

IBM WebSphere Business Integration Connect Enterprise
und Advanced Edition



Hub-Konfiguration

Version 4.2.2

IBM WebSphere Business Integration Connect Enterprise
und Advanced Edition



Hub-Konfiguration

Version 4.2.2

Hinweise

Vor Verwendung dieser Informationen und des darin beschriebenen Produkts sollten die Informationen unter „Bemerkungen und Marken“ auf Seite 159 gelesen werden.

- Die IBM Homepage finden Sie im Internet unter: **ibm.com**
- IBM und das IBM Logo sind eingetragene Marken der International Business Machines Corporation.
- Das e-business-Symbol ist eine Marke der International Business Machines Corporation.
- Infoprint ist eine eingetragene Marke der IBM.
- ActionMedia, LANDesk, MMX, Pentium und ProShare sind Marken der Intel Corporation in den USA und/oder anderen Ländern.
- C-bus ist eine Marke der Corollary, Inc. in den USA und/oder anderen Ländern.
- Java und alle auf Java basierenden Marken und Logos sind Marken der Sun Microsystems, Inc. in den USA und/oder anderen Ländern.
- Microsoft Windows, Windows NT und das Windows-Logo sind Marken der Microsoft Corporation in den USA und/oder anderen Ländern.
- PC Direct ist eine Marke der Ziff Communications Company in den USA und/oder anderen Ländern.
- SET und das SET-Logo sind Marken der SET Secure Electronic Transaction LLC.
- UNIX ist eine eingetragene Marke der Open Group in den USA und/oder anderen Ländern.
- Marken anderer Unternehmen/Hersteller werden anerkannt.

Diese Veröffentlichung ist eine Übersetzung des Handbuchs
IBM WebSphere Business Integration Connect Enterprise and Advanced Editions Hub Configuration Guide Version 4.2.2,

herausgegeben von International Business Machines Corporation, USA

© Copyright International Business Machines Corporation 2003, 2004
© Copyright IBM Deutschland Informationssysteme GmbH 2004

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
Juli 2004

Inhaltsverzeichnis

Neu in diesem Release	vii
Neu in Release 4.2.2	vii
Vorwort.	ix
Zu diesem Handbuch	ix
Zielgruppe	ix
Typografische Konventionen	ix
Zugehörige Dokumente.	x
Hilfe anfordern	x
Onlinehilfe	x
Softwareunterstützung	xi
Passport Advantage.	xi
Produktdokumentation	xi
Kapitel 1. Einführung	1
Für die Hubkonfiguration benötigte Informationen	1
Übersicht über die Dokumentverarbeitung	2
Dokumentverarbeitungskomponenten mit Handler konfigurieren.	3
Ziele	4
Document Manager	6
Fester Eingangsarbeitsablauf	7
Aktionen	10
Fester Ausgangsarbeitsablauf	11
Gateways	12
Kapitel 2. Die Konfiguration des Hubs vorbereiten	13
Verzeichnis für ein Dateiverzeichnisgateway erstellen	13
Den FTP-Server für das Empfangen von Dokumenten konfigurieren	13
Die erforderliche Verzeichnisstruktur auf dem FTP-Server konfigurieren	14
Verarbeitung der über FTP gesendeten Dateien	14
Zusätzliche FTP-Serverkonfiguration	16
Sicherheitserwägungen für den FTPS-Server	16
Den Hub für das JMS-Transportprotokoll konfigurieren	16
Verzeichnis für JMS erstellen	16
Die Standard-JMS-Konfiguration modifizieren	16
Warteschlangen und den Kanal erstellen.	17
Ihrer Umgebung eine Java-Laufzeit hinzufügen	18
Die JMS-Konfiguration definieren	18
Kapitel 3. Den Server starten und Community Console anzeigen.	19
WebSphere MQ starten	19
Die WebSphere Business Integration Connect-Komponenten starten	19
An Community Console anmelden	20
Kapitel 4. Community Console konfigurieren	23
Locale-Informationen und Konsolbranding angeben	23
Konsolbranding durchführen	24
Die Konsoldaten lokalisieren	25
Kennwortrichtlinie konfigurieren	25
Berechtigungen konfigurieren	27
Benutzern Berechtigungen erteilen.	27
Berechtigungen aktivieren oder inaktivieren	29
Kapitel 5. Den Hub konfigurieren	31

Benutzerdefinierte Handler hochladen	31
Ziele konfigurieren	32
HTTP/S-Ziel konfigurieren	34
FTP-Ziel konfigurieren.	34
SMTP-Ziel konfigurieren	34
JMS-Ziel konfigurieren	35
Dateisystemziel konfigurieren	36
Konfigurationspunkte modifizieren	36
Dokumentenflüsse und Interaktionen definieren	38
Vom System bereitgestellte Pakete und Protokolle verwenden	38
Pakete hochladen	39
Dokumentverarbeitung konfigurieren.	40
Feste Arbeitsabläufe konfigurieren.	40
Aktionen konfigurieren	41
Aktionen erstellen	42
Angepasstes XML verwalten.	44
Protokolldefinitionsformat CustomXML erstellen	44
Dokumentenflussdefinition erstellen	45
XML-Format erstellen	46
Validierungszuordnungen verwenden	48
Interaktionen erstellen.	48
Zusammenfassung	50
Kapitel 6. Teilnehmer und Teilnehmerverbindungen erstellen	51
Teilnehmer erstellen	51
Gateways für die Teilnehmer konfigurieren.	52
Gateways erstellen	52
B2B-Funktionalität konfigurieren	60
Teilnehmerverbindungen aktivieren	62
Zusammenfassung	63
Kapitel 7. Sicherheit für Eingangs- und Ausgangsaustauschvorgänge konfigurieren	65
Begriffe und Konzepte.	65
Sicherheitstypen	65
Das Dienstprogramm ikeyman	66
Community Console	66
Keystores und Truststores	66
Zertifikate erstellen und installieren	68
Eingehende SSL-Zertifikate	68
Ausgehende SSL-Zertifikate	70
Zertifikatswiderrufsliste (CRL) hinzufügen	71
Eingehendes Unterschriftszertifikat	71
Ausgehendes Unterschriftszertifikat	72
Eingehendes Verschlüsselungszertifikat	73
Ausgehendes Verschlüsselungszertifikat	75
Eingangs-SSL für Konsole und Empfänger konfigurieren	75
Kapitel 8. Die Konfiguration fertig stellen	77
Die Verwendung von APIs aktivieren.	77
Die für Ereignisse verwendeten Warteschlangen angeben	77
Alertfähige Ereignisse angeben	79
Benutzerdefiniertes Transportprotokoll aktualisieren.	79
Anhang A. Beispiele	81
Basiskonfiguration – EDI-Dokumente mit AS-Paket über HTTP austauschen.	81
Den Hub konfigurieren	81
Teilnehmer und Teilnehmerverbindungen erstellen	83
Basiskonfiguration - Sicherheit für eingehende und ausgehende Dokumente konfigurieren	87
SSL-Authentifizierung für Eingangsdokumente konfigurieren.	87
Verschlüsselung konfigurieren	90

Dokumentenunterschrift konfigurieren	91
Die Basiskonfiguration erweitern	93
FTP-Ziel erstellen	93
Den Hub zum Empfangen von Binärdateien konfigurieren	93
Den Hub für angepasste XML-Dokumente konfigurieren	95
Anhang B. RosettaNet-Austauschvorgänge konfigurieren	99
RNIF- und PIP-Dokumentenflusspakete	99
RosettaNet-Unterstützung konfigurieren	101
Verbindungen zu Teilnehmern erstellen.	102
RosettaNet-Attributwerte bearbeiten.	105
Attributwerte konfigurieren	106
PIPs inaktivieren	107
Fehlerbenachrichtigung bereitstellen.	108
Kontaktinformationen aktualisieren	108
PIP-Dokumentenflusspakete erstellen	108
Die XSD-Dateien erstellen	109
Die XML-Datei erstellen	116
Das Paket erstellen	118
Informationen zur Validierung.	119
Kardinalität	119
Format	119
Aufzählung	120
Inhalt der PIP-Dokumentenflusspakete	120
Anhang C. Web-Serviceanforderungen konfigurieren	145
Die Teilnehmer für einen Web-Service angeben	145
Dokumentenflussdefinitionen für einen Web-Service konfigurieren	146
Die WSDL-Dateien für einen Web-Service hochladen	148
Interaktion für einen neuen Web-Service konfigurieren	150
Dokumentenflüsse der B2B-Funktionalität von Teilnehmern hinzufügen.	150
Die Teilnehmerverbindung aktivieren	151
Einschränkungen und Begrenzungen der Web-Serviceunterstützung	151
Anhang D. cXML-Austauschvorgänge konfigurieren.	153
cXML-Unterstützungsübersicht	153
cXML-Dokumenttypen	154
Die Header "Content-Type" und angehängte Dokumente.	156
Gültige cXML-Interaktionen	156
cXML-Dokumentenflussdefinition erstellen	156
Bemerkungen und Marken.	159
Bemerkungen	159
Informationen zur Programmierschnittstelle	161
Marken und Servicemarken	162

Neu in diesem Release

Neu in Release 4.2.2

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

Vorwort

Zu diesem Handbuch

Diese Dokumentation beschreibt, wie Sie den IBM^(R) WebSphere^(R) Business Integration Connect-Server konfigurieren.

Zielgruppe

Diese Dokumentation richtet sich an die Person, die für das Konfigurieren des WebSphere Business Integration Connect-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 Business Integration Connect Community Console zu konfigurieren und den Hub zu betreiben.

Typografische Konventionen

Diese Dokumentation verwendet die folgenden Konventionen.

Schriftart Courier	Gibt einen Literalwert an, wie z. B. einen Befehlsnamen, Dateinamen, Informationen, die Sie eingeben, oder Informationen, die das System auf der Anzeige ausgibt.
fett	Gibt einen neuen Terminus an, wenn er zum ersten Mal erwähnt wird.
<i>kursiv, kursiv</i>	Gibt einen Variablennamen oder einen Querverweis an.
<i>blaue Kontur</i>	Eine blaue Kontur, die nur sichtbar ist, wenn Sie das Handbuch online lesen, gibt einen Querverweis-Hyperlink an. Klicken Sie innerhalb der Kontur, um zum Objekt des Verweises zu springen.
{ }	In einer Syntaxzeile umgeben geschweifte Klammern eine Gruppe von Optionen, von denen Sie nur eine auswählen dürfen.
[]	In einer Syntaxzeile umgeben eckige Klammern einen optionalen Parameter.
...	In einer Syntaxzeile geben Auslassungen eine Wiederholung des vorherigen Parameters an. So bedeutet z. B. <code>option[,...]</code> , dass Sie mehrere, durch Kommata getrennte Optionen eingeben können.
< >	In einer Namenskonvention umgeben spitze Klammern einzelne Elemente eines Namens, um sie voneinander zu unterscheiden, wie z. B. in <code><servername><verbindungsname>tmp.log</code> .
/, \	In dieser Dokumentation werden Backslashes (\) als Konvention für Verzeichnispfade verwendet. Setzen Sie für UNIX-Installationen Schrägstriche (/) für Backslashes ein. Alle IBM WebSphere InterChange Server-Pfadnamen sind relativ zum Verzeichnis, in dem das Produkt IBM WebSphere InterChange Server auf Ihrem System installiert ist.
%text% und \$text	Text in Prozentzeichen (%) gibt den Wert für den Text der Windows-Systemvariablen bzw. -Benutzervariablen an. Die entsprechende Notation in einer UNIX-Umgebung ist \$text. Sie gibt den Wert für den text der UNIX-Umgebungsvariablen an.
Produktverz	Steht für das Verzeichnis, in dem das Produkt installiert ist.

Zugehörige Dokumente

Der vollständige Dokumentationsatz, der für dieses Produkt verfügbar ist, enthält umfassende Informationen zum Installieren, Konfigurieren, Verwalten und Verwenden von WebSphere Business Integration Connect Enterprise und Advanced Edition.

Sie können die Dokumentation von der folgenden Site herunterladen, installieren und anzeigen:

<http://www.ibm.com/software/integration/wbiconnect/library/infocenter>

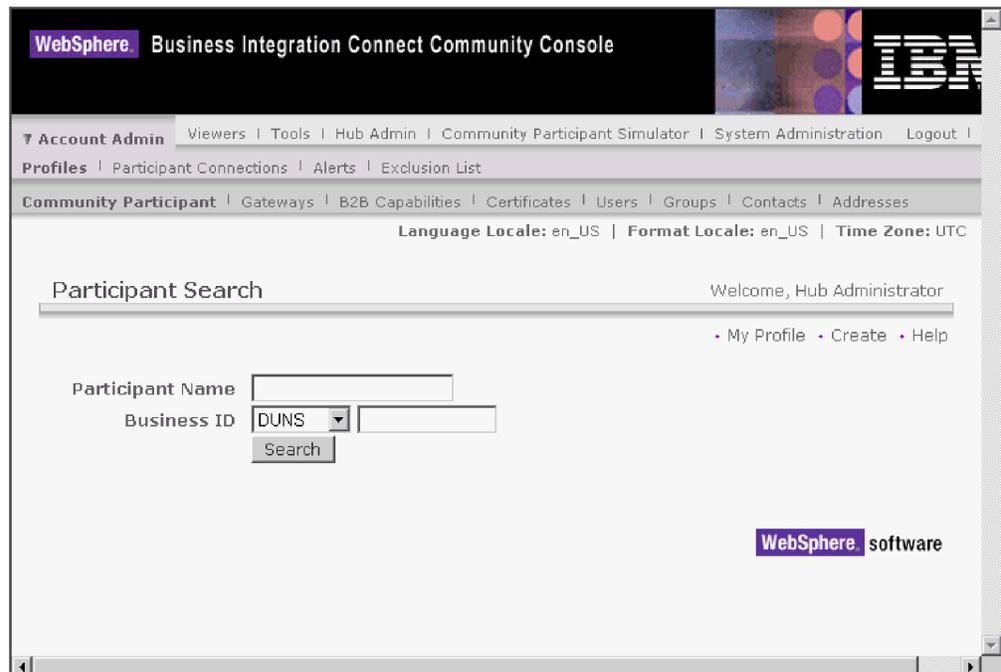
Anmerkung: Wichtige Informationen zu diesem Produkt sind unter Umständen in den technischen Hinweisen und Eilmeldungen der technischen Unterstützung enthalten, die nach Veröffentlichung dieser Dokumentation herausgegeben wurden. Diese können Sie auf der Unterstützungswebsite von WebSphere Business Integration Connect unter der folgenden Adresse finden:

<http://www.ibm.com/software/integration/wbiconnect/support>

Hilfe anfordern

Onlinehilfe

Klicken Sie auf den Link **Hilfe**, um auf die Onlinehilfe zuzugreifen.



Softwareunterstützung

<http://www.ibm.com/software/integration/wbiconnect/support>

Passport Advantage

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

Produktdokumentation

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

Kapitel 1. Einführung

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

Die Zielsetzung lautet, Community Manager zu aktivieren, damit er ein (elektronisches) Dokument an einen Teilnehmer sendet bzw. ein Dokument von einem Teilnehmer empfängt. Der Hub verwaltet den Empfang von Dokumenten, die Konvertierung 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.

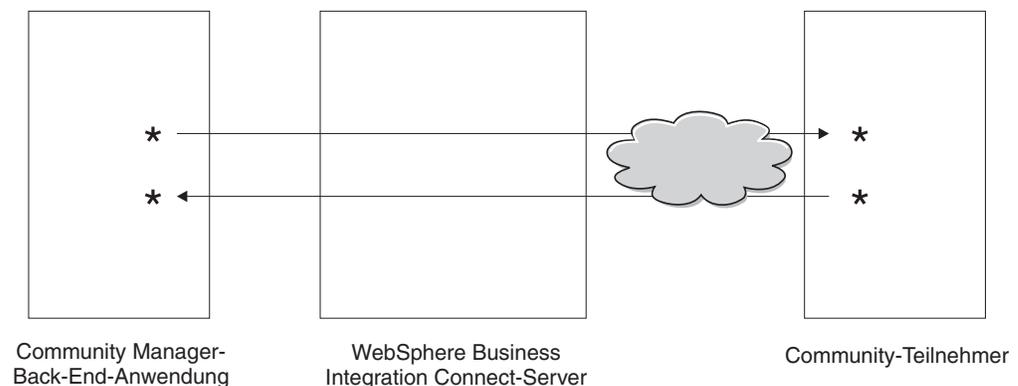


Abbildung 1. Dokumentenfluss durch den Hub

In dieser Dokumentation 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.

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 Transportprotokolltypen (z. B. HTTP oder FTP), die Community Manager und seine Teilnehmer zum Senden der Dokumente verwenden.
- Werden die Dokumente vor ihrer Übermittlung umgesetzt?
- Werden die Dokumente vor ihrer Übermittlung geprüft?
- Werden die Dokumente verschlüsselt oder digital unterzeichnet oder wird eine andere Sicherheitstechnik verwendet?

Wenn Sie diese Informationen zusammengestellt 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.

Übersicht über die Dokumentverarbeitung

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

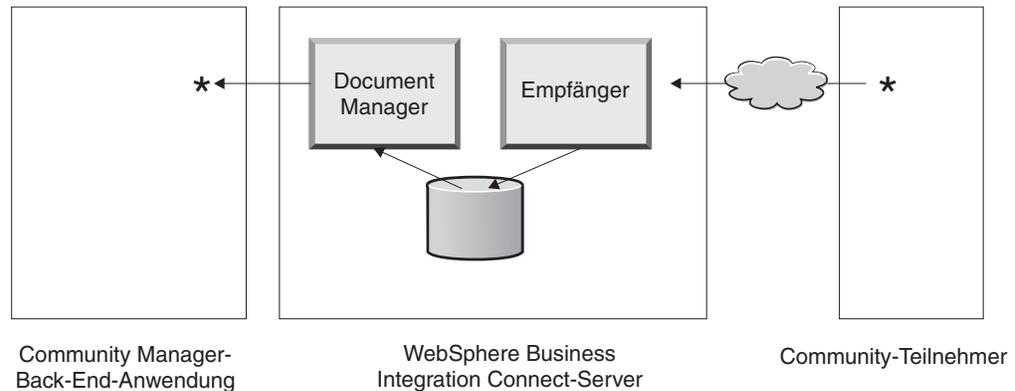


Abbildung 2. Die Komponenten "Empfänger" und "Document Manager"

Diese Abbildung 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.

Ein Dokument wird auf dem WebSphere Business Integration Connect-Server von der Empfängerkomponente empfangen. Der Empfänger schließt transportprotokollspezifische Ziele mit ein. Sie konfigurieren ein Ziel für jeden Transportprotokolltyp, den der Hub unterstützen wird. Wenn Teilnehmer z. B. Dokumente über HTTP senden, konfigurieren Sie ein HTTP-Ziel, um diese zu empfangen. Wie Sie im Abschnitt über Gateways sehen werden, konfigurieren Sie ein Gateway für den Transportprotokolltyp, der zum Senden des Dokuments vom Hub zu Community Manager verwendet wird.

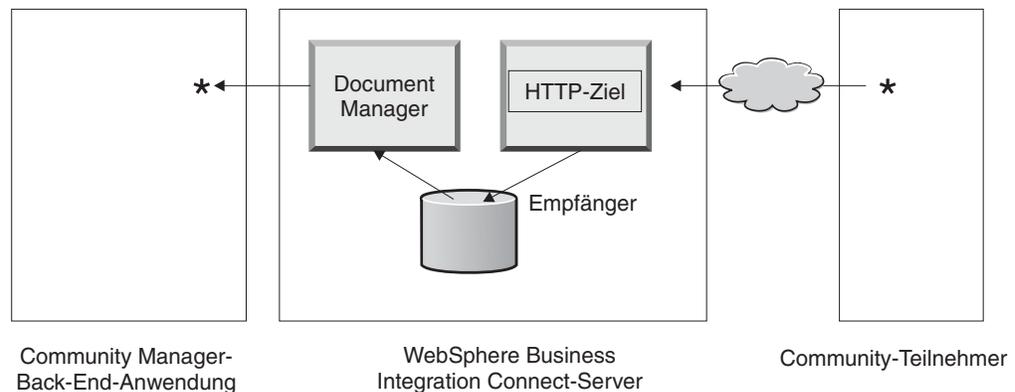


Abbildung 3. Ein HTTP-Ziel

Wenn die Community Manager-Back-End-Anwendung Dokumente über JMS senden wird, konfigurieren Sie ein JMS-Ziel auf dem Hub, um sie zu empfangen. Sie konfigurieren außerdem ein Gateway für den Transportprotokolltyp, der zum Senden des Dokuments vom Hub zum Teilnehmer verwendet wird.

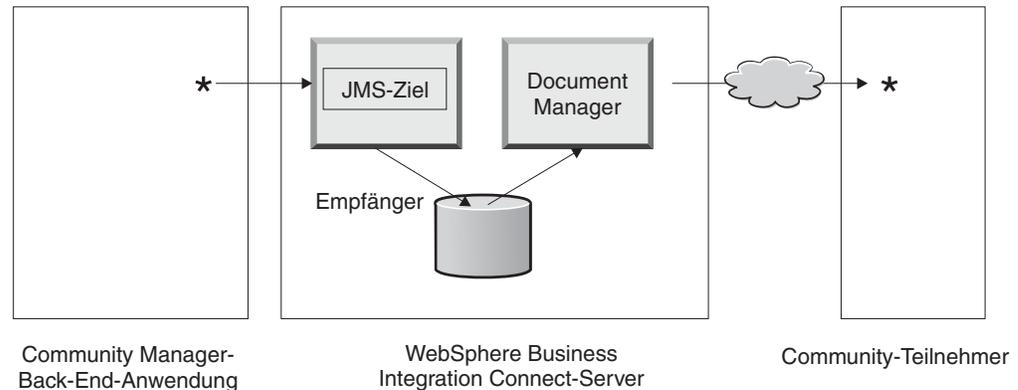


Abbildung 4. Ein JMS-Ziel

WebSphere Business Integration Connect unterstützt eine Vielzahl von Transportprotokollen, aber Sie können auch Ihr eigenes benutzerdefiniertes Transportprotokoll hochladen und es verwenden, wenn Sie ein Ziel definieren (wie in Kapitel 5 beschrieben).

Der Empfänger sendet das Dokument an ein gemeinsam benutztes Dateisystem. Die Document Manager-Komponente empfängt das Dokument vom Dateisystem und legt die Route-Informationen fest und ob eine Konvertierung erforderlich ist. Community Manager könnte z. B. ein EDI-X12-Dokument ohne Paket an den Hub senden, das an einen Teilnehmer gesendet werden soll, der erwartet, dass das EDI-X12-Dokument AS2-Header enthält. Document Manager fügt die Headerdaten hinzu und verwendet dann das Gateway, das für den Teilnehmer definiert wurde, um das Dokument an seinen Bestimmungsort zu senden.

Dokumentverarbeitungs-komponenten mit Handler konfigurieren

Dieser Abschnitt beschreibt detailliert die Komponenten von WebSphere Business Integration Connect und zeigt Ihnen die verschiedenen Punkte auf, an denen Sie das vom System bereitgestellte Verhalten der Komponenten für die Verarbeitung eines Geschäftsdokuments ändern können.

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 Business Integration Connect bereitgestellten Handler und die benutzerdefinierten Handler. Wenn Sie Informationen zur Erstellung von Handlern benötigen, lesen Sie das Handbuch *Programmer Guide*.

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.

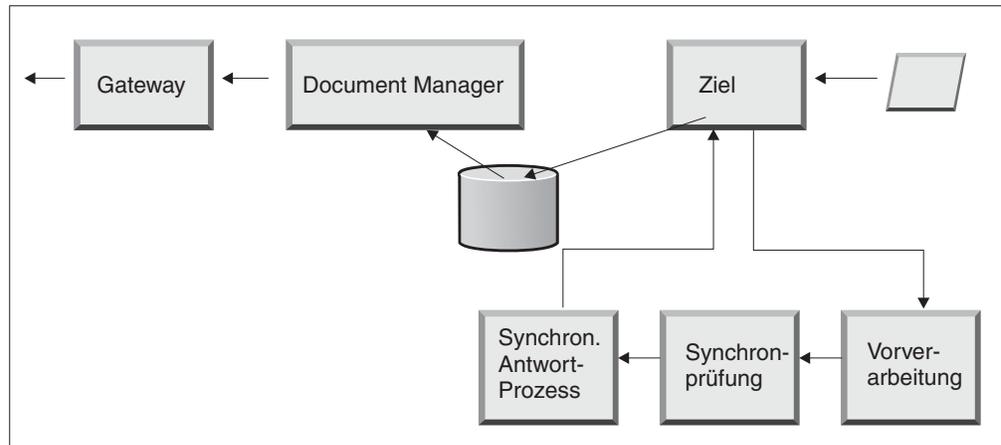


Abbildung 5. Zielkonfigurationspunkte

Die Vorverarbeitung wird im Allgemeinen für jegliche Verarbeitung am Dokument verwendet (z. B. das Splitting des Dokuments), die ausgeführt werden muss, bevor das Dokument an das gemeinsam benutzte Dateisystem gesendet wird.

Mit der Synchronprüfung wird bestimmt, ob das Dokument synchron oder asynchron ist. WebSphere Business Integration Connect stellt die folgenden Handler für die synchrone Überprüfung bereit:

- `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`

Wie Sie der Namenskonvention entnehmen können, sind die ersten vier Handler spezifisch für die vier Transporte, 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.

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

Für das HTTP/S-Transportprotokoll und für benutzerdefinierte Transportprotokolle können Sie Handler hinzufügen, die an den drei, für Ziele verfügbaren Konfigurationspunkten aufgerufen werden sollen. Für AS2-, cXML-, RNIF- und SOAP-Dokumente müssen Sie den Handler für Synchronprüfung angeben. Dies wird in „Konfigurationspunkte modifizieren“ auf Seite 36 beschrieben.

Wenn Sie einen Konfigurationspunkt während der Erstellung eines HTTP/S-Ziels oder eines benutzerdefinierten Ziels auswählen, werden zwei Listen mit Handlern angezeigt: eine **Verfügbarkeitsliste** und eine **Konfigurationsliste**.

Die Konfigurationsliste zeigt alle Handler, die für das Ziel konfiguriert wurden. Die Verfügbarkeitsliste zeigt alle Handler, die für die Konfiguration des Ziels verwendet werden können.

Sie bearbeiten die Handler in der Konfigurationsliste, indem Sie einen Handler hervorheben und die Steuertasten, wie z. B. **Nach oben** oder **Nach unten**, verwenden.

Die folgende Abbildung zeigt die Liste der Handler, die für den Konfigurationspunkt der Synchronprüfung verfügbar sind.

The screenshot displays the 'Target Configuration' window. At the top, there is a 'Gateway Type' dropdown menu set to 'Production', with 'New' and 'Edit' buttons. Below this is a 'URI' input field. The 'Sync Routing' section includes 'Max Sync Timeout' and 'Max Sync Sim Conn' fields. A 'Configuration Point Handlers' dropdown is set to 'syncCheck'. The main area is divided into two lists: 'AvailableList' and 'ConfiguredList'. The 'AvailableList' contains several handler names, including 'com.ibm.bcg.server.sync.As2SyncHdr', 'com.ibm.bcg.server.sync.CxmlSyncHdr', 'com.ibm.bcg.server.sync.RnifSyncHdr', 'com.ibm.bcg.server.sync.SoapSyncHdr', 'com.ibm.bcg.server.sync.DefaultAsynch', and 'com.ibm.bcg.server.sync.DefaultSynchr'. The 'ConfiguredList' is currently empty. To the right of the lists are 'Move Up', 'Move Down', and 'Configure' buttons. Below the lists are 'Add' and 'Remove' buttons, and 'View Details' buttons for each list. At the bottom are 'Save' and 'Cancel' buttons.

Abbildung 6. Die Verfügbarkeitsliste und die Konfigurationsliste

Sie können Ihren eigenen Handler den Handlern hinzufügen, die vom System bereitgestellt wurden, indem Sie einen benutzerdefinierten Zielhandler hochladen. Sie verwenden die Auswahl **Importieren** der Seite **Handlerliste**, um einen benutzerdefinierten Handler hochzuladen.

