt, und ein Ziel, das das transformierte Dokument darstellt.

1. Klicken Sie auf **Hubadmin > Hubkonfiguration > Dokumentenflussdefinition**.
2. Klicken Sie auf **Interaktionen verwalten** und dann auf **Interaktion erstellen**.
3. Erweitern Sie den Eintrag **Paket: N/A** und **Protokoll: X12V5R1**, und wählen Sie **Dokumentenfluss: 879** aus.

4. Erweitern Sie den Eintrag **Paket: None** und **Protokoll: FVT-XML-TEST**, und wählen Sie **Dokumentenfluss: WWRE_ITEMCREATIONINTERNAL** aus.
5. Wählen Sie in der Liste **Transformationszuordnung** den Eintrag **S_DT_EDI-_TO_XML** aus.
6. Wählen Sie in der Liste **Aktion** die Option **EDI validieren und EDI konvertieren** aus.
7. Klicken Sie auf **Speichern**.

Diese Interaktion stellt die Transformation einer EDI-X12-879-Standardtransaktion in ein anderes Format dar, und daher müssen Sie eine Transformationszuordnung auswählen.

Die Teilnehmer erstellen

Sie haben für dieses Beispiel zwei Teilnehmer: Community Manager (Manager) und einen Teilnehmer (TP1).

Erstellen Sie das Profil **Community Manager**:

1. Klicken Sie auf **Kontenadmin > Profile > Community-Teilnehmer**, und klicken Sie auf **Erstellen**.
2. Geben Sie als **Anmeldename des Unternehmens** Folgendes ein: **ComManager**.
3. Geben Sie als **Anzeigename des Teilnehmers** Folgendes ein: **Manager**.
4. Wählen Sie als **Teilnehmertyp** Folgendes aus: **Community Manager**.
5. Klicken Sie auf **Neu** für die Geschäfts-ID, und geben Sie `000000000` als unformatierte ID ein.

   Anmerkung: Stellen Sie sicher, dass Sie **Unformatiert** und nicht **DUNS** ausgewählt haben.
6. Klicken Sie erneut auf **Neu** für die Geschäfts-ID, und geben Sie `01-000000000` als unformatierte ID ein.
7. Klicken Sie auf **Speichern**.

Erstellen Sie den zweiten Teilnehmer:

1. Klicken Sie auf **Kontenadmin > Profile > Community-Teilnehmer**, und klicken Sie auf **Erstellen**.
2. Geben Sie als **Anmeldename des Unternehmens** Folgendes ein: **TP1**.
3. Geben Sie als **Anzeigename des Teilnehmers** Folgendes ein, **TP1**.
4. Wählen Sie als **Teilnehmertyp** Folgendes aus: **Community-Teilnehmer**.
5. Klicken Sie auf **Neu** für die Geschäfts-ID, und geben Sie `000000001` als unformatierte ID ein.

   Anmerkung: Stellen Sie sicher, dass Sie **Unformatiert** und nicht **DUNS** ausgewählt haben.
6. Klicken Sie erneut auf **Neu** für die Geschäfts-ID, und geben Sie `01-000000001` als unformatierte ID ein.
7. Klicken Sie auf **Speichern**.

Die Gateways erstellen

Erstellen Sie Dateiverzeichnisgateways für beide Teilnehmer im Beispiel. Erstellen Sie zuerst ein Gateway für den Manager.

1. Klicken Sie auf **Kontenadmin > Profile > Community-Teilnehmer**, und klicken Sie auf **Suchen**.
2. Klicken Sie auf das Symbol **Details anzeigen** neben dem Profil **Manager**.
3. Klicken Sie auf **Gateways** und dann auf **Erstellen**.
4. Geben Sie die folgenden Werte für das Gateway ein. Denken Sie daran, dass das Dateiverzeichnis (der vollständige Pfad) schon auf Ihrem Dateisystem vorhanden sein muss.
   a. Geben Sie als Name **Managerdateigateway** ein.
   b. Wählen Sie in der Liste **Transport** die Option **Dateiverzeichnis** aus.
   c. Geben Sie als **Adresse** Folgendes ein: **file:///Data/Manager/filegateway**
   d. Klicken Sie auf **Speichern**.
5. Klicken Sie auf **Liste**, um alle Gateways für Community Manager aufzulisten.
6. Klicken Sie auf **Standardgateways anzeigen**.
7. Wählen Sie in der Liste **Produktion** das Gateway aus, das Sie in Schritt 4 erstellt haben.
8. Klicken Sie auf **Speichern**.

Erstellen Sie als Nächstes ein Gateway für den Teilnehmer.

1. Klicken Sie auf **Kontenadmin > Profile > Community-Teilnehmer**, und klicken Sie auf **Suchen**.
2. Wählen Sie den anderen Teilnehmer aus, den Sie für dieses Beispiel erstellt haben, indem Sie auf das Symbol **Details anzeigen** neben **TP1** klicken.
3. Klicken Sie auf **Gateways** und dann auf **Erstellen**.
4. Geben Sie die folgenden Werte für das Gateway ein. Denken Sie daran, dass das Dateiverzeichnis (der vollständige Pfad) schon vorhanden sein muss.
   a. Geben Sie als Name **TP1Dateigateway** ein.
   b. Wählen Sie in der Liste **Transport** die Option **Dateiverzeichnis** aus.
   c. Geben Sie als **Adresse** Folgendes ein: **file:///Data/TP1/filegateway**
   d. Klicken Sie auf **Speichern**.
5. Klicken Sie auf **Liste**, um alle Gateways für den Teilnehmer aufzulisten.
6. Klicken Sie auf **Standardgateways anzeigen**.
7. Wählen Sie in der Liste **Produktion** das Gateway aus, das Sie in Schritt 4 erstellt haben.
8. Klicken Sie auf **Speichern**.

B2B-Funktionalität konfigurieren

Aktivieren Sie die B2B-Funktionalität der zwei Teilnehmer in diesem Austausch. In diesem Beispiel stammt der EDI-Austausch vom Community-Teilnehmer (TP1) und wird Community Manager zugestellt.

1. Klicken Sie auf **Kontenadmin > Profile > Community-Teilnehmer**, und klicken Sie auf **Suchen**.
2. Klicken Sie auf das Symbol **Details anzeigen** für den Quellenteilnehmer dieses Beispiels (**TP1**).
3. Klicken Sie auf **B2B-Funktionalität**.
4. Aktivieren Sie zwei Funktionalitätsgruppen für den Quellenteilnehmer.

a. Aktivieren Sie zuerst die Dokumentenflussdefinition, die den EDI-Umschlag darstellt:
   1) Klicken Sie zum Aktivieren auf das Symbol **Rolle ist nicht aktiv** unter **Quelle festlegen** für **Paket: None**.
   2) Erweitern Sie **Paket: None**.
   3) Klicken Sie auf das Symbol **Rolle ist nicht aktiv** unter **Quelle festlegen** für **Protokoll: EDI-X12 (ALL)**.
   4) Erweitern Sie **Protokoll: EDI-X12 (ALL)**.
   5) Klicken Sie auf das Symbol **Rolle ist nicht aktiv** unter **Quelle festlegen** für **Dokumentenfluss: ISA (ALL)**.

b. Aktivieren Sie danach die Dokumentenflussdefinition, die die Transaktion darstellt:
   1) Klicken Sie zum Aktivieren auf das Symbol **Rolle ist nicht aktiv** unter **Quelle festlegen** für **Paket: N/A**.
   2) Erweitern Sie **Paket: N/A**.
   3) Klicken Sie auf das Symbol **Rolle ist nicht aktiv** unter **Quelle festlegen** für **Protokoll: X12V5R1 (ALL)**.
   4) Erweitern Sie **Protokoll: X12V5R1 (ALL)**.
   5) Klicken Sie auf das Symbol **Rolle ist nicht aktiv** unter **Quelle festlegen** für **Dokumentenfluss: 879**.

5. Klicken Sie auf **Kontenadmin > Profile > Community-Teilnehmer**, und klicken Sie auf **Suchen**.
6. Klicken Sie auf das Symbol **Details anzeigen** für den Zielteilnehmer dieses Beispiels (**Manager**).
7. Klicken Sie auf **B2B-Funktionalität**.
8. Aktivieren Sie zwei Funktionalitätsgruppen für den Zielteilnehmer.
   a. Aktivieren Sie zuerst die Dokumentenflussdefinition:
      1) Klicken Sie zum Aktivieren auf das Symbol **Rolle ist nicht aktiv** unter **Ziel festlegen** für **Paket: N/A**.
      2) Erweitern Sie **Paket: N/A**.
      3) Klicken Sie auf das Symbol **Rolle ist nicht aktiv** unter **Ziel festlegen** für **Protokoll: EDI-X12 (ALL)**.
      4) Erweitern Sie **Protokoll: EDI-X12 (ALL)**.
      5) Klicken Sie auf das Symbol **Rolle ist nicht aktiv** unter **Ziel festlegen** für **Dokumentenfluss: ISA (ALL)**.

   b. Aktivieren Sie als Nächstes die Dokumentenflussdefinition, die das transformierte Dokument darstellt:
      1) Klicken Sie zum Aktivieren auf das Symbol **Rolle ist nicht aktiv** unter **Ziel festlegen** für **Paket: None**.
      2) Erweitern Sie **Paket: None**.
      3) Klicken Sie auf das Symbol **Rolle ist nicht aktiv** unter **Ziel festlegen** für **Protokoll: FVT-XML-TEST (ALL)**.
      4) Erweitern Sie **Protokoll: FVT-XML-TEST (ALL)**.
      5) Klicken Sie auf das Symbol **Rolle ist nicht aktiv** unter **Ziel festlegen** für **Dokumentenfluss: WWRE_ITEMCREATIONINTERNAL (ALL)**.

Die Verbindungen aktivieren

Gehen Sie wie folgt vor, um die Verbindungen zu aktivieren:

1. Klicken Sie auf **Kontenadmin > Teilnehmerverbindungen**.
2. Wählen Sie **TP1** in der Liste **Quelle** aus.
3. Wählen Sie **Manager** in der Liste **Ziel** aus.
4. Klicken Sie auf **Suchen**.
5. Klicken Sie auf **Aktivieren** für die Verbindung, die den Umschlag darstellt:

Tabelle 27. Verbindung für Umschlag

Quelle	Ziel
Paket: None (N/A) Protokoll: EDI-X12 (ALL) Dokumentenfluss: ISA (ALL)	Paket: N/A (N/A) Protokoll: EDI-X12 (ALL) Dokumentenfluss: ISA (ALL)

6. Klicken Sie auf **Aktivieren** für die Verbindung, die die 879-Transaktion darstellt, zum transformierten Dokument:

Tabelle 28. Verbindung für EDI-Transaktion zu XML-Dokument

Quelle	Ziel
Paket: N/A (N/A) Protokoll: X12V5R1 (ALL) Dokumentenfluss: 879 (ALL)	Paket: None (N/A) Protokoll: FVT-XML-TEST (ALL) Dokumentenfluss: WWRE_ITEMCREATIONINTERNAL (ALL)

Wenn an dieser Stelle TP1 einen EDI-Austausch mit einer 879-Transaktion an Community Manager gesendet hat, würde vom EDI-Austausch der Umschlag entfernt werden, wodurch eine 879-Transaktion entstände. Die 879-Transaktion würde dann transformiert werden und das transformierte Dokument würde an das Gateway von Community Manager gesendet werden.

Beispiel: XML zu EDI

Dieser Abschnitt enthält ein Beispiel davon, wie Community Manager ein XML-Dokument an den Hub sendet, auf dem es in eine EDI-Transaktion transformiert, in einem EDI-Austausch mit einem Umschlag versehen und an einen Teilnehmer gesendet wird.

In diesem Beispiel wird davon ausgegangen, dass der Zuordnungsexperte von Data Interchange Services eine Transformationszuordnung erstellt hat, die ein XML-Dokument nimmt und dieses in eine EDI-850-Standardtransaktion (die mit dem Wörterbuch MX12V3R1 definiert ist) transformiert, die vom Teilnehmer verarbeitet wird. In diesem Beispiel heißt die Zuordnung S_DT_XML_TO_EDI.eif.

Der Zuordnungsexperte von Data Interchange Services kann die Transformationszuordnung direkt in die WebSphere Partner Gateway-Datenbank exportieren. Alternativ hierzu kann der Zuordnungsexperte von Data Interchange Services Ihnen die Datei senden, in dem Fall verwenden Sie das Dienstprogramm bcgDISImport, um die Datei in WebSphere Partner Gateway zu importieren. Dieser Anhang geht vom zweiten Szenario aus.

Die Transformationszuordnung importieren

Dieser Abschnitt beschreibt die Schritte, die Sie beim Importieren einer Transformationszuordnung ausführen, die die XML-Eingabe nimmt und diese in eine EDI-

Transaktion transformiert. Beim Importieren der Transformationszuordnung können Sie auch die Dokumentdefinition importieren, die der Zuordnung zugeordnet ist.

Bevor Sie die Transformationszuordnung importieren können, muss der Zuordnungsexperte von Data Interchange Services Ihnen diese zusenden. Diese Gruppe von Schritten geht davon aus, dass sich die Datei `S_DT_XML_TO_EDI.eif` auf Ihrem System befindet.

1. Öffnen Sie ein Befehlsfenster.
2. Geben Sie den folgenden Befehl bzw. das folgende Script ein:
   - Auf einem UNIX-System:

     ```
     <Produktverz>/bin/bcgDISImport.sh <datenbankbenutzer-ID>
      <kennwort> S_DT_XML_TO_EDI.eif
     ```

   - Auf einem Windows-System:

     ```
     <Produktverz>\bin\bcgDISImport.bat <datenbankbenutzer-ID>
      <kennwort> S_DT_XML_TO_EDI.eif
     ```

     Dabei gilt Folgendes: *<datenbankbenutzer-ID>* und *<kennwort>* sind die Werte, die Sie verwendet haben, als Sie die Datenbank als Teil der WebSphere Partner Gateway-Installation installiert haben.

Die Transformationszuordnung und Dokumentenflussdefinitionen prüfen

Führen Sie die folgenden Schritte aus, um zu prüfen, ob die Transformationszuordnungen und Dokumentdefinitionen, die Sie importiert haben, in Community Console verfügbar sind:

1. Klicken Sie auf **Hubadmin > Hubkonfiguration > Zuordnungen > Transformationszuordnungen**.

   Die Zuordnung S_DT_XML_TO_EDI wird angezeigt.
2. Klicken Sie auf das Symbol **Details anzeigen** neben der Zuordnung.

   Die Dokumentenflussdefinitionen, denen diese Zuordnung zugeordnet ist:

Tabelle 29. Dokumentenflussdefinitionen, die der Zuordnung zugeordnet sind

Quelle	Ziel
Paket: None Protokoll: FVT-XML-TEST (ALL) Dokumentenfluss: ICGCPO (ALL)	Paket: N/A Protokoll: MX12V3R1 (ALL) Dokumentenfluss: 850 (ALL)

Die Zuordnung S_DT_XML_TO_EDI wurde definiert, um ein XML-Dokument zu nehmen und es in eine EDI-Transaktion zu transformieren.

Das Ziel konfigurieren

In diesem Abschnitt erstellen Sie ein Dateisystemverzeichnisziel für den Hub:

1. Klicken Sie auf **Hubadmin > Hubkonfiguration > Ziele**, und klicken Sie dann auf **Ziel erstellen**.
2. Geben Sie als **Zielname** den Namen `XMLDateiziel` ein.
3. Wählen Sie in der Liste **Transport** die Option **Dateiverzeichnis** aus.
4. Geben Sie als Stammverzeichnispfad **/Data/Manager/xmltarget** ein.
5. Wählen Sie in der Liste **Konfigurationspunkt** die Option **Vorverarbeitung** aus.

6. Wählen Sie **com.ibm.bcg.edi.receiver.preprocesshandler.XMLSplitterHandler** in der **Verfügbarkeitsliste** aus, und klicken Sie auf **Hinzufügen**, um den Handler in die **Konfigurationsliste** zu versetzen.
7. Klicken Sie auf **Speichern**.

Community Manager sendet das XML-Dokument an dieses Ziel.

Die Interaktionen erstellen

Sie erstellen zwei Interaktionen: eine für die Transformation XML zu EDI und eine für den EDI-Umschlag.

Erstellen Sie eine Interaktion, die über eine Quelle verfügt, die das XML-Dokument darstellt, und ein Ziel, das die transformierte 850-Transaktion darstellt.

1. Klicken Sie auf **Hubadmin > Hubkonfiguration > Dokumentenflussdefinition**.
2. Klicken Sie auf **Interaktionen verwalten** und dann auf **Interaktion erstellen**.
3. Erweitern Sie den Eintrag **Paket: None** und **Protokoll: FVT-XML-TEST**, und wählen Sie **Dokumentenfluss: ICGCPO** aus.
4. Erweitern Sie den Eintrag **Paket: N/A** und **Protokoll: MX12V3R1**, und wählen Sie **Dokumentenfluss: 850** aus.
5. Wählen Sie in der Liste **Transformationszuordnung** den Eintrag **S_DT_XML-_TO_EDI** aus.
6. Wählen Sie in der Liste **Aktion** die Option **XML konvertieren und EDI validieren** aus.
7. Klicken Sie auf **Speichern**.

Diese Interaktion stellt die Transformation eines XML-Dokuments in eine EDI-Transaktion dar, und daher müssen Sie eine Transformationszuordnung auswählen.

Erstellen Sie eine Interaktion, die den EDI-Umschlag darstellt.

1. Klicken Sie auf **Hubadmin > Hubkonfiguration > Dokumentenflussdefinition**.
2. Klicken Sie auf **Interaktionen verwalten** und dann auf **Interaktion erstellen**.
3. Erweitern Sie den Eintrag **Paket: N/A** und **Protokoll: EDI-X12**, und wählen Sie **Dokumentenfluss: ISA** aus.
4. Erweitern Sie den Eintrag **Paket: None** und **Protokoll: EDI-X12**, und wählen Sie **Dokumentenfluss: ISA** aus.
5. Wählen Sie in der Liste **Aktion** die Option **Pass-Through** aus.

   Anmerkung: In dieser Interaktion findet keine Transformation statt.
6. Klicken Sie auf **Speichern**.

Die Teilnehmer erstellen

Sie haben für dieses Beispiel zwei Teilnehmer: Community Manager (Manager) und einen Teilnehmer (TP1).

Erstellen Sie das Profil **Community Manager**:

1. Klicken Sie auf **Kontenadmin > Profile > Community-Teilnehmer**, und klicken Sie auf **Erstellen**.
2. Geben Sie als **Anmeldename des Unternehmens** Folgendes ein: **ComManager**.
3. Geben Sie als **Anzeigename des Teilnehmers** Folgendes ein: **Manager**.

4. Wählen Sie als **Teilnehmertyp** Folgendes aus: **Community Manager**.
5. Klicken Sie auf **Neu** für die Geschäfts-ID, und geben Sie `000000000` als unformatierte ID ein.

   Anmerkung: Stellen Sie sicher, dass Sie **Unformatiert** und nicht **DUNS** ausgewählt haben.
6. Klicken Sie erneut auf **Neu** für die Geschäfts-ID, und geben Sie `01-000000000` als unformatierte ID ein.
7. Klicken Sie auf **Speichern**.

Erstellen Sie den zweiten Teilnehmer:

1. Klicken Sie auf **Kontenadmin > Profile > Community-Teilnehmer**, und klicken Sie auf **Erstellen**.
2. Geben Sie als **Anmeldename des Unternehmens** Folgendes ein: **TP1**.
3. Geben Sie als **Anzeigename des Teilnehmers** Folgendes ein, **TP1**.
4. Wählen Sie als **Teilnehmertyp** Folgendes aus: **Teilnehmer**.
5. Klicken Sie auf **Neu** für die Geschäfts-ID, und geben Sie `000000001` als unformatierte ID ein.

   Anmerkung: Stellen Sie sicher, dass Sie **Unformatiert** und nicht **DUNS** ausgewählt haben.
6. Klicken Sie erneut auf **Neu** für die Geschäfts-ID, und geben Sie `01-000000001` als unformatierte ID ein.
7. Klicken Sie auf **Speichern**.

Die Gateways erstellen

Erstellen Sie Dateiverzeichnisgateways für beide Teilnehmer im Beispiel. Erstellen Sie zuerst ein Gateway für den Manager.

1. Klicken Sie auf **Kontenadmin > Profile > Community-Teilnehmer**, und klicken Sie auf **Suchen**.
2. Klicken Sie auf das Symbol **Details anzeigen** neben dem Profil **Manager**.
3. Klicken Sie auf **Gateways** und dann auf **Erstellen**.
4. Geben Sie die folgenden Werte für das Gateway ein. Denken Sie daran, dass das Dateiverzeichnis (der vollständige Pfad) schon auf Ihrem Dateisystem vorhanden sein muss.
   a. Geben Sie als Name **Managerdateigateway** ein.
   b. Wählen Sie in der Liste **Transport** die Option **Dateiverzeichnis** aus.
   c. Geben Sie als **Adresse** Folgendes ein: **file:///Data/Manager/filegateway**
   d. Klicken Sie auf **Speichern**.
5. Klicken Sie auf **Liste**, um alle Gateways für Community Manager aufzulisten.
6. Klicken Sie auf **Standardgateways anzeigen**.
7. Wählen Sie in der Liste **Produktion** das Gateway aus, das Sie in Schritt 4 erstellt haben.
8. Klicken Sie auf **Speichern**.

Erstellen Sie als Nächstes ein Gateway für den Teilnehmer.

1. Klicken Sie auf **Kontenadmin > Profile > Community-Teilnehmer**, und klicken Sie auf **Suchen**.

2. Wählen Sie den anderen Teilnehmer aus, den Sie für dieses Beispiel erstellt haben, indem Sie auf das Symbol **Details anzeigen** neben **TP1** klicken.
3. Klicken Sie auf **Gateways** und dann auf **Erstellen**.
4. Geben Sie die folgenden Werte für das Gateway ein. Denken Sie daran, dass das Dateiverzeichnis (der vollständige Pfad) schon vorhanden sein muss.
   a. Geben Sie als Name **TP1Dateigateway** ein.
   b. Wählen Sie in der Liste **Transport** die Option **Dateiverzeichnis** aus.
   c. Geben Sie als **Adresse** Folgendes ein: **file:///Data/TP1/filegateway**
   d. Klicken Sie auf **Speichern**.
5. Klicken Sie auf **Liste**, um alle Gateways für den Teilnehmer aufzulisten.
6. Klicken Sie auf **Standardgateways anzeigen**.
7. Wählen Sie in der Liste **Produktion** das Gateway aus, das Sie in Schritt 4 erstellt haben.
8. Klicken Sie auf **Speichern**.

B2B-Funktionalität konfigurieren

Aktivieren Sie die B2B-Funktionalität der zwei Teilnehmer in diesem Austausch. In diesem Beispiel stammt das XML-Dokument von Community Manager und wird dem Teilnehmer übermittelt.

1. Klicken Sie auf **Kontenadmin > Profile > Community-Teilnehmer**, und klicken Sie auf **Suchen**.
2. Klicken Sie auf das Symbol **Details anzeigen** für den Quellenteilnehmer dieses Beispiels (**ComMan**).
3. Klicken Sie auf **B2B-Funktionalität**.
4. Aktivieren Sie drei Funktionalitätsgruppen für den Quellenteilnehmer.
   a. Aktivieren Sie die Dokumentenflussdefinition, die das XML-Dokument darstellt:
      1) Klicken Sie zum Aktivieren auf das Symbol **Rolle ist nicht aktiv** unter **Quelle festlegen** für **Paket: None**.
      2) Erweitern Sie **Paket: None**.
      3) Klicken Sie auf das Symbol **Rolle ist nicht aktiv** unter **Quelle festlegen** für **Protokoll: FVT-XML-TEST (ALL)**.
      4) Erweitern Sie **Protokoll: FVT-XML-TEST (ALL)**.
      5) Klicken Sie auf das Symbol **Rolle ist nicht aktiv** unter **Quelle festlegen** für **Dokumentenfluss: ICGCPO (ALL)**.
   b. Aktivieren Sie als Nächstes die Dokumentenflussdefinition, die das transformierte Dokument darstellt:
      1) Klicken Sie zum Aktivieren auf das Symbol **Rolle ist nicht aktiv** unter **Quelle festlegen** für **Paket: N/A**.
      2) Erweitern Sie **Paket: N/A**.
      3) Klicken Sie auf das Symbol **Rolle ist nicht aktiv** unter **Quelle festlegen** für **Protokoll: MX12V3R1 (ALL)**.
      4) Erweitern Sie **Protokoll: MX12V3R1 (ALL)**.
      5) Klicken Sie auf das Symbol **Rolle ist nicht aktiv** unter **Quelle festlegen** für **Dokumentenfluss: 850**.
   c. Aktivieren Sie dann die Dokumentenflussdefinition, die den EDI-Umschlag darstellt:

1) Klicken Sie zum Aktivieren auf das Symbol **Rolle ist nicht aktiv** unter **Quelle festlegen** für **Paket: N/A**.
2) Erweitern Sie **Paket: N/A**.
3) Klicken Sie auf das Symbol **Rolle ist nicht aktiv** unter **Quelle festlegen** für **Protokoll: EDI-X12 (ALL)**.
4) Erweitern Sie **Protokoll: EDI-X12 (ALL)**.
5) Klicken Sie auf das Symbol **Rolle ist nicht aktiv** unter **Quelle festlegen** für **Dokumentenfluss: ISA (ALL)**.

5. Klicken Sie auf **Kontenadmin > Profile > Community-Teilnehmer**, und klicken Sie auf **Suchen**.
6. Klicken Sie auf das Symbol **Details anzeigen** für den Zielteilnehmer dieses Beispiels (**TP1**).
7. Klicken Sie auf **B2B-Funktionalität**.
8. Aktivieren Sie zwei Funktionalitätsgruppen für den Zielteilnehmer.
   a. Aktivieren Sie zuerst die Dokumentenflussdefinition, die die EDI-850-Transaktion darstellt:
      1) Klicken Sie zum Aktivieren auf das Symbol **Rolle ist nicht aktiv** unter **Ziel festlegen** für **Paket: N/A**.
      2) Erweitern Sie **Paket: N/A**.
      3) Klicken Sie auf das Symbol **Rolle ist nicht aktiv** unter **Ziel festlegen** für **Protokoll: MX12V3R1 (ALL)**.
      4) Erweitern Sie **Protokoll: MX12V3R1 (ALL)**.
      5) Klicken Sie auf das Symbol **Rolle ist nicht aktiv** unter **Ziel festlegen** für **Dokumentenfluss: 850 (ALL)**.
   b. Aktivieren Sie als Nächstes die Dokumentenflussdefinition:
      1) Klicken Sie zum Aktivieren auf das Symbol **Rolle ist nicht aktiv** unter **Ziel festlegen** für **Paket: None**.
      2) Erweitern Sie **Paket: None**.
      3) Klicken Sie auf das Symbol **Rolle ist nicht aktiv** unter **Ziel festlegen** für **Protokoll: EDI-X12 (ALL)**.
      4) Erweitern Sie **Protokoll: EDI-X12 (ALL)**.
      5) Klicken Sie auf das Symbol **Rolle ist nicht aktiv** unter **Ziel festlegen** für **Dokumentenfluss: ISA (ALL)**.

Das Umschlagsprofil erstellen

Sie erstellen als Nächstes das Profil für den Umschlag, der die transformierte 850-Transaktion enthalten wird:

1. Klicken Sie auf **Hubadmin > Hubkonfiguration > EDI > Umschlagsprofil**.
2. Klicken Sie auf **Erstellen**.
3. Geben Sie den Namen des Profils ein: **UmschProf1**.
4. Wählen Sie in der Liste **EDI-Standard** die Option **X12** aus.
5. Die Schaltfläche **Allgemein** ist standardmäßig ausgewählt. Geben Sie die folgenden Werte für die allgemeinen Attribute des Umschlags ein:
   - INTCTLLEN: **9**
   - GRPCTLLEN: **9**
   - TRXCTLLEN: **9**
   - MAXDOCS: **1000**

6. Klicken Sie auf die Schaltfläche **Austausch**, und geben Sie die folgenden Werte für die Austauschattribute ein:
   - ISA01: **01**
   - ISA02: **ISA0000002**
   - ISA03: **02**
   - ISA04: **ISA0000004**
   - ISA11: **U**
   - ISA12: **00301**
   - ISA15: **T**
7. Klicken Sie auf **Speichern**.