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

Hub Configuration | Console Configuration

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

Action | **Target** | Gateway | Fixed Workflow

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

HandlersList Welcome, Hub Administrator

• Import • HandlerTypes • Help

	HandlerType	Classname	Provider
 	RECEIVER.SYNCCHECK.HttpS	com.ibm.bcg.server.sync.As2SyncHdlr	Product
 	RECEIVER.SYNCCHECK.HttpS	com.ibm.bcg.server.sync.CxmlSyncHdlr	Product
 	RECEIVER.SYNCCHECK.HttpS	com.ibm.bcg.server.sync.RnifSyncHdlr	Product
 	RECEIVER.SYNCCHECK.HttpS	com.ibm.bcg.server.sync.SoopSyncHdlr	Product
 	RECEIVER.SYNCCHECK.HttpS	com.ibm.bcg.server.sync.DefaultAsynchronousSyncCheckHandler	Product
 	RECEIVER.SYNCCHECK.HttpS	com.ibm.bcg.server.sync.DefaultSynchronousSyncCheckHandler	Product

Legend

 Click to view details

 Where Used

Abbildung 7. Die Handlerliste

Wenn Sie einen benutzerdefinierten Zielhandler hochladen, wird der Handler der **Handlerliste** hinzugefügt. Der Handler wird auch in der **Verfügbarkeitsliste** für den Konfigurationstyp angezeigt, zu dem er gehört.

Sie können Handler von der **Verfügbarkeitsliste** in die **Konfigurationsliste** versetzen, Sie können Handler aus der **Konfigurationsliste** entfernen, oder Sie können die Reihenfolge der Handler erneut anordnen.

Anmerkung: Handler werden in der Reihenfolge aufgerufen, in der sie in der Konfigurationsliste angezeigt werden, der erste Handler ist allerdings nicht immer derjenige, der zum Konfigurieren des Ziels verwendet wird. Hierzu wird der erste *verfügbare* Handler (der erste Handler, der in der Lage ist die Anforderung zu verarbeiten) verwendet. Angenommen, für ein Ziel sind z. B. drei Handler in dieser Reihenfolge konfiguriert: **Handler1**, **Handler2** und **Handler3**. Wenn eine Anforderung für einen Handler abgesetzt wird, ist der erste Handler, der auf die Anforderung antwortet, derjenige, der sie verarbeitet und jeder nachfolgende Handler (in der Konfigurationsliste) wird nicht aufgerufen. Wenn im Beispiel **Handler2** zuerst antwortet, wird **Handler3** nie aufgerufen.

Document Manager

Wenn ein Dokument vom Ziel an das gemeinsam benutzte Dateisystem gesendet wird, wird Document Manager ausgelöst, um dieses Dokument für die Verarbeitung zu berücksichtigen. Jegliche Dokumentverarbeitung, ungeachtet des Pakets, Protokolls und des Dokumentenflusses, bezieht die Verwendung von Schritten für festen Eingangsarbeitsablauf, mindestens einer Aktion (variable Arbeitsablaufschritte) und einen Schritt für festen Ausgangsarbeitsablauf ein.

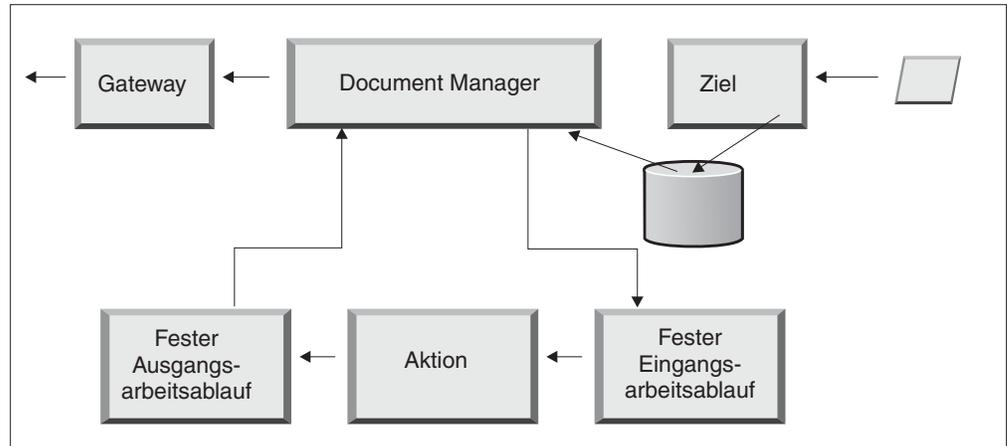


Abbildung 8. Feste Arbeitsabläufe und Aktionen

Fester Eingangsarbeitsablauf

Der feste Eingangsarbeitsablauf setzt sich aus zwei Schritten zusammen, die das Protokoll entpacken und das Dokument auswerten. 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 Business Integration Connect in einfachen Text und extrahieren Informationen, so dass die Aktion für die Nachricht bestimmt werden kann.

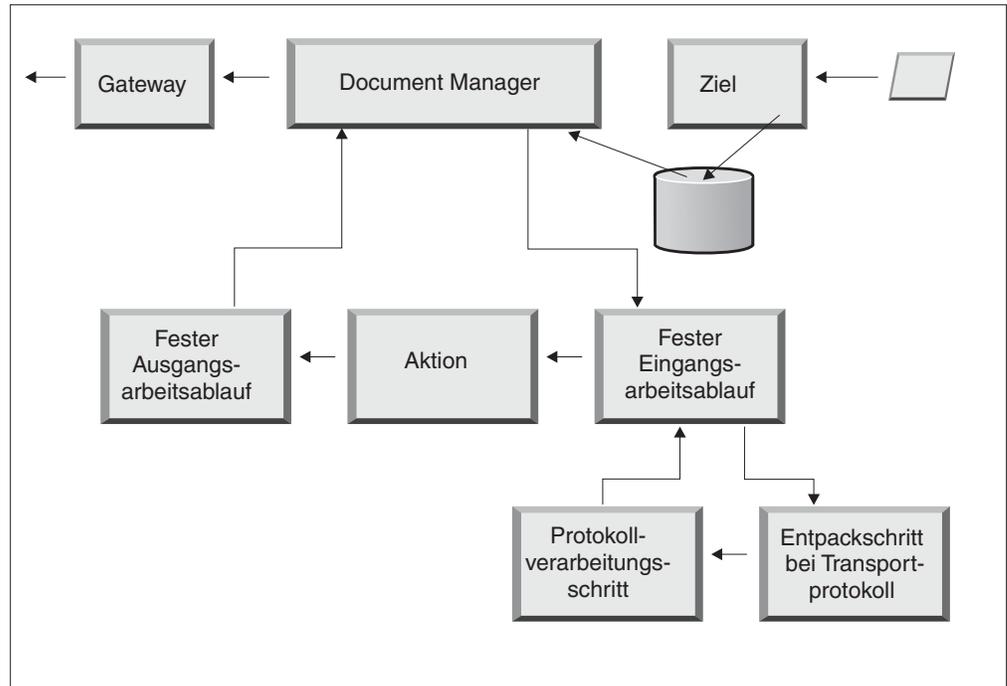


Abbildung 9. Schritte für festen Eingangsarbeitsablauf

Das Geschäftsprotokoll des Dokuments bestimmt, wie die zwei Schritte diese Informationen abrufen. Das Dokument oder die Nachricht muss mindestens die Absender- und die Empfänger-IDs sowie die Dokumentenflussdefinition (Paket, Protokoll und Dokumentenfluss) einschließen.

Sie können den Standardhandler verwenden, der auf das Protokoll für Ihr Dokument angewendet wird, oder Sie können einen anderen Handler für den Schritt für festen Arbeitsablauf angeben.

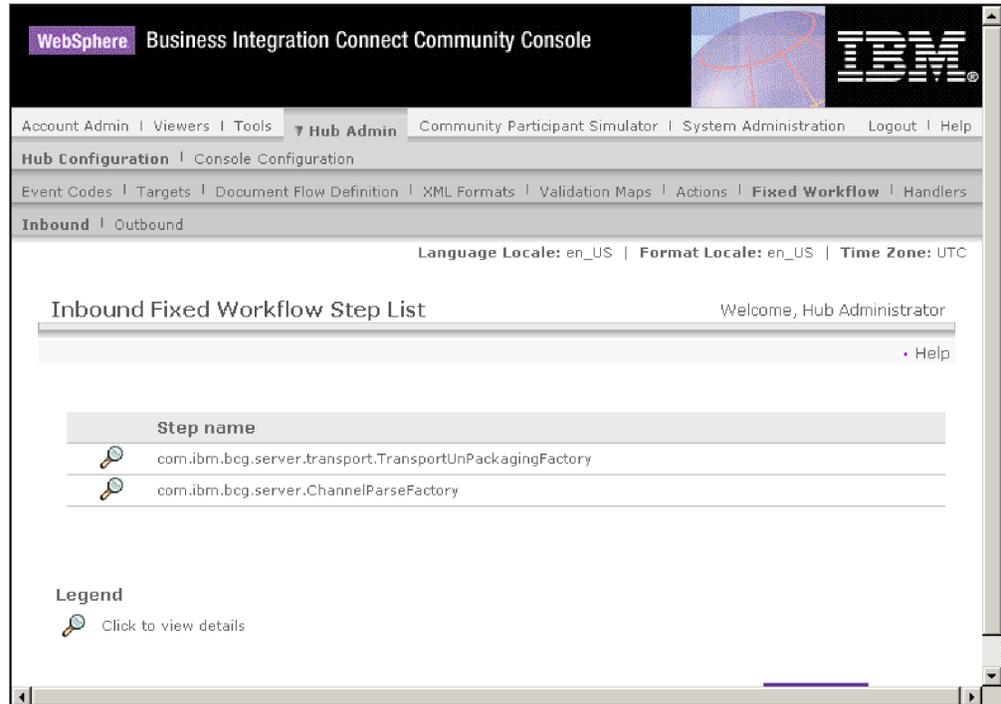


Abbildung 10. Die Schrittliste für festen Eingangsarbeitsablauf

Nachdem Sie auf das Lupensymbol geklickt haben, werden die Handler angezeigt, die Sie für jeden der Schritte für festen Eingangsarbeitsablauf auswählen können:

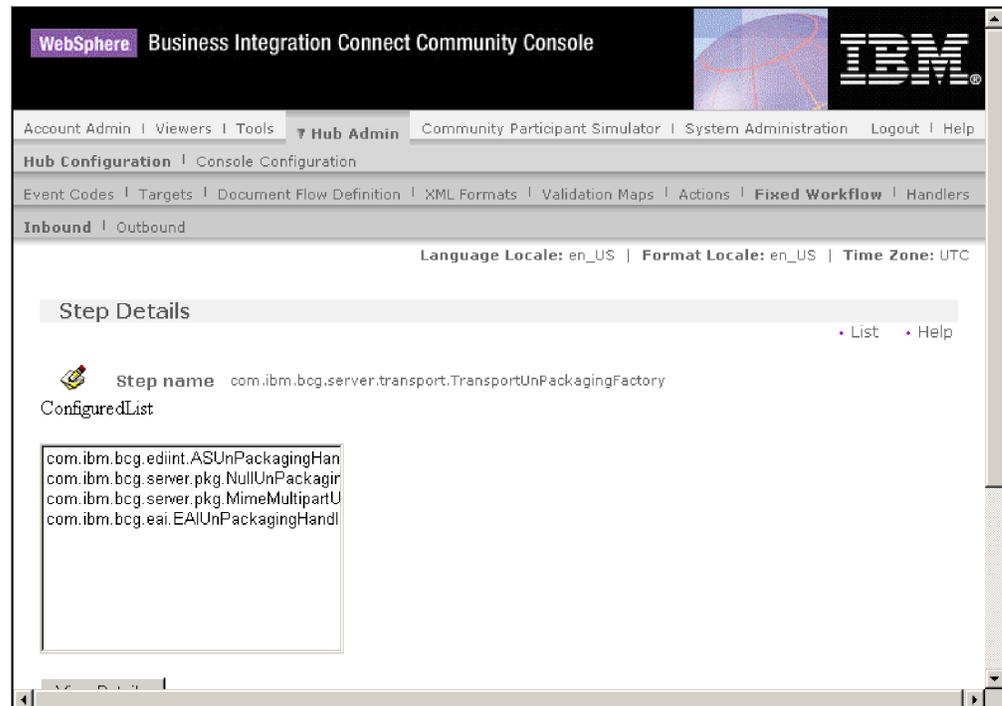


Abbildung 11. Die Seite "Schrittdetails"

Die Schritte für festen Arbeitsablauf, die im System vorkonfiguriert sind, werden in der **Konfigurationsliste** angezeigt. Sie können diese Schritte nicht modifizieren; Sie können aber durch Hinzufügen von Handlern den Schritten Logik hinzufügen.

Um benutzerdefinierte Handler einem Schritt für festen Eingangsarbeitsablauf hinzuzufügen, laden Sie die Datei hoch, die den Handler darstellt. Nachdem die Datei hochgeladen wurde, wird sie in der **Verfügbarkeitsliste** der Handler angezeigt und Sie können sie der **Konfigurationsliste** hinzufügen.

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 Prüfung eines Dokuments, so dass es einer bestimmten Gruppe von Regeln entspricht, und die Konvertierung 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.

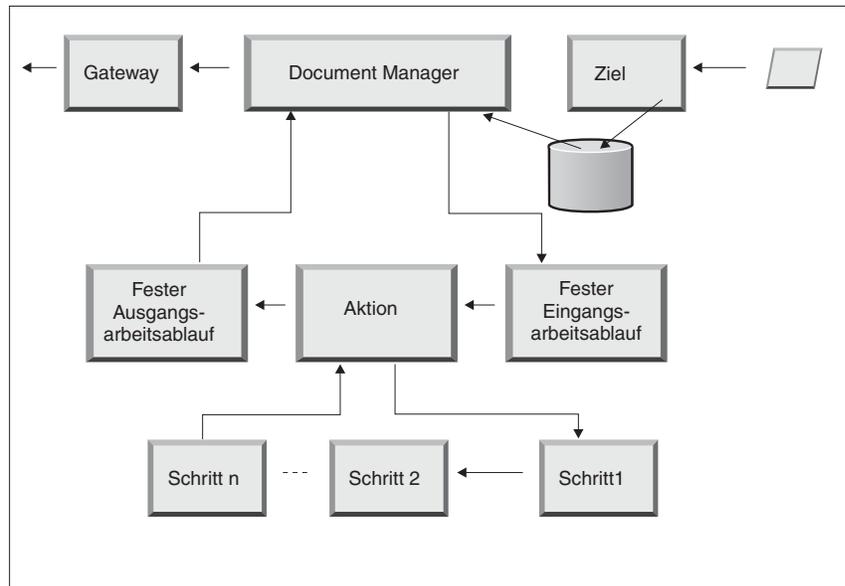


Abbildung 12. Aktionsschritte

Die Art und Weise wie Handler für Aktionen verarbeitet werden, unterscheidet sich von der Art und Weise wie sie für Ziele, Gateways und feste Arbeitsabläufe verarbeitet werden. Für Aktionen werden *alle* Handler aus der Konfigurationsliste aufgerufen und alle werden in der dort angezeigten Reihenfolge verwendet.

Fester Ausgangsarbeitsablauf

Der feste Ausgangsarbeitsablauf besteht aus einem Schritt: dem Packen des Dokuments mit seinen Protokollinformationen. Wenn dieses 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 Headerdaten hinzugefügt, bevor es an das Gateway übermittelt wird.

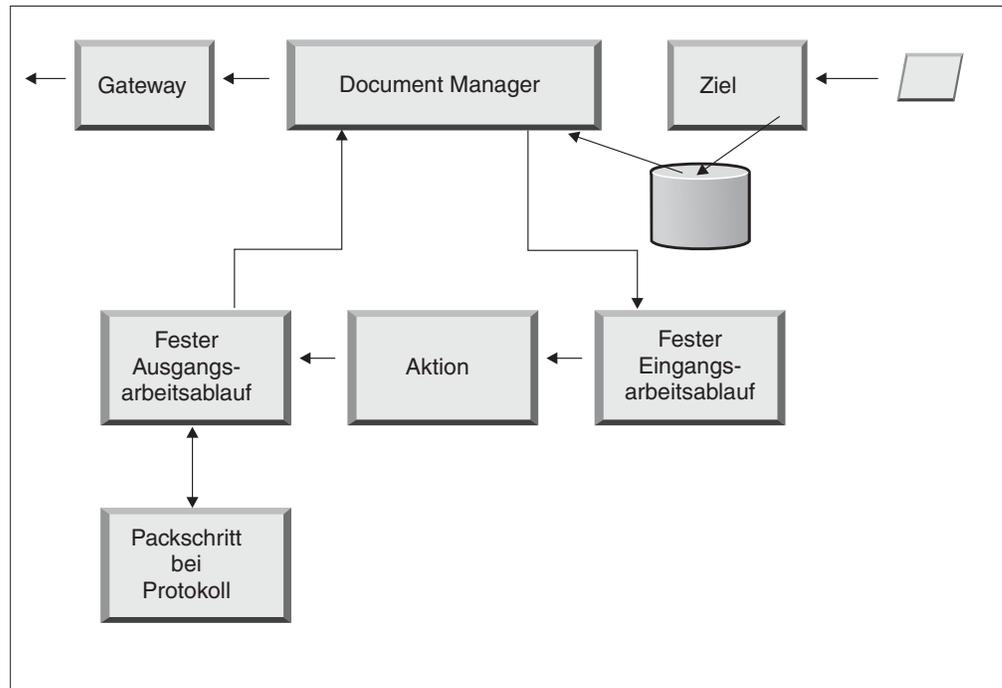


Abbildung 13. Schritte für festen Ausgangsarbeitsablauf

Sie können die vom System bereitgestellten Schritte für Ausgangsarbeitsablauf anzeigen, indem Sie **Hubkonfiguration > Fester Arbeitsablauf > Ausgang** auswählen. Zum Hochladen eines benutzerdefinierten Handlers um ihn der Liste mit den vom System bereitgestellten Handlern hinzuzufügen, wählen Sie **Hubkonfiguration > Handler > Fester Arbeitsablauf** und dann **Importieren** aus, um den benutzerdefinierten Handler hochzuladen.

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.

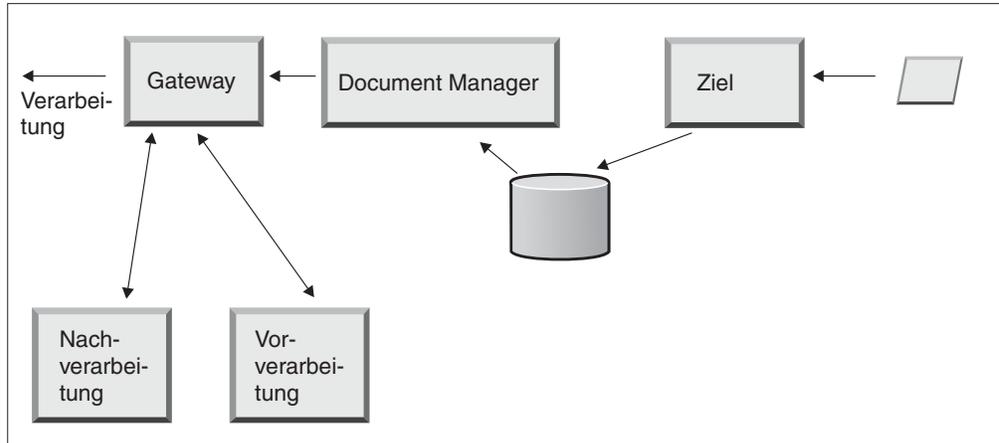


Abbildung 14. Gateway-Konfigurationspunkte

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. Die Nachverarbeitung richtet sich nach den Ergebnissen der Dokumentenübertragung (z. B. nach der Antwort, die es vom Empfänger während einer synchronen Datenübertragung empfängt).

Für die Definition von Konfigurationshandlern für die von WebSphere Business Integration Connect unterstützten Protokolle, wenn Sie ein Gateway definieren, gibt es keine Voraussetzungen (wie es sie bei bestimmten Geschäftsprotokollen gibt, die in synchronen Transaktionen verwendet werden, wenn Sie Ziele definieren).

Wenn Sie Ziele, Gateways und Dokumentenflüsse in den nächsten Abschnitten konfigurieren, werden Sie sehen, wie Sie einen Handler für einen spezifischen Konfigurationspunkt angeben können (oder müssen). Wenn Sie benutzerdefinierte Handler auf die Konfigurationspunkte anwenden, müssen Sie zuerst die Dateien, die diese Handler darstellen, in den Hub hochladen. Dies wird in „Benutzerdefinierte Handler hochladen“ auf Seite 31 beschrieben.

Anmerkung: Handler, die von WebSphere Business Integration Connect bereitgestellt werden, müssen nicht hochgeladen werden.

Kapitel 2. Die Konfiguration des Hubs vorbereiten

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

Dieses Kapitel ist für Personen gedacht, die die folgenden Gateway- oder Zieltypen konfigurieren:

- Ein Dateiverzeichnisgateway
- Ein JMS-Ziel
- Ein FTP-Ziel

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 erstellen“ auf Seite 55 und „FTPS-Gateway erstellen“ auf Seite 58 beschrieben.

Wenn Sie FTP oder FTPS als Transportprotokoll 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 Business Integration Connect installiert.
- Der Benutzer **bcguser** auf der WebSphere Business Integration Connect-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 Business Integration Connect benötigt eine bestimmte Verzeichnisstruktur, so dass die Empfänger- und Document Manager-Komponenten den Teilnehmer, der ein Eingangsdokument sendet, korrekt identifizieren können. Die Struktur sieht wie folgt aus:

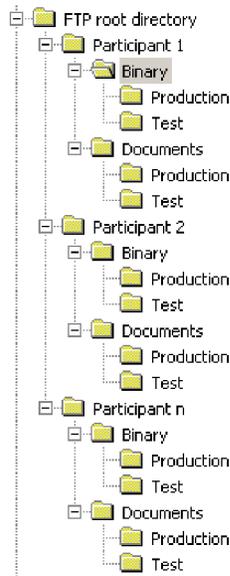


Abbildung 15. FTP-Verzeichnisstruktur

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 die Erstellung einer angepassten XML-Definition erforderlich. Siehe „Angepasstes XML verwalten“ auf Seite 44.

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.
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 Dateinamenstruktur, da die Dateien von Document Manager nicht überprüft werden.

Die Dateinamenstruktur sieht wie folgt aus:

<AnTeilnehmerID><EindeutigerDateiname>

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 Absender (**Von Teilnehmer**) verwendet und der erste Teil des Dateinamens wird zum Auswerten des Namens vom Empfänger (**An Teilnehmer**) 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 **Von Teilnehmer** ist **partnerZwei**, da die Datei im **partnerZwei**-Teil der Verzeichnisbaumstruktur gefunden wurde.
- Der Name in **An Teilnehmer** ist **partnerEins**, da der erste Teil des Dateinamens 123456789 lautet, dies ist die DUNS-ID für **partnerEins**.
- Der Transaktionstyp ist **Produktion**.

Document Manager sucht dann nach einer Teilnehmerverbindung des Typs **Produktion** von **partnerZwei** nach **partnerEins** für **None (N/A)/Binary (1.0)/Binary (1.0)** und verarbeitet die Datei.

XML-Dateien

An eine XML-Datei werden keine Dateinamenanforderungen 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. Der Name des Absenders (**Von Teilnehmer**) und des Empfängers (**An Teilnehmer**) 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.

Anmerkung: Dateien, wie z. B. EDI-Dokumente, wenn sie über FTP empfangen wurden, werden von Document Manager als Binärdateien verarbeitet. Diese Dokumente werden vom WebSphere Business Integration Connect-System als Pass-Through-Dokumente behandelt.

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 Tasks aus:

1. Fügen Sie eine neue Gruppe hinzu (z. B. WBIC).
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 14 erstellt haben. Zusätzliche Informationen finden Sie in der Dokumentation Ihres FTP-Servers.

Sicherheitserwägungen 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 Business Integration Connect bei FTPS-Eingangsdokumenten. WebSphere Business Integration Connect ruft die Dokumente vom FTP-Ziel ab (dies wird in „FTP-Ziel konfigurieren“ auf Seite 34 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.

Den Hub für das JMS-Transportprotokoll konfigurieren

Sie haben WebSphere MQ als Teil der Installation von WebSphere Business Integration Connect installiert. WebSphere MQ enthält eine JMS-Implementierung, mit der Sie eine JMS-Kommunikation konfigurieren können.

WebSphere MQ ist allerdings nicht standardmäßig für JMS konfiguriert. Dieser Abschnitt enthält die Schritte zum Konfigurieren von JMS.

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 modifizieren

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 16 definiert haben. Wenn Sie z. B. das Verzeichnis `c:/temp/JMS` definiert haben, 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-Befehls Umgebung 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(<warteschlangennamen>)
```

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(<warteschlangennamen>)
```

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-Befehls Umgebung zu verlassen:

```
end
```

Ihrer Umgebung eine Java-Laufzeit hinzufügen

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

```
set PATH=%PATH%;<pfad zum installationsverzeichnis>\_jvm\jre\bin
```

Dabei steht *installationsverzeichnis* für das Verzeichnis, in dem WebSphere Business Integration Connect 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(jms)
change ctx(jms)
```

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

```
define qcf(WBICHub)
  tran(CLIENT)
  host(<Ihre_IP-adresse>)
  port(1414)
  chan(java.channel)
  qmgr(<name des warteschlangenmanagers>)
define q(<name>) queue(<warteschlangennamen>) qmgr(<name des warteschlangenmanagers>)
define q(<name>) queue(<warteschlangennamen>) qmgr(<name des warteschlangenmanagers>)
end
```

Das folgende Beispiel stellt eine JMSAdmin-Sitzung dar, mit der die Verbindungs-factory für Warteschlangen als **WBICHub** mit einer IP-Adresse von `sample.ibm.com` definiert wird, wo 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 17 erstellt haben. Beachten Sie, dass die Benutzereingabe an der Eingabeaufforderung `>` erfolgt.

```
InitCtx> define ctx(jms)
InitCtx> change ctx(jms)
InitCtx/jms> define qcf(WBICHub)
  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
```

Kapitel 3. Den Server starten und Community Console anzeigen

In diesem Kapitel erfahren Sie, wie Sie den WebSphere Business Integration-Server starten und Community Console anzeigen.

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:
`runmglsr -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:
`runmglsr -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 Business Integration Connect-Komponenten starten

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

1. Wechseln Sie in das Verzeichnis `\IBM\WBICconnect\console\was\bin`.
2. Geben Sie den folgenden Befehl ein, um die Konsole zu starten:
 - Für Unix-basierte Systeme:
`/startserver server1`
 - Für Windows-basierte Systeme:
`startserver server1`
3. Wird die folgende Nachricht angezeigt:
`Server server1 open for business`

Wechseln Sie in das Verzeichnis `IBM\WBICconnect\receiver\was\bin`.

4. Geben Sie den folgenden Befehl ein, um den Empfänger zu starten:
startserver server1

oder
/startserver server1
5. Wird die folgende Nachricht angezeigt:
Server server1 open for business

Wechseln in das Verzeichnis `\IBM\WBICconnect\router\was\bin`.
6. Geben Sie den folgenden Befehl ein, um Document Manager zu starten:
/startserver server1

oder
startserver server1
7. Wird die folgende Nachricht angezeigt:
Server server1 open for business

Melden Sie sich an Community Console an, wie im nächsten Abschnitt beschrieben.

An Community Console anmelden

Community Console ist der Zugriffspunkt zu WebSphere Business Integration Connect. Für die meisten Tasks, 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. Benutzername: **hubadmin**
 - b. Kennwort: **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. Firmenname: **Operator**

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

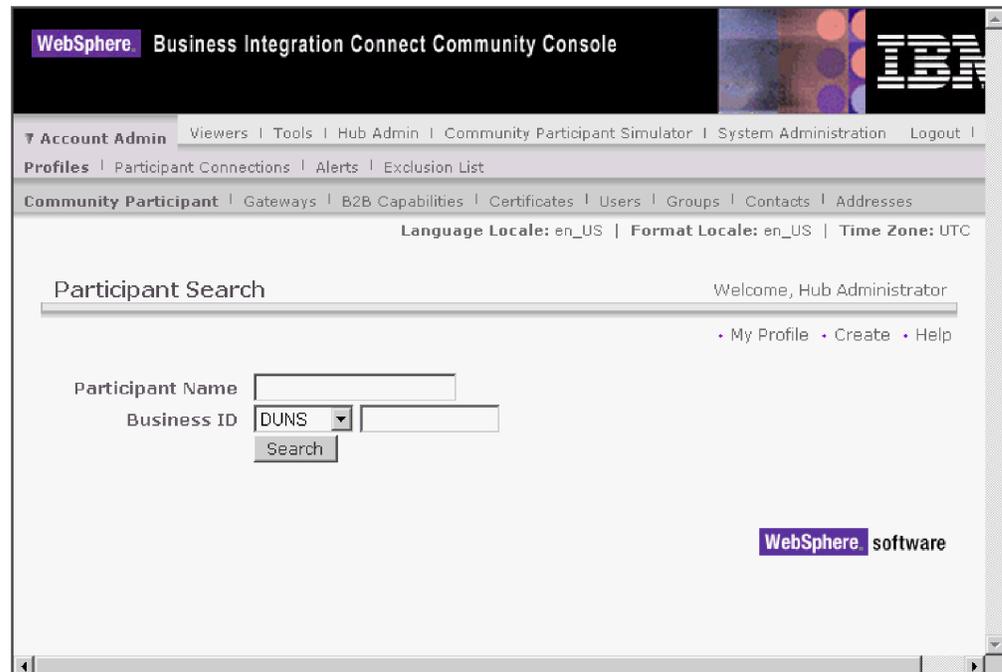


Abbildung 16. Die Seite "Teilnehmersuche"

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 Business Integration Connect 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, so dass Sie steuern können, was Teilnehmer anzeigen und wie sie sich an der Konsole anmelden können und welchen Zugriff sie auf verschiedene Konsoltasks haben. Sie können speziell die folgenden Tasks ausführen:

- Die Standarddarstellung der Konsole ändern (z. B. um ein Firmenlogo auf der Konsole einzufügen)
- Die Kennwortrichtlinie für Teilnehmer festlegen, wenn sie sich an der Konsole anmelden (z. B. wieviele Zeichen eingegeben werden müssen)
- Angeben, welche Elemente der Konsole (z. B. der Dokumentvolumenbericht) für Teilnehmer sichtbar sind

Sie müssen keine dieser Tasks ausführen, wenn Sie die von WebSphere Business Integration Connect bereitgestellten Standardeinstellungen verwenden wollen.

Locale-Informationen und Konsolbranding angeben

Die Seiten von Community Console werden standardmäßig auf Englisch dargestellt. IBM stellt unter Umständen die Übersetzung des Inhalts in anderen Sprachen als eine Gruppe von Dateien zur Verfügung, die hochgeladen werden können. Andere Konsolelemente, die unter Umständen von IBM für weitere Locales zur Verfügung gestellt werden, sind die Logo- und Bannergrafiken, das Style-Sheet, mit dem der Text in den Anzeigen formatiert wird, und die Hilfefunktion.

Sie haben außerdem die Wahl, Ihr eigenes Logo und Banner bereitzustellen, um Community Console anzupassen. Sie führen diese Tasks 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:

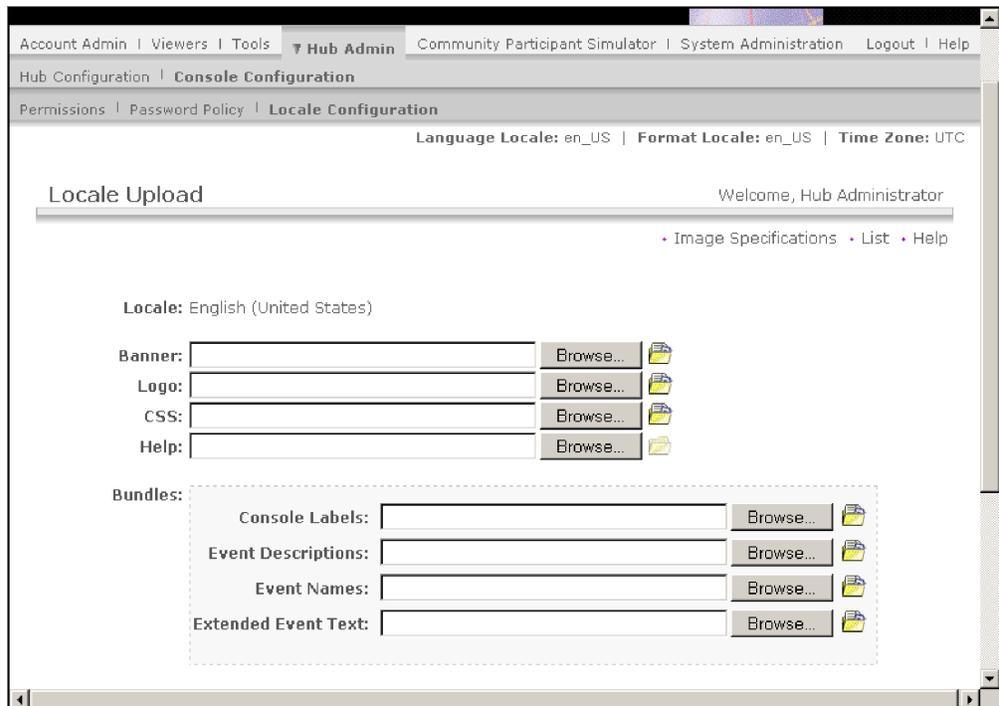


Abbildung 17. Die Seite "Locale hochladen"

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

- Konsolbranding durchführen, indem Sie ein eindeutiges Banner oder Logo (oder beides) hochladen
- Von IBM bereitgestellte Dateien hochladen, so dass Sie den Inhalt der Konsol-elemente 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 Anzeige, 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 Tasks 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.

Die Konsoldaten lokalisieren

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

- Konsolbeschriftungen. Enthalten die Zeichenfolgen, die den gesamten Text der Schnittstelle darstellen
- Ereignisbeschreibungen. Enthalten die Zeichenfolgen zur Anzeige von Ereignisdetails
- Ereignisnamen. Enthalten die Zeichenfolgen, die für Ereignisnamen stehen
- 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 Localdatei hochzuladen:

1. Führen Sie für jedes Ressourcenbündel bzw. jede Datei eine der folgenden Tasks 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 Anzeige **Kennwortrichtlinie** wird angezeigt.

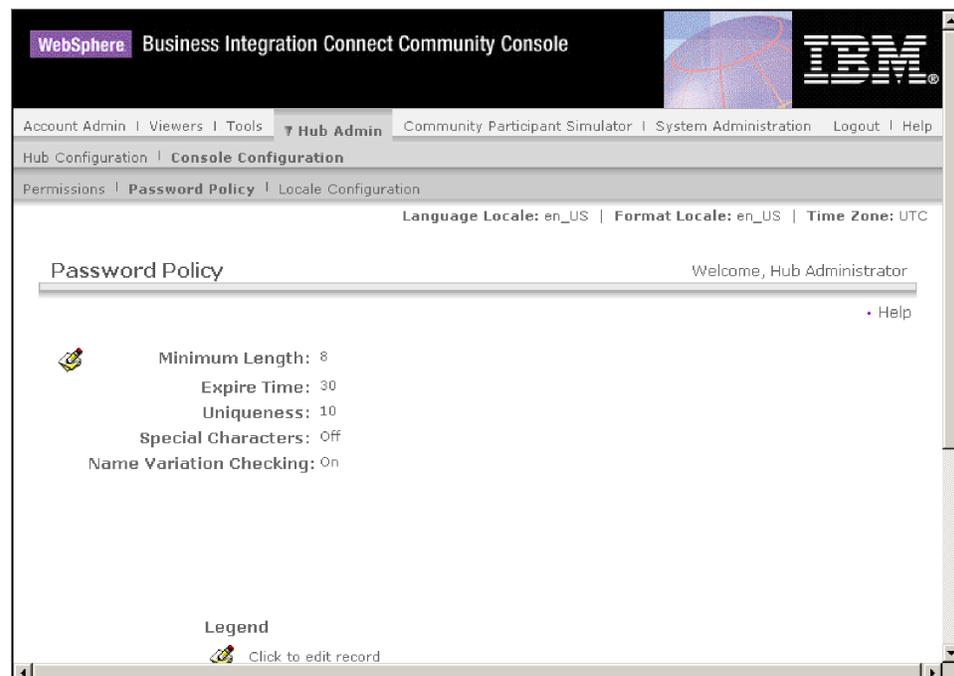


Abbildung 18. Die Seite "Kennwortrichtlinie"

2. Klicken Sie auf das Symbol .
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 „Teilnehmer erstellen“ auf Seite 51 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.

Module Name	No Access	Read Only	Read/Write
Document Viewer	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>
Event Viewer	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>
Document Volume Report	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>
Community Participant	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>
Users	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>
Contacts	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>
Document Analysis	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>
Alerts	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>
Groups	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>
Certificates	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>
RosettaNet Viewer	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>
Gateways	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>
Test Participant Connection	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>
Address	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>
B2B Capabilities	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>

Abbildung 19. Die Seite "Gruppendetails"

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), so dass, selbst wenn Sie eines dieser Module für die Verwendung durch einen Teilnehmer aktivieren, das Modul nicht auf der Seite **Gruppendetails** für den Teilnehmer angezeigt wird.

Berechtigungen aktivieren oder inaktivieren

Sie können über die Anzeige **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.

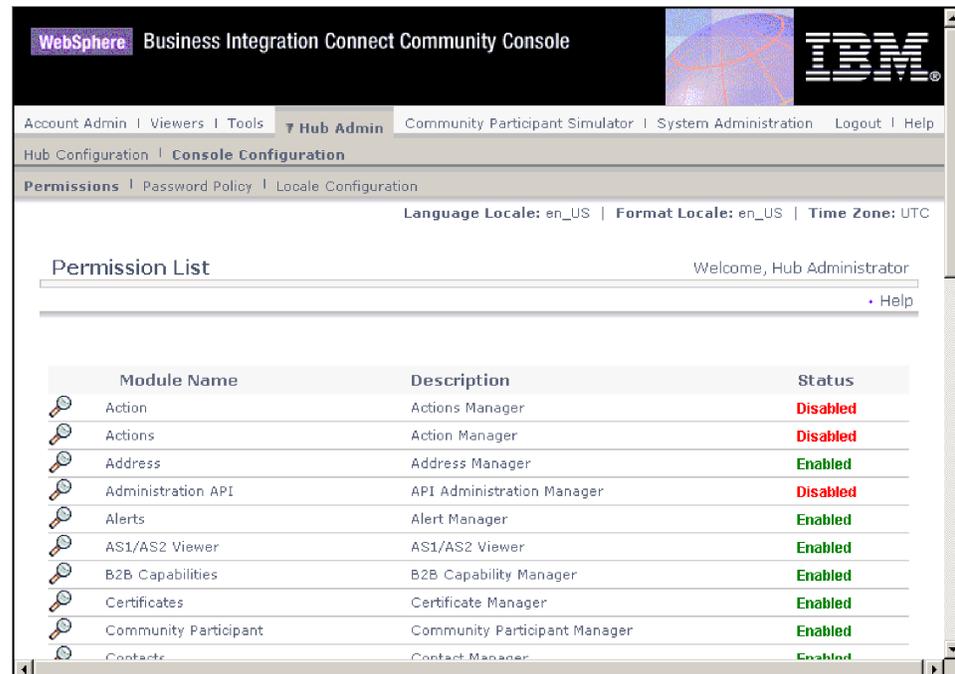


Abbildung 20. Die Seite Berechtigungsliste

2. Zeigen Sie die Standardberechtigungen an, um festzustellen, ob sie für Ihre Hub-Community angemessen sind.
 - Wenn die Standardwerte akzeptabel sind, klicken Sie auf **Abbrechen**.
 - 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 **Ja**.

Kapitel 5. Den Hub konfigurieren

WebSphere Business Integration Connect unterstützt standardmäßig eine Gruppe von Transporten wie auch Paketen (z. B. AS2) und Protokollen (z. B. EDI-X12). Sie können Ihre eigenen (benutzerdefinierten) Transporte für Ziele und Gateways hinzufügen. Darüber hinaus können Sie Handler hochladen, um die Art und Weise zu modifizieren, wie die Komponenten Dokumente verarbeiten.

Benutzerdefinierte 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 Handlerseite hochladen (wie unten beschrieben).

Anmerkung: Wie in Kapitel 1, „Einführung“ erwähnt, laden Sie nur benutzerdefinierte Handler hoch. Die Handler, die von WebSphere Business Integration Connect bereitgestellt wurden, sind bereits verfügbar.

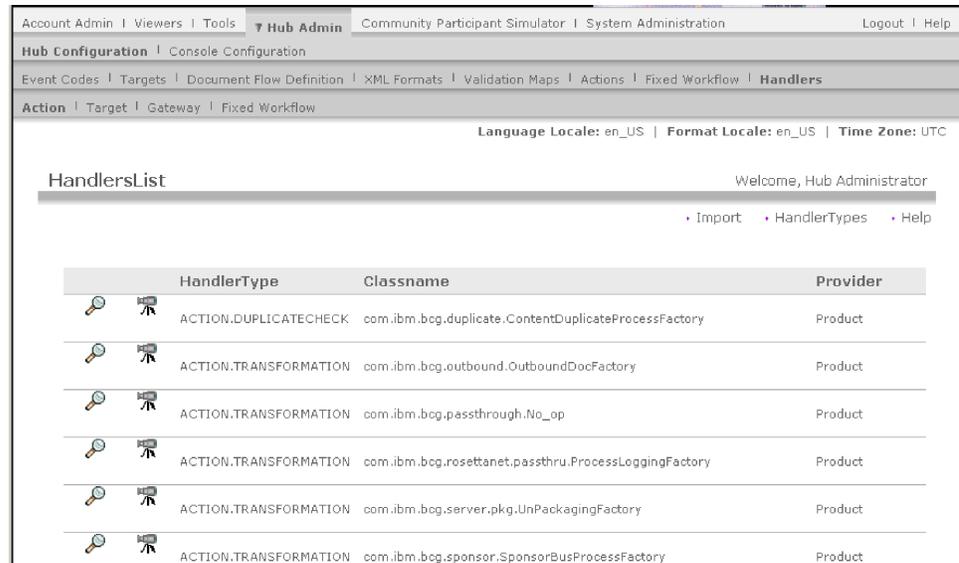
Sie können Dokumentenflüsse modifizieren, indem Sie feste Arbeitsabläufe, Aktionen, Ziele und Gateways modifizieren. Sie modifizieren diese Komponenten durch den Handler, den Sie ihnen zuordnen.

Anmerkung: Sie können die gültigen Handlertypen für Aktionen, Ziele, Gateways und feste Arbeitsabläufe auflisten, indem Sie auf **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 aus. Hier gibt es folgende Typen: **Aktion**, **Ziel**, **Gateway** oder **Fester Arbeitsablauf**.

Die Liste der Handler, die derzeit für die bestimmte Komponente definiert sind, wird angezeigt. Wenn Sie z. B. **Aktion** auswählen, wird die folgende Seite angezeigt:



Beachten Sie, dass die von WebSphere Business Integration Connect bereitgestellten Handler aufgelistet sind. Sie haben die Provider-ID **Produkt**.

3. Klicken Sie auf der Seite **Handlerliste** auf **Importieren**.
4. Geben Sie auf der Seite **Handler importieren** den Pfad zur XML-Datei an, die für den Handler steht, oder verwenden Sie **Durchsuchen**, um nach dieser XML-Datei zu suchen.

Nachdem ein Handler hochgeladen ist, können Sie mit ihm neue Aktionen und Arbeitsabläufe erstellen wie auch die Konfigurationspunkte von Zielen und Gateways anpassen.

Anmerkung: Sie können benutzerdefinierte Handler aktualisieren, indem Sie die modifizierte 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 Business Integration Connect bereitgestellten Handler nicht modifizieren oder löschen.

Ziele konfigurieren

Ziele sind die Positionen auf dem Hub, an denen Dokumente empfangen werden. Diese Dokumente können von Community-Teilnehmern (zur letztendlichen Zustellung zu Community Manager) oder von Community Manager (zur letztendlichen Zustellung zu Teilnehmern) kommen.

Sie konfigurieren mindestens ein Ziel für jeden Transportprotokolltyp, 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.

Diese Abbildung zeigt, wie vier Ziele konfiguriert wurden, um Dokumente zu handhaben, die beim Hub eingehen. Zwei der Ziele sind für Dokumente, die von Teilnehmern gesendet werden, und die anderen zwei Ziele sind für Dokumente, die von Community Manager stammen. (Beachten Sie, dass Sie Transportprotokolle

der Liste mit Transportprotokollen, die standardmäßig von WebSphere Business Integration Connect unterstützt werden, hinzufügen können.)

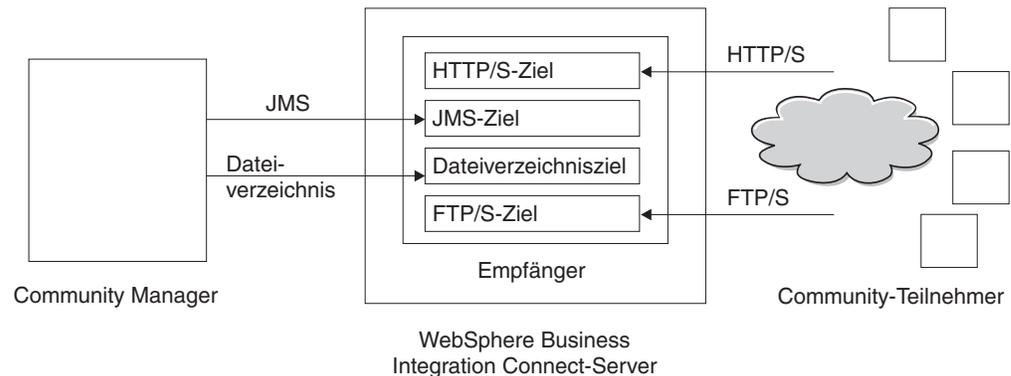


Abbildung 21. Transportprotokolle und zugeordnete Ziele

Führen Sie die folgenden Schritte aus, um Ihre Ziele zu konfigurieren:

1. Klicken Sie auf **Hubadmin > Hubkonfiguration > Ziele**.
2. Wenn Sie ein benutzerdefiniertes Transportprotokoll hochladen wollen, führen Sie die folgenden Schritte aus. Andernfalls fahren Sie mit Schritt 3 fort.
 - a. Klicken Sie auf **Transporttyp importieren**.
 - b. Geben Sie den Namen einer XML-Datei ein, die den Transport definiert oder verwenden Sie **Durchsuchen**, um zur Datei zu navigieren.
 - c. Klicken Sie auf **Hochladen**.

Anmerkung: Sie können über die **Zielliste** auch einen benutzerdefinierten Transportprotokolltyp löschen. Sie können kein Transportprotokoll löschen, das von WebSphere Business Integration Connect bereitgestellt wurde. Ebenfalls können Sie kein benutzerdefiniertes Transportprotokoll löschen, nachdem es zum Erstellen eines Ziels verwendet wurde.

3. Klicken Sie auf **Ziel erstellen**.
4. Geben Sie einen Namen für das Ziel ein. Sie könnten das Ziel z. B. `HttpTarget` nennen. Dies ist ein erforderliches Feld. Der Name, den Sie hier eingeben, wird in der Liste **Ziele** angezeigt.
5. 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.
6. Geben Sie optional eine Beschreibung für das Ziel ein.
7. Wählen Sie einen Transport in der Liste aus. Beachten Sie, dass, wenn Sie einen benutzerdefinierten Transport importieren haben, er in der Liste angezeigt wird.

Die gezeigten Schritte sind für alle Ziele gleich. Nachdem Sie ein Ziel ausgewählt haben, werden jedoch zusätzliche Felder auf der Seite angezeigt. Die Felder variieren, abhängig vom ausgewählten Transport.

Im Folgenden werden die zusätzlichen Schritte aufgeführt, die Sie ausführen, um das Ziel basierend auf seinem Transporttyp zu konfigurieren. Nachdem Sie die transportspezifischen Informationen bereitgestellt haben, um ein benutzerdefiniertes oder ein HTTP/S-Ziel zu definieren, können Sie Konfigurationspunkte für das Ziel modifizieren. Siehe „Konfigurationspunkte modifizieren“ auf Seite 36.

HTTP/S-Ziel konfigurieren

Die Empfängerkomponente verfügt über ein vordefiniertes Servlet `bcgreceiver`, das zum Empfangen von HTTP/S-POST-Nachrichten verwendet wird. Sie erstellen 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. 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.
3. Ändern Sie optional die Synchronroutingwerte:
 - a. Geben Sie für **Max. synchrones Zeitlimit** die Anzahl Millisekunden ein, die eine synchrone Verbindung geöffnet bleibt. Der Standardwert ist 600000.
 - b. Geben Sie für **Max. synchr. simult. Verbindungen** die maximale Anzahl synchroner Verbindungen ein, die das System zulässt. Der Standardwert ist 100 für die maximale Anzahl simultaner synchroner Verbindungen.
4. Wenn Sie die Konfigurationenpunkte modifizieren wollen, oder wenn Sie ein Ziel für ein AS2-, cXML-, RNIF- oder SOAP-Dokument konfigurieren, das in einen synchronen Austausch einbezogen wird, lesen Sie „Konfigurationenpunkte modifizieren“ auf Seite 36.

FTP-Ziel konfigurieren

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

1. Geben Sie in das Feld **FTP-Verzeichnis** das Stammverzeichnis FTP-Servers ein. Informationen zum Konfigurieren des Verzeichnisses für einen FTP-Server finden Sie in „Den FTP-Server für das Empfangen von Dokumenten konfigurieren“ auf Seite 13.
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 abrufen. Der Standardwert ist 3 Sekunden.
3. Geben Sie optional einen Wert für **Threadanzahl** ein, um die Anzahl Dokumente anzugeben, die Document Manager gleichzeitig verarbeitet. 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. Die Standardeinstellung ist, dass keine Dateitypen ausgeschlossen werden.

SMTP-Ziel konfigurieren

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

1. Geben Sie optional den Gateway-Typ an. Die Standardeinstellung ist **Produktion**.
2. Geben Sie die Position des POP3-Servers ein, wohin E-Mails zugestellt werden.

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 **Zeitlimit** ein, um die Anzahl Sekunden anzugeben, die das Ziel den POP3-Server auf Dokumente hin überwacht. Dieses Feld ist optional. Der Standardwert ist 1 ms.
6. Geben Sie optional einen Wert für **Threadanzahl** ein, um die Anzahl Dokumente anzugeben, die Document Manager gleichzeitig verarbeitet. Der Standardwert 1 wird hier empfohlen.
7. Wählen Sie optional die Tageszeit (Stunden und Minuten) aus, wann das SMTP-Ziel den POP3-Server nach Dokumenten abfragen soll.
8. Wählen Sie optional die Wochentage aus, wann die Abfrage erfolgen soll. Die Standardeinstellung ist eine tägliche Abfrage.
9. Wählen Sie optional die Tage im Monat aus, wann die Abfrage erfolgen soll. Die Standardeinstellung ist eine tägliche Abfrage.

JMS-Ziel konfigurieren

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

1. Geben Sie optional den Gateway-Typ an. 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 Bindungs-Datei), als Sie WebSphere Business Integration Connect für JMS konfiguriert haben, wie in „Den Hub für das JMS-Transportprotokoll konfigurieren“ auf Seite 16 beschrieben.
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.
5. Geben Sie einen Wert für den JMS-Factory-Namen ein. Dies ist ein erforderliches Feld.
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 Kapitel 2 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 **WBICHub** in das Feld **JMS-Factory-Name** ein.

Dateisystemziel konfigurieren

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

1. Geben Sie optional den Gateway-Typ an. 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 abrufen. Der Standardwert ist 3 Sekunden.
5. Geben Sie optional einen Wert für **Threadanzahl** ein, um die Anzahl Dokumente anzugeben, die Document Manager gleichzeitig verarbeitet. Der Standardwert 1 wird hier empfohlen.

Konfigurationspunkte modifizieren

Für bestimmte Geschäftsprotokolle (RosettaNet, cXML, SOAP, und AS2), die in synchrone Austauschvorgänge einbezogen werden, müssen Sie einen Handler für den Konfigurationspunkt **Synchronprüfung** angeben. Sie können auch die Art und Weise modifizieren, wie ein HTTP/S- oder benutzerdefiniertes Ziel Dokumente verarbeitet, indem Sie einen hochgeladenen benutzerdefinierten Handler oder einen vom System bereitgestellten Prozess auf andere Konfigurationspunkte des Ziels anwenden.

Um einen benutzerdefinierten Handler auf diese Konfigurationspunkte anzuwenden, müssen Sie zuerst den Handler hochladen, wie in „Benutzerdefinierte Handler hochladen“ auf Seite 31 beschrieben. Sie können auch einen vom System bereitgestellten Handler verwenden, der bereits verfügbar ist und nicht mehr hochgeladen werden muss.

Führen Sie die folgenden Schritte aus, um die Konfigurationspunkte zu modifizieren:

1. Wenn Sie dabei sind, ein Ziel zu erstellen, fahren Sie mit Schritt 2 fort. Wenn Sie eine Zielkonfiguration aktualisieren, klicken Sie auf **Hubadmin > Hubkonfiguration > Ziele**. Klicken Sie dann auf das Lupensymbol neben dem Ziel.

Klicken Sie anschließend auf das Symbol .

2. Wenn Sie einen Handler für synchrone AS2-, cXML-, SOAP- oder RNIF-Transaktionen angeben, führen Sie die folgenden Schritte aus:
 - a. Wählen Sie **SyncCheck** in der Liste **Konfigurationspunkt-Handler** aus.
 - b. Fügen Sie den entsprechenden Handler der **Konfigurationsliste** hinzu, indem Sie den Handler in der **Verfügbarkeitsliste** auswählen und auf **Hinzufügen** klicken.

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.

- Es empfiehlt 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.
- c. Wenn Sie mit dem Definieren der Handler für dieses Ziel fertig sind, klicken Sie auf **Speichern**. Andernfalls fahren Sie mit Schritt 3 fort.
3. Wählen Sie in der Liste **Konfigurationspunkt-Handler** den zu modifizierenden Konfigurationspunkt aus. Die Konfigurationspunkte, die für Ziele modifiziert werden können, sind **Vorverarbeitung** (preprocess), **Synchronprüfung** (sync-Check) und **Nachverarbeitung** (postprocess).

The screenshot shows the 'Target Configuration' window. At the top, 'Gateway Type' is set to 'Production' with 'New' and 'Edit' buttons. Below is the 'URI' field. The 'Sync Routing' section includes 'Max Sync Timeout' and 'Max Sync Sim Conn' fields. The 'Configuration Point Handlers' dropdown is set to 'syncCheck'. Below this are two lists: 'AvailableList' and 'ConfiguredList'. The 'AvailableList' contains several handler classes, including 'com.ibm.bcg.server.sync.As2SyncHdlr'. To the right of the lists are 'Move Up', 'Move Down', and 'Configure' buttons. At the bottom are 'Add', 'Remove', 'View Details', 'Save', and 'Cancel' buttons.

Abbildung 22. Konfigurationspunkt-Handler für Ziele

4. Führen Sie mindestens einen der folgenden Schritte für jeden Handler aus, den Sie modifizieren wollen.
 - a. Fügen Sie einen Handler hinzu, indem Sie den 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 der Handler verwendet wird, 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**.
 - 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.
5. Klicken Sie auf **Speichern**.

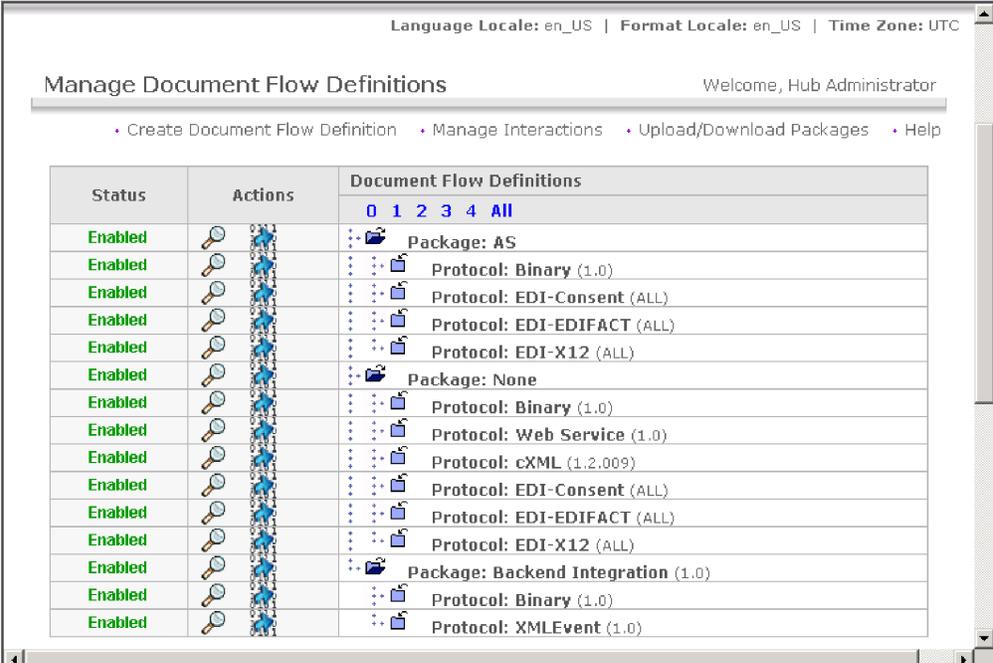
Dokumentenflüsse und Interaktionen definieren

Nachdem Sie alle Ziele erstellt haben, die Sie zum Empfangen der Dokumente von Community-Teilnehmern und Community Manager benötigen, geben Sie als nächsten Schritt die Dokumententypen an, deren Empfang Sie auf dem Hub erwarten. Sie führen dies über die Seite **Dokumentenflussdefinitionen verwalten** aus.

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.

Vom System bereitgestellte Pakete und Protokolle verwenden

Wenn Sie WebSphere Business Integration Connect installieren, wird eine Gruppe von Standardpaketen (AS, None, Backend Integration) auf dieser Seite angezeigt. Alle Standardpakete sind (standardmäßig) zur Verwendung aktiviert. Wenn Sie die Pakete erweitern, dann sehen Sie die Auswahl der Protokolle, die für dieses Paket verwendet werden können.



Status	Actions	Document Flow Definitions
Enabled		0 1 2 3 4 All
Enabled		Package: AS
Enabled		Protocol: Binary (1.0)
Enabled		Protocol: EDI-Consent (ALL)
Enabled		Protocol: EDI-EDIFACT (ALL)
Enabled		Protocol: EDI-X12 (ALL)
Enabled		Package: None
Enabled		Protocol: Binary (1.0)
Enabled		Protocol: Web Service (1.0)
Enabled		Protocol: cXML (1.2.009)
Enabled		Protocol: EDI-Consent (ALL)
Enabled		Protocol: EDI-EDIFACT (ALL)
Enabled		Protocol: EDI-X12 (ALL)
Enabled		Package: Backend Integration (1.0)
Enabled		Protocol: Binary (1.0)
Enabled		Protocol: XMLEvent (1.0)

Abbildung 23. Die Standardpakete

Sie sehen z. B. unter **AS** das Protokoll **EDI-X12**. Wenn Sie **EDI-X12** unter **AS** auswählen, wäre WebSphere Business Integration Connect in der Lage, EDI-X12-Dokumente in AS2-Paketen zu senden und zu empfangen. Wenn Sie **None** und dann **Web Service** auswählen, wäre WebSphere Business Integration Connect in der Lage, einen Web-Service von einem Teilnehmer anzufordern oder einem Teilnehmer einen Web-Service zur Verfügung zu stellen.

Wenn Sie Dokumente mit dem Protokoll **Web Service** senden oder empfangen, müssen Sie die WSDL-Datei hochladen, die dem Web-Service zugeordnet ist, dies wird in „Pakete hochladen“ auf Seite 39 beschrieben. Weitere detaillierte Informationen zur Verwendung von Web-Services finden Sie in Anhang C.

Wenn Ihre Hub-Community nur diese Kombinationen von Paketen und Protokollen verwendet, Web-Services ausgenommen, können Sie mit „Interaktionen erstellen“ auf Seite 48 fortfahren. Wenn Sie jedoch ein Paket oder Protokoll verwenden wollen, das nicht auf der Seite **Dokumentenflussdefinitionen verwalten** bereitgestellt ist, oder wenn Sie Web-Services unterstützen wollen, befolgen Sie die Prozeduren im verbleibenden Teil dieses Abschnitts. Wenn Sie außerdem die Schritte für Eingangs- oder Ausgangsarbeitsablauf modifizieren oder Sie Aktionen modifizieren bzw. erstellen wollen, lesen Sie „Dokumentverarbeitung konfigurieren“ auf Seite 40.

Pakete hochladen

Business Integration Connect bietet die Möglichkeit, vordefinierte RNIF-Dokumentenflussdefinitionen und WSDL-Dateien zu importieren. RNIF-Dokumentenflussdefinitionen werden in ZIP-Archiven, die als Pakete bezeichnet werden, hochgeladen. WSDL-Dateien können einzeln oder zusammen in einem ZIP-Archiv hochgeladen werden. Wenn Sie keine RosettaNet-Dokumente austauschen oder keine Web-Services unterstützen, überspringen Sie diesen Abschnitt, und fahren Sie mit „Dokumentverarbeitung konfigurieren“ auf Seite 40 fort.

WSDL-Pakete hochladen

Dieser Abschnitt beschreibt, wie Sie ein WSDL-Paket hochladen, das einem Web-Service zugeordnet ist. Die vollständigen Informationen zur Verwendung von Web-Services mit WebSphere Business Integration Connect finden Sie in Anhang C.

Führen Sie die folgenden Schritte aus, um ein WSDL-Paket hochzuladen:

1. Klicken Sie auf **Hubadmin > Hubkonfiguration > Dokumentenflussdefinition**.
2. Klicken Sie auf **Pakete hoch-/herunterladen**.

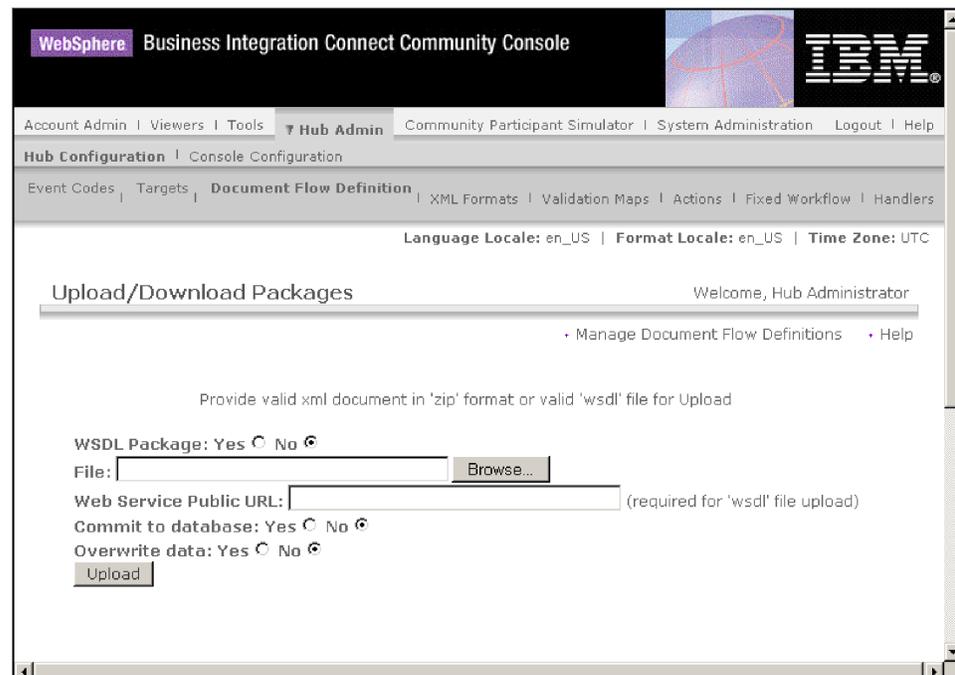


Abbildung 24. Die Seite "Pakete hoch-/herunterladen"

3. Wählen Sie **Ja** für **WSDL-Paket** aus.

4. Geben Sie für **Öffentliche Web-Service-URL-Adresse** die öffentliche URL-Adresse des Web-Services ein, der von Community Manager für den Teilnehmer bzw. vom Teilnehmer für Community Manager zur Verfügung gestellt wird.
 - Geben Sie für einen Web-Service (der von einem Teilnehmer aufgerufen wird), der von Community Manager bereitgestellt wird Folgendes ein:
`http(s)://<ziel host:port>/bcgreceiver/Receiver`
 Die URL-Adresse ist in der Regel dieselbe wie das HTTP-Produktionsziel.
 - Geben Sie für einen Web-Service (der von Community Manager aufgerufen wird), der von einem Teilnehmer bereitgestellt wird, die öffentliche URL des Teilnehmers mit einer Abfragezeichenfolge ein: Beispiel:
`http(s)://<ziel host:port>/bcgreceiver/Receiver?to=<teilnehmergegeschäfts-ID>`
5. Klicken Sie auf **Durchsuchen**, und wählen Sie die WSDL-Datei aus.
6. Stellen Sie sicher, dass **In Datenbank festschreiben** auf **Ja** gesetzt ist.
7. Klicken Sie auf **Hochladen**.
 Die WSDL-Datei wird auf dem System installiert.

RNIF-Pakete hochladen

Dieser Abschnitt beschreibt, wie Sie ein RNIF-Paket hochladen, das zum Senden und Empfangen von RosettaNet-Dokumenten verwendet werden soll. Die vollständigen Informationen zur Verwendung von RosettaNet-Dokumenten mit WebSphere Business Integration Connect finden Sie in Anhang B.

Gehen Sie wie folgt vor, um ein RNIF-Paket 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 aus.

Anmerkung: Die Datei im ZIP-Archiv muss sich in einem Verzeichnis mit dem Namen **Packages** befinden. Beispiel: **Packages/AS1.xml**.

5. Stellen Sie sicher, dass **In Datenbank festschreiben** auf **Ja** gesetzt ist.
6. Klicken Sie auf **Hochladen**.
 Das Paket wird auf dem System installiert.

Dokumentverarbeitung konfigurieren

Wie in Kapitel 1, „Einführung“ beschrieben, können Sie das vom System bereitgestellte Verhalten für die Arbeitsablaufschritte modifizieren, indem Sie den Schritten Handler hinzufügen. Sie können auch die Aktionen modifizieren, die für ein Dokument ausgeführt werden, indem Sie Handler für die Aktion konfigurieren. Sie können ebenfalls neue Aktionen erstellen.

Dieser Abschnitt beschreibt, wie Handler für Arbeitsabläufe hinzugefügt und wie Aktionen konfiguriert und erstellt werden.

Feste Arbeitsabläufe konfigurieren

In Kapitel 1, „Einführung“ wurde beschrieben, dass es zwei Schritte für festen Eingangsarbeitsablauf gibt: einen für das Entpacken eines Protokolls und einen für das syntaktische Analysieren des Protokolls. Für Ausgangsarbeitsabläufe ist ein Schritt für das Packen des Protokolls vorhanden.

WebSphere Business Integration Connect stellt eine Gruppe von Schritten für jeden Arbeitsablauftyp bereit.

Wenn Sie einen benutzerdefinierten Handler verwenden, um einen Arbeitsablaufschrift zu konfigurieren, laden Sie den Handler hoch, wie in „Benutzerdefinierte Handler hochladen“ auf Seite 31 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 Lupensymbol 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.
4. Klicken Sie auf das Bearbeitungssymbol, um die Liste der Handler zu bearbeiten.
5. Führen Sie mindestens einen der folgenden Schritte für jeden Handler aus, den Sie modifizieren wollen.
 - a. Fügen Sie einen Handler hinzu, indem Sie den Handler in der **Verfügbarkeitsliste** auswählen, und klicken Sie auf **Hinzufügen**. (Ein Handler würde in der **Verfügbarkeitsliste** angezeigt werden, wenn Sie einen benutzerdefinierten Handler hochgeladen hätten, oder wenn Sie zuvor einen Handler aus der **Konfigurationsliste** entfernt hätten.) 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.
Denken Sie daran, dass Handler in der Reihenfolge aufgerufen werden, in der sie in der **Konfigurationsliste** aufgelistet werden. Der erste verfügbare Handler, der die Anforderung verarbeiten kann, ist derjenige, der die Anforderung bearbeitet.
 - d. Damit ein Handler mehrfach verarbeitet werden kann, wählen Sie ihn aus, und klicken Sie dann auf **Wiederholen**.
6. Klicken Sie auf **Speichern**.

Aktionen konfigurieren

In Kapitel 1, „Einführung“ wird beschrieben, dass Aktionen aus mindestens einem Schritt bestehen können. WebSphere Business Integration Connect 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 42 beschrieben.

Anmerkung: Sie können die Aktionen nicht modifizieren, die von WebSphere Business Integration Connect bereitgestellt wurden, obwohl Sie eine dieser Aktionen kopieren und modifizieren können, wie in „Aktionen erstellen“ auf Seite 42 beschrieben.

Wenn Sie einen benutzerdefinierten Handler verwenden, um eine Aktion zu konfigurieren, laden Sie den Handler hoch, wie in „Benutzerdefinierte Handler hochladen“ auf Seite 31 beschrieben.

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

1. Klicken Sie auf **Hubadmin > Hubkonfiguration > Aktion**.
2. Klicken Sie auf das Lupensymbol 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 Handler (Aktionsschritt) hinzu, indem Sie den Handler in der **Verfügbarkeitsliste** auswählen, und klicken Sie auf **Hinzufügen**. (Ein Handler würde in der **Verfügbarkeitsliste** angezeigt werden, wenn Sie einen benutzerdefinierten Handler hochgeladen hätten, oder wenn Sie zuvor einen Handler aus der **Konfigurationsliste** entfernt hätten.) 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 Handler, der als Teil der Aktion aufgerufen wird, den Handler hinzu, indem Sie ihn in der **Verfügbarkeitsliste** auswählen und auf

Hinzufügen klicken. (Jeder Aktionshandler, den Sie hochgeladen haben, wird in der **Verfügbarkeitsliste** angezeigt.) 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 daher 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 den 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 Kopiersymbol neben der Aktion, die Sie kopieren wollen.