Das XML-Format erstellen

In diesem Abschnitt erstellen Sie das angepasste XML-Format.

1. Klicken Sie auf **Hubadmin > Hubkonfiguration > XML-Formate**.
2. Klicken Sie auf **XML-Format erstellen**.
3. Wählen Sie als **Routing-Format** das Format **FVT-XML-TEST ALL** aus.
4. Wählen Sie für **Dateityp** den Eintrag **XML** aus.
5. Wählen Sie als Kennungstyp **Root-Tag** aus, und geben Sie **MMDoc** ein.
6. Wählen Sie als Quellengeschäfts-ID **Konstante** aus, und geben Sie **000000000** ein.
7. Wählen Sie als Zielgeschäfts-ID **Konstante** aus, und geben Sie **000000001** ein.
8. Wählen Sie als Quellendokumentenfluss **Konstante** aus, und geben Sie **ICG-CPO** ein.
9. Wählen Sie als Quellendokumentenflussversion **Konstante** aus, und geben Sie **ALLE** ein.
10. Klicken Sie auf **Speichern**.

Die Verbindungen aktivieren

Aktivieren Sie die Teilnehmerverbindungen:

1. Klicken Sie auf **Kontenadmin > Teilnehmerverbindungen**.
2. Wählen Sie **Manager** in der Liste **Quelle** aus.
3. Wählen Sie **TP1** in der Liste **Ziel** aus.
4. Klicken Sie auf **Suchen**.
5. Klicken Sie auf **Aktivieren** für die folgende Verbindung:

Tabelle 30. Verbindung für XML-Dokument zu EDI-Transaktion

Quelle	Ziel
Paket: None (N/A) Protokoll: FVT-XML-TEST (ALL) Dokumentenfluss: ICGCPO (ALL)	Paket: N/A (N/A) Protokoll: MX12V3R1 (ALL) Dokumentenfluss: 850 (ALL)

6. Klicken Sie auf **Aktivieren** für die Verbindung, die den EDI-Umschlag darstellt:

Tabelle 31. Verbindung für EDI-Umschlag

Quelle	Ziel
Paket: N/A (N/A) Protokoll: EDI-X12 (ALL) Dokumentenfluss: ISA (ALL)	Paket: None (N/A) Protokoll: EDI-X12 (ALL) Dokumentenfluss: ISA (ALL)

Attribute konfigurieren

Konfigurieren Sie die B2B-Funktionalitätsattribute von dem Zielteilnehmer (TP1) und dem Quellenteilnehmer (Manager):

1. Klicken Sie auf **Kontenadmin > Profile > Community-Teilnehmer**, und klicken Sie auf **Suchen**.
2. Klicken Sie zum Auswählen auf das Symbol **Details anzeigen** neben **TPI**.
3. Klicken Sie auf **B2B-Funktionalität**.
4. Klicken Sie auf das Symbol **Erweitern** neben **Paket: N/A**.
5. Klicken Sie auf das Symbol **Bearbeiten** neben **Protokoll: MX12V3R1**.
6. Geben Sie die folgenden Attribute an:
   a. Wählen Sie in der Zeile **Umschlagsprofil** den Eintrag **UmschProf1** in der Liste aus.
   b. Geben Sie in der Zeile **Qualifikationsmerkmal für Austausch** den Wert **01** ein.
   c. Geben Sie in der Zeile **Kennung für Austausch** den Wert **000000001** ein.
   d. Geben Sie in der Zeile **Nutzungsanzeiger für Austausch** den Buchstaben **T** ein.
7. Klicken Sie auf **Speichern**.
8. Klicken Sie auf **Kontenadmin > Profile > Community-Teilnehmer**, und klicken Sie auf **Suchen**.
9. Klicken Sie zum Auswählen auf das Symbol **Details anzeigen** neben **Manager**.
10. Klicken Sie auf **B2B-Funktionalität**.
11. Klicken Sie auf das Symbol **Erweitern** neben **Paket: N/A**.
12. Klicken Sie auf das Symbol **Bearbeiten** neben **Protokoll: MX12V3R1 (ALL)**.
13. Geben Sie die folgenden Attribute an:
    a. Geben Sie in der Zeile **Qualifikationsmerkmal für Austausch** den Wert **01** ein.
    b. Geben Sie in der Zeile **Kennung für Austausch** den Wert **000000000** ein.
    c. Geben Sie in der Zeile **Nutzungsanzeiger für Austausch** den Buchstaben **T** ein.
14. Klicken Sie auf **Speichern**.

Wenn der Quellenteilnehmer (Community Manager) jetzt ein XML-Dokument an den Teilnehmer sendet, würde es auf dem Hub in eine EDI-Transaktion konvertiert, mit einem Umschlag versehen und dann an das Gateway des Teilnehmers gesendet werden.

Beispiel: ROD zu EDI

Dieser Abschnitt enthält ein Beispiel davon, wie Community Manager ein ROD-Dokument a den Hub sendet, auf dem es in eine EDI-Transaktion transformiert, in einem EDI-Austausch mit einem Umschlag versehen und an einen Teilnehmer gesendet wird.

In diesem Beispiel wird davon ausgegangen, dass der Zuordnungsexperte von Data Interchange Services eine Transformationszuordnung erstellt hat, die ein satzorientiertes Datendokument (ROD) nimmt und dieses in eine EDI-850-Standardtransaktion (die mit dem Wörterbuch X12V5R1 definiert ist und der Version 5010

von X12 entspricht) transformiert, die vom Teilnehmer verarbeitet wird. In diesem Beispiel heißt die Zuordnung S_DT_ROD_TO_EDI.eif.

Der Zuordnungsexperte von Data Interchange Services kann die Transformationszuordnung direkt in die WebSphere Partner Gateway-Datenbank exportieren. Alternativ hierzu kann der Zuordnungsexperte von Data Interchange Services Ihnen die Datei senden, in dem Fall verwenden Sie das Dienstprogramm bcgDISImport, um die Datei in WebSphere Partner Gateway zu importieren. Dieser Anhang geht vom zweiten Szenario aus.

Die Transformationszuordnung importieren

Dieser Abschnitt beschreibt die Schritte, die Sie beim Importieren einer Transformationszuordnung ausführen, die die ROD-Eingabe nimmt und diese in eine X12-Transaktion transformiert. Beim Importieren der Transformationszuordnung können Sie auch die Dokumentdefinition importieren, die der Zuordnung zugeordnet ist.

Bevor Sie die Transformationszuordnung importieren können, muss der Zuordnungsexperte von Data Interchange Services Ihnen diese zusenden. Diese Gruppe von Schritten geht davon aus, dass sich die Datei `S_DT_ROD_TO_EDI.eif` auf Ihrem System befindet.

1. Öffnen Sie ein Befehlsfenster.
2. Geben Sie den folgenden Befehl bzw. das folgende Script ein:
   - Auf einem UNIX-System:

     ```
     <Produktverz>/bin/bcgDISImport.sh <datenbankbenutzer-ID>
      <kennwort> S_DT_ROD_TO_EDI.eif
     ```

   - Auf einem Windows-System:

     ```
     <Produktverz>\bin\bcgDISImport.bat <datenbankbenutzer-ID>
      <kennwort> S_DT_ROD_TO_EDI.eif
     ```

     Dabei gilt Folgendes: <*datenbankbenutzer-ID*> und <*kennwort*> sind die Werte, die Sie verwendet haben, als Sie die Datenbank als Teil der WebSphere Partner Gateway-Installation installiert haben.

Die Transformationszuordnung und Dokumentenflussdefinitionen prüfen

Führen Sie die folgenden Schritte aus, um zu prüfen, ob die Transformationszuordnungen und Dokumentdefinitionen, die Sie importiert haben, in Community Console verfügbar sind:

1. Klicken Sie auf **Hubadmin > Hubkonfiguration > Zuordnungen > Transformationszuordnungen**.

   Die Zuordnung S_DT_ROD_TO_EDI wird angezeigt.
2. Klicken Sie auf das Symbol **Details anzeigen** neben der Zuordnung.

   Die Dokumentenflussdefinitionen, denen diese Zuordnung zugeordnet ist:

Tabelle 32. Dokumentenflussdefinitionen, die der Zuordnung zugeordnet sind

Quelle	Ziel
Paket: None Protokoll: ROD-TO-EDI_DICT (ALL) Dokumentenfluss: DTROD-TO-EDI_ROD (ALL)	Paket: N/A Protokoll: X12V5R1 (ALL) Dokumentenfluss: 850 (ALL)

Die Zuordnung S_DT_ROD_TO_EDI wurde definiert, um ein ROD-Dokument, das dem Wörterbuch ROD-TO-EDI_DICT zugeordnet ist, zu nehmen und dieses in eine X12-850-Transaktion zu transformieren, die mit dem X12V5R1-Standard konform ist.

Das Ziel konfigurieren

In diesem Abschnitt erstellen Sie ein Dateisystemverzeichnisziel für den Hub:

1. Klicken Sie auf **Hubadmin > Hubkonfiguration > Ziele**, und klicken Sie dann auf **Ziel erstellen**.
2. Geben Sie als **Zielname** den Namen `RODDateiziel` ein.
3. Wählen Sie in der Liste **Transport** die Option **Dateiverzeichnis** aus.
4. Geben Sie als Stammverzeichnispfad **/Data/Manager/rodtarget** ein.
5. Wählen Sie in der Liste **Konfigurationspunkt** die Option **Vorverarbeitung** aus.
6. Wählen Sie **com.ibm.bcg.edi.receiver.preprocesshandler.RODSplitterHandler** in der **Verfügbarkeitsliste** aus, und klicken Sie auf **Hinzufügen**, um den Handler in die **Konfigurationsliste** zu versetzen.
7. Wählen Sie **com.ibm.bcg.edi.receiver.preprocesshandler.RODSplitterHandler** in der **Konfigurationsliste** aus, und klicken Sie auf **Konfigurieren**.
8. Fügen Sie die in der Tabelle gezeigten Werte hinzu:

Tabelle 33. Attribute für den ROD-Verteilerhandler

Feld	Wert
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. Klicken Sie auf **Festlegen**.
10. Klicken Sie auf **Speichern**.

Community Manager sendet das ROD-Dokument an dieses Ziel.

Die Interaktionen erstellen

Sie erstellen zwei Interaktionen: eine für den EDI-Umschlag, der vom Hub gesendet wird, und eine für die Transformation des ROD-Dokuments in EDI.

Erstellen Sie eine Interaktion, die über eine Quelle verfügt, die das ROD-Dokument darstellt, und ein Ziel, das das X12-Dokument darstellt.

1. Klicken Sie auf **Hubadmin > Hubkonfiguration > Dokumentenfluss-definition**.

2. Klicken Sie auf **Interaktionen verwalten** und dann auf **Interaktion erstellen**.
3. Erweitern Sie den Eintrag **Paket: None** und **Protokoll: ROD-TO-EDI_DICT**, und wählen Sie **DTROD-TO-EDI_ROD** aus.
4. Erweitern Sie den Eintrag **Paket: N/A** und **Protokoll: X12V5R1**, und wählen Sie **Dokumentenfluss: 850** aus.
5. Wählen Sie in der Liste **Transformationszuordnung** den Eintrag **S_DT_ROD-_TO_EDI** aus.
6. Wählen Sie in der Liste **Aktion** die Option **ROD konvertieren und EDI validieren** aus.
7. Klicken Sie auf **Speichern**.

Diese Interaktion stellt die Transformation eines ROD-Dokuments in eine X12-Standardtransaktion dar, und daher müssen Sie eine Transformationszuordnung auswählen.

Erstellen Sie eine Interaktion, die den EDI-Umschlag darstellt.

1. Klicken Sie auf **Hubadmin > Hubkonfiguration > Dokumentenflussdefinition**.
2. Klicken Sie auf **Interaktionen verwalten** und dann auf **Interaktion erstellen**.
3. Erweitern Sie den Eintrag **Paket: N/A** und **Protokoll: EDI-X12**, und wählen Sie **Dokumentenfluss: ISA** aus.
4. Erweitern Sie den Eintrag **Paket: None** und **Protokoll: EDI-X12**, und wählen Sie **Dokumentenfluss: ISA** aus.
5. Wählen Sie in der Liste **Aktion** die Option **Pass-Through** aus.

   Anmerkung: In dieser Interaktion findet keine Transformation statt. In dieser Interaktion wird der EDI-Austausch mit einem Umschlag versehen.
6. Klicken Sie auf **Speichern**.

Die Teilnehmer erstellen

Sie haben für dieses Beispiel zwei Teilnehmer: Community Manager (Manager) und einen Teilnehmer (TP1).

Erstellen Sie das Profil **Community Manager**:

1. Klicken Sie auf **Kontenadmin > Profile > Community-Teilnehmer**, und klicken Sie auf **Erstellen**.
2. Geben Sie als **Anmeldename des Unternehmens** Folgendes ein: **ComManager**.
3. Geben Sie als **Anzeigename des Teilnehmers** Folgendes ein: **Manager**.
4. Wählen Sie als **Teilnehmertyp** Folgendes aus: **Community Manager**.
5. Klicken Sie auf **Neu** für die Geschäfts-ID, und geben Sie `000000000` als unformatierte ID ein.

   Anmerkung: Stellen Sie sicher, dass Sie **Unformatiert** und nicht **DUNS** ausgewählt haben.
6. Klicken Sie erneut auf **Neu** für die Geschäfts-ID, und geben Sie `01-000000000` als unformatierte ID ein.
7. Klicken Sie auf **Speichern**.

Erstellen Sie den zweiten Teilnehmer:

1. Klicken Sie auf **Kontenadmin > Profile > Community-Teilnehmer**, und klicken Sie auf **Erstellen**.

2. Geben Sie als **Anmeldename des Unternehmens** Folgendes ein: **TP1**.
3. Geben Sie als **Anzeigename des Teilnehmers** Folgendes ein, **TP1**.
4. Wählen Sie als **Teilnehmertyp** Folgendes aus: **Community-Teilnehmer**.
5. Klicken Sie auf **Neu** für die Geschäfts-ID, und geben Sie `000000001` als unformatierte ID ein.

   Anmerkung: Stellen Sie sicher, dass Sie **Unformatiert** und nicht **DUNS** ausgewählt haben.
6. Klicken Sie erneut auf **Neu** für die Geschäfts-ID, und geben Sie `01-000000001` als unformatierte ID ein.
7. Klicken Sie auf **Speichern**.

Die Gateways erstellen

Erstellen Sie Dateiverzeichnisgateways für beide Teilnehmer im Beispiel. Erstellen Sie zuerst ein Gateway für den Manager.

1. Klicken Sie auf **Kontenadmin > Profile > Community-Teilnehmer**, und klicken Sie auf **Suchen**.
2. Klicken Sie auf das Symbol **Details anzeigen** neben dem Profil **Manager**.
3. Klicken Sie auf **Gateways** und dann auf **Erstellen**.
4. Geben Sie die folgenden Werte für das Gateway ein. Denken Sie daran, dass das Dateiverzeichnis (der vollständige Pfad) schon auf Ihrem Dateisystem vorhanden sein muss.
   a. Geben Sie als Name **Managerdateigateway** ein.
   b. Wählen Sie in der Liste **Transport** die Option **Dateiverzeichnis** aus.
   c. Geben Sie als **Adresse** Folgendes ein: **file:///Data/Manager/filegateway**
   d. Klicken Sie auf **Speichern**.
5. Klicken Sie auf **Liste**, um alle Gateways für Community Manager aufzulisten.
6. Klicken Sie auf **Standardgateways anzeigen**.
7. Wählen Sie in der Liste **Produktion** das Gateway aus, das Sie in Schritt 4 erstellt haben.
8. Klicken Sie auf **Speichern**.

Erstellen Sie als Nächstes ein Gateway für den Teilnehmer.

1. Klicken Sie auf **Kontenadmin > Profile > Community-Teilnehmer**, und klicken Sie auf **Suchen**.
2. Wählen Sie den anderen Teilnehmer aus, den Sie für dieses Beispiel erstellt haben, indem Sie auf das Symbol **Details anzeigen** neben **TP1** klicken.
3. Klicken Sie auf **Gateways** und dann auf **Erstellen**.
4. Geben Sie die folgenden Werte für das Gateway ein. Denken Sie daran, dass das Dateiverzeichnis (der vollständige Pfad) schon vorhanden sein muss.
   a. Geben Sie als Name **TP1Dateigateway** ein.
   b. Wählen Sie in der Liste **Transport** die Option **Dateiverzeichnis** aus.
   c. Geben Sie als **Adresse** Folgendes ein: **file:///Data/TP1/filegateway**
   d. Klicken Sie auf **Speichern**.
5. Klicken Sie auf **Liste**, um alle Gateways für den Teilnehmer aufzulisten.
6. Klicken Sie auf **Standardgateways anzeigen**.
7. Wählen Sie in der Liste **Produktion** das Gateway aus, das Sie in Schritt 4 erstellt haben.
8. Klicken Sie auf **Speichern**.

B2B-Funktionalität konfigurieren

Aktivieren Sie die B2B-Funktionalität der zwei Teilnehmer in diesem Austausch. In diesem Beispiel stammt das ROD-Dokument von Community Manager und wird dem Teilnehmer (TP1) übermittelt.

1. Klicken Sie auf **Kontenadmin > Profile > Community-Teilnehmer**, und klicken Sie auf **Suchen**.
2. Klicken Sie auf das Symbol **Details anzeigen** für den Quellenteilnehmer dieses Beispiels (**Manager**).
3. Klicken Sie auf **B2B-Funktionalität**.
4. Aktivieren Sie zwei Funktionalitätsgruppen für den Quellenteilnehmer.
   a. Aktivieren Sie zuerst die Dokumentenflussdefinition, die das ROD-Dokument darstellt:
      1) Klicken Sie zum Aktivieren auf das Symbol **Rolle ist nicht aktiv** unter **Quelle festlegen** für **Paket: None**.
      2) Erweitern Sie **Paket: None**.
      3) Klicken Sie auf das Symbol **Rolle ist nicht aktiv** unter **Quelle festlegen** für **Protokoll: ROD-TO-EDI_DICT (ALL)**.
      4) Erweitern Sie **Protokoll: ROD-TO-EDI_DICT (ALL)**.
      5) Klicken Sie auf das Symbol **Rolle ist nicht aktiv** unter **Quelle festlegen** für **Dokumentenfluss: DTROD-TO-EDI_ROD (ALL)**.
   b. Aktivieren Sie als Nächstes die Dokumentenflussdefinition, die den EDI-Umschlag darstellt:
      1) Klicken Sie zum Aktivieren auf das Symbol **Rolle ist nicht aktiv** unter **Quelle festlegen** für **Paket: N/A**.
      2) Erweitern Sie **Paket: N/A**.
      3) Klicken Sie auf das Symbol **Rolle ist nicht aktiv** unter **Quelle festlegen** für **Protokoll: EDI-X12 (ALL)**.
      4) Erweitern Sie **Protokoll: EDI-X12 (ALL)**.
      5) Klicken Sie auf das Symbol **Rolle ist nicht aktiv** unter **Quelle festlegen** für **Dokumentenfluss: ISA (ALL)**.
5. Klicken Sie auf **Kontenadmin > Profile > Community-Teilnehmer**, und klicken Sie auf **Suchen**.
6. Klicken Sie auf das Symbol **Details anzeigen** für den Zielteilnehmer dieses Beispiels (**TP1**).
7. Klicken Sie auf **B2B-Funktionalität**.
8. Aktivieren Sie zwei Funktionalitätsgruppen für den Zielteilnehmer.
   a. Aktivieren Sie zuerst die Dokumentenflussdefinition, die die EDI-850-Transaktion darstellt:
      1) Klicken Sie zum Aktivieren auf das Symbol **Rolle ist nicht aktiv** unter **Ziel festlegen** für **Paket: N/A**.
      2) Erweitern Sie **Paket: N/A**.
      3) Klicken Sie auf das Symbol **Rolle ist nicht aktiv** unter **Ziel festlegen** für **Protokoll: X12V5R1 (ALL)**.
      4) Erweitern Sie **Protokoll: X12V5R1 (ALL)**.
      5) Klicken Sie auf das Symbol **Rolle ist nicht aktiv** unter **Ziel festlegen** für **Dokumentenfluss: 850 (ALL)**.

b. Aktivieren Sie als Nächstes die Dokumentenflussdefinition, die den Umschlag darstellt:
   1) Klicken Sie zum Aktivieren auf das Symbol **Rolle ist nicht aktiv** unter **Ziel festlegen** für **Paket: None**.
   2) Erweitern Sie **Paket: None**.
   3) Klicken Sie auf das Symbol **Rolle ist nicht aktiv** unter **Ziel festlegen** für **Protokoll: EDI-X12 (ALL)**.
   4) Erweitern Sie **Protokoll: EDI-X12 (ALL)**.
   5) Klicken Sie auf das Symbol **Rolle ist nicht aktiv** unter **Ziel festlegen** für **Dokumentenfluss: ISA (ALL)**.

Das Umschlagsprofil erstellen

Sie erstellen als Nächstes das Profil für den Umschlag, der die transformierte 850-Transaktion enthalten wird:

1. Klicken Sie auf **Hubadmin > Hubkonfiguration > EDI > Umschlagsprofil**.
2. Klicken Sie auf **Erstellen**.
3. Geben Sie den Namen des Profils ein: **UmschProf1**.
4. Wählen Sie in der Liste **EDI-Standard** die Option **X12** aus.
5. Die Schaltfläche **Allgemein** ist standardmäßig ausgewählt. Geben Sie die folgenden Werte für die allgemeinen Attribute des Umschlags ein:
   - INTCTLLEN: **9**
   - GRPCTLLEN: **9**
   - TRXCTLLEN: **9**
   - MAXDOCS: **1000**
6. Klicken Sie auf die Schaltfläche **Austausch**, und geben Sie die folgenden Werte für die Austauschattribute ein:
   - ISA01: **01**
   - ISA02: **ISA0000002**
   - ISA03: **02**
   - ISA04: **ISA0000004**
   - ISA11: \
   - ISA12: **00501**
   - ISA15: **T**
7. Klicken Sie auf **Speichern**.

Die Verbindungen aktivieren

Gehen Sie wie folgt vor, um die Verbindungen zu aktivieren:

1. Klicken Sie auf **Kontenadmin > Teilnehmerverbindungen**.
2. Wählen Sie **Manager** in der Liste **Quelle** aus.
3. Wählen Sie **TP1** in der Liste **Ziel** aus.
4. Klicken Sie auf **Suchen**.
5. Klicken Sie auf **Aktivieren** für die Verbindung, die die Verbindung vom ROD-Dokument zur EDI-Transaktion darstellt:

Tabelle 34. Verbindung für ROD zu EDI

Quelle	Ziel
Paket: N/A (N/A) Protokoll: ROD-TO-EDI_DICT (ALL) Dokumentenfluss: DTROD-TO-EDI_ROD (ALL)	Paket: None (N/A) Protokoll: X12V5R1 (ALL) Dokumentenfluss: 850

6. Klicken Sie auf **Aktivieren** für die Verbindung, die den Umschlag darstellt:

Tabelle 35. Verbindung für Umschlag

Quelle	Ziel
Paket: None (N/A) Protokoll: EDI-X12 (ALL) Dokumentenfluss: ISA (ALL)	Paket: N/A (N/A) Protokoll: EDI-X12 (ALL) Dokumentenfluss: ISA (ALL)

Attribute konfigurieren

Gehen Sie wie folgt vor, um Attribute für das Umschlagsprofil anzugeben:

1. Klicken Sie auf **Kontenadmin > Profile > Community-Teilnehmer**, und klicken Sie auf **Suchen**.
2. Wählen Sie **TP1** in der Liste aus.
3. Klicken Sie auf **B2B-Funktionalität**.
4. Klicken Sie auf das Symbol **Erweitern** neben **Paket: N/A**.
5. Klicken Sie auf das Symbol **Bearbeiten** neben **Protokoll: X12V5R1**.
6. Geben Sie die folgenden Attribute an:
   a. Wählen Sie in der Zeile **Umschlagsprofil** den Eintrag **UmschProf1** in der Liste aus.
   b. Geben Sie in der Zeile **Qualifikationsmerkmal für Austausch** den Wert **01** ein.
   c. Geben Sie in der Zeile **Kennung für Austausch** den Wert **000000001** ein.
   d. Geben Sie in der Zeile **Nutzungsanzeiger für Austausch** den Buchstaben **T** ein.
7. Klicken Sie auf **Speichern**.

Wenn Community Manager jetzt ein ROD-Dokument an den Hub sendet, würde das Dokument in eine 850-Transaktion transformiert werden, welche dann mit einem Umschlag versehen und an das Gateway des Teilnehmers gesendet würde.

Anhang C. Zusätzliche RosettaNet-Informationen

Dieser Anhang enthält weitere Informationen zur RosettaNet-Unterstützung. Er behandelt die folgenden Themen:

- „PIPs inaktivieren"
- „Fehlerbenachrichtigung bereitstellen"
- „PIP-Dokumentenflusspakete erstellen" auf Seite 247
- „Inhalt der PIP-Dokumentenflusspakete" auf Seite 259

PIPs inaktivieren

Nachdem ein PIP-Paket in WebSphere Partner Gateway hochgeladen wurde, kann es nicht mehr entfernt werden. Sie können jedoch den PIP inaktivieren, so dass er nicht mehr verwendet werden kann.

Führen Sie die folgenden Schritte aus, um ein PIP für die Kommunikation mit allen Teilnehmern zu inaktivieren:

1. Klicken Sie auf **Hubadmin > Hubkonfiguration > Dokumentenfluss-definition**.
2. Erweitern Sie die Dokumentenflussdefinitionen, um den Dokumentenfluss des PIP anzuzeigen, den Sie inaktivieren wollen.
3. Klicken Sie in der Spalte **Status** des Pakets auf **Aktiviert**. Die Spalte **Status** zeigt jetzt **Inaktiviert** an und WebSphere Partner Gateway kann die Dokumentenflussdefinition für den PIP nicht mehr verwenden.

Um eine PIP-Kommunikation mit einem bestimmten Teilnehmer zu inaktivieren, inaktivieren Sie die Verbindung mit dem Teilnehmer, die für den PIP definiert wurde.

Fehlerbenachrichtigung bereitstellen

Dieser Abschnitt beschreibt die Fehlerbenachrichtigung.

0A1 PIP

Wenn ein Fehler während der Verarbeitung einer PIP-Nachricht auftritt, verwendet WebSphere Partner Gateway den 0A1 PIP als Mechanismus, um den Fehler an den Teilnehmer bzw. das Back-End-System zu übertragen, der bzw. das die Nachricht gesendet hat. Angenommen, ein Back-End-System initiiert z. B. einen 3A4 PIP. WebSphere Partner Gateway verarbeitet die RNSC-Nachricht und sendet eine RosettaNet-Nachricht an einen Teilnehmer. WebSphere Partner Gateway wartet auf die Antwort auf die RosettaNet-Nachricht, bis die Wartezeit das Zeitlimit erreicht. Nachdem dies geschehen ist, erstellt WebSphere Partner Gateway einen 0A1 PIP und sendet ihn an den Teilnehmer. Der 0A1 PIP gibt die Ausnahmebedingung an, so dass der Teilnehmer dann den Fehler des 3A4 PIP kompensieren kann.

Zum Bereitstellen der Fehlerbenachrichtigung laden Sie ein 0A1-Paket hoch und erstellen eine PIP-Verbindung zum Teilnehmer, der dieses Paket verwendet.