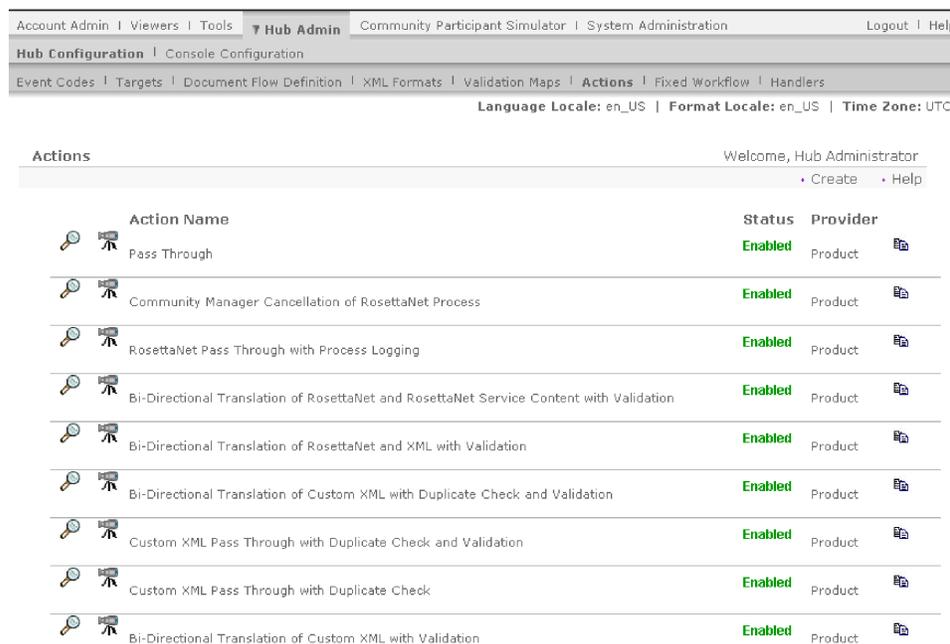


Abbildung 25. Die Seite "Aktionen"

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. Führen Sie mindestens einen der folgenden Schritte für jeden Handler aus, den Sie modifizieren wollen.
 - a. Fügen Sie einen Handler hinzu, indem Sie den Handler in der **Verfügbarkeitsliste** auswählen, und klicken Sie auf **Hinzufügen**. (Ein Handler würde in der **Verfügbarkeitsliste** angezeigt werden, wenn Sie einen benutzerdefinierten Handler hochgeladen hätten, oder wenn Sie zuvor

- einen Handler aus der **Konfigurationsliste** entfernt hätten.) 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. 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 Handler, 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**.

Angepasstes XML verwalten

Führen Sie die Schritte in diesem Abschnitt nur aus, wenn Sie ein angepasstes XML-Format verwenden.

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 95 finden.

Protokolldefinitionsformat CustomXML erstellen

Die folgenden Schritte beschreiben, wie ein angepasstes XML-Protokolldefinitionsformat erstellt wird:

1. Klicken Sie auf **Hubadmin > Dokumentenflussdefinitionen > Dokumentenflussdefinition erstellen**.

Abbildung 26. Die Seite "Dokumentenflussdefinitionen 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 allen drei Paketen 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 > Dokumentenflussdefinitionen > 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 Ordnersymbol, um jedes Paket zu erweitern, das Sie in der vorherigen Prozedur 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**.

Im Folgenden wird ein Beispiel dargestellt, das veranschaulicht, wie der Abschnitt **Paket: AS** der Seite **Dokumentenflussdefinitionen verwalten** aussehen würde, wenn Sie ein Protokoll **CustomXML** erstellt, das Protokoll dem **Paket: AS, None** und **Backend Integration** zugeordnet und einen Dokumentenfluss **XML_Tester** erstellt hätten:

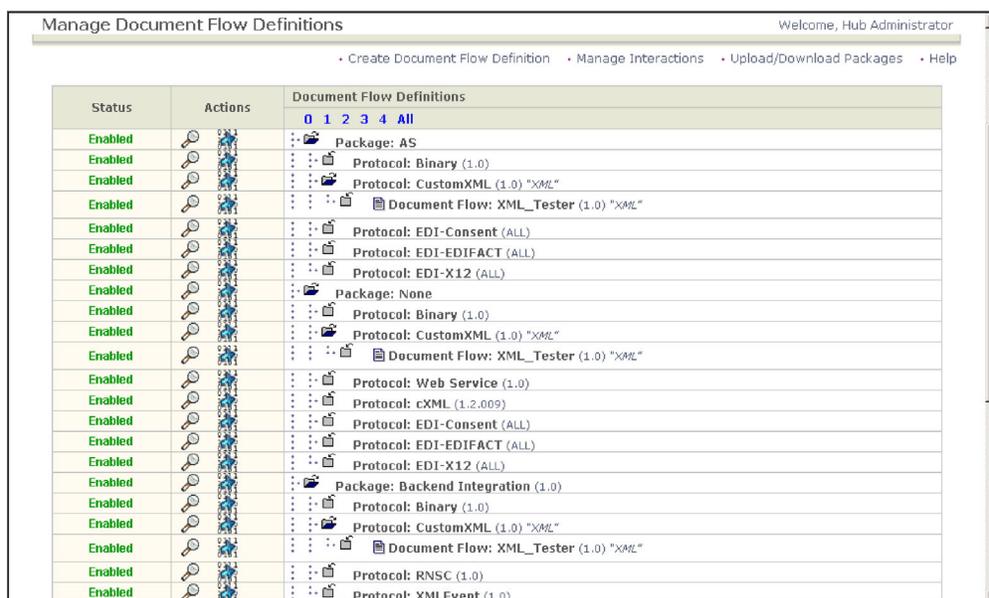


Abbildung 27. Die Seite mit Dokumentenflussdefinitionen, der ein neues Protokoll "CustomXML" sowie ein Dokumentenfluss hinzugefügt wurde

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**.

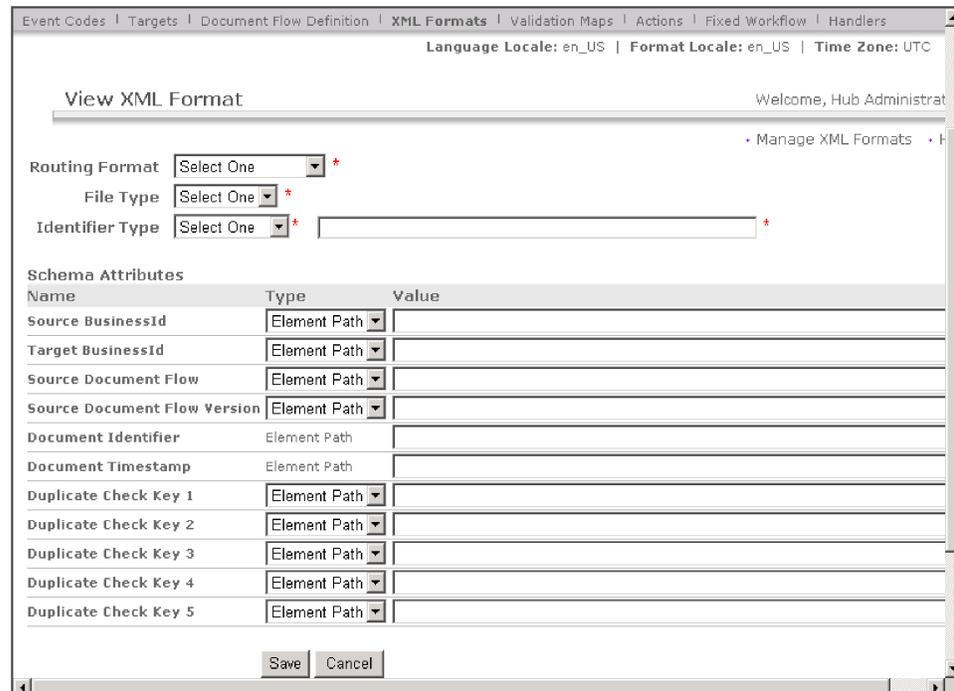


Abbildung 28. Die Seite "XML-Format anzeigen"

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 **Duplikatprüfchlüssel 1-5** die Pfade ein, mit denen die Weiterleitung einer Kopie eines Dokuments angegeben werden.
7. Klicken Sie auf **Speichern**.

Validierungszuordnungen verwenden

WebSphere Business Integration Connect verwendet Validierungszuordnungen, um die Struktur von RosettaNet- oder XML-Dokumenten zu prüfen. Wenn Sie keine Validierungszuordnungen importieren müssen, fahren Sie mit „Interaktionen erstellen“ fort.

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 prüft. Sie prüft 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 Business Integration Connect Dateien lesen kann.
2. Klicken Sie auf **Hubadmin > Hubkonfiguration > Validierungszuordnungen**.
3. Klicken Sie auf **Erstellen**.
4. Geben Sie eine Beschreibung für die Validierungszuordnung ein. Wählen Sie den Pfad und den Namen der Schemadatei aus, mit der Sie Dokumente prüfen wollen.
5. 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 > Validierungszuordnungen**. Die Konsole zeigt die Seite **Validierungszuordnungen verwalten** an.
2. Klicken Sie auf das Lupensymbol neben der Validierungszuordnung, die Sie der Dokumentenflussdefinition zuordnen wollen.
3. Klicken Sie auf das Ordnersymbol, um individuell zur Ebene **Aktion** zu erweitern, oder wählen Sie **Alle** aus, um die gesamte Baumstruktur zu erweitern.
4. Wählen Sie die Dokumentenflussdefinition aus, die Sie der Validierungszuordnung zuordnen wollen.
5. Klicken Sie auf **Übergeben**.

Interaktionen erstellen

Nachdem Sie alle Dokumentenflüsse definiert haben, die Sie auf dem Hub verwenden wollen, erstellen Sie Interaktionen. Interaktionen definieren die möglichen Kombinationen von Dokumentenflüssen, die der Hub unterstützt.

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**.

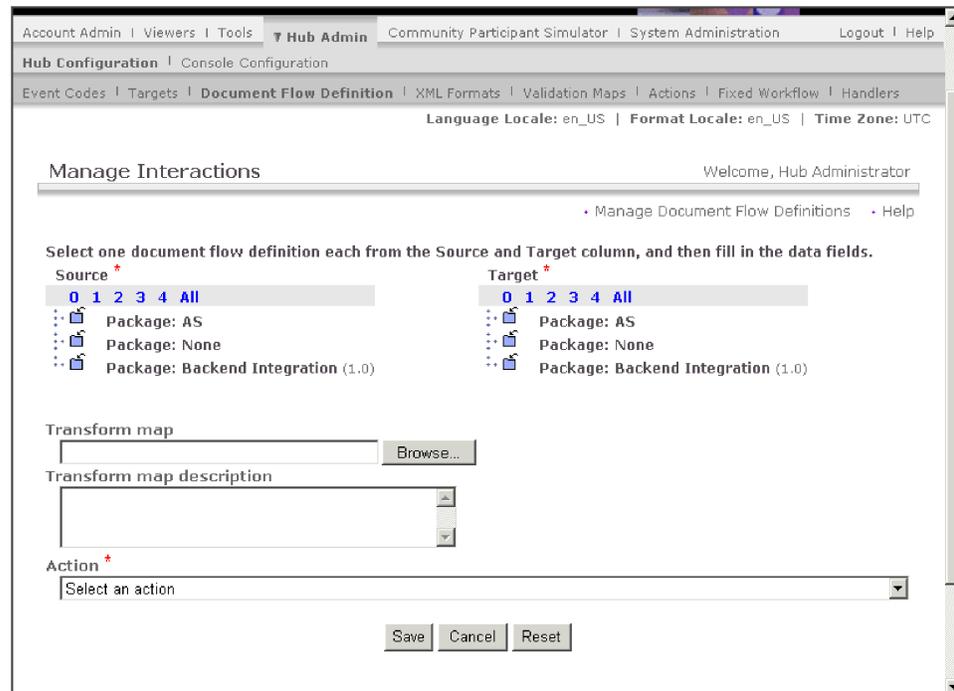


Abbildung 29. Die Seite "Interaktionen verwalten"

Die Seite **Interaktionen verwalten** enthält alle möglichen Kombinationen von Paketen, Protokollen und Dokumentenflüssen, sowohl die vom System bereitgestellt werden als auch die von Ihnen hochgeladen bzw. erstellt wurden.

4. Klicken Sie in der Baumstruktur **Quelle** auf das Ordnersymbol, um einen Knoten individuell zur entsprechenden Ebene **Dokumentenflussdefinition** zu erweitern, oder wählen Sie **Alle** aus, um die gesamte Baumstruktur zu erweitern.
5. Wählen Sie die Dokumentenflussdefinition aus, die Sie als Quelle der Interaktion verwenden wollen.
6. Klicken Sie in der Baumstruktur **Ziel** auf das Ordnersymbol, um einen Knoten individuell zur entsprechenden Ebene **Dokumentenflussdefinition** zu erweitern, oder wählen Sie **Alle** aus, um die gesamte Baumstruktur zu erweitern.
7. Wählen Sie die Dokumentenflussdefinition aus, die Sie als Ziel der Interaktion verwenden wollen.
8. Wenn Sie Daten von einem Protokoll in ein anderes Protokoll umsetzen müssen, geben Sie in das Feld **Transformationszuordnung** den Namen der Transformationszuordnungsdatei ein, oder klicken Sie auf **Durchsuchen**, um zur Datei zu navigieren.
9. Geben Sie optional in das Feld **Beschreibung für Transformationszuordnung** eine Beschreibung ein.
10. Wählen Sie im Feld **Aktion** die Aktion aus, die WebSphere Business Integration Connect in dieser Interaktion ausführen soll. Beachten Sie, dass jede erstellte Aktion aufgelistet wird.
11. Klicken Sie auf **Speichern**.

Zusammenfassung

In diesem Kapitel haben Sie den Hub konfiguriert. Sie sind jetzt soweit, um Teilnehmer zu definieren, die B2B-Funktionalität einzurichten und Verbindungen zwischen Teilnehmern und Community Manager zu definieren. Sie haben gelernt, wie Sie die folgenden Tasks ausführen:

- Ziele für alle Transportprotokolle definieren, durch die Dokumente auf dem Hub ankommen.
- WSDL- oder RNIF-Pakete hochladen, um sie bei Bedarf der Liste der Dokumentenflussdefinitionen hinzuzufügen.
- Die Verarbeitung von Dokumenten anpassen, indem Sie die Schritte für festen Arbeitsablauf und Aktionen konfigurieren oder bei Bedarf Aktionen erstellen.
- Angepasste XML-Formate erstellen, um sie bei Bedarf der Liste der Dokumentenflussdefinitionen hinzuzufügen.
- Konvertierungszuordnungen hochladen und sie bei Bedarf Dokumentenflüssen zuordnen.
- Interaktionen erstellen, um zu bestimmen, welche Kombinationen von Austauschvorgängen möglich sind.

Kapitel 6. Teilnehmer und Teilnehmerverbindungen erstellen

Nachdem Sie den Hub konfiguriert haben, einschließlich dem Einrichten der Ziele sowie dem Definieren der Dokumentenflussdefinitionen und Interaktionen, können Sie nun die Teilnehmer für Ihre Hub-Community erstellen. Nach dem Erstellen der Teilnehmer richten Sie ihre B2B-Funktionalität ein und erstellen dann die Verbindungen zwischen den Teilnehmern und Community Manager.

Teilnehmer erstellen

Zum Erstellen eines Teilnehmers müssen Sie mindestens die folgenden Informationen zu den Teilnehmern 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 (einschließlich Community Manager), 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 den Namen ein, den der Teilnehmer zum Anmelden am Hub verwendet.
4. Geben Sie den Firmennamen oder einen anderen beschreibenden Namen für den Teilnehmer ein.
5. Wählen Sie den Teilnehmertyp aus. Beachten Sie, dass WebSphere Business Integration Connect nur einen Community Manager und nur einen Community Operator unterstützt. Wenn Sie Community Manager konfigurieren, wählen Sie **Community Manager** aus. Andernfalls wählen Sie **Community-Teilnehmer** aus.
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 Business Integration Connect 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- oder EDIFACT-Dokumente sendet und empfängt, verwendet er sowohl DUNS- als auch unformatierte IDs während des Dokumentenaustauschs.

Die unformatierte ID wird durch Einfügen eines Silbentrennungsstrichs (-) zwischen der zweiten und dritten Ziffer der DUNS gebildet. Wenn z. B. 810810810 die DUNS-ID ist, würde die erforderliche unformatierte ID 81-0810810 lauten. Sowohl Community Manager als auch die Teilnehmer, die an diesen Dokumentenflusstypen beteiligt sind, sollten jeweils über eine DUNS-ID und eine unformatierte ID verfügen.

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**.

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.

Gateways für die Teilnehmer konfigurieren

WebSphere Business Integration Connect verwendet Gateways, um Dokumente an ihr ordnungsgemäßes Ziel weiterzuleiten. Das Ausgangstransportprotokoll bestimmt, welche Informationen während der Gateway-Konfiguration verwendet werden.

Die folgenden Transportprotokolle werden (standardmäßig) für Teilnehmergateways unterstützt:

- HTTP/1.1
- HTTPS/1.0
- HTTPS/1.1
- FTP
- FTPS
- JMS
- SMTP
- Dateiverzeichnis

Sie können auch ein benutzerdefiniertes Transportprotokoll angeben, das Sie während der Gateway-Erstellung hochladen.

Als Hubadmin können Sie die Gateways für Ihre Teilnehmer konfigurieren bzw. die Teilnehmer können diese Task selbst ausführen. In diesem Kapitel erfahren Sie, wie Sie diese Task für die Teilnehmer ausführen.

Gateways erstellen

Verwenden Sie die folgende Prozedur, um 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 Lupensymbol, um das Profil des Teilnehmers anzuzeigen.
4. Klicken Sie auf **Gateways**.
5. Klicken Sie auf **Erstellen**. Die Konsole zeigt die Anzeige **Gateway-Details** an.
6. Wenn Sie ein benutzerdefiniertes Transportprotokoll hochladen wollen, führen Sie die folgenden Schritte aus. Andernfalls fahren Sie mit Schritt 7 fort.
 - a. Klicken Sie auf **Transporttyp importieren**.
 - b. Geben Sie den Namen einer XML-Datei ein, die das Transportprotokoll definiert oder verwenden Sie **Durchsuchen**, um zur Datei zu navigieren.
 - c. Klicken Sie auf **Hochladen**.

Anmerkung: Sie können über die **Gateway-Liste** auch einen benutzerdefinierten Transportprotokolltyp löschen. Sie können kein Transportprotokoll löschen, das von WebSphere Business Integration Connect bereitgestellt wurde. Ebenfalls können Sie kein benutzerdefiniertes Transportprotokoll löschen, nachdem es zum Erstellen eines Gateways verwendet wurde.

7. Klicken Sie auf **Erstellen**.
8. Geben Sie einen Namen ein, um das Gateway anzugeben. Dies ist ein erforderliches Feld.
9. 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.
10. Geben Sie optional an, ob das Gateway online oder offline ist. Die Standardeinstellung ist **Online**.
11. Geben Sie optional eine Beschreibung für das Gateway ein.

Die gezeigten Schritte sind für alle Gateways gleich. Nachdem Sie ein Gateway ausgewählt haben, variieren jedoch die Auswahlmöglichkeiten in der Anzeige. Im Folgenden werden die zusätzlichen Schritte aufgeführt, die Sie ausführen, um das Gateway basierend auf seinem Transportprotokolltyp zu konfigurieren.

Beachten Sie, dass, nachdem Sie die transportprotokollspezifischen Informationen bereitgestellt haben, um ein Gateway zu definieren, Sie auch die Konfigurationspunkte für das Gateway modifizieren können.

HTTP-Gateway erstellen

Gehen Sie wie folgt vor, um ein HTTP-Gateway zu erstellen:

1. Geben Sie in das Feld **Ziel-URI** die URI ein, an die das Dokument übermittelt werden soll. Dieses Feld ist erforderlich.
Das Format lautet: `http://<servername>:<optionaler port>/<pfad>`
Beispiel für dieses Format:
`http://anotherwbicserver.ibm.com:57080/bcgreceiver/Receiver`
2. Geben Sie optional einen Benutzernamen und ein Kennwort ein, wenn ein Benutzername und ein Kennwort für den Zugriff auf den HTTPS-Server erforderlich sind.
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. Geben Sie in das Feld **Verbindungszeitlimit** die Anzahl Sekunden ein, die ein Socket ohne Datenverkehr geöffnet bleibt. Der Standardwert ist 120 Sekunden.
9. Wenn Sie den Vorverarbeitungs- oder den Nachverarbeitungsschritt für das Gateway konfigurieren wollen, fahren Sie mit „Konfigurationspunkte für Gateways modifizieren“ auf Seite 59 fort. Ansonsten klicken Sie auf **Speichern**.

HTTPS-Gateway erstellen

Gehen Sie wie folgt vor, um ein HTTPS-Gateway zu erstellen:

1. Geben Sie in das Feld **Ziel-URI** die URI ein, an die das Dokument übermittelt werden soll. Dieses Feld ist erforderlich.
Das Format lautet: `https://<servername>:<optionaler port>/<pfad>`
Beispiel:
`https://anotherwbicserver.ibm.com:57443/bcgreceiver/Receiver`
2. Geben Sie optional einen Benutzernamen und ein Kennwort ein, wenn ein Benutzername und ein Kennwort für den Zugriff auf den HTTPS-Server erforderlich sind.
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 **Client-SSL-Zertifikat prüfen** die Option **Ja** aus, wenn Sie wollen, dass das digitale Zertifikat des sendenden Partners mit der dem Dokument zugeordneten DUNS-Nummer geprüft wird. 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. Wenn Sie den Vorverarbeitungs- oder den Nachverarbeitungsschritt für das Gateway konfigurieren wollen, fahren Sie mit „Konfigurationspunkte für Gateways modifizieren“ auf Seite 59 fort. Ansonsten klicken Sie auf **Speichern**.

FTP-Gateway erstellen

Gehen Sie wie folgt vor, um ein FTP-Gateway zu erstellen:

1. Geben Sie in das Feld **Ziel-URI** die URI ein, an die das Dokument übermittelt 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.
2. Geben Sie optional einen Benutzernamen und ein Kennwort ein, wenn ein Benutzername und ein Kennwort für den Zugriff auf den FTP-Server erforderlich sind.
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. Geben Sie in das Feld **Verbindungszeitlimit** die Anzahl Sekunden ein, die ein Socket ohne Datenverkehr geöffnet bleibt. Der Standardwert ist 120 Sekunden.
9. Wenn Sie den Vorverarbeitungs- oder den Nachverarbeitungsschritt für das Gateway konfigurieren wollen, fahren Sie mit „Konfigurationspunkte für Gateways modifizieren“ auf Seite 59 fort. Ansonsten klicken Sie auf **Speichern**.

SMTP-Gateway erstellen

Gehen Sie wie folgt vor, um ein SMTP-Gateway zu erstellen:

1. Geben Sie in das Feld **Ziel-URI** die URI ein, an die das Dokument übermittelt werden soll. Dieses Feld ist erforderlich.
Das Format lautet: mailto:<benutzer@servername>
Beispiel:
mailto:admin@anotherwbicserver.ibm.com
2. Geben Sie optional einen Benutzernamen und ein Kennwort ein, wenn ein Benutzername und ein Kennwort für den Zugriff auf den SMTP-Server erforderlich sind.

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. Geben Sie im Feld **Authentifizierung erforderlich** an, ob ein Benutzername und ein Kennwort mit dem Dokument bereitgestellt werden. Die Standardeinstellung ist **Nein**.
9. Geben Sie in das Feld **Verbindungszeitlimit** die Anzahl Sekunden ein, die ein Socket ohne Datenverkehr geöffnet bleibt. Der Standardwert ist 120 Sekunden.
10. Wenn Sie den Vorverarbeitungs- oder den Nachverarbeitungsschritt für das Gateway konfigurieren wollen, fahren Sie mit „Konfigurationspunkte für Gateways modifizieren“ auf Seite 59 fort. Ansonsten klicken Sie auf **Speichern**.

JMS-Gateway erstellen

Gehen Sie wie folgt vor, um ein JMS-Gateway zu erstellen:

1. Geben Sie in das Feld **Ziel-URI** die URI ein, an die das Dokument übermittelt 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 Business Integration Connect an, wie das Dokument an sein beabsichtigtes Ziel weitergeleitet wird.

Für Teilnehmergateways stellt der Teilnehmer wahrscheinlich die ".bindings"-Datei bereit. Interne JMS-Gateways (das ist das Community Manager-Gateway) können mit JMSAdmin erstellt werden, wie in Kapitel 2, „Die Konfiguration des Hubs vorbereiten“ beschrieben.

Dieses Feld ist erforderlich.

2. Geben Sie optional einen Benutzernamen und ein Kennwort ein, wenn ein Benutzername und ein Kennwort für den Zugriff auf die JMS-Warteschlange erforderlich sind.
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. Geben Sie im Feld **Authentifizierung erforderlich** an, ob ein Benutzername und ein Kennwort mit dem Dokument bereitgestellt werden. Die Standardeinstellung ist **Nein**.
9. 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.
10. 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.
11. Geben Sie in das Feld **JMS-Nachrichtentyp** den Nachrichtentyp ein. Dies ist ein optionales Feld.
12. 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.
13. Geben Sie in das Feld **JMS-Warteschlangenname** den Namen der JMS-Warteschlange ein, an die Dokumente gesendet werden. Dieses Feld ist erforderlich.
14. 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 Kapitel 2, „Die Konfiguration des Hubs vorbereiten“ beschrieben, einrichten.
15. Geben Sie in das Feld **Verbindungszeitlimit** die Anzahl Sekunden ein, die ein Socket ohne Datenverkehr geöffnet bleibt. Der Standardwert ist 120 Sekunden.
16. Wenn Sie den Vorverarbeitungs- oder den Nachverarbeitungsschritt für das Gateway konfigurieren wollen, fahren Sie mit „Konfigurationspunkte für Gateways modifizieren“ auf Seite 59 fort. Ansonsten klicken Sie auf **Speichern**.

Dateiverzeichnisgateway erstellen

Gehen Sie wie folgt vor, um ein Dateiverzeichnisgateway zu erstellen:

1. Geben Sie in das Feld **Ziel-URI** die URI ein, an die das Dokument übermittelt 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 Business Integration Connect-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 Business Integration Connect befindet, lautet das Format: file:///<laufwerkbuchstabe>:/<pfad>

2. 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.
3. 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.
4. Geben Sie in das Feld **Anzahl Threads** die Anzahl Dokumente ein, die gleichzeitig verarbeitet werden sollen. Der Standardwert ist 3.
5. 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**.
6. 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.
7. Wenn Sie den Vorverarbeitungs- oder den Nachverarbeitungsschritt für das Gateway konfigurieren wollen, fahren Sie mit „Konfigurationspunkte für Gateways modifizieren“ auf Seite 59 fort. Ansonsten klicken Sie auf **Speichern**.

FTPS-Gateway erstellen

Gehen Sie wie folgt vor, um ein FTPS-Gateway zu erstellen:

1. Geben Sie in das Feld **Ziel-URI** die URI ein, an die das Dokument übermittelt 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.
2. Geben Sie optional einen Benutzernamen und ein Kennwort ein, wenn ein Benutzername und ein Kennwort für den Zugriff auf den FTPS-Server erforderlich sind.
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. Wenn Sie den Vorverarbeitungs- oder den Nachverarbeitungsschritt für das Gateway konfigurieren wollen, fahren Sie mit „Konfigurationspunkte für Gateways modifizieren“ fort. Ansonsten klicken Sie auf **Speichern**.

Anmerkung: Damit ein FTPS-Ausgangsgateway ordnungsgemäß arbeitet, müssen Sie mindestens das CA-Zertifikat des FTPS-Servers als Stammzertifikat in das Profil des Hub-Operators geladen haben. (Sie verwenden die Optionen **Kontenadmin** > **Profil** > **Zertifikate**, um ein Zertifikat zu laden.) Wenn Sie dieses Zertifikat laden, wird WebSphere Business Integration Connection das Zertifikat des FTPS-Servers anerkennen.

Wenn der FTPS-Server noch eine Clientauthentifizierung erfordert, müssen Sie ein Clientzertifikat als ein SSL-Zertifikat in das Profil des Hub-Operators geladen haben. WebSphere Business Integration Connect stellt dieses Zertifikat für den FTPS-Server bereit. Der FTPS-Server des Teilnehmers muss so konfiguriert sein, dass er Ihr Zertifikat anerkennt.

Weitere Informationen zur Sicherheit finden Sie in Kapitel 7, „Sicherheit für Eingangs- und Austauschvorgänge konfigurieren“.

Konfigurationspunkte für Gateways modifizieren

Wie in Kapitel 1, „Einführung“ beschrieben, können Sie zwei Verarbeitungspunkte für ein Gateway modifizieren: die Vorverarbeitung und die Nachverarbeitung.

Um einen benutzerdefinierten Handler auf diese Konfigurationspunkte anzuwenden, müssen Sie zuerst den Handler hochladen, wie in „Benutzerdefinierte Handler hochladen“ auf Seite 31 beschrieben. Sie können auch einen vom System bereitgestellten Handler verwenden, der bereits verfügbar ist und nicht mehr hochgeladen werden muss.

Gehen Sie wie folgt vor, um einen Konfigurationspunkt zu modifizieren:

1. Wenn Sie dabei sind, ein Gateway zu erstellen, fahren Sie mit Schritt 6 fort. Wenn Sie eine Gateway-Konfiguration aktualisieren, 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 Lupensymbol, um das Profil des Teilnehmers anzuzeigen.
4. Klicken Sie auf **Gateways**.
5. Klicken Sie auf das Lupensymbol, um das Gateway anzuzeigen, und klicken Sie dann auf das Bearbeitungssymbol, um das Gateway zu bearbeiten.
6. Wählen Sie in der Liste **Konfigurationspunkt-Handler** den zu modifizierenden Konfigurationspunkt aus. Die Konfigurationspunkte, die für Gateways modifiziert werden können, sind **preprocess** (Vorverarbeitung) und **postprocess** (Nachverarbeitung).

7. Führen Sie mindestens einen der folgenden Schritte für jeden Handler aus, den Sie modifizieren wollen.
 - a. Fügen Sie einen Handler hinzu, indem Sie den Handler in der **Verfügbarkeitsliste** auswählen, und klicken Sie auf **Hinzufügen**. Der Handler wird in die **Konfigurationsliste** versetzt.

Anmerkung: WebSphere Business Integration Connect stellt keine Standard-gateway-Handler bereit. In der **Verfügbarkeitsliste** werden nur die Handler angezeigt, die Sie hochgeladen haben.
 - 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 der Handler verwendet wird, indem Sie den Handler auswählen und auf **Nach oben** oder **Nach unten** klicken.
 - d. 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.
8. Klicken Sie auf **Speichern**.

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 Task selbst ausführen. In diesem Kapitel erfahren Sie, wie Sie diese Task 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 Lupensymbol, um das Profil des Teilnehmers anzuzeigen.
4. Klicken Sie auf **B2B-Funktionalität**. Die Anzeige **B2B-Funktionalität** wird angezeigt. Die rechte Seite der Anzeige zeigt die Pakete, Protokolle und Geschäftsprozesse an, die vom System als Dokumentenflussdefinitionen unterstützt werden.

Profile > ABC Company > B2B Capabilities

Welcome, Hub Administrator

Help

Set Source	Set Target	Enabled	Edit	Document Flow Definition							
				0	1	2	3	4	All		
		<input type="checkbox"/>		<input type="checkbox"/>	Package: AS						
		<input type="checkbox"/>		<input type="checkbox"/>	Package: None						
		<input type="checkbox"/>		<input type="checkbox"/>	Package: Backend Integration (1.0)						
		<input type="checkbox"/>		<input type="checkbox"/>	Package: RNIF (V02.00)						

Legend

- Edit attributes
- Tree is expanded; click to collapse.
- Tree is collapsed; click to expand.
- Role is active; click to deactivate.
- Role is not active; click to create role.
- Role is inactive; cannot activate while the capability is disabled.

Abbildung 30. Die Seite "B2B-Funktionalität"

5. Klicken Sie auf das Aktivierungssymbol in der Spalte **Quelle festlegen** für die Pakete auf der rechten Seite, die Geschäftsprozesse enthalten, welche Sie an die Teilnehmer oder Community Manager senden.
6. Wählen Sie beides aus, wenn Sie dieselben Prozesse senden und empfangen. Die Konsole zeigt einen Haken an, wenn die Dokumentenflussdefinition aktiviert ist.

Anmerkung: Die Auswahl von **Quelle festlegen** ist für alle Aktionen in einem Zweibege-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 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 auf die ausgewählte Ebene zu erweitern.
8. Wählen Sie erneut **Quelle festlegen**, **Ziel festlegen** oder beide Rollen für die unteren Protokoll-, Dokumentenfluss-, Aktions- und Aktivitätenebenen für jede Dokumentenflussdefinition aus, die Ihr System unterstützt.
Wenn eine Definition auf Dokumentenflussebene aktiviert ist, werden die beiden Aktions- und Aktivitätsdefinitionen 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 Dokumentenflussdefinitionspaket inaktiviert ist, sind alle Dokumentenflussdefinitionen der unteren Ebenen 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 Bearbeitungssymbol, 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.

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 Konsole zeigt die Anzeige **Verbindungen verwalten** an.
2. Wählen Sie unter **Quelle** eine Quelle aus.
3. Wählen Sie unter **Ziel** ein Ziel 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 Konsole zeigt die Anzeige **Verbindungen verwalten** an. Diese Anzeige 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. Klicken Sie auf **Attribute**, wenn Sie die Attributwerte anzeigen oder ändern wollen.
7. Klicken Sie auf **Aktionen**, wenn Sie eine Aktion anzeigen oder ändern wollen.
8. Klicken Sie auf **Gateways**, wenn Sie das Quellen- oder Zielgateway anzeigen oder ändern wollen.

Zusammenfassung

In diesem Kapitel haben Sie Community Manager und Teilnehmer erstellt und Informationen wie z. B. die IP-Adresse und die DUNS-ID der Teilnehmer angegeben. Nachdem Sie die Teilnehmer erstellt haben, haben Sie Gateways für sie eingerichtet, um anzugeben, wohin Dokumente weitergeleitet werden sollen.

Als Nächstes haben Sie die B2B-Funktionalität von Community Manager und den Teilnehmern ausgewählt und die Pakete, Protokolle und die Dokumentenflüsse angegeben, die Community Manager und die Teilnehmer senden und empfangen können. Schließlich haben Sie Teilnehmerverbindungen auf der Grundlage der B2B-Funktionalität von Document Manager und den Teilnehmern aktiviert.

Kapitel 7. Sicherheit für Eingangs- und Ausgangsaustauschvorgänge konfigurieren

Sie können mit WebSphere Business Integration Connect die folgenden Zertifikatstypen für Eingangs- und Ausgangstransaktionen installieren und verwenden:

- Secure Sockets Layer (SSL) für Server und Client
- Digitale Unterschrift
- Verschlüsselung

Begriffe und Konzepte

Dieser Abschnitt bietet eine allgemeine Übersicht über die Sicherheitstypen, die zum Generieren und Hochladen von Zertifikaten verwendeten Tools und die Datensammlungstypen, die von WebSphere Business Integration Connect installiert wurden.

Sicherheitstypen

Dieser Abschnitt gibt eine kurze Übersicht über SSL, digitale Unterschriften und Verschlüsselung.

SSL

WebSphere Business Integration Connect 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.

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.

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 ihr eigenes digitales Zertifikat bereitstellen.

Digitale Unterschrift

Die digitale Unterzeichnung ist der Mechanismus, um einen fälschungssicheren Herkunftsnachweis sicherzustellen. Ein fälschungssicherer Herkunftsnachweis 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.

Verschlüsselung

WebSphere Business Integration Connect 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 Paar mathematisch zusammengehöriger Schlüssel. 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 Paar Schlüssel. 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 Business Integration Connect 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 `<WBIC_installationsverz>/router/was/bin`, das WebSphere Business Installation Connect während der Installation erstellt hat.

Sie können mit ikeyman auch eine Anforderung für ein Zertifikat von einer CA (Certifying Authority) generieren.

Anmerkung: Außerdem können Sie das Dienstprogramm `createCert.sh` verwenden, um selbst unterzeichnete Zertifikate zu generieren.

Community Console

Sie installieren mit Community Console alle erforderlichen Client-, Unterschrifts- und Verschlüsselungszertifikate für den WebSphere Business Integration Connect-Speicher. Sie können mit Community Console auch Root- und CA-Zertifikate (Certifying Authority) 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 Zertifikatablaufalerts für Zertifikate mit ein, die in WebSphere Business Integration Connect gespeichert sind.

Keystores und Truststores

Wenn Sie WebSphere Business Integration Connect installieren, werden ein Keystore und 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.

Für kommerzielle CA wird das CA-Rootzertifikat hinzugefügt. Die Truststore-Datei kann eine mehr der Öffentlichkeit zugängliche Schlüsseldatei sein, die alle vertrauenswürdigen Zertifikate enthält.

Standardmäßig werden zwei Keystores und zwei Truststores im Verzeichnis `WBIC_install_root/common/security/keystore` erstellt. Sie heißen wie folgt:

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

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.

Anmerkung: Der folgende Unix-Befehl kann zum Ändern des Kennworts der Keystore-Datei verwendet werden:

```
/WBIC_install_root/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-Exemplarkonfiguration ebenfalls geändert werden. Dies kann mit Hilfe des Scripts `bcgChgPassword.jacl` geschehen. Navigieren Sie für das Konsol-exemplar zum folgenden Verzeichnis:

```
/WBIC_install_root/console/was/bin
```

Führen Sie den folgenden Befehl aus:

```
./wsadmin.sh -f /WBIC_install_root/console/scripts/
bcgChgPassword.jacl -conntype NONE
```

Wiederholen Sie diesen Schritt für die WebSphere Application Server-Exemplare des Empfängers und von Document Manager.

Sie werden aufgefordert, das neue Kennwort einzugeben.

Anmerkung: 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 Zertifikatdateinamen 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**.

Zertifikate erstellen und installieren

Die folgenden Abschnitte beschreiben, wie Sie Zertifikate erstellen und installieren, die Sie mit WebSphere Business Integration Connect verwenden wollen.

Eingehende SSL-Zertifikate

Wenn Ihre Community SSL nicht verwendet, benötigen weder Sie noch Ihre Teilnehmer ein eingehendes oder ausgehendes SSL-Zertifikat.

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 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 jedes Exemplar. 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.

Wenn Sie selbst unterzeichnete Serverzertifikate verwenden, führen Sie eine der folgenden Prozeduren aus.

- **ikeyman:**

1. Starten Sie das Dienstprogramm `ikeyman`, welches sich in `/WBIC_install_root/router/was/bin` befindet. Wenn `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.
4. Installieren Sie die Datei `pkcs12` 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 ZIP-Datei per E-Mail. Ihre Teilnehmer müssen sich an Sie wenden und das Kennwort für die ZIP-Datei anfordern.

- **createCert.sh:**

1. Verwenden Sie das Script `createCert.sh`, das sich im Verzeichnis `/WBIC_install_root/router/was/bin` befindet, um ein selbst unterzeichnetes Zertifikat in X.509-Format, einen privaten Schlüssel in PKCS 8-Format und eine Datei PKCS12 zu generieren, die sowohl den privaten Schlüssel als auch das Zertifikat enthält.
2. Installieren Sie die Datei `pkcs12` in den Keystore des Empfängers bzw. der Konsole, für den sie erstellt worden ist.

3. Verteilen Sie das Zertifikat an Ihre Teilnehmer. Die bevorzugte Verteilungsmethode ist das Senden des Zertifikats in einer kennwortgeschützten ZIP-Datei per E-Mail. Ihre Teilnehmer müssen sich an Sie wenden und das Kennwort für die ZIP-Datei anfordern.

Wenn Sie ein von einer Certificate Authority (CA) unterzeichnetes Zertifikat verwenden, führen Sie die folgende Prozedur aus.

1. Starten Sie das Dienstprogramm ikeyman, welches sich im Verzeichnis `/WBIC_install_root/router/was/bin` befindet.
2. Generieren Sie mit ikeyman eine Zertifikatsanforderung und ein Schlüsselpaar für den Empfänger.
3. Übergeben Sie eine Zertifikatsunterzeichnungsanforderung (CSR - Certificate Signing Request) an eine CA.
4. Wenn Sie das unterzeichnete Zertifikat von der CA empfangen, platzieren Sie mit ikeyman das unterzeichnete Zertifikat in den Keystore.
5. Verteilen Sie das CA-Zertifikat an alle Teilnehmer.

Clientauthentifizierung

Verwenden Sie für die Clientauthentifizierung die folgende Prozedur:

1. Rufen Sie das Zertifikat Ihres Teilnehmers ab.
2. Installieren Sie das Zertifikat mit Hilfe von ikeyman im Truststore.
3. Platzieren Sie die zugehörige CA in das CA-Verzeichnis oder 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.

Nachdem Sie das Zertifikat installiert haben, konfigurieren Sie WebSphere Application Server für die Verwendung der Clientauthentifizierung, indem Sie das Dienstprogrammscript **bcgClientAuth.jacl** ausführen.

- Navigieren Sie zum folgenden Verzeichnis:
`/WBIC_install_root/receiver/was/bin`
- Zum Aktivieren der Clientauthentifizierung rufen Sie das Script wie folgt auf:
`./wsadmin.sh -f /WBIC_install_root/receiver/scripts/bcgClientAuth.jacl -connType NONE set`
- Zum Inaktivieren der Clientauthentifizierung rufen Sie das Script wie folgt auf:
`./wsadmin.sh -f /WBIC_install_root/receiver/scripts/bcgClientAuth.jacl -connType NONE clear`

Sie müssen den WebSphere Application Server-Empfänger starten, damit diese Änderungen wirksam werden.

Es gibt eine Zusatzfunktion, die mit der SSL-Clientauthentifizierung verwendet werden kann. Diese Funktion wird über Community Console aktiviert. Für HTTPS überprüft WebSphere Business Integration Connect 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. Wählen Sie die Option **Client-SSL-Zertifikat prüfen** in der Gateway-Anzeige des Teilnehmers aus.

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 Business Integration Connect ein serverseitiges Zertifikat von den Teilnehmern an. Wenn das Zertifikat eines Teilnehmers selbst unterzeichnet ist, importieren Sie es mit Community Console in das Profil des Hub-Operators und markieren es als **Rootzertifikat**. Wenn das Zertifikat CA-unterzeichnet ist, müssen Sie nur das CA-Zertifikat in Community Console importieren und es als **Rootzertifikat** markieren.

Anmerkung: Dasselbe CA-Zertifikat kann für mehrere Teilnehmer verwendet werden. Das Zertifikat muss in X.509-DER-Format sein.

Clientauthentifizierung

Wenn SSL-Clientauthentifizierung erforderlich ist, wird der Teilnehmer seinerseits ein Zertifikat vom Hub anfordern. Importieren Sie mit Community Console Ihr Zertifikat in WebSphere Business Integration Connect. Sie können das Zertifikat mit `ikeyman` oder dem Script `createCert.sh` 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.

Wenn Sie ein selbst unterzeichnetes Zertifikat verwenden, führen Sie eine der folgenden Prozeduren aus.

- **ikeyman:**

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 ZIP-Datei per E-Mail. Ihre Teilnehmer müssen sich an Sie wenden und das Kennwort für die ZIP-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. Zeigen Sie mit **Kontenadmin > Profile > Zertifikate** die Seite **Zertifikate** an. Stellen Sie sicher, dass Sie an Community Console als Hub-Operator angemeldet sind. Installieren Sie das Zertifikat in Ihrem eigenen Profil, und markieren Sie es als **SSL-Zertifikat**.

- **createCert.sh:**

1. Verwenden Sie das Script `createCert.sh`, um ein selbst unterzeichnetes Zertifikat in X.509-Format, einen privaten Schlüssel in PKCS 8-Format und eine Datei PKCS12 zu generieren, die sowohl den privaten Schlüssel als auch das Zertifikat enthält.
2. Installieren Sie das selbst unterzeichnete Zertifikat und den Schlüssel über Community Console. Zeigen Sie mit **Kontenadmin > Profile > Zertifikate** die Seite **Zertifikate** an. Stellen Sie sicher, dass Sie an Community Console

als Hub-Operator angemeldet sind. Installieren Sie das Zertifikat in Ihrem eigenen Profil, und markieren Sie es als **SSL-Zertifikat**.

3. Senden Sie Ihr selbst unterzeichnetes Zertifikat oder CA-Rootzertifikat an alle Teilnehmer, so dass sie es als vertrauenswürdigen Zertifikat hinzufügen können.