Kontaktinformationen aktualisieren

Um die RosettaNet-Kontaktinformationen mit dem 0A1 PIP zu ändern, müssen Sie die Datei `BCG.Properties` bearbeiten, sie befindet sich im Verzeichnis `<Produktverz>/router/lib/config`.

Diese Felder füllen die Kontaktinformationen im 0A1 PIP aus. Ein Wert für Fax ist optional (der Wert kann leer sein), aber die restlichen Werte sind erforderlich.

- **bcg.0A1.fromContactName**
- **bcg.0A1.fromEMailAddr**
- **bcg.0A1.fromPhoneNbr**
- **bcg.0A1.fromFaxNbr**

Die Telefonnummern sind auf eine Länge von 30 Byte begrenzt. Die übrigen Felder sind ohne Längenbegrenzung. Wenn die Werte geändert wurden, muss Document Manager erneut gestartet werden.

RosettaNet-Attributwerte bearbeiten

Zur RosettaNet-Unterstützung verfügt eine Dokumentenflussdefinition für den Aktionstyp über eine spezifische Gruppe von Attributen. Diese Attribute stellen Informationen bereit, mit denen die PIP-Nachricht validiert wird, um die im PIP verwendeten Rollen und Services sowie die Antwort auf die Aktion zu definieren. Die PIP-Pakete, die von WebSphere Partner Gateway bereitgestellt werden, definieren automatisch Werte für diese Attribute und Sie müssen diese normalerweise nicht ändern.

Führen Sie die folgenden Schritte aus, um die RosettaNet-Attribute einer Dokumentenflussdefinition für Aktionen zu bearbeiten:

1. Klicken Sie auf **Hubadmin > Hubkonfiguration > Dokumentenflussdefinition**.
2. Klicken Sie auf die Symbole **Erweitern**, um einen Knoten individuell zur entsprechenden Dokumentenflussdefinitions-Ebene zu erweitern, oder wählen Sie **Alle** aus, um die gesamte Baumstruktur zu erweitern.
3. Die Spalte **Aktionen** enthält für jede Aktion ein Symbol **RosettaNet-Attributwerte bearbeiten**. Klicken Sie auf dieses Symbol, um die RosettaNet-Attribute der Aktion zu bearbeiten. Community Console zeigt eine Liste der definierten Attribute unter **RosettaNet-Attribute** an.
4. Vervollständigen Sie die folgenden Parameter unter **RosettaNet-Attribute**. (Diese Attribute sind automatisch definiert, wenn ein PIP auf das System hochgeladen wird.)

Tabelle 36. RosettaNet-Attribute

RosettaNet-Attribut	Beschreibung
DTD-Name	Gibt den Namen der Aktion des PIP in der von RosettaNet bereitgestellten DTD an.
Absenderservice	Enthält den Netzkomponentenservicenamen des Teilnehmers oder Back-End-Systems, der bzw. das die Nachricht sendet.
Empfängerservice	Enthält den Netzkomponentenservicenamen des Teilnehmers oder Back-End-Systems, der bzw. das die Nachricht empfängt.
Absenderrolle	Enthält den Rollennamen des Teilnehmers oder Back-End-Systems, der bzw. das die Nachricht sendet.

Tabelle 36. RosettaNet-Attribute (Forts.)

RosettaNet-Attribut	Beschreibung
Empfängerrolle	Enthält den Rollennamen des Teilnehmers oder Back-End-Systems, der bzw. das die Nachricht empfängt.
Root-Tag	Enthält den Namen des Stammelements im XML-Dokument, das dem PIP zugeordnet ist.
Antwort aus Aktionsname	Gibt die nächste Aktion an, die im PIP ausgeführt werden soll.

Anmerkung: Wenn die Konsole die Nachricht **Keine Attribute gefunden** anzeigt, sind die Attribute nicht definiert worden.

5. Wenn die Konsole diese Nachricht für eine Definition der unteren Ebene anzeigt, kann die Definition dennoch funktionieren, da sie die Attribute von der Definition der höheren Ebene übernimmt. Das Hinzufügen von Attributen und ihren Werten überschreibt die übernommenen Attribute und ändert die Funktion der Dokumentenflussdefinition.
6. Klicken Sie auf **Speichern**.

PIP-Dokumentenflusspakete erstellen

Da RosettaNet von Zeit zu Zeit PIPs hinzufügt, müssen Sie möglicherweise Ihre eigenen PIP-Pakete erstellen, um diese neuen PIPs zu unterstützen oder um Upgrades für PIPs zu unterstützen. Die Prozeduren in diesem Abschnitt beschreiben, mit Ausnahme der angegeben Stellen, wie das PIP-Dokumentenflusspaket für PIP 5C4 V01.03.00 erstellt wird. WebSphere Partner Gateway stellt ein PIP-Dokumentenflusspaket für PIP 5C4 V01.02.00 bereit. Die Prozeduren dokumentieren daher tatsächlich, wie ein Upgrade ausgeführt wird. Das Erstellen eines PIP-Dokumentenflusspakets ist allerdings gleich und die Prozeduren geben alle zusätzlichen Schritte an.

Bevor Sie beginnen, laden Sie die PIP-Spezifikationen von `www.rosettanet.org` für die neue Version und, falls Sie ein Upgrade ausführen, auch für die alte Version herunter. Wenn Sie z. B. das Upgrade ausführen, das in den Prozeduren beschrieben ist, laden Sie `5C4_DistributeRegistrationStatus_V01_03_00.zip` und `5C4_DistributeRegistrationStatus_V01_02_00.zip` herunter. Die Spezifikation umfasst die folgenden Dateitypen:

- RosettaNet-XML-Nachrichtenrichtlinien - HTML-Dateien, wie z. B. `5C4_MG_V01_03_00_RegistrationStatusNotification.htm`, die die Kardinalität, das Vokabular, die Struktur sowie die zulässigen Datenelementwerte und die Werttypen des PIP definieren.
- RosettaNet-XML-Nachrichtenschema - DTD-Dateien, wie z. B. `5C4_MS_V01_03_RegistrationStatusNotification.dtd`, die die Reihenfolge, die Elementbenennung, die Zusammensetzung und die Attribute des PIP definieren.
- PIP-Spezifikation - DOC-Datei, wie z. B. `5C4_Spec_V01_03_00.doc`, die die Geschäftsleistungsbedienelemente des PIP bereitstellt.
- PIP-Release-Informationen - DOC-Datei, wie z. B. `5C4_V01_03_00_ReleaseNotes.doc`, die den Unterschied zwischen dieser Version und der vorherigen Version beschreibt.

Das Erstellen oder Upgraden eines PIP-Dokumentenflusspakets umfasst die folgenden Prozeduren:

- Die XSD-Dateien erstellen
- Die XML-Datei erstellen
- Die Pakete erstellen

Die XSD-Dateien erstellen

Ein PIP-Dokumentenflusspaket enthält XML-Schemadateien, die die Nachrichtenformate und zulässige Werte für Elemente definieren. Die folgende Prozedur beschreibt, wie Sie diese Dateien basierend auf dem Inhalt der PIP-Spezifikationsdatei erstellen.

Sie erstellen mindestens eine XSD-Datei für jede DTD-Datei in der PIP-Spezifikationsdatei. Im Falle eines Upgrades auf PIP 5C4 V01.03.00 beschreibt die Prozedur, da das Nachrichtenformat sich geändert hat, als Beispiel wie Sie die Datei `BCG_5C4RegistrationStatusNotification_V01.03.xsd` erstellen. Weitere Informationen zu XSD-Dateien finden Sie in „Informationen zur Validierung" auf Seite 258.

Führen Sie die folgenden Schritte aus, um die XSD-Dateien für das PIP-Dokumentenflusspaket zu erstellen:

1. Importieren oder laden Sie die DTD-Datei in einen XML-Editor, wie z. B. WebSphere Studio Application Developer. Laden Sie z. B. die Datei `5C4_MS_V01_03_RegistrationStatusNotification.dtd`.
2. Konvertieren Sie mit dem XML-Editor die DTD-Datei in ein XML-Schema. Die folgenden Schritte beschreiben, wie Sie dies mit Application Developer ausführen:
   a. Öffnen Sie in der Anzeige **Navigation** der Perspektive **XML** das Projekt mit der importierten DTD-Datei.
   b. Klicken Sie mit der rechten Maustaste auf die DTD-Datei, und wählen Sie **Generieren > XML-Schema** aus.
   c. Geben Sie in der Anzeige **Generieren** die Position ein, bzw. wählen Sie diese dort aus, wo Sie die neue XSD-Datei speichern wollen. Geben Sie in das Feld **Dateiname** den Namen der neuen XSD-Datei ein. Im vorliegenden Beispiel würden Sie einen Namen, wie z. B. `BCG_5C4RegistrationStatusNotification_V01.03.xsd`, eingeben.
   d. Klicken Sie auf **Fertig stellen**.
3. Kompensieren Sie die Elemente, die über mehrere Kardinalitätswerte in den RosettaNet-XML-Richtlinien verfügen, indem Sie der neuen XSD-Datei Spezifikationen hinzufügen. Die Richtlinien stellen die Elemente in der Nachricht mit einer Baumstruktur dar und zeigen die Kardinalität jedes Elements links neben dem Element an.

   Im Allgemeinen stimmen die Elemente in den Richtlinien mit den Definitionen der Elemente in der DTD-Datei überein. Die Richtlinien könnten jedoch einige Elemente enthalten, die denselben Namen aber unterschiedliche Kardinalitäten haben. Da die DTD-Datei in diesem Fall nicht die Kardinalität zur Verfügung stellen kann, müssen Sie die XSD-Datei modifizieren. Die Richtliniendatei `5C4_MG_V01_03_00_RegistrationStatusNotification.htm` hat z. B. eine Definition für **ContactInformation** in Zeile 15, die über fünf untergeordnete Elemente mit den folgenden Kardinalitäten verfügt:

   1 contactName

   0..1 EmailAddress

   0..1 facsimileNumber

   0..1 PhysicalLocation

   0..1 telephoneNumber

Die Definition für **ContactInformation** in Zeile 150 verfügt über vier untergeordnete Elemente mit den folgenden Kardinalitäten:

1 contactName

1 EmailAddress

0..1 facsimileNumber

1 telephoneNumber

In der XSD-Datei verfügt aber jedes untergeordnete Element von **ContactInformation** über eine Kardinalität, die beiden Definitionen entspricht:

```
<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>
```

Wenn Sie das PIP-Dokumentenflusspaket auf einer anderen Version des Pakets basierend aktualisieren, und Sie eine Definition von der anderen Version wiederverwenden wollen, führen Sie die folgenden Schritte für jede dieser Definitionen aus:

a. Löschen Sie die Definition des Elements. Löschen Sie z. B. das Element **ContactInformation**.

b. Öffnen Sie das PIP-Dokumentenflusspaket der Version, die ersetzt wird. Öffnen Sie z. B. die Datei `BCG_Package_RNIFV02.00_5C4V01.02.zip`.

c. Suchen Sie die Definition, die Sie wiederverwenden wollen. Die Definition von **ContactInformation_type7** in der Datei `BCG_ContactInformation_Types.xsd` stimmt z. B. mit der Definition überein, die Sie für Zeile 15 der Richtlinien benötigen.

```
<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. Erstellen Sie in der neuen XSD-Datei, die Sie für das aktualisierte PIP-Dokumentenflusspaket erstellen, einen Verweis auf die XSD-Datei, die die wiederzuverwendende Definition enthält. Erstellen Sie z. B. einen Verweis auf `BCG_ContactInformation_Types.xsd` in der Datei `BCG_5C4RegistrationStatusNotification_V01.03.xsd` wie folgt:

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

e. Löschen Sie in der neuen XSD-Datei das Attribut **ref** jedes Elements, das auf das gelöschte Element verweist. Fügen Sie ein Attribut **type** hinzu, das auf die wiederzuverwendende Definition verweist. Löschen Sie z. B. im Element **productProviderFieldApplicationEngineer** den Verweis *ref="Contact Information"*, und fügen Sie die folgenden Informationen hinzu:

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

Wenn Sie ein PIP-Dokumentenflusspaket erstellen, oder Sie ein PIP-Dokumentenflusspaket upgraden, aber die benötigte Definition nicht in der anderen Version vorhanden ist, führen Sie die folgenden Schritte für jede Instanz des Elements aus, das Sie in den Richtlinien gefunden haben:

a. Löschen Sie die Definition des Elements. Löschen Sie z. B. das Element **ContactInformation**.

b. Erstellen Sie die Ersetzungsdefinition. Erstellen Sie z. B. die Definition **ContactInformation_localType1** so, dass diese mit der Definition in Zeile 15 der Richtlinien übereinstimmt.

```
<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. Löschen Sie für jedes Element, das auf das gelöschte Element verweist, sein Attribut **ref**, und fügen Sie ein Attribut **type** hinzu, das auf den entsprechenden komplexen Typ verweist, welchen Sie im vorherigen Schritt definiert haben. Löschen Sie z. B. im Element **productProviderFieldApplicationEngineer** den Verweis *ref="Contact Information"*, und fügen Sie die folgenden Informationen hinzu:

```
name="ContactInformation"
type="ContactInformation_localType1"
```

Abb. 35 zeigt das Element productProviderFieldApplicationEngineer, bevor es geändert wird.

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

Abbildung 35. Element **productProviderFieldApplicationEngineer** *vor der Änderung*

Abb. 36 zeigt das Element productProviderFieldApplicationEngineer, nachdem es geändert wurde.

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

Abbildung 36. Element **productProviderFieldApplicationEngineer** *nach der Änderung*

4. Geben Sie die Aufzählungswerte für Elemente an, die nur über spezifische Werte verfügen können. Die Richtlinien definieren die Aufzählungswerte in den Tabellen des Abschnitts **Guideline Information** (Richtlinieninformationen).

   In einer PIP 5C4 V01.03.00-Nachricht kann z. B. **GlobalRegistrationComplexityLevelCode** nur über die folgenden Werte verfügen: **Above average (Über dem Durchschnitt), Average (Durchschnitt), Maximum (Maximum), Minimum (Minimum), None (Kein) und Some (Einiges)**.

   Wenn Sie das PIP-Dokumentenflusspaket basierend auf einer anderen Version des Pakets aktualisieren, und Sie eine Gruppe von Aufzählungswerten von der anderen Version wiederverwenden wollen, führen Sie die folgenden Schritte für jede dieser Gruppen aus:

   a. Löschen Sie die Definition für das Element. Löschen Sie z. B. das Element **GlobalRegistrationComplexityLevelCode**:

   b. Öffnen Sie das PIP-Dokumentenflusspaket der Version, die ersetzt wird. Öffnen Sie z. B. die Datei `BCG_Package_RNIFV02.00_5C4V01.02.zip`.

   c. Suchen Sie die Definition mit den Aufzählungswerten, die Sie wiederverwenden wollen. Die Definition **_GlobalRegistrationComplexityLevelCode** in der Datei `BCG_GlobalRegistrationComplexityLevelCode.xsd` enthält die Aufzählungswertdefinitionen, die durch die Tabelle **Entity Instances** (Entitätsinstanzen) definiert werden.

      ```
      <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. Erstellen Sie in der neuen XSD-Datei, die Sie für das aktualisierte PIP-Dokumentenflusspaket erstellen, einen Verweis auf die XSD-Datei, die die wiederzuverwendende Definition enthält. Erstellen Sie z. B. einen Verweis auf `BCG_GlobalRegistrationComplexityLevelCode.xsd` in der Datei `BCG_5C4RegistrationStatusNotification_V01.03.xsd` wie folgt:

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

   e. Löschen Sie in der neuen XSD-Datei das Attribut **ref** jedes Elements, das auf das gelöschte Element verweist. Fügen Sie ein Attribut **type** hinzu, das auf die wiederzuverwendende Definition verweist. Löschen Sie z. B. im Element **DesignAssemblyInformation** den Verweis *ref*="GlobalRegistrationComplexityLevelCode", und fügen Sie die folgenden Informationen hinzu:

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

   Wenn Sie ein PIP-Dokumentenflusspaket erstellen, oder Sie ein PIP-Dokumentenflusspaket upgraden, aber die benötigten Aufzählungswertdefinitionen nicht in der anderen Version vorhanden sind, führen Sie die folgenden Schritte für jedes Element mit Aufzählungswerten in den Richtlinien aus:

   a. Löschen Sie die Definition des Elements. Löschen Sie z. B. das Element **GlobalRegistrationComplexityLevelCode**.

b. Erstellen Sie die Ersetzungsdefinition. Erstellen Sie z. B. die Definition **GlobalRegistrationComplexityLevelCode_localType**, und schließen Sie die Aufzählungswertdefinitionen, wie von der Tabelle beschrieben, mit ein.

```
<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. Löschen Sie für jedes Element, das auf das gelöschte Element verweist, sein Attribut **ref**, und fügen Sie ein Attribut **type** hinzu, das auf den entsprechenden komplexen Typ verweist, welchen Sie im vorherigen Schritt definiert haben. Löschen Sie z. B. *ref="GlobalRegistrationComplexityLevelCode"*, und fügen Sie die folgenden Informationen hinzu:

```
        name="GlobalRegistrationComplexityLevelCode"
type="GlobalRegistrationComplexityLevelCode_localType"
```

Abb. 37 zeigt das Element `DesignAssemblyInformation`, bevor es geändert wird.

```
<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>
```

Abbildung 37. Element **DesignAssemblyInformation** *vor der Änderung*

Abb. 38 auf Seite 253 zeigt das Element `DesignAssemblyInformation`, nachdem es geändert wurde.

```
<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>
```

Abbildung 38. Element **DesignAssemblyInformation** *nach der Änderung*

5. Legen Sie **Data Type** (Datentyp), **Min** (minimale Länge) und **Max** (maximale Länge) und **Representation** (Darstellung) von **Data Entities** (Datenentitäten) fest. Die RosettaNet-XML-Nachrichtenrichtlinien stellen diese Informationen in der Tabelle **Fundamental Business Data Entities** (Grundlegende Geschäftsdatenentitäten) bereit.

   Wenn Sie das PIP-Dokumentenflusspaket basierend auf einer anderen Version des Pakets aktualisieren, und Sie eine Datenentitätsdefinition von der anderen Version wiederverwenden wollen, führen Sie die folgenden Schritte für jede Gruppe aus:

   a. Löschen Sie die Definition für das Datenentitätselement. Löschen Sie z. B. das Element **DateStamp**.
   b. Öffnen Sie das PIP-Dokumentenflusspaket der Version, die Sie ersetzen. Öffnen Sie z. B. die Datei `BCG_Package_RNIFV02.00_5C4V01.02.zip`.
   c. Suchen Sie die Definition, die Sie wiederverwenden wollen. Die Definition **_common_DateStamp_R** in der Datei `BCG_common.xsd` enthält die folgende Definition, welche den in den Richtlinien gegebenen Informationen entspricht.

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

   d. Erstellen Sie in der neuen XSD-Datei, die Sie für das aktualisierte PIP-Dokumentenflusspaket erstellen, einen Verweis auf die XSD-Datei, die die wiederzuverwendende Definition enthält. Erstellen Sie z. B. einen Verweis auf `BCG_common.xsd` in der Datei `BCG_5C4RegistrationStatusNotification_V01.03.xsd` wie folgt:

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

   e. Löschen Sie in der neuen XSD-Datei das Attribut **ref** jedes Elements, das auf das gelöschte Element verweist. Fügen Sie ein Attribut **type** hinzu, das auf

die wiederzuverwendende Definition verweist. Löschen Sie z. B. im Element **DesignAssemblyInformation** den Verweis *ref*=″DateStamp″, und fügen Sie die folgenden Informationen hinzu:

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

Wenn Sie ein PIP-Dokumentenflusspaket erstellen, oder Sie ein PIP-Dokumentenflusspaket upgraden, aber die benötigte Datenentitätsdefinition nicht in der anderen Version vorhanden ist, führen Sie die folgenden Schritte für jedes Datenentitätselement aus:

a. Löschen Sie die Definition des Elements. Löschen Sie z. B. das Element **DateStamp**.

b. Erstellen Sie die Ersetzungsdefinition. Verwenden Sie z. B. die Informationen zum Datentyp, zur minimalen Länge und zur maximalen Länge sowie zur Darstellung, um die Definition **DateStamp_localType** zu erstellen.

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

c. Löschen Sie für jedes Element, das auf das gelöschte Element verweist, sein Attribut **ref**, und fügen Sie ein Attribut **type** hinzu, das auf den entsprechenden komplexen Typ verweist, welchen Sie im vorherigen Schritt definiert haben. Löschen Sie z. B. *ref=″DateStamp″*, und fügen Sie die folgenden Informationen hinzu:

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

Abb. 39 zeigt das Element `beginDate`, bevor es geändert wird.

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

Abbildung 39. Element **beginDate** *vor der Änderung*

Abb. 40 zeigt das Element `beginDate`, nachdem es geändert wurde.

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

Abbildung 40. Element **beginDate** *nach der Änderung*

Die XML-Datei erstellen

Nachdem Sie die XSD-Dateien für Ihr PIP-Dokumentenflusspaket erstellt haben, können Sie nun die XML-Datei für das Paket **RNIF** und die XML-Datei für das Paket **Backend Integration** erstellen. Diese Pakete heißen z. B. `BCG_Package_RNIFV02.00_5C4V01.03.zip` und `BCG_Package_RNSC1.0_RNIFV02.00_5C4V01.03.zip`. Die folgende Prozedur beschreibt, wie Sie die XML-Datei für das RNIF-Paket erstellen:

1. Extrahieren Sie die XML-Datei von einer RNIF-PIP-Dokumentenflusspaketdatei. Wenn Sie ein Upgrade durchführen, extrahieren Sie die Datei von der vorherigen Version des Pakets (z. B. `BCG_Package_RNIFV02.00_5C4V01.02.zip`). Wenn Sie ein neues Paket erstellen, extrahieren Sie die Datei von einem PIP-Dokumentenflusspaket, das dem zu erstellenden Paket gleicht. Wenn Sie z. B. ein Paket erstellen, um einen Doppelaktions-PIP zu unterstützen, kopieren Sie die XML-Datei von einem anderen Doppelaktions-PIP-Paket.
2. Kopieren Sie die Datei, und benennen Sie diese entsprechend um (z. B. `BCG_RNIFV02.00_5C4V01.03.xml`).
3. Aktualisieren Sie in der neuen Datei die Elemente, die Informationen zum PIP enthalten. Die folgende Tabelle listet z. B. die Informationen auf, die Sie im 5C4 PIP-Beispiel aktualisieren müssen. Beachten Sie, dass die Informationen mehr als einmal in der Datei vorkommen könnten. Stellen Sie sicher, dass Sie alle Instanzen aktualisieren.

Tabelle 37. 5C4 PIP-Aktualisierungsinformationen

Zu ändernde Informationen	**Alter Wert**	**Neuer Wert**
PIP-ID	5C4	5C4
PIP-Version	V01.02	V01.03
Der Name der Anforderungsnachrichten-DTD-Datei ohne Dateierweiterung	5C4_MS_V01_02_ RegistrationStatusNotification	5C4_MS_V01_03_ RegistrationStatusNotification
Der Name der Bestätigungsnachrichten-DTD-Datei ohne Dateierweiterung (nur für Doppelaktions-PIPs)	N/V	N/V
Der Name der Anforderungsnachrichten-XSD-Datei ohne Dateierweiterung	BCG_5C4RegistrationStatus Notification_V01.02	BCG_5C4RegistrationStatus Notification_V01.03
Der Name der Bestätigungsnachrichten-XSD-Datei ohne Dateierweiterung (nur für Doppelaktions-PIPs)	N/V	N/V
Rootelementname in der XSD-Datei für die Anforderungsnachricht	Pip5C4RegistrationStatus Notification	Pip5C4RegistrationStatus Notification
Rootelementname in der XSD-Datei für die Bestätigungsnachricht (nur für Doppelaktions-PIPs)	N/V	N/V

4. Öffnen Sie das PIP-Spezifikationsdokument, und verwenden Sie es, um die in der folgenden Tabelle aufgelisteten Informationen zu aktualisieren. Wenn Sie eine Aktualisierung durchführen, vergleichen Sie die Spezifikationen für die Versionen, da Sie diese Werte unter Umständen nicht aktualisieren müssen.

Tabelle 38. 5C4 PIP-Aktualisierungsinformationen von der PIP-Spezifikation

Zu aktualisierende Informationen	Beschreibung	Wert im 5C4-Paket
Aktivitätsname	Angegeben in Tabelle 3-2	Distribute Registration Status
Initiatorrollenname	Angegeben in Tabelle 3-1	Product Provider
Responderrollenname	Angegeben in Tabelle 3-1	Demand Creator
Anforderungsaktionsname	Angegeben in Tabelle 4-2	Registration Status Notification
Bestätigungsaktionsname	Angegeben in Tabelle 4-2 (nur für Doppelaktions-PIPs)	N/V

5. Aktualisieren Sie die Paketattributwerte. Wenn Sie eine Aktualisierung durchführen, vergleichen Sie die Spezifikationen für die Versionen, da Sie diese Werte unter Umständen nicht aktualisieren müssen.

   Anmerkung: Wenn Sie das Paket **Backend Integration** erstellen, überspringen Sie diesen Schritt, und fahren Sie mit Schritt 6 auf Seite 257 fort.

Tabelle 39. 5C4 PIP-Attributaktualisierungen

Zu aktualisierende Informationen	Beschreibung	Wert im 5C4-Paket	Elementpfad in der XML-Datei
NonRepudiation Required	Angegeben in Tabelle 3-3	N	ns1:Package ns1:Protocol ns1:Process ns1:Attribute (sein ATTRIBUTEKEY ist NonRepudiationRequired) ns1:AttributeValue AttributePickListItem ATTRVALUEKEY
NonRepudiationOf Receipt	Angegeben in Tabelle 3-3	N	ns1:Package ns1:Protocol ns1:Process ns1:Attribute (sein ATTRIBUTEKEY ist NonRepudiationOfReceipt) ns1:AttributeValue AttributePickListItem ATTRVALUEKEY
DigitalSignature Required	Angegeben in Tabelle 5-1	Y	ns1:Package ns1:Protocol ns1:Process ns1:Attribute (sein ATTRIBUTEKEY ist DigitalSignatureRequired) ns1:AttributeValue AttributePickListItem ATTRVALUEKEY
TimeToAcknowledge	Angegeben in Tabelle 3-3	2 (120 min)	ns1:Package ns1:Protocol ns1:Process ns1:Attribute (sein ATTRIBUTEKEY ist TimeToAcknowledge) ns1:AttributeValue ATTRVALUE

Tabelle 39. 5C4 PIP-Attributaktualisierungen (Forts.)

Zu aktualisierende Informationen	Beschreibung	Wert im 5C4-Paket	Elementpfad in der XML-Datei
TimeToPerform	Angegeben in Tabelle 3-3	2 (120 min)	ns1:Package ns1:Protocol ns1:Process ns1:Attribute (sein ATTRIBUTEKEY ist TimeToPerform) ns1:AttributeValue ATTRVALUE
RetryCount	Angegeben in Tabelle 3-3	3	ns1:Package ns1:Protocol ns1:Process ns1:Attribute (sein ATTRIBUTEKEY ist RetryCount) ns1:AttributeValue ATTRVALUE

6. Aktualisieren Sie die Elemente **ns1:Package/ns1:Protocol/GuidelineMap**, um nicht mehr verwendete XSD-Dateien zu entfernen und um jede XSD-Datei hinzuzufügen, die Sie erstellt oder auf die Sie verwiesen haben.

Um das Paket **Backend Integration** zu erstellen, wiederholen Sie Schritt 1 bis 6, mit Ausnahme der folgenden Unterschiede:

- Extrahieren Sie in Schritt 1 auf Seite 255 die XML-Datei aus dem Paket **Backend Integration** (z. B. `BCG_Package_RNSC1.0_RNIFV02.00_5C4V01.02.zip`).
- Führen Sie Schritt 5 auf Seite 256 nicht aus.

Nachdem Sie die XML- und XSD-Dateien erstellt haben, können Sie die PIP-Dokumentenflusspakete erstellen.

Das Paket erstellen

Führen Sie die folgenden Schritte aus, um das RNIF-Paket zu erstellen:

1. Erstellen Sie ein Verzeichnis `GuidelineMaps`, und kopieren Sie die XSD-Dateien des Pakets in dieses Verzeichnis.
2. Erstellen Sie ein Verzeichnis `Packages`, und kopieren Sie die RNIF-XML-Datei in dieses Verzeichnis.
3. Gehen Sie in das übergeordnete Verzeichnis, und erstellen Sie ein PIP-Dokumentenflusspaket (ZIP-Datei), die die Verzeichnisse `GuidelineMaps` und `Packages` enthält. Sie müssen die Verzeichnisstruktur in der ZIP-Datei beibehalten.

Um das Paket **Backend Integration** zu erstellen, führen Sie die Schritte 1 bis 3 aus, aber verwenden Sie die Backend Integration-XML-Datei anstelle der RNIF-Datei.

Nachdem Sie das PIP-Paket erstellt haben, können Sie es mit der im Abschnitt „RNIF- und PIP-Dokumentenflusspakete" auf Seite 72 beschriebenen Prozedur hochladen.

Informationen zur Validierung

WebSphere Partner Gateway validiert den Serviceinhalt einer RosettaNet-Nachricht mit Hilfe von Validierungszuordnungen. Diese Validierungszuordnungen definieren die Struktur einer gültigen Nachricht und definieren die Kardinalität, das Format und die gültigen Werte (Aufzählung) der Elemente in der Nachricht. In jedem PIP-Dokumentenflusspaket stellt WebSphere Partner Gateway die Validierungszuordnungen als XSD-Dateien im Verzeichnis `GuidelineMaps` bereit.

Da RosettaNet das Format einer PIP-Nachricht angibt, müssen Sie in der Regel die Validierungszuordnungen nicht anpassen. Wenn Sie dies jedoch durchführen, finden Sie in „PIP-Dokumentenflusspakete erstellen" auf Seite 247 Informationen zu den Schritten, die zum Upgraden der XSD-Dateien nötig sind, mit denen die Nachrichten validiert werden, und dazu, wie Sie ein angepasstes PIP-Dokumentenflusspaket erstellen.

Kardinalität

Die Kardinalität bestimmt, wie häufig ein bestimmtes Element in einer Nachricht angezeigt werden kann oder muss. In den Validierungszuordnungen bestimmen die Attribute **minOccurs** und **maxOccurs** die Kardinalität des Attributs, wie im folgenden Beispiel aus der Datei `BCG_5C4RegistrationStatusNotification_V01.02.xsd` gezeigt wird:

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

Wenn WebSphere Partner Gateway nicht die Kardinalität eines Elements überprüfen muss, sind die Werte für die Attribute **minOccurs** und **maxOccurs** des Elements in den Validierungszuordnungen mit ″0″ und ″unbounded″ angegeben, wie im Beispiel dargestellt:

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

Format

Das Format bestimmt die Anordnung bzw. das Layout der Daten für den Typ eines Elements. In den Validierungszuordnungen verfügt der Typ über mindestens eine Einschränkung, wie in den folgenden Beispielen dargestellt:

Beispiel 1

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

Alle Elemente des Typs **_common_LineNumber_R** in einer Nachricht müssen Zeichenfolgen (string) sein und 1 bis 6 Zeichen lang sein.

Beispiel 2

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

Alle Elemente des Typs **_GlobalLocationIdentifier** in einer Nachricht müssen Zeichenfolgen (string) sein und über neun numerische Datenzeichen gefolgt von einem bis vier alphanumerischen Datenzeichen verfügen. Die minimale Länge beträgt daher 10 Zeichen und die maximale Länge sind 13 Zeichen.

Beispiel 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>
```

Alle Elemente des Typs **_DayofMonth** in einer Nachricht müssen positive ganze Zahlen (positiveInteger) sein und über ein oder zwei Zeichen verfügen und einen Wert von 1 bis inklusive 31 haben.