Wenn Sie ein von einer CA 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 Zertifikatsunterzeichnungsanforderung (CSR - Certificate Signing Request) an eine CA.
3. Wenn Sie das unterzeichnete Zertifikat von der CA empfangen, platzieren Sie mit `ikeyman` das unterzeichnete Zertifikat in den Keystore.
4. Verteilen Sie das unterzeichnende CA-Zertifikat an alle Teilnehmer.

Zertifikatswiderrufsliste (CRL) hinzufügen

Business Integration Connect enthält eine CRL-Funktion (CRL - Certificate Revocation List - Zertifikatswiderrufsliste). Die CRL, die von einer Certificate Authority (CA) herausgegeben wird, gibt Teilnehmer an, die Zertifikate vor ihrem terminierten Ablaufdatum widerrufen haben. Teilnehmern mit widerrufenen Zertifikaten wird der Zugriff auf Business Integration Connect 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`. Business Integration Connect verwendet die Einstellung `bcg.http.CRLDir` in der Datei `bcg.properties`, um die Position des CRL-Verzeichnisses anzugeben.

Erstellen Sie eine `.crl`-Datei, die die widerrufenen Zertifikate enthält, und platzieren Sie diese im CRL-Verzeichnis.

In der Datei `bcg.properties` würden Sie z. B. die folgende Einstellung verwenden:

```
bcg.http.CRLDir=/<gemeinsames datenverzeichnis>/security/crl.
```

Eingehendes Unterschriftszertifikat

Document Manager verwendet das unterzeichnete Zertifikat des Teilnehmers, um die Unterschrift des Senders 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 Unterschriftszertifikat des Teilnehmers in X.509-DER-Format.
2. Installieren Sie die Zertifikate über Community Console im Profil des Teilnehmers. Verwenden Sie **Kontenadmin > Profile > Community-Teilnehmer**, und suchen Sie nach dem Profil des Teilnehmers. Klicken Sie auf **Zertifikate**, und

laden Sie dann das Zertifikat als Zertifikatstyp **Digitale Unterschrift** hoch. Vergessen Sie nicht, dieses Zertifikat in der Bestätigungsanzeige zu aktivieren und zu speichern.

3. Wenn das Zertifikat von einer CA unterzeichnet wurde und das CA-Rootzertifikat nicht bereits im Profil des Hub-Operators installiert ist, installieren Sie es jetzt. Zeigen Sie mit **Kontenadmin > Profile > Zertifikate** die Seite **Zertifikate** an. Stellen Sie sicher, dass Sie an Community Console als Hub-Operator angemeldet sind, und installieren Sie das Zertifikat in Ihrem eigenen Profil.

Anmerkung: Sie müssen den vorherigen Schritt nicht ausführen, wenn das CA-Zertifikat bereits installiert ist.

4. Führen Sie die Aktivierung auf der Ebene für Pakete (höchste Ebene), Teilnehmer oder Verbindungen (unterste Ebene) aus. 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.

Wenn Sie ein selbst unterzeichnetes Zertifikat verwenden, führen Sie eine der folgenden Prozeduren aus.

ikeyman:

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 ZIP-Datei per E-Mail. Ihre Teilnehmer müssen sich an Sie wenden und das Kennwort für die ZIP-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 die Zertifikatsfunktion von Community Console. Zeigen Sie mit **Kontenadmin > Profile > Zertifikate** die Seite **Zertifikate** an. Stellen Sie sicher, dass Sie an Community Console als Hub-Operator angemeldet sind, und installieren Sie das Zertifikat in Ihrem eigenen Profil. Markieren Sie das Zertifikat als Typ **Digitale Unterschrift**. Stellen Sie sicher, dass Sie das Zertifikat in der Bestätigungsanzeige aktivieren und speichern.

createCert.sh:

1. Verwenden Sie das Script `createCert.sh`, um ein selbst unterzeichnetes Zertifikat in X.509-Format, einen privaten Schlüssel in PKCS-8-Format und eine PKCS12-Datei zu generieren, die sowohl den privaten Schlüssel als auch das Zertifikat enthält.

2. Installieren Sie das selbst unterzeichnete Zertifikat und den Schlüssel über die Zertifikatsfunktion von Community Console. Zeigen Sie mit **Kontenadmin > Profile > Zertifikate** die Seite **Zertifikate** an. Stellen Sie sicher, dass Sie an Community Console als Hub-Operator angemeldet sind, und installieren Sie das Zertifikat in Ihrem eigenen Profil. Markieren Sie das Zertifikat als Typ **Digitale Unterschrift**. Stellen Sie sicher, dass Sie das Zertifikat in der Bestätigungsanzeige aktivieren und speichern.
3. Verteilen Sie das Zertifikat an Ihre Teilnehmer. Die bevorzugte Verteilungsmethode ist das Senden des Zertifikats in einer kennwortgeschützten ZIP-Datei per E-Mail. Ihre Teilnehmer müssen sich an Sie wenden und das Kennwort für die ZIP-Datei anfordern.
4. Führen Sie die Aktivierung auf der Ebene für Pakete (höchste Ebene), Teilnehmer oder Verbindungen (unterste Ebene) aus. 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**.

Wenn Sie ein von einer CA 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 Zertifikatsunterzeichnungsanforderung (CSR - Certificate Signing Request) an eine CA.
4. Wenn Sie das unterzeichnete Zertifikat von der CA empfangen, platzieren Sie mit ikeyman das unterzeichnete Zertifikat in den Keystore.
5. Verteilen Sie das unterzeichnende CA-Zertifikat an alle Teilnehmer.

Eingehendes Verschlüsselungszertifikat

Dieses Zertifikat wird vom Empfänger verwendet, um verschlüsselte Dateien zu entschlüsseln, die von Teilnehmern empfangen wurden. Der Empfänger 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.

Wenn Sie ein selbst unterzeichnetes Zertifikat verwenden, führen Sie eine der folgenden Prozeduren aus.

- **ikeyman:**

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 exportieren.
6. Installieren Sie das selbst unterzeichnete Zertifikat und das private Schlüsselpaar in Form einer PKCS12-Datei über Community Console. Zeigen Sie mit **Kontenadmin > Profile > Zertifikate** die Seite **Zertifikate** an. Stellen Sie sicher, dass Sie an Community Console als Hub-Operator angemeldet sind, und installieren Sie das Zertifikat in Ihrem eigenen Profil. Markieren Sie das Zertifikat als Typ **Verschlüsselung** und, stellen Sie sicher, dass Sie das installierte Zertifikat in der Bestätigungsanzeige aktivieren und speichern.
7. Führen Sie die Aktivierung auf der Ebene für Pakete (höchste Ebene), Teilnehmer oder Verbindungen (unterste Ebene) aus. 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**.

- **createCert.sh:**

1. Verwenden Sie das Script `createCert.sh`, um ein selbst unterzeichnetes Zertifikat in X.509-Format, einen privaten Schlüssel in PKCS-8-Format und eine PKCS12-Datei zu generieren, die sowohl den privaten Schlüssel als auch das Zertifikat enthält.
2. Installieren Sie das selbst unterzeichnete Zertifikat und den Schlüssel über die Zertifikatsfunktion von Community Console. Zeigen Sie mit **Kontenadmin > Profile > Zertifikate** die Seite **Zertifikate** an. Stellen Sie sicher, dass Sie an Community Console als Hub-Operator angemeldet sind, und installieren Sie das Zertifikat in Ihrem eigenen Profil. Markieren Sie das Zertifikat als Typ **Verschlüsselung**. Stellen Sie sicher, dass Sie das installierte Zertifikat in der Bestätigungsanzeige aktivieren und speichern.
3. 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.
4. Führen Sie die Aktivierung auf der Ebene für Pakete (höchste Ebene), Teilnehmer oder Verbindungen (unterste Ebene) aus. 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 Sie ein von einer CA 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 Zertifikatsunterzeichnungsanforderung (CSR - Certificate Signing Request) an eine CA.
4. Wenn Sie das unterzeichnete Zertifikat von der CA empfangen, platzieren Sie mit ikeyman das unterzeichnete Zertifikat 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. Business Integration Connect verschlüsselt Dokumente mit den öffentlichen Schlüsseln der Teilnehmer und die Teilnehmer entschlüsseln die Dokumente mit ihren privaten Schlüsseln.

1. Rufen Sie das Verschlüsselungszertifikat des Teilnehmers ab. Das Zertifikat muss in X.509-DER-Format sein.
2. Installieren Sie das Zertifikat über die Zertifikatsfunktion von Community Console. Sie führen diese Task aus, wenn Sie an der Konsole als Hub-Operator angemeldet sind, und installieren Sie das Zertifikat im Profil des jeweiligen Teilnehmers. Verwenden Sie **Kontenadmin > Profile > Community-Teilnehmer**, und suchen Sie nach dem Profil des Teilnehmers. Klicken Sie dann auf **Zertifikate**, und laden Sie das Zertifikat als Zertifikatstyp **Verschlüsselung** hoch. Stellen Sie sicher, dass Sie dieses Zertifikat in der Bestätigungsanzeige aktivieren und speichern.
3. Wenn das Zertifikat von einer CA unterzeichnet ist, und Sie das CA-Zertifikat nicht auf Ihrem System installiert haben, melden Sie sich an der Konsole als Hub-Operator an, und installieren Sie dieses Zertifikat in Ihrem eigenen Profil. Zeigen Sie mit **Kontenadmin > Profile > Zertifikate** die Seite **Zertifikate** an. Installieren Sie das Zertifikat in Ihrem eigenen Profil. Sie müssen ein CA-Zertifikat nur einmal laden.
4. Führen Sie die Aktivierung auf der Ebene für Pakete (höchste Ebene), Teilnehmer oder Verbindungen (unterste Ebene) aus. 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**.

Eingangs-SSL für Konsole und Empfänger konfigurieren

Die WebSphere Business Integration Connect-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 Business Integration Connect zu konfigurieren.

1. Rufen Sie die folgenden Informationen ab.
 - Die vollständigen Pfadnamen der Schlüsseldatei und der Anerkennungsdatei für z. B. den Empfänger:
WBIC_install_root/common/security/keystore/receiver.jks
und
WBIC_install_root/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 folgendes Verzeichnis:

```
/WBIC_install_root/receiver/was/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.