Aufzählung

Die Aufzählung bestimmt die gültigen Werte für ein Element. In den Validierungszuordnungen verfügt der Typ des Elements über mindestens eine Aufzählungseinschränkung, wie in dem folgenden Beispiel dargestellt:

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

Alle Elemente des Typs **_local_GlobalDesignRegistrationNotificationCode** in einer Nachricht dürfen nur ″Initial″ oder ″Update″ als Werte haben.

Inhalt der PIP-Dokumentenflusspakete

Die folgenden Abschnitte zeigen die PIP-Dokumentenflusspakete, die von WebSphere Partner Gateway für jeden PIP bereitgestellt werden. In jedem Paket ist eine XML-Datei in einem Verzeichnis `Packages` und es sind mehrere XSD-Dateien in einem Verzeichnis `GuidelineMaps` enthalten, die alle PIP-Dokumentenflusspakete für den PIP gemeinsam haben.

0A1 Notification of Failure V1.0

Der folgende Abschnitt beschreibt den Inhalt für den PIP **0A1 Notification of Failure V1.0**.

Inhalt der Paketdatei

Die folgende Tabelle zeigt die ZIP-Dateien und entsprechenden XML-Dateien für den PIP **0A1 Notification of Failure V1.0**. Die Richtlinienzuordnungen, die für alle Versionen gleich sind, werden im nachfolgenden Abschnitt gezeigt.

Tabelle 40. ZIP- und XML-Dateien für PIP **0A1 Notification of Failure V1.0**

ZIP-Dateiname	XML-Dateiname
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

Inhalt der Richtlinienzuordnungen

Dieser Abschnitt listet den Inhalt der Richtlinienzuordnungen für **0A1 Notification of Failure V1.0** auf:

- 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

Der folgende Abschnitt beschreibt den Inhalt für den PIP **0A1 Notification of Failure V02.00**.

Inhalt der Paketdatei

Die folgende Tabelle zeigt die ZIP-Dateien und entsprechenden XML-Dateien für den PIP **0A1 Notification of Failure V02.00**. Die Richtlinienzuordnungen, die für alle Versionen gleich sind, werden im nachfolgenden Abschnitt gezeigt.

Tabelle 41. ZIP- und XML-Dateien für PIP **0A1 Notification of Failure V02.00**

ZIP-Dateiname	XML-Dateiname
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

Inhalt der Richtlinienzuordnungen

Dieser Abschnitt listet den Inhalt der Richtlinienzuordnungen für **0A1 Notification of Failure V02.00** auf:

- 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

Der folgende Abschnitt beschreibt den Inhalt für den PIP **2A1 Distribute New Product Information**.

Inhalt der Paketdatei

Die folgende Tabelle zeigt die ZIP-Dateien und entsprechenden XML-Dateien für den PIP **2A1 Distribute New Product Information**. Die Richtlinienzuordnungen, die für alle Versionen gleich sind, werden im nachfolgenden Abschnitt gezeigt.

Tabelle 42. ZIP- und XML-Dateien für **2A1 Distribute New Product Information**

ZIP-Dateiname	XML-Dateiname
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

Tabelle 42. ZIP- und XML-Dateien für **2A1 Distribute New Product Information** *(Forts.)*

ZIP-Dateiname	XML-Dateiname
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

Inhalt der Richtlinienzuordnungen

Dieser Abschnitt listet den Inhalt der Richtlinienzuordnungen für **2A1 Distribute New Product Information** auf:

- 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

Der folgende Abschnitt beschreibt den Inhalt für den PIP **2A12 Distribute Product Master**.

Inhalt der Paketdatei

Die folgende Tabelle zeigt die ZIP-Dateien und entsprechenden XML-Dateien für den PIP **2A12 Distribute Product Master**. Die Richtlinienzuordnungen, die für alle Versionen gleich sind, werden im nachfolgenden Abschnitt gezeigt.

Tabelle 43. ZIP- und XML-Dateien für **2A12 Distribute Product Master**

ZIP-Dateiname	XML-Dateiname
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

Inhalt der Richtlinienzuordnungen

Dieser Abschnitt listet den Inhalt der Richtlinienzuordnungen für **2A12 Distribute Product Master** auf:

- 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

Der folgende Abschnitt beschreibt den Inhalt des PIP **3A1 Request Quote**.

Inhalt der Paketdatei

Die folgende Tabelle zeigt die ZIP-Dateien und entsprechenden XML-Dateien für den PIP **3A1 Request Quote**. Die Richtlinienzuordnungen, die für alle Versionen gleich sind, werden im nachfolgenden Abschnitt gezeigt.

Tabelle 44. ZIP- und XML-Dateien für PIP **3A1 Request Quote**

ZIP-Dateiname	XML-Dateiname
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

Inhalt der Richtlinienzuordnungen

Dieser Abschnitt listet den Inhalt der Richtlinienzuordnungen für **3A1 Request Quote** auf:

- 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

Der folgende Abschnitt beschreibt den Inhalt des PIP **3A2 Request Price and Availability**.

Inhalt der Paketdatei

Die folgende Tabelle zeigt die ZIP-Dateien und entsprechenden XML-Dateien für den PIP **3A2 Request Price and Availability**. Die Richtlinienzuordnungen, die für alle Versionen gleich sind, werden im nachfolgenden Abschnitt gezeigt.

Tabelle 45. ZIP- und XML-Dateien für **3A2 Request Price and Availability**

ZIP-Dateiname	XML-Dateiname
BCG_Package_RNIF1.1_3A2R02.01.zip	BCG_RNIF1.1_3A2R02.01.xml

Tabelle 45. ZIP- und XML-Dateien für **3A2 Request Price and Availability** *(Forts.)*

ZIP-Dateiname	XML-Dateiname
BCG_Package_RNIFV02.00_3A2R02.01.zip	BCG_RNIFV02.00_3A2R02.01.xml
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

Inhalt der Richtlinienzuordnungen

Dieser Abschnitt listet den Inhalt der Richtlinienzuordnungen für **3A2 Request Price and Availability** auf:

- 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

Der folgende Abschnitt beschreibt den Inhalt des PIP **3A4 Request Purchase Order V02.00**.

Inhalt der Paketdatei

Die folgende Tabelle zeigt die ZIP-Dateien und entsprechenden XML-Dateien für den PIP **3A4 Request Purchase Order**. Die Richtlinienzuordnungen, die für alle Versionen gleich sind, werden im nachfolgenden Abschnitt gezeigt.

Tabelle 46. ZIP- und XML-Dateien für **3A4 Request Purchase Order**

ZIP-Dateiname	XML-Dateiname
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

Inhalt der Richtlinienzuordnungen

Dieser Abschnitt listet den Inhalt der Richtlinienzuordnungen für **3A4 Request Purchase Order** auf:

- 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

Der folgende Abschnitt beschreibt den Inhalt des PIP **3A4 Request Purchase Order V02.02**.

Inhalt der Paketdatei

Die folgende Tabelle zeigt die ZIP-Dateien und entsprechenden XML-Dateien für den PIP **3A4 Request Purchase Order**. Die Richtlinienzuordnungen, die für alle Versionen gleich sind, werden im nachfolgenden Abschnitt gezeigt.

Tabelle 47. ZIP- und XML-Dateien für **3A4 Request Purchase Order**

ZIP-Dateiname	XML-Dateiname
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

Inhalt der Richtlinienzuordnungen

Dieser Abschnitt listet den Inhalt der Richtlinienzuordnungen für **3A4 Request Purchase Order** auf:

- 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

Der folgende Abschnitt beschreibt den Inhalt des PIP **3A5 Query Order Status**.

Inhalt der Paketdatei

Die folgende Tabelle zeigt die ZIP-Dateien und entsprechenden XML-Dateien für den PIP **3A5 Query Order Status**. Die Richtlinienzuordnungen, die für alle Versionen gleich sind, werden im nachfolgenden Abschnitt gezeigt.

Tabelle 48. ZIP- und XML-Dateien für **3A5 Query Order Status**

ZIP-Dateiname	XML-Dateiname
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

Inhalt der Richtlinienzuordnungen

Dieser Abschnitt listet den Inhalt der Richtlinienzuordnungen für **3A5 Query Order Status** auf:

- 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

Der folgende Abschnitt beschreibt den Inhalt des PIP **3A6 Distribute Order Status**.

Inhalt der Paketdatei

Die folgende Tabelle zeigt die ZIP-Dateien und entsprechenden XML-Dateien für den PIP **3A6 Distribute Order Status**. Die Richtlinienzuordnungen, die für alle Versionen gleich sind, werden im nachfolgenden Abschnitt gezeigt.

Tabelle 49. ZIP- und XML-Dateien für **3A6 Distribute Order Status**

ZIP-Dateiname	XML-Dateiname
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

Inhalt der Richtlinienzuordnungen

Dieser Abschnitt listet den Inhalt der Richtlinienzuordnungen für **3A6 Distribute Order Status** auf:

- 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

Der folgende Abschnitt beschreibt den Inhalt des PIP **3A7 Notify of Purchase Order Update**.

Inhalt der Paketdatei

Die folgende Tabelle zeigt die ZIP-Dateien und entsprechenden XML-Dateien für den PIP **3A7 Notify of Purchase Order Update**. Die Richtlinienzuordnungen, die für alle Versionen gleich sind, werden im nachfolgenden Abschnitt gezeigt.

Tabelle 50. ZIP- und XML-Dateien für **3A7 Notify of Purchase Order Update**

ZIP-Dateiname	XML-Dateiname
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

Inhalt der Richtlinienzuordnungen

Dieser Abschnitt listet den Inhalt der Richtlinienzuordnungen für **3A7 Notify of Purchase Order Update** auf:

- 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

Der folgende Abschnitt beschreibt den Inhalt des PIP **3A8 Request Purchase Order Change V01.02**.

Inhalt der Paketdatei

Die folgende Tabelle zeigt die ZIP-Dateien und entsprechenden XML-Dateien für den PIP **3A8 Request Purchase Order Change**. Die Richtlinienzuordnungen, die für alle Versionen gleich sind, werden im nachfolgenden Abschnitt gezeigt.

Tabelle 51. ZIP- und XML-Dateien für **3A8 Request Purchase Order Change**

ZIP-Dateiname	XML-Dateiname
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

Tabelle 51. ZIP- und XML-Dateien für **3A8 Request Purchase Order Change** *(Forts.)*

ZIP-Dateiname	XML-Dateiname
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

Inhalt der Richtlinienzuordnungen

Dieser Abschnitt listet den Inhalt der Richtlinienzuordnungen für **3A8 Request Purchase Order Change** auf:

- 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

Der folgende Abschnitt beschreibt den Inhalt des PIP **3A8 Request Purchase Order Change V01.03**.

Inhalt der Paketdatei

Die folgende Tabelle zeigt die ZIP-Dateien und entsprechenden XML-Dateien für den PIP **3A8 Request Purchase Order Change**. Die Richtlinienzuordnungen, die für alle Versionen gleich sind, werden im nachfolgenden Abschnitt gezeigt.

Tabelle 52. ZIP- und XML-Dateien für **3A8 Request Purchase Order Change**

ZIP-Dateiname	XML-Dateiname
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

Inhalt der Richtlinienzuordnungen

Dieser Abschnitt listet den Inhalt der Richtlinienzuordnungen für **3A8 Request Purchase Order Change** auf:

- 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

Der folgende Abschnitt beschreibt den Inhalt des PIP **3A9 Request Purchase Order Cancellation**.

Inhalt der Paketdatei

Die folgende Tabelle zeigt die ZIP-Dateien und entsprechenden XML-Dateien für den PIP **3A9 Request Purchase Order Cancellation**. Die Richtlinienzuordnungen, die für alle Versionen gleich sind, werden im nachfolgenden Abschnitt gezeigt.

Tabelle 53. ZIP- und XML-Dateien für **3A9 Request Purchase Order Cancellation**

ZIP-Dateiname	XML-Dateiname
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

Inhalt der Richtlinienzuordnungen

Dieser Abschnitt listet den Inhalt der Richtlinienzuordnungen für **3A9 Request Purchase Order Cancellation** auf:

- 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

Der folgende Abschnitt beschreibt den Inhalt des PIP **3B2 Notify of Advance Shipment**.

Inhalt der Paketdatei

Die folgende Tabelle zeigt die ZIP-Dateien und entsprechenden XML-Dateien für den PIP **3B2 Notify of Advance Shipment**. Die Richtlinienzuordnungen, die für alle Versionen gleich sind, werden im nachfolgenden Abschnitt gezeigt.

Tabelle 54. ZIP- und XML-Dateien für **3B2 Notify of Advance Shipment**

ZIP-Dateiname	XML-Dateiname
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

Inhalt der Richtlinienzuordnungen

Dieser Abschnitt listet den Inhalt der Richtlinienzuordnungen für **3B2 Notify of Advance Shipment** auf:

- 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

Der folgende Abschnitt beschreibt den Inhalt des PIP **3B3 Distribute Shipment Status**.

Inhalt der Paketdatei

Die folgende Tabelle zeigt die ZIP-Dateien und entsprechenden XML-Dateien für den PIP **3B3 Distribute Shipment Status**. Die Richtlinienzuordnungen, die für alle Versionen gleich sind, werden im nachfolgenden Abschnitt gezeigt.

Tabelle 55. ZIP- und XML-Dateien für **3B3 Distribute Shipment Status**

ZIP-Dateiname	XML-Dateiname
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

Inhalt der Richtlinienzuordnungen

Dieser Abschnitt listet den Inhalt der Richtlinienzuordnungen für **3B3 Distribute Shipment Status** auf:

- 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

Der folgende Abschnitt beschreibt den Inhalt des PIP **3B11 Notify of Shipping Order**.

Inhalt der Paketdatei

Die folgende Tabelle zeigt die ZIP-Dateien und entsprechenden XML-Dateien für den PIP **3B11 Notify of Shipping Order**. Die Richtlinienzuordnungen, die für alle Versionen gleich sind, werden im nachfolgenden Abschnitt gezeigt.

Tabelle 56. ZIP- und XML-Dateien für **3B11 Notify of Shipping Order**

ZIP-Dateiname	XML-Dateiname
BCG_Package_RNIF1.1_3B11R01.00A.zip	BCG_RNIF1.1_3B11R01.00A.xml
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

Inhalt der Richtlinienzuordnungen

Dieser Abschnitt listet den Inhalt der Richtlinienzuordnungen für **3B11 Notify of Shipping Order** auf:

- 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

Der folgende Abschnitt beschreibt den Inhalt des PIP **3B12 Request of Shipping Order**.

Inhalt der Paketdatei

Die folgende Tabelle zeigt die ZIP-Dateien und entsprechenden XML-Dateien für den PIP **3B12 Request Shipping Order**. Die Richtlinienzuordnungen, die für alle Versionen gleich sind, werden im nachfolgenden Abschnitt gezeigt.

Tabelle 57. ZIP- und XML-Dateien für **3B12 Request Shipping Order**

ZIP-Dateiname	XML-Dateiname
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

Inhalt der Richtlinienzuordnungen

Dieser Abschnitt listet den Inhalt der Richtlinienzuordnungen für **3B12 Request Shipping Order** auf:

- 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

Der folgende Abschnitt beschreibt den Inhalt des PIP **3B13 Notify of Shipping Order Confirmation**.

Inhalt der Paketdatei

Die folgende Tabelle zeigt die ZIP-Dateien und entsprechenden XML-Dateien für den PIP **3B13 Notify of Shipping Order Confirmation**. Die Richtlinienzuordnungen, die für alle Versionen gleich sind, werden im nachfolgenden Abschnitt gezeigt.

Tabelle 58. ZIP- und XML-Dateien für **3B13 Notify of Shipping Order Confirmation**

ZIP-Dateiname	XML-Dateiname
BCG_Package_RNIF1.1_3B13V01.01.zip	BCG_RNIF1.1_3B13V01.01.xml
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

Inhalt der Richtlinienzuordnungen

Dieser Abschnitt listet den Inhalt der Richtlinienzuordnungen für **3B13 Notify of Shipping Order Confirmation** auf:

- 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

Der folgende Abschnitt beschreibt den Inhalt des PIP **3B14 Request Shipping Order Cancellation**.

Inhalt der Paketdatei

Die folgende Tabelle zeigt die ZIP-Dateien und entsprechenden XML-Dateien für den PIP **3B14 Request Shipping Order Cancellation**. Die Richtlinienzuordnungen, die für alle Versionen gleich sind, werden im nachfolgenden Abschnitt gezeigt.

Tabelle 59. ZIP- und XML-Dateien für **3B14 Request Shipping Order Cancellation**

ZIP-Dateiname	XML-Dateiname
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

Inhalt der Richtlinienzuordnungen

Dieser Abschnitt listet den Inhalt der Richtlinienzuordnungen für **3B14 Request Shipping Order Cancellation** auf:

- 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

Der folgende Abschnitt beschreibt den Inhalt des PIP **3B18 Notify of Shipping Documentation**.

Inhalt der Paketdatei

Die folgende Tabelle zeigt die ZIP-Dateien und entsprechenden XML-Dateien für den PIP **3B18 Notify of Shipping Documentation**. Die Richtlinienzuordnungen, die für alle Versionen gleich sind, werden im nachfolgenden Abschnitt gezeigt.

Tabelle 60. ZIP- und XML-Dateien für **3B18 Notify of Shipping Documentation**

ZIP-Dateiname	XML-Dateiname
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

Inhalt der Richtlinienzuordnungen

Dieser Abschnitt listet den Inhalt der Richtlinienzuordnungen für **3B18 Notify of Shipping Documentation** auf:

- 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

Der folgende Abschnitt beschreibt den Inhalt des PIP **3C1 Return Product**.

Inhalt der Paketdatei

Die folgende Tabelle zeigt die ZIP-Dateien und entsprechenden XML-Dateien für den PIP **3C1 Return Product**. Die Richtlinienzuordnungen, die für alle Versionen gleich sind, werden im nachfolgenden Abschnitt gezeigt.

Tabelle 61. ZIP- und XML-Dateien für **3C1 Return Product**

ZIP-Dateiname	XML-Dateiname
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

Inhalt der Richtlinienzuordnungen

Dieser Abschnitt listet den Inhalt der Richtlinienzuordnungen für **3C1 Return Product** auf:

- 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

Der folgende Abschnitt beschreibt den Inhalt des PIP **3C3 Notify of Invoice**.

Inhalt der Paketdatei

Die folgende Tabelle zeigt die ZIP-Dateien und entsprechenden XML-Dateien für den PIP **3C3 Notify of Invoice**. Die Richtlinienzuordnungen, die für alle Versionen gleich sind, werden im nachfolgenden Abschnitt gezeigt.

Tabelle 62. ZIP- und XML-Dateien für **3C3 Notify of Invoice**

ZIP-Dateiname	XML-Dateiname
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

Inhalt der Richtlinienzuordnungen

Dieser Abschnitt listet den Inhalt der Richtlinienzuordnungen für **3C3 Notify of Invoice** auf:

- 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

Der folgende Abschnitt beschreibt den Inhalt des PIP **3C4 Notify of Invoice Reject**.

Inhalt der Paketdatei

Die folgende Tabelle zeigt die ZIP-Dateien und entsprechenden XML-Dateien für den PIP **3C4 Notify of Invoice Reject**. Die Richtlinienzuordnungen, die für alle Versionen gleich sind, werden im nachfolgenden Abschnitt gezeigt.

Tabelle 63. ZIP- und XML-Dateien für **3C4 Notify of Invoice Reject**

ZIP-Dateiname	XML-Dateiname
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

Inhalt der Richtlinienzuordnungen

Dieser Abschnitt listet den Inhalt der Richtlinienzuordnungen für **3C4 Notify of Invoice Reject** auf:

- 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

Der folgende Abschnitt beschreibt den Inhalt des PIP **3C6 Notify of Remittance Advice**.

Inhalt der Paketdatei

Die folgende Tabelle zeigt die ZIP-Dateien und entsprechenden XML-Dateien für den PIP **3C6 Notify of Remittance Advice**. Die Richtlinienzuordnungen, die für alle Versionen gleich sind, werden im nachfolgenden Abschnitt gezeigt.

Tabelle 64. ZIP- und XML-Dateien für **3C6 Notify of Remittance Advice**

ZIP-Dateiname	XML-Dateiname
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

Inhalt der Richtlinienzuordnungen

Dieser Abschnitt listet den Inhalt der Richtlinienzuordnungen für **3C6 Notify of Remittance Advice** auf:

- 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

Der folgende Abschnitt beschreibt den Inhalt des PIP **3C7 Notify of Self-Billing Invoice**.

Inhalt der Paketdatei

Die folgende Tabelle zeigt die ZIP-Dateien und entsprechenden XML-Dateien für den PIP **3C7 Notify of Self-Billing Invoice**. Die Richtlinienzuordnungen, die für alle Versionen gleich sind, werden im nachfolgenden Abschnitt gezeigt.

Tabelle 65. ZIP- und XML-Dateien für **3C7 Notify of Self-Billing Invoice**

ZIP-Dateiname	XML-Dateiname
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

Inhalt der Richtlinienzuordnungen

Dieser Abschnitt listet den Inhalt der Richtlinienzuordnungen für **3C7 Notify of Self-Billing Invoice** auf:

- 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

Der folgende Abschnitt beschreibt den Inhalt des PIP **3D8 Distribute Work in Process**.

Inhalt der Paketdatei

Die folgende Tabelle zeigt die ZIP-Dateien und entsprechenden XML-Dateien für den PIP **3D8 Distribute Work in Process**. Die Richtlinienzuordnungen, die für alle Versionen gleich sind, werden im nachfolgenden Abschnitt gezeigt.

Tabelle 66. ZIP- und XML-Dateien für **3D8 Distribute Work in Process**

ZIP-Dateiname	XML-Dateiname
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

Inhalt der Richtlinienzuordnungen

Dieser Abschnitt listet den Inhalt der Richtlinienzuordnungen für **3D8 Distribute Work in Process** auf:

- 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

Der folgende Abschnitt beschreibt den Inhalt des PIP **4A1 Notify of Strategic Forecast**.

Inhalt der Paketdatei

Die folgende Tabelle zeigt die ZIP-Dateien und entsprechenden XML-Dateien für den PIP **4A1 Notify of Strategic Forecast**. Die Richtlinienzuordnungen, die für alle Versionen gleich sind, werden im nachfolgenden Abschnitt gezeigt.

Tabelle 67. ZIP- und XML-Dateien für **4A1 Notify of Strategic Forecast**

ZIP-Dateiname	XML-Dateiname
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

Tabelle 67. ZIP- und XML-Dateien für **4A1 Notify of Strategic Forecast** *(Forts.)*

ZIP-Dateiname	XML-Dateiname
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

Inhalt der Richtlinienzuordnungen

Dieser Abschnitt listet den Inhalt der Richtlinienzuordnungen für **4A1 Notify of Strategic Forecast** auf:

- 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

Der folgende Abschnitt beschreibt den Inhalt des PIP **4A3 Notify of Threshold Release Forecast**.

Inhalt der Paketdatei

Die folgende Tabelle zeigt die ZIP-Dateien und entsprechenden XML-Dateien für den PIP **4A3 Notify of Threshold Release Forecast**. Die Richtlinienzuordnungen, die für alle Versionen gleich sind, werden im nachfolgenden Abschnitt gezeigt.

Tabelle 68. ZIP- und XML-Dateien für **4A3 Notify of Threshold Release Forecast**

ZIP-Dateiname	XML-Dateiname
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

Inhalt der Richtlinienzuordnungen

Dieser Abschnitt listet den Inhalt der Richtlinienzuordnungen für **4A3 Notify of Threshold Release Forecast** auf:

- 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

Der folgende Abschnitt beschreibt den Inhalt des PIP **4A4 Notify of Planning Release Forecast**.

Inhalt der Paketdatei

Die folgende Tabelle zeigt die ZIP-Dateien und entsprechenden XML-Dateien für den PIP **4A4 Notify of Planning Release Forecast**. Die Richtlinienzuordnungen, die für alle Versionen gleich sind, werden im nachfolgenden Abschnitt gezeigt.