```
./wsadmin.sh -f /WBIC_install_root/receiver/  
scripts/bcgssl.jacl -conntype NONE install  
<schlüsseldatei pfadname>  
<schlüsseldatei kennwort> <schlüsseldatei format>  
<anerkennungsdatei pfadname>  
<anerkennungsdatei kennwort> <anerkennungsdatei format>
```

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.

Kapitel 8. Die Konfiguration fertig stellen

Dieses Kapitel beschreibt zusätzliche Tasks, die Sie ausführen können, um den Hub zu konfigurieren.

Die Verwendung von APIs aktivieren

WebSphere Business Integration Connect 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 APIs zu aktivieren, so dass Teilnehmer API-Aufrufe auf dem WebSphere Business Integration Connect-Server durchführen können:

1. Klicken Sie im Hauptmenü auf **Systemverwaltung > Funktionsverwaltung > Administrations-API**.
2. Klicken Sie auf das Symbol  neben **Die Administrations-API aktivieren**.
3. Wählen Sie das Markierungsfeld aus, um die Verwendung der API zu aktivieren.
4. Klicken Sie auf **Speichern**.

Die für Ereignisse verwendeten Warteschlangen angeben

Sie können den Hub konfigurieren, um Ereignisse an eine externe Warteschlange zu übermitteln, die mit 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.

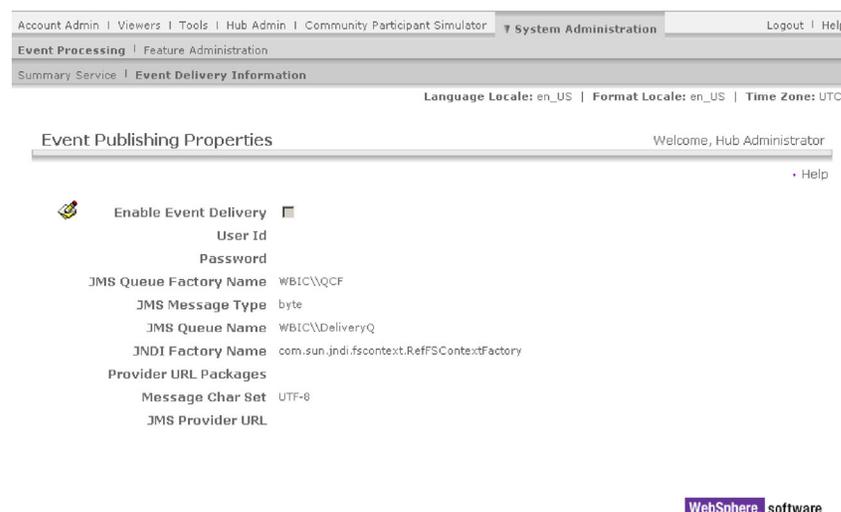


Abbildung 31. Die Seite "Merkmale für Ereignisveröffentlichung"

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 <router-root-verz>/was/wbic/config/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  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.
- Geben Sie für **JMS-Nachrichtentyp** den Nachrichtentyp ein, der übermittelt wird. Die Auswahlmöglichkeiten sind hier **byte** oder **text**.
- Geben Sie für **JMS-Warteschlangename** 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.
- 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. Dies ist <router-root-verz>/was/jndi/WBIC.

- 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 Business Integration Connect auftritt, wird ein Ereigniscode generiert. Mit der Anzeige **Ereigniscode**s können Sie den alertfähigen Status des Ereigniscode festlegen. Wenn ein Ereignis als alertfähig festgelegt wurde, wird das Ereignis in der Liste **Ereignisname** der Anzeige **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 > Ereigniscode**s.
Die Anzeige **Ereigniscode**s wird angezeigt.
2. Gehen Sie für jedes Ereignis, das Sie alertfähig machen wollen, wie folgt vor:
 - a. Klicken Sie auf das Lupensymbol neben dem Ereigniscode. Die Anzeige **Ereigniscodedetails** wird angezeigt.
 - b. Wählen Sie **Alertfähig?** aus.

Benutzerdefiniertes Transportprotokoll aktualisieren

Wie in Kapitel 5, „Den Hub konfigurieren“ und Kapitel 6, „Teilnehmer und Teilnehmerverbindungen erstellen“ beschrieben, können Sie eine XML-Datei hochladen, die ein benutzerdefiniertes Transportprotokoll beschreibt. Sie können mit **Transporttyp importieren** die Datei hochladen. Nachdem Sie die XML-Datei hochgeladen haben, ist das Transportprotokoll zur Verwendung verfügbar, wenn Sie ein Ziel oder Gateway definieren.

Die XML-Datei, die das benutzerdefinierte Transportprotokoll beschreibt, schließt die Attribute für das Transportprotokoll mit ein. Diese Attribute werden im Abschnitt **Angepasste Transportattribute** auf der Ziel- oder Gateway-Seite angezeigt, wenn Sie ein benutzerdefiniertes Transportprotokoll angeben. Ein benutzerdefiniertes Transportprotokoll für ein Gateway könnte z. B. das Attribut **Gateway-RetryCount** mit einschließen.

Der Autor der XML-Datei, die das Transportprotokoll beschreibt, kann die Attribute aktualisieren, indem er die Attribute hinzufügt, löscht oder modifiziert. Wenn die XML-Datei modifiziert wurde, verwenden Sie erneut **Transporttyp importieren**, um die Datei hochzuladen. Jede Änderung an den Attributen wird in der Gateway- oder Zielanzeige widergegeben.

Anhang A. Beispiele

Dieser Anhang stellt ein grundlegendes Beispiel zum Konfigurieren eines Hubs, zum Erstellen eines Teilnehmers und von Verbindungen sowie zum Anwenden der Sicherheit für Eingangs- und Ausgangsdokumente bereit. Es wird dabei die Reihenfolge eingehalten, die in diesem Handbuch vorgegeben ist. Nach dem Beispiel für die Basiskonfiguration finden Sie Beispiele für die Konfiguration anderer Transportprotokolle und Protokolle.

Basiskonfiguration – EDI-Dokumente mit AS-Paket über HTTP 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 wurden, verwenden die Dokumentenflussdefinitionen, die von WebSphere Business Integration Connect zur Verfügung gestellt werden. Aus diesem Grund müssen Sie die Verbindungen nur auf der Basis dieser Flüsse erstellen. In diesem Beispiel wird kein kundenspezifisches XML verwendet.

Den Hub konfigurieren

Der erste Schritt in der Konfiguration des Hubs besteht darin, die zwei Ziele zu erstellen.

- Ein HTTP-Ziel (namens "HttpTarget") zum Empfangen von Dokumenten über HTTP (von **Partner Zwei**), die an das Back-End-System von Community Manager (**Partner Eins**) gesendet werden sollen.
- Ein Dateiverzeichnisziel (namens "FileSystemTarget") zum Abrufen der Dokumente vom Dateisystem (vom Back-End-System von **Partner Eins**), die an **Partner Zwei** gesendet werden sollen.

Die Ziele definieren

Gehen Sie wie folgt vor, um ein Ziel für den Empfang von HTTP zu erstellen:

1. Klicken Sie auf **Hubadmin > Hubkonfiguration > Ziele**.
2. Klicken Sie auf **Ziel erstellen**.
3. Geben Sie als **Zielname** den Namen HttpTarget 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 FileSystemTarget 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\FileSystemTarget`

Anmerkung: Dadurch wird ein Verzeichnis **FileSystemTarget** innerhalb des Verzeichnisses **C:\temp** erstellt. Stellen Sie sicher, dass ein Verzeichnis **C:\temp** im Dateisystem vorhanden ist.

7. Klicken Sie auf **Speichern**.

Dokumentenflüsse und Interaktionen definieren

In diesem Beispiel definieren Sie die folgenden Austauschvorgänge:

- Ein EDI-X12-Dokument im AS2-Paket von **Partner Zwei** zu **Partner Eins** senden
- Ein EDI-X12-Dokument ohne Paket von **Partner Zwei** zu **Partner Eins** senden
- Ein EDI-X12-Dokument im AS2-Paket von **Partner Eins** zu **Partner Zwei** senden
- Ein EDI-X12-Dokument ohne Paket von **Partner Eins** zu **Partner Zwei** 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. Sie benötigen zwei Interaktionen:

- Eine Interaktion, in der die Quelle ein EDI-X12-Dokument ohne Paket und das Ziel ein EDI-X12-Dokument mit AS2-Paket ist.
- Eine Interaktion, in der die Quelle ein EDI-X12-Dokument im AS2-Paket und das Ziel ein EDI-X12-Dokument ohne Paket ist.

Erstellen Sie die erste Interaktion, in der das Quellenformat ein EDI-X12-Dokument ohne Paket und das Zielformat ein EDI-X12-Dokument mit AS-Paket ist.

1. Klicken Sie auf **Hubadmin > Hubkonfiguration > Dokumentenflussdefinition**.
2. Klicken Sie auf **Interaktionen verwalten** und dann auf **Interaktion erstellen**.
3. Wählen Sie in der Spalte **Quelle** Folgendes aus:
 - a. Paket: **None**
 - b. Protokoll: **EDI-X12**
 - c. Dokumentenfluss: **All**
4. Wählen Sie in der Spalte **Ziel** Folgendes aus:
 - a. Paket: **AS**
 - b. Protokoll: **EDI-X12**
 - c. Dokumentenfluss: **All**
5. Setzen Sie **Aktion** auf **Pass-Through**.
6. Klicken Sie auf **Speichern**.

Erstellen Sie eine zweite Interaktion, in der das Quellenformat ein EDI-X12-Dokument im AS2-Paket und das Zielformat ein EDI-X12-Dokument ohne Paket ist:

1. Klicken Sie auf **Interaktion erstellen**.
2. Wählen Sie in der Spalte **Quelle** Folgendes aus:
 - a. Paket: **AS**
 - b. Protokoll: **EDI-X12**

- c. Dokumentenfluss: **All**
- 3. Wählen Sie in der Spalte **Ziel** Folgendes aus:
 - a. Paket: **None**
 - b. Protokoll: **EDI-X12**
 - c. Dokumentenfluss: **All**
- 4. Setzen Sie **Aktion** auf **Pass-Through**.
- 5. 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 Standardtransportprotokolle. Es sind keine Konfigurationspunkte für die Gateways definiert.

Die Teilnehmer erstellen

Erstellen Sie zwei neue Teilnehmer. Gehen Sie wie folgt vor, um **Partner Eins** zu definieren:

1. Klicken Sie auf **Kontenadmin** vom Hauptmenü. Die Seite **Teilnehmersuche** ist die Standardanzeige.
2. Klicken Sie auf **Erstellen**.
3. Geben Sie als **Teilnehmeranmeldename** Folgendes ein: **partnerEins**.
4. Geben Sie als **Teilnehmername** Folgendes ein: **Partner Eins**.
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.
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 **Teilnehmeranmeldename** Folgendes ein: **partnerZwei**.
4. Geben Sie als **Teilnehmername** 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 **Partner Eins** als auch **Partner Zwei** für den Hub definiert.

Zu den nächsten Schritten gehört nun das Konfigurieren von Gateways für **Partner Eins** und **Partner Zwei**.

Die Gateways erstellen

Bevor Sie ein Dateiverzeichnisgateway für **Partner Eins** erstellen, müssen Sie die Verzeichnisstruktur erstellen, die von diesem Gateway verwendet wird. Erstellen Sie ein neues Verzeichnis **FileSystemGateway** auf dem Stammlaufwerk. In diesem Verzeichnis speichert **Partner Eins** Dateien, die von Teilnehmern empfangen wurden.

In dem Fall von **Partner Eins**, der als Community Manager fungiert, stellt das Gateway den Einstiegspunkt in das Back-End-System dar.

Gehen Sie wie folgt vor, um ein Gateway für **Partner Eins** zu erstellen:

1. Klicken Sie auf **Kontenadmin > Profile > Community-Teilnehmer**.
2. Klicken Sie auf **Suchen**.
3. Wählen Sie **Partner Eins** aus, indem Sie auf das Symbol  klicken.
4. Klicken Sie auf **Gateways** in der horizontalen Navigationsleiste.
5. Klicken Sie auf **Erstellen**.
6. Geben Sie als **Gateway-Name** Folgendes ein: **FileSystemGateway**.
7. Wählen Sie als **Transport** die Option **Dateiverzeichnis** aus.
8. Geben Sie als **Ziel-URI-Datei** Folgendes ein: **file://C:\FileSystemGateway**
9. Klicken Sie auf **Speichern**.

Legen Sie nun dieses neu erstellte Gateway als das Standardgateway für **Partner Eins** fest.

1. Klicken Sie auf **Liste**, um alle Gateways anzuzeigen, die für **Partner Eins** konfiguriert sind.
2. Klicken Sie auf **Standardgateways anzeigen**.
3. Wählen Sie in der Liste den Eintrag **FileSystemGateway** als **Produktionsgateway-Typ** 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 Lupensymbol 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 **Ziel-URI-Datei** 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: **partnerEins**.
9. Geben Sie als **Kennwort** Folgendes ein: **partnerEins**.
10. Klicken Sie auf **Speichern**.

Beachten Sie, dass in diesem Beispiel davon ausgegangen wird, dass Teilnehmer, die sich am System von **Partner Two** anmelden wollen, einen Benutzernamen und ein Kennwort benötigen.

Für diesen Teilnehmer müssen Sie auch ein Standardgateway definieren.

1. Klicken Sie auf **Liste** und dann auf **Standardgateways anzeigen**.
2. Wählen Sie in der Liste den Eintrag **HttpGateway** als Gateway des Typs **Produktion** aus.
3. Klicken Sie auf **Speichern**.

B2B-Funktionalität konfigurieren

Definieren Sie als Nächstes die B2B-Funktionalität für **Partner Eins** (Community Manager).

1. Klicken Sie im Hauptmenü auf **Kontenadmin > Profile > Community-Teilnehmer**.
2. Klicken Sie auf **Suchen**.
3. Wählen Sie **Partner Eins** aus, indem Sie auf das Lupensymbol 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: ALL** aus, indem Sie die folgenden Schritte ausführen:
 - a. Klicken Sie auf das Aktivierungssymbol unter **Quelle festlegen** für **Paket: AS**.
 - b. Klicken Sie auf das Aktivierungssymbol unter **Ziel festlegen** für **Paket: AS**.
 - c. Klicken Sie auf das Ordnersymbol neben **Paket: AS**, um den Ordner zu erweitern.
 - d. Klicken Sie auf das Aktivierungssymbol zu **Protokoll: EDI-X12 (ALL)** für die Quelle und das Ziel.
 - e. Klicken Sie auf das Ordnersymbol neben **Protokoll: EDI-X12 (ALL)**, um den Ordner zu erweitern.
 - f. Klicken Sie auf das Aktivierungssymbol zu **Dokumentenfluss: ALL** für die Quelle und das Ziel.
6. Legen Sie die Quelle und das Ziel für das **Paket: None**, das **Protokoll: EDI-X12** und den **Dokumentenfluss: ALL** fest, indem Sie die folgenden Schritte ausführen:
 - a. Klicken Sie auf das Aktivierungssymbol unter **Quelle festlegen** für **Paket: None**.
 - b. Klicken Sie auf das Aktivierungssymbol unter **Ziel festlegen** für **Paket: None**.
 - c. Klicken Sie auf das Ordnersymbol neben **Paket: None**, um den Ordner zu erweitern.
 - d. Klicken Sie auf das Aktivierungssymbol zu **Protokoll: EDI-X12 (ALL)** für die Quelle und das Ziel.
 - e. Klicken Sie auf das Ordnersymbol neben **Protokoll: EDI-X12 (ALL)**, um den Ordner zu erweitern.
 - f. Klicken Sie auf das Aktivierungssymbol zu **Dokumentenfluss: ALL** 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 Lupensymbol 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: ALL** aus, indem Sie die folgenden Schritte ausführen:
 - a. Klicken Sie auf das Aktivierungssymbol unter **Quelle festlegen** für **Paket: AS**.
 - b. Klicken Sie auf das Aktivierungssymbol unter **Ziel festlegen** für **Paket: AS**.
 - c. Klicken Sie auf das Ordnersymbol neben **Paket: AS**, um den Ordner zu erweitern.
 - d. Klicken Sie auf das Aktivierungssymbol zu **Protokoll: EDI-X12 (ALL)** für die Quelle und das Ziel.
 - e. Klicken Sie auf das Ordnersymbol neben **Protokoll: EDI-X12 (ALL)**, um den Ordner zu erweitern.
 - f. Klicken Sie auf das Aktivierungssymbol zu **Dokumentenfluss: ALL** für die Quelle und das Ziel.
6. Legen Sie die Quelle und das Ziel für das **Paket: Kein(e)**, das **Protokoll: EDI-X12** und den **Dokumentenfluss: ALLE** fest, indem Sie die folgenden Schritte ausführen:
 - a. Klicken Sie auf das Aktivierungssymbol unter **Quelle festlegen** für **Paket: None**.
 - b. Klicken Sie auf das Aktivierungssymbol unter **Ziel festlegen** für **Paket: None**.
 - c. Klicken Sie auf das Ordnersymbol neben **Paket: None**, um den Ordner zu erweitern.
 - d. Klicken Sie auf das Aktivierungssymbol zu **Protokoll: EDI-X12 (ALL)** für die Quelle und das Ziel.
 - e. Klicken Sie auf das Ordnersymbol neben **Protokoll: EDI-X12 (ALL)**, um den Ordner zu erweitern.
 - f. Klicken Sie auf das Aktivierungssymbol zu **Dokumentenfluss: ALL** für die Quelle und das Ziel.

Teilnehmerverbindungen definieren

Definieren Sie die Teilnehmerverbindung für EDI-Dokumente ohne Paket, die von **Partner Eins** eingehen und an **Partner Zwei** übermittelt werden sollen.

1. Klicken Sie auf **Kontenadmin > Teilnehmerverbindungen**.
2. Wählen Sie in der Liste **Quelle** den Eintrag **Partner Eins** 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: **ALL (ALL)**
 - b. **Ziel**
 - 1) Paket: **AS (N/A)**
 - 2) Protokoll: **EDI-X12 (ALL)**
 - 3) Dokumentenfluss: **ALL (ALL)**

Definieren Sie als Nächstes die Verbindung für EDI-Dokumente im AS2-Paket, die von **Partner Zwei** eingehen und an **Partner Eins** ohne Paket übermittelt 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 **Partner Eins** 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: **ALL (ALL)**
 - b. **Ziel**
 - 1) Paket: **None (N/A)**
 - 2) Protokoll: **EDI-X12 (ALL)**
 - 3) Dokumentenfluss: **ALL (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 in der Anzeige vorblättern, und klicken Sie auf das Ordnersymbol 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 dem ikeyman-Tool, 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 ikeyman-Anwendung, indem Sie die Datei **ikeyman.bat** von **C:\ProgramFiles\IBM\WBICconnect\receiver\bin** öffnen.
2. Öffnen Sie den Standardschlüsselspeicher des Empfängers, **receiver.jks**. Wählen Sie in der Menüleiste **Key Database File Open** aus. Bei einer Standardinstallation befindet sich **receiver.jks** im folgenden Verzeichnis:
\WBICconnect\common\security\keystore

3. Wenn Sie dazu aufgefordert werden, geben Sie das Standardkennwort für `receiver.jks` ein. Dieses Kennwort lautet **WebAS**.
4. Es wird davon ausgegangen, dass Sie `receiver.jks` zum ersten Mal öffnen, löschen Sie daher 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 im vorherigen Schritt 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 im Tool 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 **partnerEinsÖffentlich** 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 PKCS12-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 **partnerEinsPrivat** 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 das HTTPS-Transportprotokoll 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 CA (Certifying Authority) ausgestellt wurde, die für das Einrichten einer Zertifikatkette verwendet wurde. 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 Lupensymbol auswählen.
4. Klicken Sie auf **Zertifikate** und dann auf **Zertifikat laden**.
5. Setzen Sie den **Zertifikatstyp** auf **Rootzertifikat**.
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 Lupensymbol klicken.
3. Klicken Sie auf **Gateways** in der horizontalen Navigationsleiste. Wählen Sie als Nächstes **HttpGateway** aus, indem Sie auf das Lupensymbol klicken.
4. Bearbeiten Sie es, indem Sie auf das Bearbeitungssymbol klicken.
5. Ändern Sie den Transportprotokollwert in **HTTPS/1.1**.

6. Ändern Sie den Wert der Ziel-URI 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, das aus dem selbst unterzeichneten Zertifikat extrahiert worden ist, und die Verschlüsselung von Dokumenten konfigurieren, die zum Hub gesendet werden.

WebSphere Business Integration Connect 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 Task 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 Lupensymbol 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 **Partner Eins privat**.
7. Wählen Sie **Aktiviert** aus.
8. Klicken Sie auf **Durchsuchen**, und navigieren Sie zum Verzeichnis, in dem die PKCS12-Datei `partnerEinsPrivat.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 es 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 Lupensymbol 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 `partnerZweiDecrypt.der` gespeichert ist.
11. Wählen Sie das Zertifikat aus, und klicken Sie auf **Öffnen**.
12. Übernehmen Sie den Gateway-Typ **Produktion**, 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 modifizieren, die zwischen **Partner Eins** und **Partner Zwei** vorhanden ist.

Gehen Sie wie folgt vor, um die Teilnehmerverbindung über Community Console zu modifizieren:

1. Klicken Sie auf **Kontenadmin > Profile > Teilnehmerverbindungen** in der horizontalen Navigationsleiste.
2. Wählen Sie in der Liste **Quelle** den Eintrag **Partner Eins** 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 Ordnersymbol neben **Paket: AS (N/A)** klicken.

Anmerkung: Sie müssen in der Anzeige vorblättern, damit diese Option angezeigt wird.

7. Aktualisieren Sie in der Liste das Attribut **AS verschlüsselt** in **Ja**, und klicken Sie auf **Speichern**.

Dokumentenunterschrift konfigurieren

Wenn Sie eine Transaktion oder Nachricht digital unterzeichnen, verwendet WebSphere Business Integration Connect den privaten Schlüssel des Teilnehmers, 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 Business Integration Connect 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 Lupensymbol 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 **Partner Eins unterzeichnend**.
8. Setzen Sie den **Status** auf **Aktiviert**.
9. Klicken Sie auf **Durchsuchen**.
10. Navigieren Sie zum Verzeichnis, in dem das digitale 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, das als CA (Certifying Authority) importiert wurde, 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 Lupensymbol neben **Hub-Operator**.
3. Klicken Sie auf das Lupensymbol neben **Partner Eins privat**.

Anmerkung: Dies war das private Zertifikat, das Sie zuvor in den Hub geladen haben.

4. Klicken Sie auf das Bearbeitungssymbol.
5. Wählen Sie das Markierungsfeld neben **Digitale Unterschrift** aus.
6. Klicken Sie auf **Speichern**.

Als Nächstes ändern Sie die Attribute der vorhandenen Teilnehmerverbindung zwischen **Partner Eins** 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 > Profile > Teilnehmerverbindungen** in der horizontalen Navigationsleiste.
2. Wählen Sie **Partner Eins** 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 Ordnersymbol 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 Business Integration Connect an den Teilnehmer erforderlich ist.

Die Basiskonfiguration erweitern

Dieser Abschnitt zeigt Ihnen, wie Sie die in diesem Anhang beschriebene Basis-konfiguration modifizieren können. Dieser Abschnitt beschreibt unter Verwendung derselben, zuvor beschriebenen Partner und Konfiguration (ein Community Manager namens **PartnerEins** 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:

- Das FTP-Transportprotokoll
- Angepasste XML-Dokumente
- Binärdateien (ohne Paket)

FTP-Ziel erstellen

Das FTP-Ziel empfängt Dateien und übergibt sie zur Verarbeitung an Document Manager. Wie in Kapitel 2, „Die Konfiguration des Hubs vorbereiten“ 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 **Erstellen**.
3. Geben Sie die folgenden Informationen ein:
 - a. Zielname: **FTP_Receiver**
 - b. Transportprotokoll: **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 **Partner Eins** senden will.

Gültige Interaktion für Binärdokumente erstellen

Standardmäßig ist für WebSphere Business Integration Connect keine Interaktion zwischen Binärdokumenten konfiguriert. In diesem Abschnitt erstellen Sie die erforderliche Interaktion, damit Binärdokumente über das System übergeben 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 von **Aktion** die Option **Pass-Through** aus.
7. Klicken Sie auf **Speichern**.

Die B2B-Funktionalität für "Partner Eins" aktualisieren

Dieser Abschnitt zeigt, wie Sie **Partner Eins** 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 Lupensymbol neben **Partner Eins**.
4. Klicken Sie auf **B2B-Funktionalität**.
5. Klicken Sie auf das Aktivierungssymbol unter **Quelle festlegen** für **Paket: None**, um es zu aktivieren.
6. Klicken Sie auf das Aktivierungssymbol unter **Ziel festlegen** für **Paket: None**, um es zu aktivieren.
7. Klicken Sie auf das Ordnersymbol neben **Paket: None**.
8. Klicken Sie auf das Aktivierungssymbol zu **Protokoll: Binary (1.0)** für die Quelle und das Ziel.
9. Klicken Sie auf das Ordnersymbol neben **Protokoll: Binary (1.0)**.
10. Klicken Sie schließlich auf das Aktivierungssymbol zu **Dokumentenfluss: Binary (1.0)** für die Quelle und das Ziel.

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 Lupensymbol neben **Partner Zwei**.
4. Klicken Sie auf **B2B-Funktionalität**.
5. Klicken Sie auf das Aktivierungssymbol unter **Quelle festlegen** für **Paket: None**, um es zu aktivieren.
6. Klicken Sie auf das Aktivierungssymbol unter **Ziel festlegen** für **Paket: None**, um es zu aktivieren.
7. Klicken Sie auf das Ordnersymbol neben **Paket: None**.
8. Klicken Sie auf das Aktivierungssymbol zu **Protokoll: Binary (1.0)** für die Quelle und das Ziel.
9. Klicken Sie auf das Ordnersymbol neben **Protokoll: Binary (1.0)**.
10. Klicken Sie schließlich auf das Aktivierungssymbol zu **Dokumentenfluss: Binary (1.0)** für die Quelle und das Ziel.

Neue Teilnehmerverbindung erstellen

Dieser Abschnitt zeigt, wie Sie eine neue Teilnehmerverbindung zwischen **Partner Eins** 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 **Partner Eins** 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 Kapitel 5, „Den Hub konfigurieren“ beschrieben, müssen Sie den Hub konfigurieren, damit er 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 Namenswerte für die Felder **Von Teilnehmer** und **An Teilnehmer** zu identifizieren.

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. Geben Sie die folgenden Informationen ein:
 - a. Dokumentenflusstyp: **Protokoll**
 - b. Code: **CustomXML**
 - c. Version: **1.0**
 - d. Beschreibung: **CustomXML**
4. Setzen Sie **Dokumentebene** auf **Nein**.
5. Setzen Sie **Status** auf **Aktiviert**.
6. Setzen Sie **Sichtbarkeit: Community Operator** auf **Ja**.
7. Setzen Sie **Sichtbarkeit: Community Manager** auf **Ja**.
8. Setzen Sie **Sichtbarkeit: Community-Teilnehmer** auf **Ja**.
9. Wählen Sie Folgendes aus:
 - a. Paket: **AS**
 - b. Paket: **None**
 - c. Paket: **Backend Integration**.
10. 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. Geben Sie die folgenden Informationen ein:
 - a. Dokumentenflusstyp: **Dokumentenfluss**
 - b. Code: **XML_Tester**
 - c. Version: **1.0**
 - d. Beschreibung: **XML_Tester**
4. Setzen Sie **Dokumentebene** auf **Ja**.
5. Setzen Sie **Status** auf **Aktiviert**.
6. Setzen Sie **Sichtbarkeit: Community Operator** auf **Ja**.
7. Setzen Sie **Sichtbarkeit: Community Manager** auf **Ja**.
8. Setzen Sie **Sichtbarkeit: Community-Teilnehmer** auf **Ja**.
9. Klicken Sie auf das Ordnersymbol neben **Paket: AS**, und wählen Sie **Protokoll: CustomXML** aus.
10. Klicken Sie auf das Ordnersymbol neben **Paket: None**, und wählen Sie **Protokoll: CustomXML** aus.
11. Klicken Sie auf das Ordnersymbol neben **Paket: Backend Integration**, und wählen Sie **Protokoll: CustomXML** aus.
12. 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. Geben Sie die folgenden Informationen ein:
 - a. Routing-Format: **CustomXML 1.0**
 - b. Dateityp: **XML**
 - c. Kennungstyp: **Root-Tag**
 - d. Wert für Kennungstyp: **Tester**
 - e. Quellengeschäfts-ID: **Elementpfad**
 - f. Wert für Quellengeschäfts-ID: **/Tester/From**
 - g. Zielgeschäfts-ID: **Elementpfad**
 - h. Wert für Zielgeschäfts-ID: **Tester/To**
 - i. Quellendokumentenfluss: **Konstante**
 - j. Wert für Quellendokumentenfluss: **XML_Tester**
 - k. Quellendokumentenflussversion: **Konstante**
 - l. Wert für Quellendokumentenflussversion: **1.0**
4. Klicken Sie auf **Speichern**.

Gültige Interaktion für XML-Dokumente von "XML_Tester" erstellen

Sie verfügen nun über ein neues Protokoll und einen Dokumentenfluss, mit dem Sie eine gültige 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 von **Aktion** die Option **Pass-Through** aus.
7. Klicken Sie auf **Speichern**.

Die B2B-Funktionalität für "partnerEins" 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 Lupensymbol neben **Partner Eins**.
4. Klicken Sie auf **B2B-Funktionalität**.
5. Klicken Sie auf das Aktivierungssymbol unter **Quelle festlegen** für **Paket: None**, um es zu aktivieren.
6. Klicken Sie auf das Aktivierungssymbol unter **Ziel festlegen** für **Paket: None**, um es zu aktivieren.
7. Klicken Sie auf das Ordnersymbol neben **Paket: None**.
8. Klicken Sie auf das Aktivierungssymbol zu **Protokoll: CustomXML (1.0)** für die Quelle und das Ziel.
9. Klicken Sie auf das Ordnersymbol neben **Protokoll: CustomXML (1.0)**.
10. Klicken Sie schließlich auf das Aktivierungssymbol zu **Dokumentenfluss: XML_Tester (1.0)** für die Quelle und das Ziel.

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 Lupensymbol neben **Partner Zwei**.
4. Klicken Sie auf **B2B-Funktionalität**.
5. Klicken Sie auf das Aktivierungssymbol unter **Quelle festlegen** für **Paket: None**, um es zu aktivieren.
6. Klicken Sie auf das Aktivierungssymbol unter **Ziel festlegen** für **Paket: None**, um es zu aktivieren.
7. Klicken Sie auf das Ordnersymbol neben **Paket: None**.
8. Klicken Sie auf das Aktivierungssymbol zu **Protokoll: CustomXML (1.0)** für die Quelle und das Ziel.
9. Klicken Sie auf das Ordnersymbol neben **Protokoll: CustomXML (1.0)**.
10. Klicken Sie schließlich auf das Aktivierungssymbol zu **Dokumentenfluss: XML_Tester (1.0)** für die Quelle und das Ziel.

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 **Partner Eins** 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.

Anhang B. RosettaNet-Austauschvorgänge konfigurieren

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 <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 Business Integration Connect unterstützt RosettaNet-Nachrichtenübertragung mit RNIF 1.1 und 2.0. Wenn der Hub eine PIP-Nachricht empfängt, prüft und wandelt er die Nachricht um, um sie an das entsprechende Back-End-System zu senden. WebSphere Business Integration Connect stellt ein Protokoll für das 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 wurden, 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, die Sie verwenden wollen, bereit.

Neben der Bereitstellung der Routing-Funktion für RosettaNet-Nachrichten verwaltet WebSphere Business Integration Connect 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 übermittelt werden kann. Der Hub kann außerdem automatisch OA1 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 Business Integration Connect zwei Gruppen von ZIP-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

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

Für RNIF V02.00

- 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 Business Integration Connect den PIP handhabt, 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 ZIP-Dateien für 0A1 PIPs verfügen auch über eine XML-Datei, die der Hub als Vorlage zur Erstellung von 0A1-Dokumenten verwendet.

WebSphere Business Integration Connect stellt für die folgenden PIPs PIP-Dokumentenflusspakete bereit:

- PIP 0A1 Notification of Failure v1.0
- PIP 0A1 Notification of Failure V02.00.00
- PIP 2A12 Distribute Product Master V01.03.00
- PIP 3A1 Request Quote V02.00.00
- PIP 3A2 Request Price and Availability R02.01.00B
- PIP 3A4 Request Purchase Order V02.02.00
- PIP 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 Order Update V02.02.00
- PIP 3A8 Request Purchase Order Change V01.02.00
- PIP 3A9 Request Purchase Order Cancellation V01.01.00
- PIP 3B12 Shipping Order Request V01.01
- PIP 3B13 Shipping Order Confirmation Notification V01.01
- PIP 3B18 Shipping Documentation Notification V01.00
- PIP 3B2 Notify of Advance Shipment V01.01.00
- PIP 3C3 Notify of Invoice V01.01.00
- PIP 3C4 Notify of Invoice Reject V01.00.00
- PIP 3C6 Notify of Remittance Advice V01.00.00
- PIP 3C7 Self Billing Invoice Notification V01.00
- 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 Planning Release Forecast Notification V02.00
- PIP 4A5 Notify of Forecast Reply V02.00.00
- PIP 4B2 Notify of Shipment Receipt V01.00.00
- PIP 4C1 Distribute Inventory Report V02.03.00
- PIP 4C1 Inventory Report Notification V02.01
- PIP 5C1 Distribute Product List V01.00.00
- PIP 5C4 Distribute Registration Status V01.02.00
- PIP 5D1 Request Ship From Stock And Debit Authorization V01.00.00

- PIP 7B1 Distribute Work in Process V01.00.00
- PIP 7B5 Notify of Manufacturing Work Order V01.00
- PIP 7B6 Notify of Manufacturing Work OrderReply V01.00

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, so dass Sie erkennen können, ob das Paket für Nachrichten zwischen WebSphere Business Integration Connect und Teilnehmern oder zwischen WebSphere Business Integration Connect 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 Business Integration Connect 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 Business Integration Connect 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 Prüfen der Dokumente für Version 02.02 des 3A4 PIP, die zwischen Teilnehmern und WebSphere Business Integration Connect 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*.

RosettaNet-Unterstützung konfigurieren

Für die RosettaNet-Nachrichtenübermittlung benötigt WebSphere Business Integration Connect die RNIF-Pakete für die Version von RNIF, mit der die Nachrichten gesendet werden. Für jeden PIP, den Business Integration Connect unterstützt, benötigt es die zwei PIP-Dokumentenflusspakete des PIP für die RNIF-Version. Business Integration Connect 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 Business Integration Connect für das Übergeben von 3A4-Nachrichten zwischen Teilnehmern und Back-End-Systemen mit RNIF 2.0.

Gehen Sie wie folgt vor, um die RosettaNet-Nachrichtenübermittlung zu unterstützen:

1. Wenn Business Integration Connect die RNIF-Pakete nicht für die RNIF-Version, die Sie verwenden wollen, geladen hat, importieren Sie diese. Informationen zum Importieren der Pakete in Business Integration Connect finden Sie in „RNIF-Pakete hochladen“ auf Seite 40.
2. Laden Sie für jeden PIP, den Sie unterstützen wollen, das PIP-Dokumentenflusspaket für den PIP und für die unterstützte RNIF-Version hoch. Informationen zur Konvention, die zum Benennen dieser Pakete verwendet wird, finden Sie in „RNIF- und PIP-Dokumentenflusspakete“ auf Seite 99. Wenn Business Integration Connect 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 108.

Verbindungen zu Teilnehmern erstellen

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

Bevor Sie beginnen, stellen Sie sicher, dass die folgenden Bedingungen zutreffen:

- Sie sind als Hubadmin angemeldet.
- Die entsprechenden RNIF-Dokumentenflussdefinitionen wurden hochgeladen und die Pakete für den PIP, den Sie verwenden wollen, wurden hochgeladen. Die Namen für diese Pakete finden Sie in „RosettaNet-Unterstützung konfigurieren“ auf Seite 101.

Gehen Sie wie folgt vor, um eine Verbindung für einen bestimmten PIP zu erstellen:

1. Erstellen Sie die Interaktion für die Verbindung:
 - a. Klicken Sie auf **Hubadmin > Hubkonfiguration > Dokumentenflussdefinition**.
 - b. Klicken Sie auf **Interaktionen verwalten**.
 - c. Klicken Sie auf **Interaktion erstellen**.
 - d. Erweitern Sie die Quellenbaumstruktur der Dokumentenflussdefinition auf die Ebene **Aktion**, und erweitern Sie die Zielbaumstruktur der Dokumentenflussdefinition auf die Ebene **Aktion**.
 - e. 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 in den Baumstrukturen aus:

Tabelle 1. 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 in den Baumstrukturen aus:

Tabelle 2. 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 3. 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 4. 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)
Aktivität: Request Purchase Order	Aktivität: Request Purchase Order
Aktion: Purchase Order Request Action	Aktion: Purchase Order Request Action

- f. Wählen Sie im Feld **Aktion** den Eintrag **Bidirektionale Übersetzung von RosettaNet und RosettaNet-Service-Content mit Prüfung** aus.
- g. Klicken Sie auf **Speichern**.
- h. Wenn Sie einen Doppelaktions-PIP konfigurieren, wiederholen Sie die Schritte c bis g, 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 5. 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 6. 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

2. Wenn ein Teilnehmerprofil für den Teilnehmer nicht vorhanden ist, erstellen Sie eines. Informationen darüber, wie Sie dies ausführen, finden Sie in „Teilnehmer erstellen“ auf Seite 51. Es muss ebenfalls ein Teilnehmerprofil des Typs **Community Manager** für das Back-End-System vorhanden sein.
3. Wenn ein Gateway mit dem unterstützten Protokoll nicht zwischen dem Teilnehmer und Business Integration Connect bzw. zwischen einem Back-End-System und Business Integration Connect vorhanden ist, erstellen Sie eines. Informationen darüber, wie Sie dies ausführen, finden Sie in „Gateways erstellen“ auf Seite 52. Die unterstützten Protokolle für RosettaNet-Nachrichten zwischen einem Teilnehmer und Business Integration Connect sind HTTP und HTTPS. Die unterstützten Protokolle für RosettaNet-Nachrichten zwischen einem Back-End-System und Business Integration Connect sind HTTP, HTTPS und JMS.
4. Aktivieren Sie die Dokumentenflussdefinitionen, die Business Integration Connect verwendet, um den PIP zu verarbeiten. Aktivieren Sie hierzu die Definitionen des Teilnehmers und des Back-End-Systems für das Paket, das Protokoll und den Dokumentenfluss für den PIP. Die Richtung der Nachricht bestimmt die Quelle und das Ziel. Business Integration Connect aktiviert automatisch die Aktivität, Aktionen und Signale, wenn Sie den übergeordneten Dokumentenfluss aktivieren. Informationen dazu, wie Sie Dokumentenflussdefinitionen aktivieren, finden Sie in „B2B-Funktionalität konfigurieren“ auf Seite 60.

Teilnehmer

- Paket: RNIF (1.1 oder V02.00, abhängig davon, welche RNIF-Version Sie verwenden)
- Protokoll: RosettaNet (1.1 oder V02.00, abhängig davon, welche RNIF-Version Sie verwenden)
- Dokumentenflüsse: <PIP-Name und -Version>

Back-End-System

- Paket: Backend Integration (1.0)
- Protokoll: RNSC (1.0)
- Dokumentenflüsse: <PIP-Name und -Version>

5. Aktivieren Sie die Verbindung, indem Sie die Quelle und das Ziel in der Anzeige **Teilnehmerverbindungen** konfigurieren. Wenn der Teilnehmer der Initiator des PIP ist, legen Sie das Profil des Teilnehmers als Quelle und das Community Manager-Profil als Ziel fest. Wenn das Back-End-System der Initiator

ist, legen Sie das Community Manager-Profil als Quelle und das Teilnehmerprofil als Ziel fest. Informationen dazu, wie Sie nach Verbindungen suchen und diese aktivieren, finden Sie in „Interaktionen erstellen“ auf Seite 48. Wenn der PIP ein Doppelaktions-PIP ist, müssen Sie auch die Verbindung in die andere Richtung aktivieren, 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.

6. Wenn in Business Integration Connect kein Ziel für jedes der Protokolle definiert ist, dann erstellen Sie es. Informationen darüber, wie Sie dies ausführen, finden Sie in „Ziele konfigurieren“ auf Seite 32.

RosettaNet-Attributwerte bearbeiten

Zur RosettaNet-Unterstützung verfügt die Dokumentenflussdefinition des Typs **Aktion** über eine spezifische Gruppe von Attributen. Diese Attribute stellen Informationen bereit, mit denen die PIP-Nachricht geprüft wird, um die im PIP verwendeten Rollen und Services sowie die Antwort auf die Aktion zu definieren. Die PIP-Pakete, die von Business Integration Connect bereitgestellt werden, definieren automatisch Werte für diese Attribute und Sie müssen diese in der Regel nicht ändern.

Gehen Sie wie folgt vor, um die RosettaNet-Attribute einer Dokumentenflussdefinition des Typs **Aktion** zu bearbeiten:

1. Klicken Sie auf **Hubadmin > Hubkonfiguration > Dokumentenflussdefinition**.
2. Klicken Sie auf Ordnersymbole, um einen Knoten individuell zur entsprechenden Dokumentenflussdefinitionsebene zu erweitern, oder wählen Sie **Alle** aus, um die gesamte Baumstruktur zu erweitern.
3. Die Spalte **Aktionen** enthält für jede Dokumentenflussdefinition des Typs **Aktion** ein RosettaNet-Attributsymbol. Klicken Sie auf dieses Symbol, um die RosettaNet-Attribute der Aktion zu bearbeiten. Die Konsole 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 7. 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.
Empfängerrolle	Enthält den Rollennamen des Teilnehmers oder Back-End-Systems, der bzw. das die Nachricht empfängt.
Root-Tag	Enthält den Namen des Rootelements im XML-Dokument der PIP-Nachricht.
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 Funktionalität der Dokumentenflussdefinition.
6. Klicken Sie auf **Speichern**.

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 Business Integration Connect 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 OKB 200 wird an den Teilnehmer zurückgegeben.

Wenn Sie die Attribute mit dem Dokumentenflussdefinitions-kontext setzen wollen, führen Sie Folgendes aus.

1. Klicken Sie auf **Hubadmin > Hubkonfiguration > Dokumentenflussdefinition**.

2. Klicken Sie auf Ordnersymbole, um einen Knoten individuell zur entsprechenden Dokumentenflussdefinitionsebene zu erweitern, oder wählen Sie **Alle** aus, um alle angezeigten Dokumentenflussdefinitionsknoten zu erweitern.
3. Klicken Sie in der Spalte **Aktionen** auf das Symbol zum Bearbeiten von Attributwerten für das Paket, das Sie bearbeiten wollen, wie z. B. **Paket: RNIF (1.1)** oder **Paket: RNIF (V02.00)**.
4. Gehen Sie im Abschnitt **Attribute für Dokumentenflusskontexte** in die Spalte **Aktualisieren** des Attributs, das Sie setzen wollen, und wählen Sie den neuen Wert im Aktualisierungsfeld aus bzw. geben Sie ihn dort ein. Wiederholen Sie dies für jedes Attribut, das Sie setzen wollen.
5. Klicken Sie auf **Speichern**.

Wenn Sie den Wert der Attribute für jede Verbindung setzen wollen, gehen Sie wie folgt vor:

1. Klicken Sie auf **Kontenadmin > Teilnehmerverbindungen**.
2. Wählen Sie die Quelle und das Ziel der zu ändernden Verbindung aus, und klicken Sie dann auf **Suchen**.
3. Die Konsole zeigt eine Liste der Verbindungen an, die mit den Suchkriterien für die Quelle und das Ziel übereinstimmen. Jede Verbindung zeigt zwei Gruppen von Dokumentenflussdefinitionen (Quelle und Ziel) und eine Gruppe von Schaltflächen, einschließlich zweier Schaltflächen **Attribute**. Zum Bearbeiten der Dokumentenflussdefinitionsattribute klicken Sie auf die Schaltfläche **Attribute**, die der Quelle bzw. dem Ziel, die bzw. das Sie bearbeiten wollen, am nächsten ist.
4. Erweitern Sie im Fenster **Verbindungsattribute** den Knoten **Package**.
5. Gehen Sie in die Spalte **Aktualisieren** des Attributs, das Sie setzen wollen, und wählen Sie den neuen Wert im Aktualisierungsfeld aus bzw. geben Sie ihn dort ein. Wiederholen Sie dies für jedes Attribut, das Sie setzen wollen.
6. Klicken Sie auf **Speichern**.

PIPs inaktivieren

Nachdem ein PIP-Paket in Business Integration Connect hochgeladen wurde, kann es nicht mehr entfernt werden. Sie können jedoch den PIP inaktivieren, so dass er nicht mehr verwendet werden kann.

Gehen Sie wie folgt vor, um ein PIP für die Kommunikation mit allen Teilnehmern zu inaktivieren:

1. Klicken Sie auf **Hubadmin > Hubkonfiguration > Dokumentenflussdefinition**.
2. Erweitern Sie die Baumstruktur der Dokumentenflussdefinitionen, um die Dokumentenflussdefinition 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 Business Integration Connect 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

Wenn ein Fehler während der Verarbeitung einer PIP-Nachricht auftritt, verwendet Business Integration Connect 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. Business Integration Connect verarbeitet die RNSC-Nachricht und sendet eine RosettaNet-Nachricht an einen Teilnehmer. Business Integration Connect wartet auf die Antwort auf die RosettaNet-Nachricht, bis die Wartezeit das Zeitlimit erreicht. Sobald dieses erreicht ist, erstellt Business Integration Connect 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 `<install_root>/wbic/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 Rufnummern sind auf eine Länge von 30 Byte begrenzt. Die übrigen Felder sind ohne Längenbegrenzung. Wenn sie geändert werden, muss der Router erneut gestartet werden.

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 angegebenen Stellen, wie das PIP-Dokumentenflusspaket für PIP 5C4 V01.03.00 erstellt wird. Business Integration Connect stellt ein PIP-Dokumentenflusspaket für PIP 5C4 V01.02.00 bereit, so dass die Prozeduren tatsächlich dokumentieren, 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 119.

Gehen Sie wie folgt vor, 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. 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:

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

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 basierend auf einer anderen Version des Pakets aktualisieren, und Sie eine Definition von der anderen Version wiederverwenden wollen, führen Sie für jede dieser Definitionen Folgendes 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_EmailAddress_R"
      minOccurs="0"/>
    <xsd:element name="facsimileNumber"
      type="common_CommunicationsNumber_R" minOccurs="0"/>
    <xsd:element name="PhysicalLocation"
      type="PhysicalLocation_type1" minOccurs="0" />
    <xsd:element name="telephoneNumber"
      type="common_CommunicationsNumber_R minOccurs="0" />
  </xsd:sequence>
</xsd:complexType>
```

- d. 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 Folgendes 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 Folgendes für jedes Exemplar 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 Folgendes hinzu:

```
name="ContactInformation
type="ContactInformation_localType1"
```

Element **productProviderFieldApplicationEngineer** vor der Modifikation

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

Element **productProviderFieldApplicationEngineer** nach der Modifikation

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

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). **GlobalRegistrationComplexityLevelCode** verfügt über die folgende Tabelle:

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

Daher kann in einer PIP 5C4 V01.03.00-Nachricht **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 für jede dieser Gruppen Folgendes 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** (Entitätsexemplare) 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:restriction>
</xsd:simpleType>
```

```

        <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 Folgendes 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 Folgendes 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 Folgendes hinzu:

```

name="GlobalRegistrationComplexityLevelCode"
type="GlobalRegistrationComplexityLevelCode_localType"

```

Element **DesignAssemblyInformation** vor der Modifikation

```

<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:sequence>
    </xsd:complexType>
</xsd:element>

```

```

<xsd:element maxOccurs="1" minOccurs="0"
  ref="GlobalRegistrationComplexityLevelCode"/>
<xsd:element maxOccurs="1" minOccurs="0"
  ref="GlobalRegistrationInvolvementLevelCode"/>
<xsd:element maxOccurs="1" minOccurs="0"
  ref="RegistrationStatus"/>
</xsd:sequence>
</xsd:complexType>
</xsd:element>

```

Element **DesignAssemblyInformation** nach der Modifikation

```

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

      <xsd:element maxOccurs="1" minOccurs="0"
        ref="GlobalRegistrationInvolvementLevelCode"/>
      <xsd:element maxOccurs="1" minOccurs="0"
        ref="RegistrationStatus"/>
    </xsd:sequence>
  </xsd:complexType>
</xsd:element>

```

5. 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, wie in der folgenden Abbildung dargestellt:

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

- 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 für jede Gruppe Folgendes aus:
- a. Löschen Sie die Definition für das Datenentitätselement. Löschen Sie z. B. das Element **DateStamp** (Datumszeitmarke):
 - 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 Folgendes 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 Folgendes 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 Folgendes hinzu:

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

Element **beginDate** vor der Modifikation

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

Element **beginDate** nach der Modifikation

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

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. jeweils `BCG_RNIFV02.00_5C4V01.03.zip` und `BCG_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, wie 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, wie z. B. `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 können, stellen Sie daher sicher, dass Sie alle Exemplare aktualisieren.