Tabelle 69. ZIP- und XML-Dateien für **4A4 Notify of Planning Release Forecast**

ZIP-Dateiname	XML-Dateiname
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

Inhalt der Richtlinienzuordnungen

Dieser Abschnitt listet den Inhalt der Richtlinienzuordnungen für **4A4 Notify of Planning Release Forecast** auf:

- 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

Der folgende Abschnitt beschreibt den Inhalt des PIP **4A5 Notify of Forecast Reply**.

Inhalt der Paketdatei

Die folgende Tabelle zeigt die ZIP-Dateien und entsprechenden XML-Dateien für den PIP **4A5 Notify of Forecast Reply**. Die Richtlinienzuordnungen, die für alle Versionen gleich sind, werden im nachfolgenden Abschnitt gezeigt.

Tabelle 70. ZIP- und XML-Dateien für **4A5 Notify of Forecast Reply**

ZIP-Dateiname	XML-Dateiname
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

Inhalt der Richtlinienzuordnungen

Dieser Abschnitt listet den Inhalt der Richtlinienzuordnungen für **4A5 Notify of Forecast Reply** auf:

- 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

Der folgende Abschnitt beschreibt den Inhalt des PIP **4B2 Notify of Shipment Receipt**.

Inhalt der Paketdatei

Die folgende Tabelle zeigt die ZIP-Dateien und entsprechenden XML-Dateien für den PIP **4B2 Notify of Shipment Receipt**. Die Richtlinienzuordnungen, die für alle Versionen gleich sind, werden im nachfolgenden Abschnitt gezeigt.

Tabelle 71. ZIP- und XML-Dateien für **4B2 Notify of Shipment Receipt**

ZIP-Dateiname	XML-Dateiname
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

Inhalt der Richtlinienzuordnungen

Dieser Abschnitt listet den Inhalt der Richtlinienzuordnungen für **4B2 Notify of Shipment Receipt** auf:

- 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

Der folgende Abschnitt beschreibt den Inhalt des PIP **4B3 Notify of Consumption**.

Inhalt der Paketdatei

Die folgende Tabelle zeigt die ZIP-Dateien und entsprechenden XML-Dateien für den PIP **4B3 Notify of Consumption**. Die Richtlinienzuordnungen, die für alle Versionen gleich sind, werden im nachfolgenden Abschnitt gezeigt.

Tabelle 72. ZIP- und XML-Dateien für **4B3 Notify of Consumption**

ZIP-Dateiname	XML-Dateiname
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

Inhalt der Richtlinienzuordnungen

Dieser Abschnitt listet den Inhalt der Richtlinienzuordnungen für **4B3 Notify of Consumption** auf:

- 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

Der folgende Abschnitt beschreibt den Inhalt für den PIP **4C1 Distribute Inventory Report V02.01**.

Inhalt der Paketdatei

Die folgende Tabelle zeigt die ZIP-Dateien und entsprechenden XML-Dateien für den PIP **4C1 Distribute Inventory Report**. Die Richtlinienzuordnungen, die für alle Versionen gleich sind, werden im nachfolgenden Abschnitt gezeigt.

Tabelle 73. ZIP- und XML-Dateien für **4C1 Distribute Inventory Report**

ZIP-Dateiname	XML-Dateiname
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

Inhalt der Richtlinienzuordnungen

Dieser Abschnitt listet den Inhalt der Richtlinienzuordnungen für **4C1 Distribute Inventory Report** auf:

- 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

Der folgende Abschnitt beschreibt den Inhalt des PIP **4C1 Distribute Inventory Report V02.03**.

Inhalt der Paketdatei

Die folgende Tabelle zeigt die ZIP-Dateien und entsprechenden XML-Dateien für den PIP **4C1 Distribute Inventory Report**. Die Richtlinienzuordnungen, die für alle Versionen gleich sind, werden im nachfolgenden Abschnitt gezeigt.

Tabelle 74. ZIP- und XML-Dateien für **4C1 Distribute Inventory Report**

ZIP-Dateiname	XML-Dateiname
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

Inhalt der Richtlinienzuordnungen

Dieser Abschnitt listet den Inhalt der Richtlinienzuordnungen für **4C1 Distribute Inventory Report** auf:

- 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

Der folgende Abschnitt beschreibt den Inhalt für den PIP **5C1 Distribute Product List**.

Inhalt der Paketdatei

Die folgende Tabelle zeigt die ZIP-Dateien und entsprechenden XML-Dateien für den PIP **5C1 Distribute Product List**. Die Richtlinienzuordnungen, die für alle Versionen gleich sind, werden im nachfolgenden Abschnitt gezeigt.

Tabelle 75. ZIP- und XML-Dateien für **5C1 Distribute Product List**

ZIP-Dateiname	XML-Dateiname
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

Inhalt der Richtlinienzuordnungen

Dieser Abschnitt listet den Inhalt der Richtlinienzuordnungen für **5C1 Distribute Product List** auf:

- 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

Der folgende Abschnitt beschreibt den Inhalt des PIP **5C2 Request Design Registration**.

Inhalt der Paketdatei

Die folgende Tabelle zeigt die ZIP-Dateien und entsprechenden XML-Dateien für den PIP **5C2 Request Design Registration**. Die Richtlinienzuordnungen, die für alle Versionen gleich sind, werden im nachfolgenden Abschnitt gezeigt.

Tabelle 76. ZIP- und XML-Dateien für **5C2 Request Design Registration**

ZIP-Dateiname	XML-Dateiname
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

Inhalt der Richtlinienzuordnungen

Dieser Abschnitt listet den Inhalt der Richtlinienzuordnungen für **5C2 Request Design Registration** auf:

- 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

Der folgende Abschnitt beschreibt den Inhalt des PIP **5C4 Distribute Registration Status**.

Inhalt der Paketdatei

Die folgende Tabelle zeigt die ZIP-Dateien und entsprechenden XML-Dateien für den PIP **5C4 Distribute Registration Status**. Die Richtlinienzuordnungen, die für alle Versionen gleich sind, werden im nachfolgenden Abschnitt gezeigt.

Tabelle 77. ZIP- und XML-Dateien für **5C4 Distribute Registration Status**

ZIP-Dateiname	XML-Dateiname
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

Inhalt der Richtlinienzuordnungen

Dieser Abschnitt listet den Inhalt der Richtlinienzuordnungen für **5C4 Distribute Registration Status** auf:

- 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

Der folgende Abschnitt beschreibt den Inhalt des PIP **5D1 Request Ship From Stock And Debit Authorization**.

Inhalt der Paketdatei

Die folgende Tabelle zeigt die ZIP-Dateien und entsprechenden XML-Dateien für den PIP **5D1 Request Ship From Stock And Debit Authorization**. Die Richtlinienzuordnungen, die für alle Versionen gleich sind, werden im nachfolgenden Abschnitt gezeigt.

Tabelle 78. ZIP- und XML-Dateien für **5D1 Request Ship From Stock And Debit Authorization**

ZIP-Dateiname	XML-Dateiname
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

Tabelle 78. ZIP- und XML-Dateien für **5D1 Request Ship From Stock And Debit Authorization** *(Forts.)*

ZIP-Dateiname	XML-Dateiname
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

Inhalt der Richtlinienzuordnungen

Dieser Abschnitt listet den Inhalt der Richtlinienzuordnungen für **5D1 Request Ship From Stock And Debit Authorization** auf:

- 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

Der folgende Abschnitt beschreibt den Inhalt des PIP **6C1 Query Service Entitlement**.

Inhalt der Paketdatei

Die folgende Tabelle zeigt die ZIP-Dateien und entsprechenden XML-Dateien für den PIP **6C1 Query Service Entitlement**. Die Richtlinienzuordnungen, die für alle Versionen gleich sind, werden im nachfolgenden Abschnitt gezeigt.

Tabelle 79. ZIP- und XML-Dateien für **6C1 Query Service Entitlement**

ZIP-Dateiname	XML-Dateiname
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

Inhalt der Richtlinienzuordnungen

Dieser Abschnitt listet den Inhalt der Richtlinienzuordnungen für **6C1 Query Service Entitlement** auf:

- 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

Der folgende Abschnitt beschreibt den Inhalt des PIP **6C2 Request Warranty Claim**.

Inhalt der Paketdatei

Die folgende Tabelle zeigt die ZIP-Dateien und entsprechenden XML-Dateien für den PIP **6C2 Request Warranty Claim**. Die Richtlinienzuordnungen, die für alle Versionen gleich sind, werden im nachfolgenden Abschnitt gezeigt.

Tabelle 80. ZIP- und XML-Dateien für **6C2 Request Warranty Claim**

ZIP-Dateiname	XML-Dateiname
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

Inhalt der Richtlinienzuordnungen

Dieser Abschnitt listet den Inhalt der Richtlinienzuordnungen für **6C2 Request Warranty Claim** auf:

- 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

Der folgende Abschnitt beschreibt den Inhalt des PIP **7B1 Distribute Work in Process**.

Inhalt der Paketdatei

Die folgende Tabelle zeigt die ZIP-Dateien und entsprechenden XML-Dateien für den PIP **7B1 Distribute Work in Process**. Die Richtlinienzuordnungen, die für alle Versionen gleich sind, werden im nachfolgenden Abschnitt gezeigt.

Tabelle 81. ZIP- und XML-Dateien für **7B1 Distribute Work in Process**

ZIP-Dateiname	XML-Dateiname
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
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

Inhalt der Richtlinienzuordnungen

Dieser Abschnitt listet den Inhalt der Richtlinienzuordnungen für **7B1 Distribute Work in Process** auf:

- 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

Der folgende Abschnitt beschreibt den Inhalt des PIP **7B5 Notify Of Manufacturing Work Order**.

Inhalt der Paketdatei

Die folgende Tabelle zeigt die ZIP-Dateien und entsprechenden XML-Dateien für den PIP **7B5 Notify Of Manufacturing Work Order**. Die Richtlinienzuordnungen, die für alle Versionen gleich sind, werden im nachfolgenden Abschnitt gezeigt.

Tabelle 82. ZIP- und XML-Dateien für **7B5 Notify Of Manufacturing Work Order**

ZIP-Dateiname	XML-Dateiname
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
BCG_Package_RNSC1.0_RNIFV02.00_7B5V01.00.zip	BCG_RNSC1.0_RNIFV02.00_7B5V01.00.xml

Inhalt der Richtlinienzuordnungen

Dieser Abschnitt listet den Inhalt der Richtlinienzuordnungen für **7B5 Notify Of Manufacturing Work Order** auf:

- 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

Der folgende Abschnitt beschreibt den Inhalt des PIP **7B6 Notify Of Manufacturing Work Order Reply**.

Inhalt der Paketdatei

Die folgende Tabelle zeigt die ZIP-Dateien und entsprechenden XML-Dateien für den PIP **7B6 Notify Of Manufacturing Work Order Reply**. Die Richtlinienzuordnungen, die für alle Versionen gleich sind, werden im nachfolgenden Abschnitt gezeigt.

Tabelle 83. ZIP- und XML-Dateien für **7B6 Notify Of Manufacturing Work Order Reply**

ZIP-Dateiname	XML-Dateiname
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
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

Inhalt der Richtlinienzuordnungen

Dieser Abschnitt listet den Inhalt der Richtlinienzuordnungen für **7B6 Notify Of Manufacturing Work Order Reply** auf:

- 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

Anhang D. Attribute

Dieser Anhang beschreibt die Attribute, die Sie über Community Console festlegen können. Die folgenden Attribute werden beschrieben:

- „EDI-Attribute"
- „AS-Attribute" auf Seite 314
- „RosettaNet-Attribute" auf Seite 318
- „Backend Integration-Attribute" auf Seite 320

EDI-Attribute

Dieser Abschnitt enthält eine Beschreibung der EDI-Attribute, die Sie verwenden können, während Sie Ihre EDI-Austauschvorgänge konfigurieren. Einige von diesen Attributen sind in der Steuerzeichenfolge vordefiniert, die die Transformationszuordnung darstellt, welche dem EDI-Dokument zugeordnet ist. Die in der Steuerzeichenfolge festgelegten Werte (auf dem Data Interchange Services-Client) überschreiben jeden Wert, den Sie in Community Console eingeben.

Attribute für Umschlagsprofil

Sie können verschiedene Attribute für ein EDI-Umschlagsprofil festlegen. Die verfügbaren Attribute hängen vom EDI-Typ ab. Im Allgemeinen entsprechen die Attribute einem EDI-Standard und die zulässigen Werte hängen vom EDI-Standard ab, den das Umschlagsprofil darstellt.

Für keines der Attribute ist ein Wert erforderlich. Für einige der Attribute wird ein Standardwert verwendet, wenn Sie keinen Wert eingeben. Die Tabellen in diesem Abschnitt listen die Attribute, denen Standardwerte zugeordnet sind, und deren Standardwerte auf.

Anmerkung: Die Merkmale des Umschlagsprofils, die nicht aufgelistet sind, verfügen über keine Standardwerte. Der von Ihnen angegebene Textwert wird verwendet, wenn er nicht von generischen oder spezifischen Umschlagsmerkmalen überschrieben werden, die in der Zuordnung oder in einer Verbindung festgelegt sind.

X12-Attribute

Die Tabellen in diesem Abschnitt listen die X12-Attribute auf, für die Standardwerte bereitgestellt sind.

Allgemeine Attribute: Tabelle 84 listet die allgemeinen Attribute auf, für die Standardwerte bereitgestellt sind.

Tabelle 84. Allgemeine Attribute

Feldname	Erforderlich?	Beschreibung	Standardwert
INTCTLLEN (Länge der Austauschkontrollnummer)	Nein	Definiert eine bestimmte Länge für die Austauschkontrollnummer. Falls Sie einen Wert eingeben, muss dieser eine ganze Zahl sein. Wenn Sie keinen Wert eingeben, wird die Standardlänge verwendet.	9

Tabelle 84. Allgemeine Attribute (Forts.)

Feldname	Erforderlich?	Beschreibung	Standardwert
GRPCTLLEN (Länge der Gruppenkontrollnummer)	Nein	Definiert eine bestimmte Länge für die Gruppenkontrollnummer. Falls Sie einen Wert eingeben, muss dieser eine ganze Zahl sein. Wenn Sie keinen Wert eingeben, wird die Standardlänge verwendet.	9
TRXCTLLEN (Länge der Transaktionskontrollnummer)	Nein	Definiert eine bestimmte Länge für die Transaktionskontrollnummer. Falls Sie einen Wert eingeben, muss dieser eine ganze Zahl sein. Wenn Sie keinen Wert eingeben, wird die Standardlänge verwendet.	9
ENVTYPE (Umschlagstyp)	Nein	Dieses Attribut wird nicht vom Hubadmin festgelegt, sondern wird von dem Umschlagsprofiltyp abgeleitet, der erstellt wird.	X12
MAXDOCS (Max. Anzahl an Transaktionen)	Nein	Maximale Anzahl an Transaktionen in einem Umschlag. Falls Sie einen Wert eingeben, muss dieser eine ganze Zahl sein.	Keine maximale Anzahl
CTLNUMFLAG (Kontrollnummern nach Transaktions-ID)	Nein	**Ja** gibt an, dass separate Gruppen mit Kontrollnummern auf der Basis des EDI-Transaktionstyps aufbewahrt werden. **Nein** gibt an, dass eine allgemeine Gruppe mit Kontrollnummern für jeden EDI-Transaktionstyp verwendet werden sollte.	Nein

Austauschattribute: Es sind keine X12-Austauschattribute erforderlich und die Attribute verfügen über keine Standardwerte.

Gruppenattribute: Tabelle 85 listet die Gruppenattribute auf, für die Standardwerte bereitgestellt sind.

Tabelle 85. Gruppenattribute

Feldname	Erforderlich?	Beschreibung	Standardwert
GS01 (ID der funktionalen Gruppe)	Nein	Die Gruppen-ID.	Der Standardwert kommt aus dem Header der Steuerzeichenfolge. Sie können diesen Wert auf dem Data Interchange Services-Client anzeigen, indem Sie sich die Spalte **Funktionsgruppe** auf der Seite **EDI-Dokumentdefinitionen** ansehen.
GS08 (Gruppenversion)	Nein	Die Gruppenversion.	Der Standardwert gilt pro Standard.

Transaktionsattribute: Es sind keine Transaktionsattribute erforderlich. Die Attribute verfügen über keine Standardwerte.

UCS-Attribute

Dieser Abschnitt listet auf, ob Standardwerte auf einen UCS-Austausch, eine UCS-Gruppe und eine UCS-Transaktion angewendet werden.

Allgemeine Attribute: Tabelle 86 auf Seite 303 listet die allgemeinen Attribute auf, für die Standardwerte bereitgestellt sind.

Tabelle 86. Allgemeine Attribute

Feldname	Erforderlich?	Beschreibung	Standardwert
INTCTLLEN (Länge der Austauschkontrollnummer)	Nein	Definiert eine bestimmte Länge für die Austauschkontrollnummer. Falls Sie einen Wert eingeben, muss dieser eine ganze Zahl sein. Wenn Sie keinen Wert eingeben, wird die Standardlänge verwendet.	5
GRPCTLLEN (Länge der Gruppenkontrollnummer)	Nein	Definiert eine bestimmte Länge für die Gruppenkontrollnummer. Falls Sie einen Wert eingeben, muss dieser eine ganze Zahl sein. Wenn Sie keinen Wert eingeben, wird die Standardlänge verwendet.	9
TRXCTLLEN (Länge der Transaktionskontrollnummer)	Nein	Definiert eine bestimmte Länge für die Transaktionskontrollnummer. Falls Sie einen Wert eingeben, muss dieser eine ganze Zahl sein. Wenn Sie keinen Wert eingeben, wird die Standardlänge verwendet.	9
ENVTYPE (Umschlagstyp)	Nein	Dieses Attribut wird nicht vom Hubadmin festgelegt, sondern wird von dem Umschlagsprofiltyp abgeleitet, der erstellt wird.	UCS
MAXDOCS (Max. Anzahl an Transaktionen)	Nein	Maximale Anzahl an Transaktionen in einem Umschlag. Falls Sie einen Wert eingeben, muss dieser eine ganze Zahl sein.	Keine maximale Anzahl
CTLNUMFLAG (Kontrollnummern nach Transaktions-ID)	Nein	**Ja** gibt an, dass separate Gruppen mit Kontrollnummern auf der Basis des EDI-Transaktionstyps aufbewahrt werden. **Nein** gibt an, dass eine allgemeine Gruppe mit Kontrollnummern für jeden EDI-Transaktionstyp verwendet werden sollte.	Nein

Austauschattribute: Es sind keine Austauschattribute erforderlich. Die Attribute verfügen über keine Standardwerte.

Gruppenattribute: Tabelle 87 listet die Gruppenattribute auf, für die Standardwerte bereitgestellt sind.

Tabelle 87. Gruppenattribute

Feldname	Erforderlich?	Beschreibung	Standardwert
GS01 (ID der funktionalen Gruppe)	Nein	Die Gruppen-ID.	Der Standardwert kommt aus dem Header der Steuerzeichenfolge. Sie können diesen Wert auf dem Data Interchange Services-Client anzeigen, indem Sie sich die Spalte **Funktionsgruppe** auf der Seite **EDI-Dokumentdefinitionen** ansehen.
GS08 (Gruppenversion)	Nein	Die Gruppenversion.	Der Standardwert gilt pro Standard.

Transaktionsattribute: Es sind keine Transaktionsattribute erforderlich. Die Attribute verfügen über keine Standardwerte.

EDIFACT-Attribute

Dieser Abschnitt listet auf, ob Standardwerte auf einen EDIFACT-Austausch, eine EDIFACT-Gruppe und eine EDIFACT-Nachricht angewendet werden.

Allgemeine Attribute: Tabelle 88 listet die allgemeinen Attribute auf, für die Standardwerte bereitgestellt sind.

Tabelle 88. Allgemeine Attribute

Feldname	Erforderlich?	Beschreibung	Standardwert
INTCTLLEN (Länge der Austauschkontrollnummer)	Nein	Definiert eine bestimmte Länge für die Austauschkontrollnummer. Falls Sie einen Wert eingeben, muss dieser eine ganze Zahl sein. Wenn Sie keinen Wert eingeben, wird die Standardlänge verwendet.	9
GRPCTLLEN (Länge der Gruppenkontrollnummer)	Nein	Definiert eine bestimmte Länge für die Gruppenkontrollnummer. Falls Sie einen Wert eingeben, muss dieser eine ganze Zahl sein. Wenn Sie keinen Wert eingeben, wird die Standardlänge verwendet.	9
TRXCTLLEN (Länge der Transaktionskontrollnummer)	Nein	Definiert eine bestimmte Länge für die Transaktionskontrollnummer. Falls Sie einen Wert eingeben, muss dieser eine ganze Zahl sein. Wenn Sie keinen Wert eingeben, wird die Standardlänge verwendet.	9
ENVTYPE (Umschlagstyp)	Nein	Dieses Attribut wird nicht vom Hubadmin festgelegt, sondern wird von dem Umschlagsprofiltyp abgeleitet, der erstellt wird.	EDIFACT
EDIFACTGRP (Gruppen für EDI erstellen)	Nein	Dieser Wert ist nur für EDIFACT-Umschlagstypen. (Die Gruppenebene ist in EDIFACT veraltet.) **Ja** gibt an, dass funktionale Gruppen (UNG/UNE-Segmente) für EDIFACT DATA erstellt werden sollen. **Nein** gibt an, dass sie nicht erstellt werden sollen.	Nein
MAXDOCS (Max. Anzahl an Transaktionen)	Nein	Maximale Anzahl an Transaktionen in einem Umschlag. Falls Sie einen Wert eingeben, muss dieser eine ganze Zahl sein.	Keine maximale Anzahl
CTLNUMFLAG (Kontrollnummern nach Transaktions-ID)	Nein	**Ja** gibt an, dass separate Gruppen mit Kontrollnummern auf der Basis des EDI-Transaktionstyps aufbewahrt werden. **Nein** gibt an, dass eine allgemeine Gruppe mit Kontrollnummern für jeden EDI-Transaktionstyp verwendet werden sollte.	Nein

Austauschattribute: Es sind keine Austauschattribute erforderlich. Die Attribute verfügen über keine Standardwerte.

Gruppenattribute: Tabelle 89 auf Seite 305 listet die Gruppenattribute auf, für die Standardwerte bereitgestellt sind.

Tabelle 89. Gruppenattribute

Feldname	Erforderlich?	Beschreibung	Standardwert
UNG01 (ID der funktionalen Gruppe)	Nein	Die Gruppen-ID.	Der Standardwert kommt aus dem Header der Steuerzeichenfolge. Sie können diesen Wert auf dem Data Interchange Services-Client anzeigen, indem Sie sich die Spalte **Funktionsgruppe** auf der Seite **EDI-Dokumentdefinitionen** ansehen.

Nachrichtenattribute: Tabelle 90 listet die Nachrichtenattribute auf, für die Standardwerte bereitgestellt sind.

Tabelle 90. Nachrichtenattribute

Feldname	Erforderlich?	Beschreibung	Standardwert
UNH0201 (Nachrichtentyp)	Nein	Der Nachrichtentyp.	Der Standardwert kommt aus dem Header der Steuerzeichenfolge. Sie können diesen Wert auf dem Data Interchange Services-Client anzeigen, indem Sie sich die Seite **EDI-Dokumentdefinitionen** ansehen.
UNH0202 (Nachrichtenversion)	Nein	Die Version der Nachricht.	D
UNH0203 (Nachrichtenrelease)	Nein	Der Release der Nachricht.	Pro Standard
UNH0204 (Kontrollierende Stelle)	Nein	Der Code, der eine kontrollierende Stelle angibt.	UN

Attribute für Dokumentenflussdefinition und Verbindung

Dieser Abschnitt listet Dokumentenflussdefinitions-Attribute für den Umschlag auf. Einige dieser Attribute können nur, wie angegeben, auf der Protokoll- oder Verbindungsebene festgelegt werden.

Trennzeichen- und Begrenzerattribute

Dieser Abschnitt listet die Zeichen auf, die als Begrenzer oder Trennzeichen in einem EDI-Austausch verwendet werden. Tabelle 91 auf Seite 306 zeigt das Attribut, wie es in Community Console angezeigt wird, den entsprechenden Begriff in X12 und EDIFACT (ISO 9735 Version 4, Release 1), ob das Attribut erforderlich ist, und eine Beschreibung des Attributs. Im Anschluss an die Tabelle wird ein Beispiel aufgeführt, wie diese Zeichen in einem EDI-Dokument angezeigt werden.

Attributbeschreibungen: Die Trennzeichen- und Begrenzerattribute werden in Tabelle 91 auf Seite 306 aufgelistet.

Anmerkung: Einige Zeichen (wie angegeben) können Hexadezimalwerte sein. Diese können Unicode-Werte oder Werte eines anderen Codierungstyps sein. Verwenden Sie für Unicode das Format \unnnn. Bei einer anderen Codierung verwenden Sie das Format 0xnn.

Tabelle 91. Attribute für Umschlagsprofil

Attribut	X12-Begriff	EDIFACT-Begriff	Beschreibung
Segmentbegrenzer	Segmentabschluss-zeichen	Segmentabschluss-zeichen	Dies ist ein einzelnes Zeichen, das am letzten Zeichen eines Segments angezeigt wird. Das Zeichen kann ein Hexadezimalwert sein. Der Standardwert basiert auf dem EDI-Typ. **X12** ~ (Tilde) **EDIFACT** ‘ (einfaches Anführungszeichen) **UCS** ~ (Tilde)
Begrenzer für Datenelemente	Trennzeichen für Datenelemente	Trennzeichen für Datenelemente	Dies ist ein einzelnes Zeichen, das die Datenelemente eines Segments trennt. Das Zeichen kann ein Hexa-dezimalwert sein. Der Standardwert basiert auf dem EDI-Typ. **X12** * (Stern) **EDIFACT** + (Pluszeichen) **UCS** * (Stern)
Begrenzer für Unterelemente	Trennzeichen für Komponenten-elemente	Trennzeichen für Komponenten-datenelemente	Dies ist ein einzelnes Zeichen, das die Komponenten-elemente eines zusammengesetzten Datenelements trennt. Das Zeichen kann ein Hexadezimalwert sein. Der Standardwert basiert auf dem EDI-Typ. **X12** \ (Backslash) **EDIFACT** : (Doppelpunkt) **UCS** \ (Backslash)
Freigabezeichen		Freigabezeichen	Dies ist ein einzelnes Zeichen, das die Bedeutung des nächsten Zeichens überschreibt, und ermöglicht, dass ein Trennzeichen in einem Datenelement angezeigt wird. Das Zeichen kann ein Hexadezimalwert sein. Es wird nur auf EDIFACT angewendet. **EDIFACT** ? (Fragezeichen)
Zeichen für wie-derholte Daten-elemente	Wiederholungs-trennzeichen	Wiederholungs-trennzeichen	Dies ist ein einzelnes Zeichen, das die Instanzen eines wiederholten Datenelements trennt. Dieses Zeichen kann ein Hexadezimalwert sein. Der Standardwert basiert auf dem EDI-Typ für X12 oder EDIFACT. **X12** ^ (Zirkumflex) **EDIFACT** * (Stern)
Dezimal-schreibweise		Dezimal-schreibweise (veraltet)	Dieses Attribut wurde im Dezimalformat oder beim Parsing verwendet und ist jetzt veraltet. Es kann nur ein Punkt bzw. nur ein Komma sein. Der Standardwert ist ein Punkt.

Beispiel für EDI-Struktur: Dieser Abschnitt zeigt einen einfachen EDI-Austausch und wie die in Tabelle 91 auf Seite 306 beschriebenen Attribute in einem Austausch verwendet werden.

Eine EDI-Nachricht besteht aus einer Gruppe von Segmenten in einer besonderen Reihenfolge. Ein Segment besteht aus einer Gruppe von Elementen. In einem Segment kann ein Element ein einfaches Datenelement sein, das nur ein Informationselement enthält. Ein Element kann außerdem ein zusammengesetztes Datenelement sein, das zwei oder mehr einfache Datenelemente enthält. Die einfachen Elemente, die ein zusammengesetztes Element ausmachen, heißen Komponentendatenelemente.

Es gibt keine Verschachtelung von zusammengesetzten Datenelementen. Ein zusammengesetztes Element kann nur einfache Datenelemente, keine anderen Kombinationen enthalten. Obwohl dies hier nicht gezeigt wird, kann ein Komponentendatenelement auch als wiederholtes Datenelement definiert werden.

Betrachten Sie das folgende Beispiel:

```
ABC*123*AA\BB\CC*001^002^003*star?*power~
```

In diesem Beispiel gilt Folgendes:

- ″ABC″ ist der Segmentname (EDIFACT bezeichnet dies als ″Segment-Tag″); dies würde als ″ABC-Segment″ bezeichnet werden.
- ″*″ (Stern) ist das Datenelementtrennzeichen.

  Der entsprechende Attributname in Community Console lautet **Segmentbegrenzer**.
- ″123″ ist das erste Datenelement, ein einfaches Datenelement, in manchen Kontexten könnte es auch als ABC01 bezeichnet werden.
- ″AA\BB\CC″ ist das zweite Datenelement (ABC02), es ist ein zusammengesetztes Element, das aus Komponentendatenelementen besteht.
  - ″\″ (Backslash) ist das Komponentendatenelement-Trennzeichen.

    Der entsprechende Attributname in Community Console lautet **Begrenzer für Datenelemente**.
  - ″AA″ ist das erste Komponentendatenelement von ABC02 (welches auch als ABC0201 bezeichnet werden könnte).
  - ″BB″ ist das zweite Komponentendatenelement von ABC02 (ABC0202).
  - ″CC″ ist das dritte Komponentendatenelement von ABC02 (ABC0203).
- ″001^002^003″ ist das dritte Datenelement (ABC03), es ist ein wiederholtes Datenelement.
  - ″^″ (Zirkumflex) ist das Wiederholungstrennzeichen.

    Der entsprechende Attributname in Community Console lautet **Zeichen für wiederholte Datenelemente**.
  - ″001″,″002″,″003″ sind die Wiederholungen (alle könnten als ABC03 bezeichnet werden).
- ″star?*power″ ist das vierte Datenelement (ABC04).
  - ″?″ (Fragezeichen) ist das Freigabezeichen und bedeutet, der nachfolgende Stern wird nicht als Trennzeichen für Datenelemente behandelt.
  - ″star*power″ ist der Ergebniswert von ABC04.
- ″~″ (Tilde) ist das Segmentabschlusszeichen.

  Der entsprechende Attributname in Community Console lautet **Segmentbegrenzer**.

Zusätzliche EDI-Attribute

Dieser Abschnitt listet zusätzliche EDI-Attribute auf, die Sie auf der Dokumentenflussdefinitions-Ebene oder auf der Verbindungsebene festlegen können.

Tabelle 92. Zusätzliche EDI-Attribute

Attribut	Erforderlich	Beschreibung	Einschränkungen	Standardwert
Segmentausgabe	Nein	Wenn dies in der EDI/XML-Transformation verwendet wird, zeigt dies an, ob ein Zeilenumbruch nach jedem EDI-Segment oder jedem XML-Element auftreten soll.	Beschränkt auf Protokoll oder Verbindung	Ja
Dokumente mit doppelten Dokument-IDs zulassen	Nein	**Ja** gibt an, dass doppelte Dokument-IDs (Austauschkontrollnummern) zulässig sind. **Nein** gibt an, dass doppelte Austauschkontrollnummern als Fehler behandelt werden sollen.	Beschränkt auf Protokoll oder Verbindung	Nein
Höchste Fehlerkategorie bei der Umsetzung	Nein	Gibt die maximale Anzahl Fehler an, die während einer Transformation auftreten können, bevor die Transformation fehlschlägt. Gültige Werte sind 0, 1 oder 2. Wenn die Transformationszuordnung einen Fehlerbefehl enthält, um einen benutzerdefinierten Fehler anzuzeigen, und der Ebenenparameter des Fehlerbefehls größer als dieser Wert ist, schlägt die Transformation fehl.	Beschränkt auf Protokoll oder Verbindung	0
EDI FA-Zuordnungen	Nein	Stellt die Zuordnung bereit, die für das Konvertieren der internen generischen FA in die bestimmte FA verwendet werden soll. **Anmerkung:** Sie wählen dieses Attribut in einer Liste mit Zuordnungen aus, die als FA-Zuordnungen (Zuordnungstyp "K") angegeben sind.	Beschränkt auf Protokoll oder Verbindung	
Umschlagsprofil	Ja	Der Name des EDI-Umschlagsprofils, der für das Versehen mit einem Umschlag verwendet werden soll. Alle Umschlagsprofile, die Sie definiert haben, sind in der Liste verfügbar.		
XMLNS aktiv	Nein	Führen Sie eine Namespaceverarbeitung für das Eingabe-XML-Dokument aus. Dieses Attribut wird vom XML-Transfomationsschritt verwendet. Gültige Werte sind **Ja** oder **Nein**.		Schema: Ja DTD: Nein

Tabelle 92. Zusätzliche EDI-Attribute (Forts.)

Attribut	Erforderlich	Beschreibung	Einschränkungen	Standardwert
Höchste Validierungsfehlerkategorie	Nein	Die höchste akzeptable Validierungsfehlerkategorie (die Fehlerkategorie zum Akzeptieren bevor die Transaktion als ″failed″ (fehlgeschlagen) betrachtet wird). Gültige Werte sind 0, 1 oder 2. **0** Nur Validierung ohne Fehler zulassen **1** Keine Dokumente fehlschlagen lassen, die nur einfache Elementvalidierungsfehler aufweisen **2** Keine Dokumente fehlschlagen lassen, die Element- oder Segmentvalidierungsfehler aufweisen		0
Stufe der Validierung	Nein	Zeigt die Überprüfungsstufe an, die auf der Transaktionsebene ausgeführt werden soll. Ein Wert von 2 bedeutet, dass die Werte verwendet werden, die für die Attribute **Alphanumerische Validierungstabelle** und **Validierungstabelle für Zeichensatz** festgelegt wurden. Dieses Attribut wird auch auf das Attribut **Detaillierte Validierung des Segments** angewendet, wenn für dieses Attribut **Ja** festgelegt wurde. Gültige Werte sind 0, 1 oder 2. **0** Nur Basisvalidierung ausführen, wie z. B. das Überprüfen auf fehlende obligatorische Elemente und Segmente sowie auf Mindest- und Höchstlängen. Kein Validieren von Elementwerten für die Datentypen oder Codelisten, die in der Transaktionsdefinition angegeben sind. **1** Validierung der Stufe 0 ausführen und validieren der Elementwerte für die Codelisten, die für das Datenelement angegeben sind. **2** Validierung der Stufe 1 ausführen und validieren, ob der Elementwert für den Datentyp des Elements korrekt ist.		0
Validierungstabelle für Zeichensatz	Nein	Gibt die Tabelle an, die für die Zeichensatzvalidierung verwendet werden soll. Diese Tabelle wird nur verwendet, wenn das Attribut **Stufe der Validierung** den Wert 2 hat. Dieses Attribut bezieht sich auf die virtuelle Codelistentabelle. Der Benutzer kann neue Codelisten auf der Registerkarte **Codelisten** des Zuordnungsbereichs im Data Interchange Services-Client erstellen. Dieser Bereich enthält außerdem Codelisten, die für andere Zwecke verwendet werden, wie z. B. die Validierung bestimmter EDI-Elemente.		CHARSET

Tabelle 92. Zusätzliche EDI-Attribute (Forts.)

Attribut	Erforderlich	Beschreibung	Einschränkungen	Standardwert
Alphanumerische Validierungstabelle	Nein	Gibt die Tabelle an, die für die alphanumerische Validierung verwendet werden soll. Diese Tabelle wird nur verwendet, wenn das Attribut **Stufe der Validierung** den Wert 2 hat. Das Attribut bezieht sich auf die virtuellen Codelistentabellen. Der Benutzer kann neue Codelisten auf der Registerkarte **Codelisten** des Zuordnungsbereichs im Data Interchange Services-Client erstellen. Dieser Bereich enthält außerdem Codelisten, die für andere Zwecke verwendet werden, wie z. B. die Validierung bestimmter EDI-Elemente.		ALPHANUM
Informationen auf Gruppenebene nur in funktionaler Bestätigung generieren	Nein	Dieses Attribut gilt für EDI-X12. Die Werte sind **Ja** oder **Nein**. **Ja** Informationen auf Gruppenebene nur für funktionale Bestätigung generieren **Nein** Vollständiges funktionales Bestätigungsdetail für jede einzelne Transaktion und Segmente und Elemente in einer Transaktion generieren.	Beschränkt auf Protokoll oder Verbindung	Nein
Jahr für Jahrhundertsteuerung	Nein	Wenn Datumsangaben von zweistelligen Jahresangaben in vierstellige Jahresangaben konvertiert werden, wird bei zweistelligen Jahresangaben nach diesem Wert ein Jahrhundertwert von “19” angenommen. Bei zweistelligen Jahresangaben gleich oder vor diesem Wert wird von einem Jahrhundertwert von “20” ausgegangen. Der gültige Bereich ist 0-99.	Beschränkt auf Protokoll oder Verbindung	10

Tabelle 92. Zusätzliche EDI-Attribute (Forts.)

Attribut	Erforderlich	Beschreibung	Einschränkungen	Standardwert
Detaillierte Validierung des Segments	Nein	Dieses Attribut gilt für die folgenden Segmentheader und -trailer. • X12 – ISA, IEA – GS, GE – ST, SE • EDIFACT – UNA – UNB, UNZ – UNG, UNE – UNH, UNT • UNTUCS – BG, EG – GS, GE – ST, SE Gültige Werte sind **Ja** oder **Nein**. **Ja** Detaillierte Umschlagssegmentvalidierung ausführen. Die Überprüfungstiefe wird vom Attribut **Stufe der Validierung** gesteuert. **Nein** Detaillierte Umschlagssegmentvalidierung nicht ausführen.	Beschränkt auf Protokoll oder Verbindung	Nein
TA1-Anforderung zulassen	Nein	Generierung einer TA1-Anforderung zulassen, wenn dies im Austauschumschlagsegment angegeben ist. Gilt nur für EDI-X12. Wenn auf **Ja** gesetzt, wird eine TA1 generiert, falls dies im Austauschumschlagsegment angegeben ist. Wenn auf **Nein** gesetzt, wird keine TA1 generiert, selbst wenn dies im Austauschumschlagsegment angegeben ist.	Beschränkt auf Protokoll oder Verbindung	Ja
Umschlag bei Fehlern löschen	Nein	Dieses Attribut wird bei vielgestaltiger Verarbeitung verwendet. Im Falle eines Stapels, der durch das Entfernen des Umschlags entstanden ist, gibt dieses Attribut an, ob der gesamte Stapel gelöscht werden soll, wenn eine der Transaktionen fehlschlägt. Gültige Werte sind **Ja** und **Nein**.	Beschränkt auf Protokoll oder Verbindung	Nein

Tabelle 92. Zusätzliche EDI-Attribute (Forts.)

Attribut	Erforderlich	Beschreibung	Einschränkungen	Standardwert
Qualifikationsmerkmal1 für Verbindungsprofil	Nein	Dieses Attribut wird vom Programm zur Umschlaggenerierung verwendet, um zu ermitteln, welches Profil für eine Austauschverbindung verwendet werden soll. Transaktionen mit verschiedenen Werten für dieses Attribut werden in verschiedene Austauschvorgänge gestellt.		
Qualifikationsmerkmal für Austausch	Nein	Der Code, mit dem das Format der Kennung für Austausch vom Absender oder Empfänger angegeben wird.		
Kennung für Austausch	Nein	Gibt den spezifischen Absender oder Empfänger des Dokuments an. Der eingegebene Datentyp wird vom Attribut **Qualifikationsmerkmal für Austausch** bestimmt.		
Nutzungsanzeiger für Austausch	Nein	Gibt an, ob die konvertierten Quellendokumente als Produktions-, Test- oder Informationsdokumente klassifiziert werden. Gültige Werte sind **P**, **T** und **I**.		
Kennung für Absender der Gruppenanwendung	Nein	Gibt den spezifischen Absender der Transaktion an. Dieses Attribut, wenn es von den Handelspartnern festgesetzt wurde, ermöglicht die Adressierung innerhalb eines Unternehmens.		
Kennung für Empfänger der Gruppenanwendung	Nein	Gibt den spezifischen Empfänger oder die spezifische Anwendung der Transaktion an. Dieses Attribut, wenn es von den Handelspartnern festgesetzt wurde, ermöglicht die Adressierung innerhalb eines Unternehmens.		
Umgekehrtes Routing für Austausch	Nein	Gibt die Adresse an, an die der Empfänger jede Antwort richten sollte.		
Routing-Adresse für Austausch	Nein	Der Unteradressencode für vorwärts gerichtetes Routing.		
Qualifikationsmerkmal für Absender der Gruppenanwendung	Nein	Der Code, mit dem das Format der Kennung für Absender der Gruppenanwendung angegeben wird.		
Qualifikationsmerkmal für Empfänger der Gruppenanwendung	Nein	Der Code, mit dem das Format der Kennung für Empfänger der Gruppenanwendung angegeben wird.		
Kennwort für Gruppenanwendung	Nein	Dieses Attribut definiert Sicherheitsinformationen.		

Data Interchange Services-Clientmerkmale

Dieser Abschnitt listet die Merkmale auf, die als Teil der Transformationszuordnung im Data Interchange Services-Client und ihren entsprechenden WebSphere Partner Gateway-Attributen festgelegt werden können.

Tabelle 93. Zuordnung der Merkmale und ihrer entsprechenden Attribute

Data Interchange Services-Clientmerkmal	Überschreibt WebSphere Partner Gateway-Attribut
AckReq	Bestätigung angefordert
Alphanum	Alphanumerische Validierungstabelle
Charset	Validierungstabelle für Zeichensatz
CtlNumFlag	Kontrollnummern nach Transaktions-IDs
EdiDecNot (Dezimalschreibweise)	Dezimalschreibweise
EdiDeDlm (Datenelementtrennzeichen)	Begrenzer für Datenelemente
EdiDeSep (wiederholtes Datenelementtrennzeichen)	Trennzeichen für wiederholte Datenelemente
EdifactGrp	Gruppen für EDI erstellen
EdiRlsChar (Freigabezeichen)	Freigabezeichen
EdiSeDlm (Komponentendatenelement-Trennzeichen)	Begrenzer für Unterelemente
EdiSegDlm (Segmentabschlusszeichen)	Segmentbegrenzer
EnvProfName	Umschlagsprofil
EnvType	Umschlagstyp
MaxDocs	Max. Anzahl an Transaktionen
Reroute	Umgekehrtes Routing für Austausch
SegOutput	Segmentausgabe
ValLevel	Stufe der Validierung
ValErrLevel	Höchste Validierungsfehlerkategorie
ValMap	Validierungszuordnung

Tabelle 94 listet zusätzliche Data Interchange Services-Clientmerkmale und deren zugeordnete WebSphere Partner Gateway-Attribute auf.

Tabelle 94. Data Interchange Services-Clientmerkmale und deren zugeordnete Attribute

Data Interchange Services-Clientmerkmal	Überschreibt WebSphere Partner Gateway-Attribut
IchgCtlNum	Austauschkontrollnummer
IchgSndrQl	Qualifikationsmerkmal für Absender des Austauschs
IchgSndrId	Austauschabsender-ID
IchgRcvrQl	Qualifikationsmerkmal für Empfänger des Austauschs
IchgRcvrId	Austauschempfänger-ID
IchgDate	Datum für Austausch
IchgTime	Zeit für Austausch
IchgPswd	Kennwort für Austausch
IchgUsgInd	Nutzungsanzeiger für Austausch
IchgAppRef	Anwendungsreferenz für Austausch
IchgVerRel	Version und Release für Austausch

Tabelle 94. Data Interchange Services-Clientmerkmale und deren zugeordnete Attribute (Forts.)

Data Interchange Services-Clientmerkmal	Überschreibt WebSphere Partner Gateway-Attribut
IchgGrpCnt	Anzahl von Gruppen im Austausch
IchgCtlTotal	Kontrollsumme vom Austauschtrailersegment
IchgTrxCnt	Anzahl von Dokumenten im Austausch
GrpCtlNum	Kontrollnummer der Gruppe
GrpFuncGrpId	ID der funktionalen Gruppe
GrpAppSndrId	Kennung für Absender der Gruppenanwendung
GrpAppRcvrId	Kennung für Empfänger der Gruppenanwendung
GrpDate	Gruppendatum
GrpTime	Gruppenzeit
GrpPswd	Gruppenkennwort
GrpVer Gruppenversion.	Gruppenversion
GrpRel Gruppenrelease.	Gruppenrelease
GrpTrxCnt	Anzahl von Dokumenten in der Gruppe
TrxCtlNum	Kontrollnummer der Transaktion
TrxCode	Transaktionscode
TrxVer	Transaktionsversion
TrxRel	Transaktionsrelease
TrxSegCnt	Anzahl EDI-Segmente im Dokument

AS-Attribute

Dieser Abschnitt beschreibt die AS-Attribute.

Tabelle 95. AS-Attribute

Attribut	Erforderlich	Beschreibung	Einschränkungen	Standardwert
Bestätigungszeit	Nein	Die Wartezeit für eine MDN-Bestätigung, bevor die ursprüngliche Anforderung erneut gesendet wird. Dieses Attribut funktioniert in Verbindung mit **Wiederholungszähler**. Die Einheiten sind in Minuten.	Beschränkt auf Paket oder Verbindung	30
Wiederholungszähler	Nein	Wie oft eine Anforderung gesendet werden soll, wenn kein MDN empfangen wird. Dieses Attribut funktioniert in Verbindung mit **Bestätigungszeit**. Wenn für dieses Attribut z. B. 3 festgelegt wurde, kann die Anforderung theoretisch viermal gesendet werden: das erste Mal und dann drei Wiederholungen.	Beschränkt auf Paket oder Verbindung	3
AS komprimiert	Nein	Die Daten komprimieren. Dieses Attribut funktioniert in Verbindung mit **AS-Komprimierung vor Unterzeichnung**.	Beschränkt auf Paket oder Verbindung	Nein

Tabelle 95. AS-Attribute (Forts.)

Attribut	Erforderlich	Beschreibung	Einschränkungen	Standardwert
AS-Komprimierung vor Unterzeichnung	Nein	Gibt an, ob die AS-Komprimierung auf sowohl die Nutzinformationen als auch die Unterschrift oder nur auf die Nutzinformationen angewendet wird. Wenn Sie **Ja** auswählen, werden die Nutzinformationen komprimiert, bevor die Nachricht unterzeichnet wird. Dieses Attribut funktioniert in Verbindung mit **AS komprimiert**.	Beschränkt auf Paket oder Verbindung	Ja
AS verschlüsselt	Nein	Gibt an, ob eine Verschlüsselung ausgeführt werden sollte. **Anmerkung:** Dies entspricht nicht der SSL-Verschlüsselung. Dies gibt für die Seite ″AN″ eines Austauschs an, wenn Sie Dokumente an einen Partner senden, ob das Dokument verschlüsselt werden soll. Für die Seite ″VON″ eines Austauschs, wenn Sie Dokumente von einem Partner empfangen, muss eine vom Partner gesendete AS-Anforderung verschlüsselt werden, falls für das Attribut **Ja** festgelegt ist. Wenn für das Attribut **Nein** festgelegt ist, kann das Dokument vom Partner verschlüsselt bzw. unverschlüsselt sein. Gültige Werte sind **Ja** oder **Nein**. **Ja** Eine Verschlüsselung ist erforderlich. **Nein** Eine Verschlüsselung ist nicht erforderlich.	Beschränkt auf Paket oder Verbindung	Nein
AS-MDN angefordert	Nein	Gibt an, ob eine MDN-Antwort erforderlich ist. Wenn für das Attribut **Ja** festgelegt ist, bewirkt dies, dass der Header “transport Disposition-notification-to” (Transport für Dispositionsbenachrichtigung an) mit dem Wert vom Attribut **AS-MDN-E-Mail-Adresse** gefüllt wird. Gültige Werte sind **Ja** und **Nein**. **Ja** Eine MDN anfordern. **Nein** Keine MDN anfordern.	Beschränkt auf Paket oder Verbindung	Ja

Tabelle 95. AS-Attribute (Forts.)

Attribut	Erforderlich	Beschreibung	Einschränkungen	Standardwert
AS-MDN-E-Mail-Adresse	Ja, falls das Attribut **AS-MDN asynchron** auf **Ja** gesetzt ist und Sie AS1 verwenden.	Gibt die E-Mail-Adresse für den zu verwendenden Partner an, wenn Sie eine asynchrone MDN senden. Dieses Attribut wird in Verbindung mit dem Attribut **AS-MDN angefordert** verwendet. Der Wert von **AS-MDN-E-Mail-Adresse** wird im Feld "Disposition-notification-to" (Dispositionsbenachrichtigung an) verwendet. Nur für AS1: Dieses Attribut funktioniert in Verbindung mit dem Attribut **AS-MDN asynchron** im Format mailto:xxx@company.com.	Beschränkt auf Paket oder Verbindung	
AS-MDN-Http-URL-Adresse	Ja, falls das Attribut **AS-MDN asynchron** auf **Ja** gesetzt ist und Sie AS2 verwenden.	Dieses Attribut gilt für AS2 und mit ihr wird die URL-Adresse angegeben, an die ein Partner eine asynchrone MDN senden sollte. Dieses Attribut funktioniert in Verbindung mit **AS-MDN asynchron**.	Beschränkt auf Paket oder Verbindung	
AS-MDN asynchron	Nein	Gibt an, ob die MDN synchron oder asynchron zurückgegeben werden soll. Der Wert dieses Attributs beeinflusst, ob das Attribut **AS-MDN-Http-URL-Adresse** oder **AS-MDN-E-Mail-Adresse** verwendet wird. Gültige Werte sind **Ja** und **Nein**. **Ja** Asynchron **Nein** Synchron Wenn für dieses Attribut **Ja** festgelegt ist, wird das Feld ″receipt-delivery-option″ (Empfangszustellungsoption) basierend auf dem Attribut **AS-MDN-Http-URL-Adresse** (für AS2) oder **AS-MDN-E-Mail-Adresse** (für AS1) gefüllt.	Beschränkt auf Paket oder Verbindung	Ja

Tabelle 95. AS-Attribute (Forts.)

Attribut	Erforderlich	Beschreibung	Einschränkungen	Standardwert
AS MDN unterzeichnet	Nein	Gibt an, ob die Anforderung erfordert, dass eine unterzeichnete MDN zurückgegeben wird. Dieses Attribut funktioniert in Verbindung mit **AS-MDN angefordert**. Wenn der Wert **Ja** lautet, wird "Disposition-notification-options: signed-receipt-protocol" (Dispositionsbenachrichtigungsoptionen: unterzeichnetes Empfangsprotokoll) gefüllt. Gültige Werte sind **Ja** und **Nein**. **Ja** Unterzeichnete MDN angefordert **Nein** Keine unterzeichnete MDN angefordert Wenn für dieses Attribut **Ja** festgelegt ist, muss die vom Partner gesendete MDN unterzeichnet sein. Wenn für dieses Attribut **Nein** festgelegt ist, kann die MDN unterzeichnet bzw. nicht unterzeichnet sein.	Beschränkt auf Paket oder Verbindung	Nein
AS Message Digest Algorithm	Nein	Der Nachrichtenauszugsalgorithmus, der beim Unterzeichnen verwendet wird. Dieses Attribut wird in Verbindung mit den Attributen **AS unterzeichnet** und **AS MDN unterzeichnet** verwendet. Bei unterzeichneten MDNs wird dieser Wert verwendet, um den Header "Disposition-notification-options: signed-receipt-micalg" (Dispositionsbenachrichtigungsoptionen: unterzeichneter Empfangs-MIC-Algorithmus) zu füllen.	Beschränkt auf Paket oder Verbindung	sha1
AS unterzeichnet	Nein	Gibt an, ob das Dokument unterzeichnet werden soll. Dies gibt für die Seite ″AN″ eines Austauschs an, wenn Sie Dokumente an einen Partner senden, ob das Dokument unterzeichnet werden soll. Für die Seite ″VON″ des Austauschs, wenn Sie Dokumente von einem Partner empfangen, muss eine vom Partner gesendete AS-Anforderung unterzeichnet werden, falls für das Attribut **Ja** festgelegt ist. Wenn für das Attribut **Nein** festgelegt ist, kann das Dokument vom Partner unterzeichnet bzw. nicht unterzeichnet sein. **Ja** Das Dokument unterzeichnen. **Nein** Ein unterzeichnetes Dokument ist nicht erforderlich.	Beschränkt auf Paket oder Verbindung	Nein

Tabelle 95. AS-Attribute (Forts.)

Attribut	Erforderlich	Beschreibung	Einschränkungen	Standardwert
AS-Geschäfts-ID	Nein	Die AS-Geschäfts-ID, die im Header "AS2-To" (AS2 an) verwendet werden soll. Wenn kein Wert bereitgestellt ist, verwendet WebSphere Partner Gateway die Geschäfts-ID des Empfängers, die im Quellendokument verwendet wird. **Anmerkung:** Der Header "AS2-From" (AS2 von) wird vom ursprünglichen Quellendokument festgelegt, das bei WebSphere Partner Gateway angekommen ist und das als AS gesendet wird.	Beschränkt auf Paket oder Verbindung	

RosettaNet-Attribute

Dieser Abschnitt beschreibt die RosettaNet-Attribute.

Tabelle 96. RosettaNet-Attribute

Attribut	Erforderlich	Beschreibung	Einschränkungen	Standardwert
Bestätigungszeit	Ja	Die Wartezeit für eine Empfangsbestätigung, bevor die ursprüngliche Anforderung erneut gesendet wird. Dieses Attribut funktioniert in Verbindung mit **Wiederholungszähler**. Die Einheiten sind in Minuten. Der Standardwert wird aus dem RosettaNet-PIP-Spezifikationsdokument bezogen.	Beschränkt auf Paket oder Verbindung	120
Ausführungszeit	Ja	Die Wartezeit für eine Antwort auf eine Aktionsanforderung, bevor eine Fehlerbenachrichtigung gesendet wird.	Beschränkt auf Paket oder Verbindung	
Wiederholungszähler	Ja	Wie oft eine Anforderung gesendet werden soll, wenn keine Empfangsbestätigung empfangen wurde. Dieses Attribut funktioniert in Verbindung mit **Bestätigungszeit**. Mit einer Einstellung von z. B. 3 kann die Anforderung theoretisch viermal gesendet werden: das erste Mal und die drei Wiederholungen. Der Standardwert wird aus dem RosettaNet-PIP-Spezifikationsdokument bezogen.	Beschränkt auf Paket oder Verbindung	3
Digitale Unterschrift erforderlich	Nein	Gibt an, ob die PIP-Nachricht eine digitale Unterschrift erfordert. Der Standardwert wird aus dem RosettaNet-PIP-Spezifikationsdokument bezogen.	Beschränkt auf Paket oder Verbindung	Ja
Unbestreitbarkeit erforderlich	Nein	Gibt an, ob das ursprüngliche Dokument im Unbestreitbarkeitsspeicher gespeichert werden soll. Der Standardwert wird aus dem RosettaNet-PIP-Spezifikationsdokument bezogen.	Beschränkt auf Paket oder Verbindung	Ja

Tabelle 96. RosettaNet-Attribute (Forts.)

Attribut	Erforderlich	Beschreibung	Einschränkungen	Standardwert
Unbestreitbarkeit des Empfangs	Nein	Gibt an, ob das Dokument der Empfangsbestätigung im Unbestreitbarkeitsspeicher gespeichert werden soll. Der Standardwert wird aus dem RosettaNet-PIP-Spezifikationsdokument bezogen.	Beschränkt auf Paket oder Verbindung	Ja
Sync unterstützt		Gibt an, ob der PIP (Partner Interface Process) die synchrone Übertragung unterstützt. Der Standardwert wird bereitgestellt basierend auf der PIP-Spezifikation.	Beschränkt auf Paket oder Verbindung Dieses Attribut ist nur für RNIF 2.0 verfügbar.	
Sync-Bestätigung erforderlich		Gibt an, ob der PIP eine synchrone Empfangsbestätigung erfordert. Der Standardwert wird bereitgestellt basierend auf der PIP-Spezifikation.	Beschränkt auf Paket oder Verbindung Dieses Attribut ist nur für RNIF 2.0 verfügbar.	
Globaler Lieferkettencode	Für RNIF 1.1 erforderlich	Der Code, der die Lieferkette für die Funktion des Teilnehmers angibt. Gültige Werte: • Elektronische Komponenten • Informationstechnologie • Halbleiterfertigung	Beschränkt auf Paket oder Verbindung	

Tabelle 96. RosettaNet-Attribute (Forts.)

Attribut	Erforderlich	Beschreibung	Einschränkungen	Standardwert
Verschlüsselung		Dieses Attribut gibt an, ob eine Verschlüsselung ausgeführt werden sollte. **Anmerkung:** Dies entspricht nicht der SSL-Verschlüsselung. Dies gibt für die Seite ″AN″ eines Austauschs an, wenn Sie Dokumente an einen Partner senden, ob das Dokument verschlüsselt werden soll. Für die Seite ″VON″ eines Austauschs, wenn Sie Dokumente von einem Partner empfangen, muss eine vom Partner gesendete RNIF-Anforderung verschlüsselt werden, falls für das Attribut **Ja** festgelegt ist. Wenn für das Attribut **Nein** festgelegt ist, kann das Dokument vom Partner verschlüsselt bzw. unverschlüsselt sein. Gültige Werte: **Kein(e)** Eine Verschlüsselung ist nicht erforderlich. **Nutzinformationen** Nur RosettaNet Service Content verschlüsseln. **Nutzinformationen und Container** RosettaNet Service Content und den Service Header zusammen verschlüsseln.	Beschränkt auf Paket oder Verbindung Dieses Attribut ist nur für RNIF 2.0 verfügbar.	Kein(e)

Backend Integration-Attribute

Dieser Abschnitt beschreibt das Attribut, das dem Paket **Backend Integration** zugeordnet ist.

Tabelle 97. Backend Integration-Attribut

Attribut	Beschreibung	Standardwert
Umschlagsmarkierung	Dieses Attribut gibt an, ob das Dokument mit einem XML-Umschlag versehen werden soll. Gültige Werte sind **Ja** und **Nein**.	Nein

Anhang E. Bemerkungen

Möglicherweise bietet IBM die in dieser Dokumentation beschriebenen Produkte, Services oder Funktionen nicht allen Ländern oder Regionen an. Informationen über die gegenwärtig im jeweiligen Land verfügbaren Produkte und Services sind beim IBM Ansprechpartner erhältlich. Hinweise auf IBM Lizenzprogramme oder andere IBM Produkte bedeuten nicht, dass nur Programme, Produkte oder Dienstleistungen von IBM verwendet werden können. Anstelle der IBM Produkte, Programme oder Dienstleistungen können auch andere ihnen äquivalente Produkte, Programme oder Dienstleistungen verwendet werden, solange diese keine gewerblichen oder anderen Schutzrechte der IBM verletzen. Die Verantwortung für den Betrieb von Fremdprodukten, Fremdprogrammen und Fremdservices liegt beim Kunden.

Für in diesem Handbuch beschriebene Erzeugnisse und Verfahren kann es IBM Patente oder Patentanmeldungen geben. Mit der Auslieferung dieses Handbuchs ist keine Lizenzierung dieser Patente verbunden. Lizenzanforderungen sind schriftlich an folgende Adresse zu richten (Anfragen an diese Adresse müssen auf Englisch formuliert werden):

IBM Europe
Director of Licensing
92066 Paris La Defense Cedex
France

Trotz sorgfältiger Bearbeitung können technische Ungenauigkeiten oder Druckfehler in dieser Veröffentlichung nicht ausgeschlossen werden. Die Angaben in diesem Handbuch werden in regelmäßigen Zeitabständen aktualisiert. Die Änderungen werden in Überarbeitungen oder in Technical News Letters (TNLs) bekannt gegeben. IBM kann ohne weitere Mitteilung jederzeit Verbesserungen und/oder Änderungen an den in dieser Veröffentlichung beschriebenen Produkten und/oder Programmen vornehmen.

Verweise in diesen Informationen auf Websites anderer Anbieter dienen lediglich als Benutzerinformationen und stellen keinerlei Billigung des Inhalts dieser Websites dar. Das über diese Websites verfügbare Material ist nicht Bestandteil des Materials für dieses IBM Produkt. Die Verwendung dieser Websites geschieht auf eigene Verantwortung.

Werden an IBM Informationen eingesandt, können diese beliebig verwendet werden, ohne dass eine Verpflichtung gegenüber dem Einsender entsteht.

Lizenznehmer des Programms, die Informationen zu diesem Produkt wünschen mit der Zielsetzung: (i) den Austausch von Informationen zwischen unabhängigen, erstellten Programmen und anderen Programmen (einschließlich des vorliegenden Programms) sowie (ii) die gemeinsame Nutzung der ausgetauschten Informationen zu ermöglichen, wenden sich an folgende Adresse:

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

Die Bereitstellung solcher Informationen kann von bestimmten Bedingungen abhängig sein, in einigen Fällen auch von der Zahlung einer Gebühr.

Die Lieferung des im Handbuch aufgeführten Lizenzprogramms sowie des zugehörigen Lizenzmaterials erfolgt im Rahmen der Allgemeinen Geschäftsbedingungen der IBM, der Internationalen Nutzungsbedingungen der IBM für Programmpakete oder einer äquivalenten Vereinbarung.

Alle in diesem Dokument enthaltenen Leistungsdaten stammen aus einer gesteuerten Umgebung. Die Ergebnisse, die in anderen Betriebsumgebungen erzielt werden, können daher erheblich von den hier erzielten Ergebnissen abweichen. Einige Daten stammen möglicherweise von Systemen, deren Entwicklung noch nicht abgeschlossen ist. Eine Gewährleistung, dass diese Daten auch in allgemein verfügbaren Systemen erzielt werden, kann nicht gegeben werden. Darüber hinaus wurden einige Daten unter Umständen durch Extrapolation berechnet. Die tatsächlichen Ergebnisse können abweichen. Benutzer dieses Dokuments sollten die entsprechenden Daten in ihrer spezifischen Umgebung prüfen.

Alle Informationen zu Produkten anderer Anbieter stammen von den Anbietern der aufgeführten Produkte, deren veröffentlichten Ankündigungen oder anderen allgemein verfügbaren Quellen. IBM hat diese Produkte nicht getestet und kann daher keine Aussagen zu Leistung, Kompatibilität oder anderen Merkmalen machen. Fragen zu den Leistungsmerkmalen von Produkten anderer Anbieter sind an den jeweiligen Anbieter zu richten.

Diese Veröffentlichung enthält möglicherweise Beispiele für Daten und Berichte des alltäglichen Geschäftsablaufes. Sie sollen nur die Funktionen des Lizenzprogrammes illustrieren; sie können Namen von Personen, Firmen, Marken oder Produkten enthalten. Alle diese Namen sind frei erfunden; Ähnlichkeiten mit tatsächlichen Namen und Adressen sind rein zufällig.

Die oben genannten Erklärungen bezüglich der Produktstrategien und Absichtserklärungen von IBM stellen die gegenwärtige Absicht der IBM dar, unterliegen Änderungen oder können zurückgenommen werden, und repräsentieren nur die Ziele der IBM.

COPYRIGHTLIZENZ

Diese Veröffentlichung enthält möglicherweise Beispielanwendungsprogramme, die in Quellensprache geschrieben sind. Sie dürfen diese Beispielprogramme kostenlos kopieren, ändern und verteilen, wenn dies zu dem Zweck geschieht, Anwendungsprogramme zu entwickeln, verwenden, vermarkten oder zu verteilen, die mit der Anwendungsprogrammierschnittstelle konform sind, für die diese Beispielprogramme geschrieben werden. Die Beispiele wurden eventuell nicht unter allen denkbaren Bedingungen getestet. IBM kann deshalb nicht garantieren, dass die Zuverlässigkeit, Wartungsfreundlichkeit und Funktion dieser Programme gegeben ist.

WebSphere Partner Gateway enthält den Code ICU4J, für den Sie unter den Bedingungen der Internationalen Nutzungsbedingungen für Programmpakete, unter Vorbehalt der Bedingungen für ausgeschlossene Komponenten, eine Lizenz von IBM erhalten. Die Bereitstellung des folgenden Hinweises durch IBM ist jedoch erforderlich:

COPYRIGHT- UND BERECHTIGUNGSHINWEIS

Copyright (c) 1995-2003 International Business Machines Corporation und andere

Alle Rechte vorbehalten.

Hiermit wird jeder Person, die eine Kopie dieser Software und der zugehörigen Dokumentationsdateien (die "Software") erhält, die kostenlose Genehmigung erteilt, uneingeschränkt mit der Software zu handeln. Dazu gehört ohne Einschränkung das Recht, Kopien der Software zu nutzen, zu kopieren, zu ändern, zusammenzufügen, zu veröffentlichen, zu verteilen und/oder zu verkaufen und den Personen, denen die Software zur Verfügung gestellt wird, das gleiche Recht einzuräumen, vorausgesetzt, dass der obige Copyrightvermerk und dieser Berechtigungshinweis auf allen Kopien der Software sowie der zugehörigen Dokumentation erscheinen.

DIE SOFTWARE WIRD OHNE WARTUNG (AUF "AS-IS"-BASIS) UND OHNE GEWÄHRLEISTUNG (VERÖFFENTLICHT ODER STILLSCHWEIGEND), EINSCHLIESSLICH, ABER NICHT BEGRENZT AUF DIE IMPLIZIERTE GEWÄHRLEISTUNG FÜR DIE HANDELSÜBLICHKEIT, DIE VERWENDUNGSFÄHIGKEIT FÜR EINEN BESTIMMTEN ZWECK UND DIE FREIHEIT DER RECHTE DRITTER ZUR VERFÜGUNG GESTELLT. UNTER KEINEN UMSTÄNDEN IST DER ODER SIND DIE COPYRIGHTINHABER HAFTBAR FÜR SPEZIELLE, UNMITTELBARE, MITTELBARE ODER FOLGESCHÄDEN ODER SCHÄDEN DURCH NUTZUNGSAUSFALL, DATENVERLUST, GEWINNEINBUSSEN. DIES GILT UNABHÄNGIG VON DER HAFTUNGSGRUNDLAGE, SEI SIE VERSCHULDENSABHÄNGIG ODER VERSCHULDENSUNABHÄNGIG, SOFERN SIE IN IRGENDEINER FORM AUF DIE NUTZUNG DER SOFTWARE ZURÜCKZUFÜHREN WÄRE.

Mit Ausnahme der Verwendung in diesem Hinweis darf der Name eines Copyrightinhabers ohne seine vorherige schriftliche Genehmigung nicht zu Werbezwecken, anderen Arten der Verkaufsförderung oder zur Nutzung in dieser Software verwendet werden.

Informationen zur Programmierschnittstelle

Werden Informationen zur Programmierschnittstelle bereitgestellt, ermöglichen Ihnen diese das Erstellen von Anwendungssoftwareprogrammen mit Hilfe dieses Programms. Allgemeine Programmierschnittstellen ermöglichen Ihnen das Schreiben von Anwendungssoftwareprogrammen, die die Services der Tools des vorliegenden Programms nutzen. Diese Informationen enthalten möglicherweise auch Diagnose-, Änderungs- und Optimierungsinformationen. Diese Informationen werden bereitgestellt, um Ihnen die Behebung von Fehlern in Ihren Anwendungssoftwareprogrammen zu erleichtern.

Achtung:: Diese Diagnose-, Änderungs- und Optimierungsinformationen dürfen nicht als Programmierschnittstelle verwendet werden, da sie jederzeit geändert werden können.

Marken und Servicemarken

Folgende Namen sind in gewissen Ländern Marken oder eingetragene Marken der International Business Machines Corporation:

i5/OS
IBM
Das 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 und das Windows-Logo sind in gewissen Ländern Marken oder eingetragen Marken der Microsoft Corporation.

MMX, Pentium und ProShare sind in gewissen Ländern Marken oder eingetragene Marken der Intel Corporation.

Java und alle Java-basierten Marken sind in gewissen Ländern Marken der Sun Microsystems, Inc.

Linux ist in gewissen Ländern eine Marke von Linus Torvalds.

Andere Namen von Unternehmen, Produkten oder Services können Marken oder Servicemarken anderer Unternehmen sein.

WebSphere Partner Gateway Enterprise und Advanced Edition enthält Software, die vom Eclipse Project (www.eclipse.org) entwickelt wurde.

WebSphere Partner Gateway Enterprise und Advanced Edition Version 6.0.

Index

Sonderzeichen

&DT99724, Zuordnung 133
&DT99735, Zuordnung 133
&DT99933, Zuordnung 133
&DTCTL, Zuordnung 133
&DTCTL21, Zuordnung 133
&WDIEVAL, Zuordnung 133
&X44TA1, Zuordnung 133

Numerische Stichwörter

0A1 Notification of Failure
  V02.02, PIP 260
  V1.0, PIP 259
0A1 PIP 245
2048-Byte, Verschlüsselungszertifikat, Maximum 173
2A1 Distribute New Product, PIP 260
2A12 Distribute Product Master, PIP 262
3A1 Request Quote, PIP 262
3A2 Request Price and Availability, PIP 263
3A4 Request Purchase Order
  V02.00, PIP 264
  V02.02, PIP 266
3A5 Query Order Status, PIP 267
3A6 Distribute Order Status, PIP 268
3A7 Notify of Purchase Order, PIP 269
3A8 Request Purchase Order Change
  V01.02, PIP 270
  V01.03, PIP 272
3A9 Request Purchase Order Cancellation, PIP 273
3B11 Notify of Shipping Order, PIP 276
3B12 Request Shipping Order, PIP 277
3B13 Notify of Shipping Order Confirmation, PIP 278
3B14 Request Shipping Order Cancellation 279
3B18 Notify of Shipping Documentation, PIP 279
3B2 Notify of Advance Shipment, PIP 274
3B3 Distribute Shipment Status, PIP 275
3C1 Return Product, PIP 281
3C3 Notify of Invoice, PIP 282
3C4 Notify of Invoice Reject, PIP 283
3C6 Notify of Remittance Advice, PIP 284
3C7 Notify of Self-Billing Invoice, PIP 284
3D8 Distribute Work in Process, PIP 285
4A1 Notify of Strategic Forecast, PIP 286
4A3 Notify of Threshold Release Forecast, PIP 287
4A4 Notify of Planning Release Forecast, PIP 288
4A5 Notify of Forecast Reply, PIP 289
4B2 Notify of Shipment Receipt, PIP 290
4B3 Notify of Consumption, PIP 291
4C1 Distribute Inventory Report
  V02.01, PIP 291
  V02.03, PIP 292
5C1 Distribute Product List, PIP 293
5C2 Request Design Registration, PIP 294
5C4 Distribute Registration Status, PIP 295
5D1 Request Ship From Stock and Debit Authorization, PIP 295
6C1 Query Service Entitlement, PIP 296
6C2 Request Warranty Claim, PIP 297
7B1 Distribute Work in Process, PIP 298
7B5 Notify of Manufacturing Work Order, PIP 299
7B6 Notify of Manufacturing Work Order Reply, PIP 300

A

Abgelaufenes Zertifikat, ersetzen 172
Administrator
  Community Manager 138
  erstellen 36
  Teilnehmer 162
Aktionen
  Beschreibung 15
  erstellen 63
  Handler 62
  kopieren 63
Alertfähige Ereignisse 191
Allgemein, Attribute, Umschlagsprofil 111
Alphanumerische Validierungstabelle, Attribut 310
Alter der Warteschlange, Programm zur Umschlagsgenerierung 109
Angepasste XML-Protokolldefinitionen 89
Anmelden an Community Console 30
Anwendungsabsender 114
Anwendungsabsender-ID 114
Anwendungsempfänger 114
Anwendungsempfänger-ID 114
Anwendungskennwort 114
Anwendungsreferenz 113
APIs, aktivieren 189
Arbeitsabläufe
  ausgehend, fest 16
  benutzerdefinierte Handler 60
  eingehend, fest 13
AS, Paket 4
AS-Attribute
  AS-Geschäfts-ID 140, 166, 318
  AS komprimiert 314
  AS-Komprimierung vor Unterzeichnung 315
  AS-MDN angefordert 315
  AS-MDN asynchron 316
AS-Attribute *(Forts.)*
  AS-MDN-E-Mail-Adresse 316
  AS-MDN-Http-URL-Adresse 316
  AS MDN unterzeichnet 317
  AS Message Digest Algorithm 317
  AS unterzeichnet 182, 317
  AS verschlüsselt 184, 186, 315
  Bestätigungszeit 314
  Wiederholungszähler 314
AS-Geschäfts-ID, Attribut 140, 166, 318
AS komprimiert, Attribut 314
AS-Komprimierung vor Unterzeichnung, Attribut 315
AS-MDN angefordert, Attribut 315
AS-MDN asynchron, Attribut 316
AS-MDN-E-Mail-Adresse, Attribut 316
AS-MDN-Http-URL-Adresse, Attribut 316
AS MDN unterzeichnet, Attribut 317
AS Message Digest Algorithm, Attribut 317
AS unterzeichnet, Attribut 182, 317
AS verschlüsselt, Attribut 184, 186, 315
AS1, Standard 4
AS2, Standard 4
AS2-Synchronprüfungshandler 56
ascii, Befehl 48, 154
Attribute
  B2B-Funktionalität 66, 99
  Begrenzer 305
  Dokumentenflussdefinition 65, 97
  EDI, Liste mit 301
  EDI-Dokumentenflussebene 125
  EDI-Protokollebene 124
  EDIFACT-Umschlag 304
  globaler Transport 41
  Teilnehmerverbindung 67, 99
  Trennzeichen 305
  UCS-Umschlag 302
  Umschlagsprofil 110, 301
  Verbindungsprofil 115
  Verteilerhandler 53
  Vorrangstellung 165
  X12-Umschlag 301
Aufzählung 259
Ausführungszeit, Attribut 318
Ausgehend, SSL
  Clientauthentifizierung 178
  Serverauthentifizierung 177
Ausgehende Unterschriftszertifikate 182
Austauschvorgänge
  Struktur 93
  Verarbeitung von 104
  Verbindungsprofile 116
Autorisierungsinformationen 112

B

B2B-Funktionalität
  Attribute 66, 99
  Beschreibung 66, 98

B2B-Funktionalität *(Forts.)*
Community Manager 139
Teilnehmer 163
Backend Integration, Paket
Beschreibung 4
erstellen 257
Banner, hinzufügen 33
BCG_BATCHDOCS, Attribut 53, 103, 109
bcg.CRLDir, Merkmal 179
BCG.Properties, Datei
aktualisieren, 0A1 PIP, Kontaktinformationen 246
bcg.CRLDir 179
bcgChgPassword.jacl, Script 171
bcgClientAuth.jacl, Script
konfigurieren, Clientauthentifizierung 176
zurücksetzen nach Verwendung von bcgssl.jacl 187
bcgDISImport, Dienstprogramm 123
bcgreceiver, Servlet 41
bcgssl.jacl, Script 187
Befehle, FTP 48, 154
Begrenzer für Datenelemente, Attribut 306, 307
Begrenzer für Unterelemente, Attribut 306
Begrenzerattribute 305
Beispiele
EDI mit Pass-Through 193
EDI zu ROD 211
EDI zu XML 225
funktionale Bestätigungen 221
ROD zu EDI 237
Sicherheit 199
TA1-Bestätigung 217
XML zu EDI 230
Benutzerdefinierte Handler
aktualisieren 60
Arbeitsablauf 60
hochladen 40, 59
Benutzerdefinierte Transporte
aktualisieren 191
Gateway 158
löschen 52, 159
Ziel 52
Berechtigungen
ändern, Standard 37
Beschreibung 36
Bestätigung angefordert 112
Bestätigungsanforderung 113
Bestätigungszeit, Attribut 314, 318
BG01, Kommunikations-ID 113
BG02, Kommunikationskennwort 113
Binärdateien
Namenskonvention 23
Verarbeitung 23
Binäre Dokumente 69
binary, Befehl 48, 154
Binary, Protokoll 6
Binary, Verzeichnis 23
Branding der Community Console durchführen 33
bye, Befehl 49, 155

C

cd, Befehl 48, 155
Client-SSL-Zertifikat prüfen, Option 177
Clientauthentifizierung
ausgehend, SSL 178
eingehend, SSL 176
konfigurieren 176
common_LineNumber_R, Typelemente 258
Community Console
anmelden an 30
Banner 33
Branding 33
Hintergrund, Kopfzeile 33
Logo, hinzufügen 33
starten 29
Community Manager
B2B-Funktionalität 139
Beschreibung 2, 137
Profil 137
Content-Type, Header, cXML 87
CRL (Zertifikatswiderrufsliste)
hinzufügen 179
Verteilungspunkte 180
CTLNUMFLAG (Kontrollnummern nach Transaktions-ID) 302, 303, 304
cXML, Protokoll 6
cXML-Dokumente
Anforderungstyp 85
Antworttyp 86
Beispiel 85
Content-Type, Header 87
Dokumentenflussdefinitionen 88
DTDs 84
Nachrichtentyp 86
Stammelement 84
cXML-Synchronprüfungshandler 56

D

Data Interchange Services
Zuordnungen, importieren 123
Data Interchange Services-Client
Beschreibung 28, 122
Merkmale 313
Zuordnungsexperte 28, 95
Dateisystemziele 47
Dateiverzeichnisgateways 21
Datenelemente
Beschreibung 94
einfach 307
Komponente 307
zusammengesetzt 307
DayofMonth, Typelement 259
delete, Befehl 48, 155
Detaillierte Validierung des Segments, Attribut 311
Dezimalschreibweise 306
Dezimalschreibweise, Attribut 306
Digitale Unterschrift
aktivieren 182
Beschreibung 170
Digitale Unterschrift erforderlich, Attribut 318
Distribute Inventory Report
V02.01, PIP 291
Distribute Inventory Report *(Forts.)*
V02.03, PIP 292
Distribute New Product Information, PIP 260
Distribute Order Status, PIP 268
Distribute Product List, PIP 293
Distribute Product Master, PIP 262
Distribute Registration Status, PIP 295
Distribute Shipment Status, PIP 275
Distribute Work in Process, PIP 285, 298
Document Manager
Beschreibung 12
starten 30
Documents, Verzeichnis 23
Dokumentanzeige 92, 135
Dokumentdefinitionen, Data Interchange Services 122
Dokumente mit doppelten Dokument-IDs zulassen, Attribut 308
Dokumentenflussdefinitionen
Attribute 65, 97
Beschreibung 65, 97
RNIF 72
Sicherstellen der Verfügbarkeit 65, 97
Typen 68
Übersicht 3
Validierungszuordnungen, zuordnen 92
Web-Services 80
Dokumentenflüsse
angepasst 90
Beschreibung 7
Dokumentenflusspakete, PIP 73
DTDs
cXML-Dokumente 84
konvertieren in XML-Schema 248

E

EDI
Attribute, Liste mit 301
Austauschvorgänge 93
Datenelemente 94
Segmente 94
Transaktionen 93
Übersicht 93
EDI-Attribute
Alphanumerische Validierungstabelle 310
Detaillierte Validierung des Segments 311
Dokumente mit doppelten Dokument-IDs zulassen 308
EDI FA-Zuordnungen 308
Höchste Fehlerkategorie bei der Umsetzung 308
Höchste Validierungsfehlerkategorie 309
Informationen auf Gruppenebene nur in funktionaler Bestätigung generieren 310
Jahr für Jahrhundertsteuerung 310
Kennung für Absender der Gruppenanwendung 312
Kennung für Austausch 312
Kennung für Empfänger der Gruppenanwendung 312

EDI-Attribute *(Forts.)*
Kennwort für Gruppenanwendung 312
Nutzungsanzeiger für Austausch 312
Qualifikationsmerkmal für Absender der Gruppenanwendung 312
Qualifikationsmerkmal für Austausch 312
Qualifikationsmerkmal für Empfänger der Gruppenanwendung 312
Qualifikationsmerkmal1 für Verbindungsprofil 116, 312
Routing-Adresse für Austausch 312
Segmentausgabe 308
Stufe der Validierung 309
TA1-Anforderung zulassen 311
Umgekehrtes Routing für Austausch 312
Umschlag bei Fehlern löschen 311
Validierungstabelle für Zeichensatz 309
XMLNS aktiv 308
EDI-Austauschvorgänge
Struktur 93, 94
Verarbeitung von 104
EDI-Consent, Protokoll 6
EDI-EDIFACT, Protokoll 6
EDI FA-Zuordnungen, Attribut 308
EDI mit Pass-Through, Dokumentenfluss
Beispiel 193
konfigurieren 69
EDI-Umschlagsattribute 113
Begrenzer 306
BG01, Kommunikations-ID 113
BG02, Kommunikationskennwort 113
CRPCTLLEN, Länge der Gruppenkontrollnummer 303
CTLNUMFLAG, Kontrollnummern nach Transaktions-ID 302, 303, 304
EDIFACTGRP, Gruppen für EDI erstellen 304
GRPCTLLEN, Länge der Gruppenkontrollnummer 304
GS01, ID der funktionalen Gruppe 113, 302, 303
GS02, Anwendungsabsender 114
GS03, Anwendungsempfänger 114
GS07, Gruppenstelle 114
GS08, Gruppenversion 114, 302, 303
INTCTLLEN, Länge der Austauschkontrollnummer 301, 303, 304
ISA01, Qualifikationsmerkmal für Autorisierungsinformationen 112
ISA02, Autorisierungsinformationen 112
ISA03, Qualifikationsmerkmal für Sicherheitsinformationen 112
ISA04, Sicherheitsinformationen 112
ISA11, Austauschstandards 112
ISA12, ID der Austauschversion 112
ISA14, Bestätigung angefordert 112
Kontrollnummern nach Transaktions-IDs 112
Länge der Austauschkontrollnummer 112
Länge der Gruppenkontrollnummer 112, 302
EDI-Umschlagsattribute *(Forts.)*
Länge der Transaktionskontrollnummer 112
Max. Anzahl an Transaktionen 112
MAXDOCS, Max. Anzahl an Transaktionen 302, 303, 304
Trennzeichen 306
TRXCTLLEN, Länge der Transaktionskontrollnummer 302, 303, 304
UNB0101, Syntax-ID 113
UNB0102, Syntaxversion 113
UNB0601, Referenz/Kennwort des Empfängers 113
UNB0602, Qualifikationsmerkmal für Referenz/Kennwort des Empfängers 113
UNB07, Anwendungsreferenz 113
UNB08, Priorität 113
UNB09, Bestätigungsanforderung 113
UNB10, ID der Kommunikationsvereinbarung 113
UNB11, Testanzeiger (Nutzungsanzeiger) 113
UNG01, ID der funktionalen Gruppe 114, 305
UNG0201, Anwendungsabsender-ID 114
UNG0202, Qualifikationsmerkmal für Anwendungsabsender-ID 114
UNG0301, Anwendungsempfänger-ID 114
UNG0302, Qualifikationsmerkmal für Anwendungsempfänger-ID 114
UNG06, Kontrollierende Stelle 114
UNG0701, Nachrichtenversion 114
UNG0702, Nachrichtenrelease 114
UNG0703, Zugeordnete Assoziation 114
UNG08, Anwendungskennwort 114
UNH0201, Nachrichtentyp 114, 305
UNH0202, Nachrichtenversion 114, 305
UNH0203, Nachrichtenrelease 115, 305
UNH0204, Kontrollierende Stelle 115, 305
UNH0205, Von Assoziation zugeordneter Code 115
UNH03, Referenz für allgemeinen Zugriff 115
EDI-Verteilerhandler 54, 55
EDI-X12, Protokoll 6
EDI-X12-Austauschstruktur 94
EDI zu EDI, Dokumentenfluss
Beschreibung 99
konfigurieren 124
EDI zu ROD, Dokumentenfluss
Beispiel 211
Beschreibung 100
konfigurieren 126
EDI zu XML, Dokumentenfluss
Beispiel 225
Beschreibung 100
konfigurieren 126
EDIFACT-Umschlagsattribute 304
EDIFACTGRP (Gruppen für EDI erstellen) 304
Einfaches Datenelement 307
Eingehend, SSL
Clientauthentifizierung 176
konfigurieren mit nicht standardmäßigen Keystores 186
Serverauthentifizierung 175
Eingehende Unterschriftszertifikate 181
Empfänger
Beschreibung 8, 39
starten 30
Encoding, Attribut 53
ENVTYPE, Umschlagstyp 302, 303, 304
Ereignisanzeige 186
Ereignisse, alertfähig 191
Ereigniswarteschlangen, angeben 189

F

Fehlerbenachrichtigung, PIP-Verarbeitung 245
Feste Ausgangsarbeitsabläufe
benutzerdefinierte Handler 60
Beschreibung 16
Handler 61
Feste Eingangsarbeitsabläufe
benutzerdefinierte Handler 60
Beschreibung 13
Handler 61
Firmenlogo, hinzufügen 33
Format, Validierungzuordnungen 258
Freigabezeichen 306
Freigabezeichen, Attribut 306, 307
From Packaging Name, Attribut 53
From Packaging Version, Attribut 53
From Process Code, Attribut 54
From Process Version, Attribut 54
From Protocol Name, Attribut 53
From Protocol Version, Attribut 53
FTP-Befehle
ascii 48, 154
Binary 48, 154
bye 49, 155
cd 48, 155
delete 48, 155
get 48
getdel 49
mget 49
mgetdel 49
mkdir 49, 155
mput 155
open 49, 155
passive 48, 154
quit 49, 155
quote 49, 155
rename 49
rmdir 49, 155
site 49, 155
FTP-Gateways 147
FTP-Scripting-Ziele 48
FTP-Scripts
Befehle, zulässig in 48, 154
Beschreibung 28
Gateways 154
Ziele 48
FTP-Server
Binary, Verzeichnis 23
Documents, Verzeichnis 23

FTP-Server *(Forts.)*
konfigurieren 24
Verzeichnisstruktur 22
FTP-Ziele 42
FTPS-Server, Sicherheitsaspekte 24
Funktionale Bestätigung (FA)
Beispiel 221
Beschreibung 132
Funktionale Bestätigung (FA), Zuordnungen
Beschreibung 95
vom System bereitgestellt 133
funktionale Bestätigungen
Beispiel 221
Beschreibung 132

G

Gateways
benutzerdefinierte Transporte 158
Beschreibung 17
Dateiverzeichnis 21, 151
FTP 147
FTP-Scripting 154, 155
FTPS 152
HTTP 144
HTTPS 145
JMS 149
Konfigurationspunkte 17
Nachverarbeitung, Konfigurationspunkt 17, 158
SMTP 148
Standard 159
Transporte, unterstützt 141
Vorverarbeitung, Konfigurationspunkt 17, 158
Generischer Dokumentenflusshandler 55
Geschäfts-ID 138, 161, 162
Geschäftsprotokolle 6
get, Befehl 48
getdel, Befehl 49
Globale Transportattribute
Gateway 142
Ziel 41
Globaler Lieferkettencode, Attribut 319
GlobalLocationIdentifier, Typelement 258
GRPCTLLEN (Länge der Gruppenkontrollnummer) 302, 303, 304
Gruppe, Attribute, Umschlagsprofil 113
Gruppen, EDI
Beschreibung 94
Headersegmente 94
Trailersegmente 94
Gruppen für EDI erstellen 304
Gruppenstelle 114
Gruppenversion 114, 302, 303
GS-Attribute 113
GS01, ID der funktionalen Gruppe 113, 302, 303
GS02, Anwendungsabsender 114
GS03, Anwendungsempfänger 114
GS07, Gruppenstelle 114
GS08, Gruppenversion 114, 302, 303

H

Handler
benutzerdefiniert 59, 60
Beschreibung 10
hochladen 40, 59
Protokoll entpacken 61
Protokoll packen 61
Protokollverarbeitung 61
Handlerliste, Seite 57
Handlertypen 59
Handshake, SSL 174
Headersegment 94
Hilfesystem, starten 30
Höchstalter der Warteschlange, Feld 109
Höchste Fehlerkategorie bei der Umsetzung, Attribut 308
Höchste Validierungsfehlerkategorie, Attribut 309
HTTP-Ziele
konfigurieren 41
Synchronprüfungshandler 56
Hubadmin, Benutzer xi, 30

I

IBM Key Management Tool (iKeyman)
Beschreibung 170
Position 170
ID der Austauschstandards 112
ID der Austauschversion 112
ID der funktionalen Gruppe 113, 114, 302, 305
ID der Kommunikationsvereinbarung 113
iKeyman, Dienstprogramm
Beschreibung 170
Position 170
Informationen auf Gruppenebene nur in funktionaler Bestätigung generieren, Attribut 310
INTCTLLEN (Länge der Austauschkontrollnummer) 301, 303, 304
Interaktionen
Beschreibung 66, 98
cXML-Dokumente 88
RosettaNet-Dokumente 76
Web-Services 84
Intermediate, Zertifikate 172
Intervallbasierte Zeitplanung
FTP-Scripting-Ziele 51
Programm zur Umschlagsgenerierung 109
SMTP-Ziel (POP3) 44
ISA01, Qualifikationsmerkmal für Autorisierungsinformationen 112
ISA02, Autorisierungsinformationen 112
ISA03, Qualifikationsmerkmal für Sicherheitsinformationen 112
ISA04, Sicherheitsinformationen 112
ISA11, ID der Austauschstandards 112
ISA12, ID der Austauschversion 112
ISA14, Bestätigung angefordert 112
ISA15, Testanzeiger 113

J

Jahr für Jahrhundertsteuerung, Attribut 310
Java-Laufzeit, hinzufügen 26
JMS, Ändern der Standardkonfiguration 25
JMS-Gateways 149
JMS-Konfiguration, definieren 27
JMS-Kontext, definieren 27
JMS-Verzeichnisse, erstellen 25
JMS-Ziele
konfigurieren 45
Synchronprüfungshandler 56
JMSAdmin.config, Datei 25
JRE-Standortrichtliniendateien (Jurisdiction Policy Files) 173

K

Kalenderbasierte Zeitplanung
FTP-Scripting-Ziele 51
Programm zur Umschlagsgenerierung 109
SMTP-Ziel (POP3) 44
Kardinalität 258
Keine Attribute gefunden 247
Kennung für Absender der Gruppenanwendung, Attribut 312
Kennung für Austausch, Attribut 312
Kennung für Empfänger der Gruppenanwendung, Attribut 312
Kennwort für Gruppenanwendung, Attribut 312
Kennwörter
Keystore, Standard 171
Standard 30
Truststore, Standard 171
Kennwortrichtlinie, konfigurieren 35
Ketten, Zertifikat 172
Keystores
Beschreibung 171
Standardkennwort 171
verwenden, nicht standardmäßig 186
Kommunikations-ID 113
Kommunikationskennwort 113
Komponentendatenelemente 307
Konfigurationspunkte
Gateways 17, 158
Nachverarbeitung 11, 57, 158
synchrone Austauschvorgänge 52
Synchronprüfung 11, 56
Vorverarbeitung 11, 53, 158
Ziel 10, 52
Konfigurationspunkte, Gateway ändern 158
Nachverarbeitung 17, 158
Vorverarbeitung 17, 158
Konfigurationspunkte, Ziel ändern 57
Nachverarbeitung 11, 57
Synchronprüfung 11, 56
Übersicht 10
Vorverarbeitung 11, 53
Kontaktinformationen, 0A1 PIP 246
Kontrollierende Stelle 114, 115, 305

Kontrollnummern
anzeigen 121
Beschreibung 118
Initialisierung 120
Masken 118
Kontrollnummern nach Transaktions-IDs 112, 302, 303, 304
Kopfhintergrund, hinzufügen 33

L

Länge der Austauschkontroll-nummer 112, 301, 303, 304
Länge der Gruppenkontrollnummer 112, 302, 303, 304
Länge der Transaktionskontroll-nummer 112, 302, 303, 304
Logo, hinzufügen, Firma 33

M

Masken, Kontrollnummer 118
Max. Anzahl an Transaktionen 112, 302, 303, 304
MAXDOCS (Max. Anzahl an Transaktio-nen) 302, 303, 304
Maximale Sperrenzeit, Feld 109
maxOccurs, Attribut 258
Mehrere Dokumente in einer Datei 96
Mehrere Zertifikate 172
Merkmale
Data Interchange Services-Client 313
Transformationszuordnung 313
Metadictionary, Attribut 54
Metadocument, Attribut 54
Metasyntax, Attribut 54
mget, Befehl 49
mgetdel, Befehl 49
minOccurs, Attribut 258
mkdir, Befehl 49, 155
mput, Befehl 155

N

N/A-Spezifikation 5
Nachrichtenrelease 115, 305
Nachrichtenrelease-ID 114
Nachrichtentyp 114, 305
Nachrichtenversion 114, 305
Nachverarbeitung, Konfigurationspunkt
Gateway 17, 158
Handlertypen 57
Ziel 11, 57
No valid encryption certificate found, Nachricht 186
None, Paket 5
Notification of Failure
V02.00, PIP 260
V1.0, PIP 259
Notify of Advance Shipment, PIP 274
Notify of Consumption, PIP 291
Notify of Forecast Reply, PIP 289
Notify of Invoice, PIP 282
Notify of Invoice Reject, PIP 283
Notify Of Manufacturing Work Order, PIP 299
Notify Of Manufacturing Work Order Reply, PIP 300
Notify of Planning Release Forecast, PIP 288
Notify of Purchase Order Update, PIP 269
Notify of Remittance Advice, PIP 284
Notify of Self-Billing Invoice, PIP 284
Notify of Shipment Receipt, PIP 290
Notify of Shipping Documentation, PIP 279
Notify of Shipping Order, PIP 276
Notify of Shipping Order Confirmation, PIP 278
Notify of Strategic Forecast, PIP 286
Notify of Threshold Release Forecast, PIP 287
Nutzungsanzeiger für Austausch, Attri-but 312

O

öffentliche WSDL-Dateien 81
Öffentlicher Schlüssel 170
open, Befehl 49, 155

P

Paket
AS 4
Backend Integration 4
Beschreibung 4
N/A-Konzept 5
None 5
RNIF 5
Partner Interface Process (PIP) 71
passive, Befehl 48, 154
PIP-Pakete
aktualisieren 247
erstellen 247
PIP-Paketinhalt
0A1 Notification of Failure 259
0A1 Notification of Failure V02.00 260
2A1 Distribute New Product Informa-tion 260
2A12 Distribute Product Master 262
3A1 Request Quote 262
3A2 Request Price and Availabili-ty 263
3A4 Request Purchase Order V02.00 264
3A4 Request Purchase Order V02.02 266
3A5 Query Order Status 267
3A6 Distribute Order Status 268
3A7 Notify of Purchase Order Update 269
3A8 Request Purchase Order Change V01.02 270
3A8 Request Purchase Order Change V01.03 272
3A9 Request Purchase Order Cancella-tion 273
3B11 Notify of Shipping Order 276
3B12 Request Shipping Order 277
PIP-Paketinhalt *(Forts.)*
3B13 Notify of Shipping Order Confir-mation 278
3B14 Request Shipping Order Cancel-lation 279
3B18 Notify of Shipping Documentati-on 279
3B2 Notify of Advance Shipment 274
3B3 Distribute Shipment Status 275
3C1 Return Product 281
3C3 Notify of Invoice 282
3C4 Notify of Invoice Reject 283
3C6 Notify of Remittance Advice 284
3C7 Notify of Self-Billing Invoice 284
3D8 Distribute Work in Process 285
4A1 Notify of Strategic Forecast 286
4A3 Notify of Threshold Release Fore-cast 287
4A4 Notify of Planning Release Fore-cast 288
4A5 Notify of Forecast Reply 289
4B2 Notify of Shipment Receipt 290
4B3 Notify of Consumption 291
4C1 Distribute Inventory Report V02.01 291
4C1 Distribute Inventory Report V02.03 292
5C1 Distribute Product List 293
5C2 Request Design Registration 294
5C4 Distribute Registration Sta-tus 295
5D1 Request Ship From Stock and Debit Authorization 295
6C1 Query Service Entitlement 296
6C2 Request Warranty Claim 297
7B1 Distribute Work in Process 298
7B5 Notify Of Manufacturing Work Order 299
7B6 Notify Of Manufacturing Work Order Reply 300
PIP-Release-Informationen 247
PIPs
0A1 245
Beschreibung 71
Dokumentenflusspakete 73
Fehlerbenachrichtigung 245
Hochladen von Paketen 75
inaktivieren 245
Inhalt der Dokumentenfluss-pakete 259
Liste der unterstützten 72
Nachrichtenverarbeitung 71
XML-Schemadateien, erstellen
Schemata 248
XSD-Datei, erstellen 248
POP3-Ziele 44
Primäre Zertifikate
ausgehend, SSL 178
ausgehende digitale Unterschrift 182
ausgehende Verschlüsselung 185
Beschreibung 172
Priorität 113
private WSDL-Dateien 81
Privater Schlüssel 170
Production, Verzeichnis 22
Profile
Community Manager 137

Profile *(Forts.)*
Teilnehmer 161
Umschlag 110
Verbindung 115
Programm zur Umschlagsgenerierung
Beschreibung 108
intervallbasierte Zeitplanung 109
maximale Sperrenzeit 109
sperren 108
Standardwerte, ändern 109
Stapelbetrieb 109
Warteschlangenalter 109
Protokoll entpacken
Handler 61
Schritt, Beschreibung 14
Protokoll packen
Handler 61
Schritt, Beschreibung 16
Protokolle
angepasstes XML 89
Binary 6
cXML 6
EDI-Consent 6
EDI-EDIFACT 6
EDI-X12 6
Liste 6
RNSC 6
RosettaNet 6
Web Service 6
XMLEvent 6
Protokollverarbeitung
Handler 61
Schritt, Beschreibung 14

Q

Qualifikationsmerkmal für Absender der Gruppenanwendung, Attribut 312
Qualifikationsmerkmal für Anwendungsabsender-ID 114
Qualifikationsmerkmal für Anwendungsempfänger-ID 114
Qualifikationsmerkmal für Austausch, Attribut 312
Qualifikationsmerkmal für Autorisierungsinformationen 112
Qualifikationsmerkmal für Empfänger der Gruppenanwendung, Attribut 312
Qualifikationsmerkmal für Referenz/Kennwort des Empfängers 113
Qualifikationsmerkmal für Sicherheitsinformationen 112
Qualifikationsmerkmal1, Feld 116
Qualifikationsmerkmal1 für Verbindungsprofil, Attribut 116, 312
Query Order Status, PIP 267
Query Service Entitlement, PIP 296
quit, Befehl 49, 155
quote, Befehl 49, 155

R

Referenz für allgemeinen Zugriff 115
Referenz/Kennwort des Empfängers 113
rename, Befehl 49
Request Design Registration, PIP 294
Request Purchase Order
V02.00, PIP 264
V02.02, PIP 266
Request Purchase Order Cancellation, PIP 273
Request Purchase Order Change
V01.02, PIP 270
V01.03, PIP 272
Request Quote, PIP 262
Request Ship From Stock and Debit Authorization, PIP 295
Request Shipping Order, PIP 277
Request Shipping Order Cancellation, PIP 279
Request Warranty Claim, PIP 297
Ressourcenbündel 34
Return Product, PIP 281
rmdir, Befehl 49, 155
RNIF, Beschreibung von 71
RNIF, Paket 5
RNIF-Pakete
erstellen 257
Position 72
RNIF-Synchronprüfungshandler 56
RNSC, Protokoll 6
RNSC-Nachrichten 71
ROD-Dokumente
Beschreibung 96
Verarbeitung von 107
ROD-Dokumente zu EDI, Dokumentenfluss
Beschreibung 102
konfigurieren 129
ROD-Verteilerhandler 54, 55, 96
ROD zu EDI, Dokumentenfluss
Beispiel 237
Beschreibung 101
konfigurieren 128
ROD zu ROD, Dokumentenfluss
Beschreibung 103
konfigurieren 131
ROD zu XML, Dokumentenfluss
Beschreibung 103
konfigurieren 131
RosettaNet
Beschreibung 71
Website 71
RosettaNet, Protokoll 6
RosettaNet-Attribute
Ausführungszeit 318
bearbeiten 246
Bestätigungszeit 318
Digitale Unterschrift erforderlich 318
globaler Lieferkettencode 75
Globaler Lieferkettencode 319
Sync-Bestätigung erforderlich 75, 319
Sync unterstützt 75, 319
Unbestreitbarkeit des Empfangs 319
Unbestreitbarkeit erforderlich 318
Verschlüsselung 75, 320
Wiederholungszähler 318
RosettaNet Implementation Framework 71
RosettaNet-Nachrichten
Ereignisbenachrichtigung 71
Versionen, unterstützt 71
RosettaNet Service Content-Nachrichten (RNSC) 71
RosettaNet-XML-Nachrichtenrichtlinien 247
RosettaNet-XML-Nachrichtenschema 247
Routing-Adresse für Austausch, Attribut 312

S

Satzorientierte Datendokumente (ROD) 96
Schemata
PIP-Pakete 248
WSDL-Dateien 82
Schlüssel
öffentlich 170
privat 170
Security Sockets Layer (SSL), Beschreibung 169
Segment, Beschreibung 307
Segment-Tag 94, 307
Segmentabschlusszeichen 306, 307
Segmentausgabe, Attribut 308
Segmentbegrenzer 306
Segmentbegrenzer, Attribut 307
Segmente, EDI 94
Segmentname 94, 307
Sekundäre Zertifikate
ausgehend, SSL 178
ausgehende digitale Unterschrift 182
ausgehende Verschlüsselung 185
Beschreibung 172
Selbst unterzeichnetes Zertifikat 172
Serverauthentifizierung
ausgehend, SSL 177
eingehend, SSL 175
Servicesegmente 94
Sicherheit
Beispiel 199
FTPS-Server, Aspekte 24
Typen, unterstützt 169
Übersicht 169
Zertifikatsliste 187
Sicherheitsinformationen 112
site, Befehl 49, 155
SMTP-Gateways 148
SMTP-Ziele 44
SOAP-Synchronprüfungshandler 56
Sperren
FTP-Scripting-Transport 41, 142
Programm zur Umschlagsgenerierung 108, 109
SSL-Beschreibung 169
SSL-Handshake 174
SSL-Zertifikate
Clientauthentifizierung, ausgehend 178
Clientauthentifizierung, eingehend 176
eingehend 175
Serverauthentifizierung, ausgehend 177
Serverauthentifizierung, eingehend 175
Stammzertifizierungsstelle 172

Standardgateway, festlegen 159
Standortrichtliniendateien (Jurisdiction Policy Files), JRE 173
Stapelbetrieb 109
Stapelbetrieb verwenden, Feld 109
Steuerungssegmente 94
Stufe der Validierung, Attribut 309
Style-Sheet, ändern 34
Sync-Bestätigung erforderlich, Attribut 319
Sync unterstützt, Attribut 319
Synchrone Austauschvorgänge, Konfigurationspunktanforderung 52
Synchronprüfung, Konfigurationspunkt
  Beschreibung 11
  HTTP/S-Ziel 56
  JMS-Ziel 56
  Liste mit Handlern 56
  Reihenfolge der Handler 57
  wenn erforderlich 52
Syntax-ID 113
Syntaxversion 113

T

TA1-Anforderung zulassen, Attribut 311
TA1-Bestätigungen
  Beispiel 217
  Beschreibung 133
Teilnehmer
  B2B-Funktionalität 163
  erstellen 161
Teilnehmerverbindungen
  aktivieren 165
  Attribute 67, 99
  Beschreibung 67, 99
Test, Verzeichnis 22
Testanzeiger 113
Testanzeiger (Nutzungsanzeiger) 113
Trailersegment 94
Transaktion, Attribute, Umschlagsprofil 114
Transaktionen, EDI
  Beschreibung 93, 94
  Headersegmente 94
  Trailersegmente 94
  Verbindungsprofile 115
Transformationszuordnungen
  Beschreibung 95
  importieren 122
  Merkmale 313
Transporte
  Gateway, vom System bereitgestellt 141
  Übersicht 2
Transporte, benutzerdefiniert
  aktualisieren 191
  Gateway 158
  löschen 52, 159
  Ziel 52
Trennzeichen für Datenelemente 306, 307
Trennzeichen für Komponentendatenelemente 306
Trennzeichen für Komponentenelemente 306
Trennzeichenattribute 305
Trust Anchor (Vertrauensanker) 172
Truststores
  Beschreibung 171
  Standardkennwort 171
TRXCTLLEN (Länge der Transaktionskontrollnummer) 302, 303, 304

U

UCS
  Beschreibung 93
  Umschlagsattribute 302
Umgekehrtes Routing für Austausch, Attribut 312
Umschlag bei Fehlern löschen, Attribut 311
Umschlag von Austauschvorgängen entfernen 104
Umschlagsattribute 110
Umschlagsmarkierung, Attribut 320
Umschlagsprofile
  Allgemein, Attribute 111
  Attribute 110, 301
  Austausch, Attribute 112
  Beschreibung 110
  erstellen 111
  Gruppe, Attribute 113
  Transaktion, Attribute 114
Umschlagstyp 302, 303, 304
UN/EDIFACT 93
UNB0101, Syntax-ID 113
UNB0102, Syntaxversion 113
UNB0601, Referenz/Kennwort des Empfängers 113
UNB0602, Qualifikationsmerkmal für Referenz/Kennwort des Empfängers 113
UNB07, Anwendungsreferenz 113
UNB08, Priorität 113
UNB09, Bestätigungsanforderung 113
UNB10, ID der Kommunikationsvereinbarung 113
UNB11, Testanzeiger (Nutzungsanzeiger) 113
Unbestreitbarkeit 170
Unbestreitbarkeit des Empfangs, Attribut 319
Unbestreitbarkeit erforderlich, Attribut 318
unformatierte Dokumente, anzeigen 92
Unformatierte Dokumente, anzeigen 135
UNG01, ID der funktionalen Gruppe 114, 305
UNG0201, Anwendungsabsender-ID 114
UNG0202, Qualifikationsmerkmal für Anwendungsabsender-ID 114
UNG0301, Anwendungsempfänger-ID 114
UNG0302, Qualifikationsmerkmal für Anwendungsempfänger-ID 114
UNG06, Kontrollierende Stelle 114
UNG0701, Nachrichtenversion 114
UNG0702, Nachrichtenrelease 114
UNG0703, Zugeordnete Assoziation 114
UNG08, Anwendungskennwort 114
UNH0201, Nachrichtentyp 114, 305
UNH0202, Nachrichtenversion 114, 305
UNH0203, Nachrichtenrelease 115, 305
UNH0204, Kontrollierende Stelle 115, 305
UNH0205, Von Assoziation zugeordneter Code 115
UNH03, Referenz für allgemeinen Zugriff 115
Unterschriftszertifikate
  ausgehend 182
  eingehend 181

V

Validierungstabelle für Zeichensatz, Attribut 309
Validierungszuordnungen
  Beschreibung 91
  Dokumentenflussdefinitionen, zuordnen 92
  Format 258
  hinzufügen 92
  importieren 122
  RosettaNet 258
  Standard-EDI 96
Verbindungen, Teilnehmer
  aktivieren 165
  Attribute 67, 99
  Beschreibung 67, 99
Verbindungsprofile
  Attribute 115
  Austauschvorgänge 116
  Beschreibung 115
  für Transaktionen 115
  konfigurieren 117
Verkettung, Zuordnung 95
Verschlüsselung
  aktivieren 184, 186
  Beschreibung 170
Verschlüsselung, Attribut 320
Verschlüsselungszertifikate, Begrenzungen bei Länge 173
Verteiler 96
Verteilerhandler
  Attribute 53
  Beschreibung 96
  Liste mit 54
Verzeichnisse
  Binary 23
  Documents 23
  FTP-Server 22
  JMS 25
  Production 22
  Test 22
Von Assoziation zugeordneter Code 115
Vorverarbeitung, Konfigurationspunkt
  Gateway 17, 158
  Ziel 11, 53

W

Warteschlangen
  Ereignis 189
  JMS, erstellen 26
Web Service, Protokoll 6
Web-Services
  Dokumentenflussdefinitionen 80

Web-Services *(Forts.)*
Einschränkungen 84
Standards, unterstützt 84
Teilnehmer, angeben 79
WebSphere MQ
Ändern der JMS-Implementierung 25
starten 29
Widerrufene Zertifikate 179
Wiederholungstrennzeichen 306
Wiederholungszähler, Attribut 314, 318
WSDL-Dateien
importieren 81
öffentlich 81
privat 81
XML-Schemata 82
ZIP-Archiv, Anforderungen 81

X

X12
Austauschstruktur 94
Beschreibung 93
X12-Umschläge, Attribute 301
XML-basierte APIs, aktivieren 189
XML-Dateien
erstellen für Pakete 'Backend Integration' 254
erstellen für RNIF-Pakete 254
Verarbeitung 24
XML-Dokumente
Beschreibung 96
Verarbeitung von 107
XML-Dokumente zu EDI, Dokumentenfluss
Beschreibung 102
konfigurieren 129
XML-Formate
Beschreibung 89
erstellen 89, 91
XML-Protokolldefinitionen, angepasst 89
XML-Schemata
konvertieren von DTD-Datei 248
PIP-Pakete 248
WSDL-Dateien 82
XML-Verteilerhandler 54, 55
XML zu EDI, Dokumentenfluss
Beispiel 230
Beschreibung 101
konfigurieren 128
XML zu ROD, Dokumentenfluss
Beschreibung 103
konfigurieren 131
XML zu XML, Dokumentenfluss
Beschreibung 103
konfigurieren 131
XMLEvent, Protokoll 6, 78
XMLNS aktiv, Attribut 308

Z

Zeichen für wiederholte Datenelemente, Attribut 306, 307
Zeitplanung
FTP-Scripting-Ziele 51
Zeitplanung *(Forts.)*
Programm zur Umschlagsgenerierung 109
SMTP-Ziel (POP3) 44
Zertifikat widerrufen oder abgelaufen, Nachricht 186
Zertifikate
abgelaufen, ersetzen 172
Format, konvertieren 177
Intermediate 172
Liste mit 187
primär 172
sekundär 172
selbst unterzeichnet 172
Unterschrift 181, 182
widerrufen 179
Ziel 172
Zertifikatketten 172
Zertifikatswiderrufsliste (CRL)
hinzufügen 179
Verteilungspunkte 180
Ziele
Beschreibung 8, 39
Dateisystem 47
FTP 42
FTP-Scripting 48
globale Transportattribute 41
HTTP 41
JMS 45
Konfigurationspunkte 10, 52
Nachverarbeitung, Konfigurationspunkt 57
SMTP 44
Synchronprüfung, Konfigurationspunkt 52
Verteilerhandler 53
Vorverarbeitung, Konfigurationspunkt 53
Zielzertifikate 172
ZIP-Archiv, Anforderungen für WSDL-Dateien 81
Zugeordnete Assoziation 114
Zuordnungen
Funktionale Bestätigung 95
importieren 122
Transformation 95
Validierung 91, 92, 96
Zuordnungen der funktionalen Bestätigungen
Beschreibung 95
importieren 122
vom System bereitgestellt 133
Zuordnungsexperte 28, 95
Zuordnungsverkettung 95
Zusammengesetztes Datenelement 307