Tabelle 8. 5C4 PIP-Aktualisierungsinformationen

Zu ändernde Informationen	Alter Wert	Neuer Wert
PIP-ID	5C4	5C4
PIP-Version	V01.02	V01.03
Der Name der Anforderungsnachrichtent-DTD-Datei ohne Dateierweiterung	5C4_MS_V01_02_RegistrationStatusNotification	5C4_MS_V01_03_RegistrationStatusNotification
Der Name der Bestätigungsnachrichtent-DTD-Datei ohne Dateierweiterung (nur für Doppelaktions-PIPs)	N/A	N/A
Der Name der Anforderungsnachrichtent-XSD-Datei ohne Dateierweiterung	BCG_5C4RegistrationStatusNotification_V01.02	BCG_5C4RegistrationStatusNotification_V01.03
Der Name der Bestätigungsnachrichtent-XSD-Datei ohne Dateierweiterung (nur für Doppelaktions-PIPs)	N/A	N/A
Rootelementname in der XSD-Datei für die Anforderungsnachricht	Pip5C4RegistrationStatusNotification	Pip5C4RegistrationStatusNotification
Rootelementname in der XSD-Datei für die Bestätigungsnachricht (nur für Doppelaktions-PIPs)	N/A	N/A

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 9. 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/A

- 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.

Tabelle 10. 5C4 PIP-Attributaktualisierungen

Zu aktualisierende Informationen	Beschreibung	Wert im 5C4-Paket	Elementpfad in der XML-Datei
NonRepudiationRequired	Angegeben in Tabelle 3-3	N	ns1:Package ns1:Protocol ns1:Process ns1:Attribute (sein ATTRIBUTEKEY ist NonRepudiationRequired) ns1:AttributeValue AttributePickListItem ATTRVALUEKEY
NonRepudiationOfReceipt	Angegeben in Tabelle 3-3	N	ns1:Package ns1:Protocol ns1:Process ns1:Attribute (sein ATTRIBUTEKEY ist NonRepudiationOfReceipt) ns1:AttributeValue AttributePickListItem ATTRVALUEKEY
DigitalSignatureRequired	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
TimeToPerform	Angegeben in Tabelle 3-3	2 (120 min)	ns1:Package ns1:Protocol ns1:Process ns1:Attribute (sein ATTRIBUTEKEY ist TimeToPerform) ns1:AttributeValue ATTRVALUE

Tabelle 10. 5C4 PIP-Attributaktualisierungen (Forts.)

RetryCount	Angegeben in Tabelle 3-3	3	ns1:Package ns1:Protocol ns1:Process ns1:Attribute (sein ATTRIBUTEKEY ist RetryCount) ns1:AttributeValue ATTRVALUE
------------	-----------------------------	---	--

- 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, wie im folgenden Beispiel für `BCG_common.xsd` gezeigt wird.

Um das Paket **Backend Integration** zu erstellen, wiederholen Sie die oben aufgeführte Prozedur, mit Ausnahme der folgenden Unterschiede:

- Extrahieren Sie in Schritt 1 die XML-Datei aus dem Paket **Backend Integration**, wie z. B. `BCG_Package_RNSC1.0_RNIFV02.00_5C4V01.02.zip`.
- Führen Sie Schritt 5 nicht aus.

Nachdem Sie die XML- und XSD-Dateien erstellt haben, können Sie die PIP-Dokumentenflusspakete erstellen.

Das Paket erstellen

Gehen Sie wie folgt vor, um das RNIF-Paket zu erstellen:

- Erstellen Sie ein Verzeichnis `GuidelineMaps`, und kopieren Sie die XSD-Dateien des Pakets in dieses Verzeichnis.
- Erstellen Sie ein Verzeichnis `Packages`, und kopieren Sie die RNIF-XML-Datei in dieses Verzeichnis.
- 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 oben aufgeführte Prozedur 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-Pakete hochladen** beschriebenen Prozedur hochladen.

Informationen zur Validierung

Business Integration Connect prüft den Serviceinhalt einer RosettaNet-Nachricht mit 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 Business Integration Connect 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 108 Informationen zu den Schritten, die zum Upgraden der XSD-Dateien nötig sind, mit denen die Nachrichten geprüft 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 Business Integration Connect nicht die Kardinalität eines Elements überprüfen muss, sind die Werte für die Attribute **minOccurs** und **maxOccurs** des Elements in den Validierungszuordnungen jeweils 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 **_GlobalLocationIdentifier** 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 Validierungs-zuordnungen verfügt der Typ des Elements über mindestens eine Aufzählungs-einschränkung, 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 Wert haben.

Inhalt der PIP-Dokumentenflusspakete

Die folgenden Tabelle zeigt die PIP-Dokumentenflusspakete, die von Business Integration Connect 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.

Tabelle 11. Inhalt der PIP-Dokumentenflusspakete

ZIP-Dateiname des Pakets	Paketinhalt	Inhalt von GuidelineMaps
PIP 2A12 Distribute Product Master		
BCG_Package_ RNIF1.1_2A12V01.03.zip	BCG_RNIF1.1_2A12V01.03.xml	BCG_2A12ProductMaster Notification_V01.03.xsd BCG_common.xsd BCG_ContactInformation_Types.xsd BCG_PhysicalAddress_Types.xsd BCG_PartnerDescription_Types.xsd BCG_GlobalAssemblyLevelCode.xsd BCG_GlobalIntervalCode.xsd BCG_GlobalLeadTimeClassification Code.xsd BCG_GlobalPartnerRoleClassification Code.xsd
BCG_Package_ RNIFV02.00_2A12V01.03.zip	BCG_RNIFV02.00_ 2A12V01.03.xml	BCG_GlobalProductUnitOfMeasure Code.xsd BCG_GlobalProductLifeCycleStatus Code.xsd BCG_GlobalProductProcurementType Code.xsd
BCG_Package_RNSC1.0_ RNIF1.1_2A12V01.03.zip	BCG_RNSC1.0_ RNIF1.1_2A12V01.03.xml	BCG_BusinessDescription_Types.xsd BCG_BusinessTaxIdentifier_Types.xsd BCG_GlobalCountryCode.xsd BCG_GlobalPartnerClassificationCode.xsd BCG_string_len_0.xsd BCG_xml.xsd
BCG_Package_RNSC1.0_ RNIFV02.00_2A12V01.03.zip	BCG_RNSC1.0_ RNIFV02.00_2A12V01.03.xml	
PIP 3A1 Request Quote		
BCG_Package_ RNIF1.1_3A1V02.00.zip	BCG_RNIF1.1_3A1V02.00.xml	BCG_3A1QuoteConfirmation_V02.00.xsd BCG_3A1QuoteRequest_V02.00.xsd BCG_common.xsd BCG_ContactInformation_Types.xsd BCG_PhysicalAddress_Types.xsd BCG_PartnerDescription_Types.xsd BCG_GlobalCurrencyCode.xsd
BCG_Package_ RNIFV02.00_3A1V02.00.zip	BCG_RNIFV02.00_3A1V02.00.xml	BCG_GlobalGovernmentPriorityRating Code.xsd BCG_GlobalMonetaryAmountType Code.xsd BCG_GlobalPartnerRoleClassification Code.xsd BCG_GlobalProductUnitOfMeasure Code.xsd
BCG_Package_RNSC1.0_ RNIF1.1_3A1V02.00.zip	BCG_RNSC1.0_ RNIF1.1_3A1V02.00.xml	BCG_GlobalQuoteTypeCode.xsd BCG_GlobalStockIndicatorCode.xsd BCG_GlobalTaxExemptionCode.xsd BCG_BusinessTaxIdentifier_Types.xsd BCG_GlobalProductSubstitutionReason Code.xsd
BCG_Package_RNSC1.0_ RNIFV02.00_3A1V02.00.zip	BCG_RNSC1.0_ RNIFV02.00_3A1V02.00.xml	BCG_GlobalProductTermsCode.xsd BCG_GlobalQuoteLineItemStatusCode.xsd BCG_BusinessDescription_Types.xsd BCG_GlobalCountryCode.xsd BCG_GlobalPartnerClassificationCode.xsd BCG_string_len_0.xsd BCG_xml.xsd

Tabelle 11. Inhalt der PIP-Dokumentenflusspakete (Forts.)

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

Tabelle 11. Inhalt der PIP-Dokumentenflusspakete (Forts.)

PIP 3A4 Request Purchase Order		
BCG_Package_ RNIF1.1_3A4V02.02.zip	BCG_RNIF1.1_3A4V02.02.xml	BCG_3A4PurchaseOrder Confirmation_V02.02.xsd BCG_3A4PurchaseOrder Request_V02.02.xsd BCG_common.xsd BCG_ContactInformation_Types.xsd BCG_PhysicalAddress_Types.xsd BCG_PartnerDescription_Types.xsd BCG_BusinessTaxIdentifier_Types.xsd BCG_GlobalCountryCode.xsd BCG_GlobalCurrencyCode.xsd BCG_GlobalAccountClassificationCode.xsd
BCG_Package_ RNIFV02.00_3A4V02.02.zip	BCG_RNIFV02.00_3A4V02.02.xml	BCG_GlobalCreditCardClassification Code.xsd BCG_GlobalDocumentReferenceType Code.xsd BCG_GlobalFinanceTermsCode.xsd BCG_GlobalGovernmentPriorityRating Code.xsd BCG_GlobalMonetaryAmountType Code.xsd BCG_GlobalPartnerRoleClassification Code.xsd BCG_GlobalPaymentConditionCode.xsd
BCG_Package_RNSC1.0_ RNIF1.1_3A4V02.02.zip	BCG_RNSC1.0_ RNIF1.1_3A4V02.02.xml	BCG_GlobalProductUnitOfMeasure Code.xsd BCG_GlobalPriceUnitOfMeasureCode.xsd BCG_GlobalPurchaseOrderFillPriority Code.xsd BCG_GlobalPurchaseOrderTypeCode.xsd BCG_GlobalShipmentTermsCode.xsd BCG_GlobalShippingServiceLevelCode.xsd BCG_GlobalSpecialFulfillmentRequest Code.xsd BCG_GlobalSpecialHandlingCode.xsd
BCG_Package_RNSC1.0_ RNIFV02.00_3A4V02.02.zip	BCG_RNSC1.0_ RNIFV02.00_3A4V02.02.xml	BCG_InvoiceChargeTypeCode.xsd BCG_GlobalTaxExemptionCode.xsd BCG_GlobalConfirmationTypeCode.xsd BCG_GlobalProductSubstitutionReason Code.xsd BCG_GlobalPurchaseOrder AcknowledgmentReasonCode.xsd BCG_GlobalPurchaseOrderStatusCode.xsd BCG_BusinessDescription_Types.xsd BCG_GlobalPartnerClassificationCode.xsd BCG_string_len_0.xsd BCG_xml.xsd

Tabelle 11. Inhalt der PIP-Dokumentenflusspakete (Forts.)

PIP 3A4PurchaseOrderRequest		
BCG_Package_ RNIF1.1_3A4V02.00.zip	BCG_RNIF1.1_3A4V02.00.xml	BCG_3A4PurchaseOrder Request_V02.00.xsd BCG_3A4PurchaseOrder Confirmation_V02.00.xsd BCG_common_V422.xsd BCG_ContactInformation_Types.xsd BCG_PhysicalAddress_Types.xsd BCG_PhysicalAddress_Types_V422.xsd BCG_PartnerDescription_Types.xsd BCG_BusinessTaxIdentifier_Types.xsd BCG_GlobalCountryCode.xsd BCG_GlobalCurrencyCode.xsd BCG_GlobalAccountClassificationCode.xsd BCG_GlobalCreditCardClassification Code.xsd
BCG_Package_ RNIFV02.00_3A4V02.00.zip	BCG_RNIFV02.00_3A4V02.00.xml	BCG_GlobalDocumentReferenceType Code.xsd BCG_GlobalDocumentReferenceType Code_V422.xsd BCG_GlobalFinanceTermsCode.xsd BCG_GlobalGovernmentPriorityRating Code.xsd BCG_GlobalMonetaryAmountType Code.xsd BCG_GlobalPartnerRoleClassification Code_V422.xsd BCG_GlobalPaymentConditionCode.xsd BCG_GlobalProductUnitOfMeasure Code.xsd
BCG_Package_RNSC1.0_ RNIF1.1_3A4V02.00.zip	BCG_RNSC1.0_ RNIF1.1_3A4V02.00.xml	BCG_GlobalPriceUnitOfMeasureCode.xsd BCG_GlobalPurchaseOrderFillPriority Code.xsd BCG_GlobalPurchaseOrderTypeCode.xsd BCG_GlobalShipmentTermsCode.xsd BCG_GlobalShipmentTermsCode_V422.xsd BCG_GlobalShippingServiceLevelCode.xsd BCG_GlobalSpecialFulfillmentRequest Code.xsd BCG_InvoiceChargeTypeCode.xsd BCG_GlobalTaxExemptionCode.xsd BCG_GlobalTaxExemptionCode_V422.xsd
BCG_Package_RNSC1.0_ RNIFV02.00_3A4V02.00.zip	BCG_RNSC1.0_ RNIFV02.00_3A4V02.00.xml	BCG_GlobalSpecialHandling Code_V422.xsd BCG_BusinessDescription_Types.xsd BCG_BusinessDescription_Types_V422.xsd BCG_GlobalConfirmationTypeCode.xsd BCG_GlobalProductSubstitutionReason Code.xsd BCG_GlobalPurchaseOrder AcknowledgmentReasonCode.xsd BCG_GlobalPurchaseOrderStatusCode.xsd BCG_common.xsd BCG_GlobalPartnerClassificationCode.xsd BCG_string_len_0.xsd BCG_xml.xsd

Tabelle 11. Inhalt der PIP-Dokumentenflusspakete (Forts.)

PIP 3A5 Query Order Status		
BCG_Package_ RNIF1.1_3A5R02.00.zip	BCG_RNIF1.1_3A5R02.00.xml	BCG_3A5PurchaseOrderStatus Query_R02.00.xsd BCG_3A5PurchaseOrderStatus Response_R02.00.xsd BCG_common.xsd BCG_ContactInformation_Types.xsd BCG_PhysicalAddress_Types.xsd BCG_PartnerDescription_Types.xsd BCG_BusinessTaxIdentifier_Types.xsd BCG_GlobalCreditCardClassification Code.xsd BCG_GlobalAccountClassification Code.xsd
BCG_Package_ RNIFV02.00_3A5R02.00.zip	BCG_RNIFV02.00_3A5R02.00.xml	BCG_GlobalDocumentReferenceType Code.xsd BCG_GlobalFinanceTermsCode.xsd BCG_GlobalGovernmentPriorityRating Code.xsd BCG_GlobalPurchaseOrder AcknowledgmentReasonCode.xsd BCG_GlobalPurchaseOrderStatus Code.xsd BCG_GlobalShippingServiceLevel Code.xsd BCG_GlobalSpecialFulfillmentRequest Code.xsd
BCG_Package_RNSC1.0_ RNIF1.1_3A5R02.00.zip	BCG_RNSC1.0_ RNIF1.1_3A5R02.00.xml	BCG_GlobalSpecialHandlingCode.xsd BCG_GlobalLineItemStatusCode.xsd BCG_GlobalProductUnitOfMeasure Code.xsd BCG_GlobalOrderQuantityTypeCode.xsd BCG_GlobalPartnerClassificationCode.xsd BCG_GlobalCurrencyCode.xsd BCG_GlobalProductSubstitutionReason Code.xsd BCG_GlobalTaxExemptionCode.xsd BCG_GlobalPartnerRoleClassification Code.xsd
BCG_Package_RNSC1.0_ RNIFV02.00_3A5R02.00.zip	BCG_RNSC1.0_ RNIFV02.00_3A5R02.00.xml	BCG_GlobalPurchaseOrderFillPriority Code.xsd BCG_GlobalPurchaseOrderTypeCode.xsd BCG_GlobalShipmentTermsCode.xsd BCG_GlobalFreeOnBoardCode.xsd BCG_GlobalTransportEventCode.xsd BCG_GlobalCustomerTypeCode.xsd BCG_BusinessDescription_Types.xsd BCG_GlobalCountryCode.xsd BCG_string_len_0.xsd BCG_xml.xsd

Tabelle 11. Inhalt der PIP-Dokumentenflusspakete (Forts.)

PIP 3A6 Distribute Order Status		
BCG_Package_ RNIF1.1_3A6V02.02.zip	BCG_RNIF1.1_3A6V02.02.xml	BCG_3A6PurchaseOrderStatus Notification_V02.02.xsd BCG_common.xsd BCG_ContactInformation_Types.xsd BCG_PhysicalAddress_Types.xsd BCG_PartnerDescription_Types.xsd BCG_BusinessTaxIdentifier_Types.xsd BCG_GlobalCountryCode.xsd BCG_GlobalCurrencyCode.xsd BCG_GlobalAccountClassificationCode.xsd BCG_GlobalCreditCardClassification Code.xsd
BCG_Package_ RNIFV02.00_3A6V02.02.zip	BCG_RNIFV02.00_3A6V02.02.xml	BCG_GlobalDocumentReferenceType Code.xsd BCG_GlobalFinanceTermsCode.xsd BCG_GlobalGovernmentPriorityRating Code.xsd BCG_GlobalMonetaryAmountType Code.xsd BCG_GlobalLineItemStatusCode.xsd BCG_GlobalNotificationReasonCode.xsd BCG_GlobalOrderQuantityTypeCode.xsd BCG_GlobalPartnerRoleClassification Code.xsd BCG_GlobalPaymentConditionCode.xsd BCG_GlobalPriceUnitOfMeasureCode.xsd BCG_GlobalProductUnitOfMeasure Code.xsd BCG_GlobalProductSubstitutionReason Code.xsd BCG_GlobalPurchaseOrderFillPriority Code.xsd BCG_GlobalPurchaseOrder AcknowledgmentReasonCode.xsd BCG_GlobalPurchaseOrderStatusCode.xsd BCG_GlobalPurchaseOrderTypeCode.xsd BCG_GlobalShipmentTermsCode.xsd BCG_GlobalShippingServiceLevelCode.xsd BCG_GlobalSpecialFulfillmentRequest Code.xsd BCG_GlobalSpecialHandlingCode.xsd BCG_GlobalTrackingReferenceType Code.xsd BCG_InvoiceChargeTypeCode.xsd BCG_GlobalTaxExemptionCode.xsd BCG_BusinessDescription_Types.xsd BCG_GlobalPartnerClassificationCode.xsd BCG_string_len_0.xsd BCG_xml.xsd
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	

Tabelle 11. Inhalt der PIP-Dokumentenflusspakete (Forts.)

PIP 3A7 Notify of Purchase

Order Update

BCG_Package_ RNIF1.1_3A7V02.02.zip	BCG_RNIF1.1_3A7V02.02.xml	BCG_3A7PurchaseOrderUpdate Notification_V02.02.xsd BCG_common.xsd BCG_string_len_0.xsd BCG_ContactInformation_Types.xsd BCG_PhysicalAddress_Types.xsd BCG_PartnerDescription_Types.xsd BCG_BusinessTaxIdentifier_Types.xsd BCG_GlobalActionCode.xsd BCG_GlobalCountryCode.xsd BCG_GlobalCurrencyCode.xsd BCG_GlobalAccountClassificationCode.xsd
BCG_Package_ RNIFV02.00_3A7V02.02.zip	BCG_RNIFV02.00_3A7V02.02.xml	BCG_GlobalConfirmationTypeCode.xsd BCG_GlobalCreditCardClassification Code.xsd BCG_GlobalDocumentReferenceType Code.xsd BCG_GlobalFinanceTermsCode.xsd BCG_GlobalGovernmentPriorityRating Code.xsd BCG_GlobalMonetaryAmountType Code.xsd BCG_GlobalPartnerRoleClassification Code.xsd
BCG_Package_RNSC1.0_ RNIF1.1_3A7V02.02.zip	BCG_RNSC1.0_ RNIF1.1_3A7V02.02.xml	BCG_GlobalPaymentConditionCode.xsd BCG_GlobalProductUnitOfMeasure Code.xsd BCG_GlobalProductSubstitutionReason Code.xsd BCG_GlobalPriceUnitOfMeasureCode.xsd BCG_GlobalPurchaseOrderFillPriority Code.xsd BCG_GlobalPurchaseOrder AcknowledgmentReasonCode.xsd
BCG_Package_RNSC1.0_ RNIFV02.00_3A7V02.02.zip	BCG_RNSC1.0_ RNIFV02.00_3A7V02.02.xml	BCG_GlobalPurchaseOrderStatusCode.xsd BCG_GlobalPurchaseOrderTypeCode.xsd BCG_GlobalShipmentTermsCode.xsd BCG_GlobalShippingServiceLevelCode.xsd BCG_GlobalSpecialFulfillmentRequest Code.xsd BCG_GlobalSpecialHandlingCode.xsd BCG_InvoiceChargeTypeCode.xsd BCG_GlobalTaxExemptionCode.xsd BCG_BusinessDescription_Types.xsd BCG_GlobalPartnerClassificationCode.xsd BCG_xml.xsd

Tabelle 11. Inhalt der PIP-Dokumentenflusspakete (Forts.)

PIP 3A8 Request Purchase Order Change		
BCG_Package_ RNIF1.1_3A8V01.02.zip	BCG_RNIF1.1_3A8V01.02.xml	BCG_3A8PurchaseOrderChange Confirmation_V01.02.xsd BCG_3A8PurchaseOrderChange Request_V01.02.xsd BCG_common.xsd BCG_ContactInformation_Types.xsd BCG_PhysicalAddress_Types.xsd BCG_PartnerDescription_Types.xsd BCG_BusinessTaxIdentifier_Types.xsd BCG_GlobalCountryCode.xsd BCG_GlobalCurrencyCode.xsd BCG_GlobalActionCode.xsd
BCG_Package_ RNIFV02.00_3A8V01.02.zip	BCG_RNIFV02.00_3A8V01.02.xml	BCG_GlobalAccountClassificationCode.xsd BCG_GlobalCreditCardClassification Code.xsd BCG_GlobalDocumentReferenceType Code.xsd BCG_GlobalFinanceTermsCode.xsd BCG_GlobalGovernmentPriorityRating Code.xsd BCG_GlobalMonetaryAmountType Code.xsd BCG_GlobalPartnerRoleClassification Code.xsd
BCG_Package_RNSC1.0_ RNIF1.1_3A8V01.02.zip	BCG_RNSC1.0_ RNIF1.1_3A8V01.02.xml	BCG_GlobalPaymentConditionCode.xsd BCG_GlobalProductUnitOfMeasure Code.xsd BCG_GlobalPriceUnitOfMeasureCode.xsd BCG_GlobalPurchaseOrderFillPriority Code.xsd BCG_GlobalPurchaseOrderTypeCode.xsd BCG_GlobalShipmentTermsCode.xsd BCG_GlobalShippingServiceLevelCode.xsd BCG_GlobalSpecialFulfillmentRequest Code.xsd
BCG_Package_RNSC1.0_ RNIFV02.00_3A8V01.02.zip	BCG_RNSC1.0_ RNIFV02.00_3A8V01.02.xml	BCG_GlobalSpecialHandlingCode.xsd BCG_InvoiceChargeTypeCode.xsd BCG_GlobalTaxExemptionCode.xsd BCG_GlobalConfirmationTypeCode.xsd BCG_GlobalProductSubstitution ReasonCode.xsd BCG_GlobalPurchaseOrder AcknowledgmentReasonCode.xsd BCG_GlobalPurchaseOrderStatusCode.xsd BCG_BusinessDescription_Types.xsd BCG_GlobalPartnerClassificationCode.xsd BCG_string_len_0.xsd BCG_xml.xsd

Tabelle 11. Inhalt der PIP-Dokumentenflusspakete (Forts.)

PIP 3A9 Request Purchase Order Cancellation		
BCG_Package_ RNIF1.1_3A9V01.01.zip	BCG_RNIF1.1_3A9V01.01.xml	BCG_3A9PurchaseOrderCancellation Confirmation_V01.01.xsd BCG_3A9PurchaseOrderCancellation Request_V01.01.xsd
BCG_Package_ RNIFV02.00_3A9V01.01.zip	BCG_RNIFV02.00_3A9V01.01.xml	BCG_common.xsd BCG_ContactInformation_Types.xsd BCG_PhysicalAddress_Types.xsd BCG_PartnerDescription_Types.xsd BCG_GlobalPurchaseOrderCancellation Code.xsd
BCG_Package_RNSC1.0_ RNIF1.1_3A9V01.01.zip	BCG_RNSC1.0_ RNIF1.1_3A9V01.01.xml	BCG_GlobalPurchaseOrderCancellation ResponseCode.xsd BCG_BusinessDescription_Types.xsd BCG_BusinessTaxIdentifier_Types.xsd
BCG_Package_RNSC1.0_ RNIFV02.00_3A9V01.01.zip	BCG_RNSC1.0_ RNIFV02.00_3A9V01.01.xml	BCG_GlobalCountryCode.xsd BCG_GlobalPartnerClassificationCode.xsd BCG_string_len_0.xsd BCG_xml.xsd
PIP 3B2 Notify of Advance Shipment		
BCG_Package_ RNIF1.1_3B2V01.01.zip	BCG_RNIF1.1_3B2V01.01.xml	BCG_3B2AdvanceShipment Notification_V01.01.xsd BCG_common.xsd BCG_ContactInformation_Types.xsd BCG_PhysicalAddress_Types.xsd BCG_PartnerDescription_Types.xsd BCG_BusinessTaxIdentifier_Types.xsd BCG_GlobalIncotermsCode.xsd
BCG_Package_ RNIFV02.00_3B2V01.01.zip	BCG_RNIFV02.00_ 3B2V01.01.xml	BCG_GlobalShipmentChangeDisposition Code.xsd BCG_GlobalShipmentModeCode.xsd BCG_GlobalShippingServiceLevelCode.xsd BCG_GlobalShipDateCode.xsd BCG_GlobalPackageTypeCode.xsd BCG_GlobalPhysicalUnitOfMeasure Code.xsd
BCG_Package_RNSC1.0_ RNIF1.1_3B2V01.01.zip	BCG_RNSC1.0_ RNIF1.1_3B2V01.01.xml	BCG_GlobalProductUnitOfMeasure Code.xsd BCG_GlobalDocumentReferenceType Code.xsd BCG_GlobalLotQuantityClassification Code.xsd BCG_NationalExportControl ClassificationCode.xsd
BCG_Package_RNSC1.0_ RNIFV02.00_3B2V01.01.zip	BCG_RNSC1.0_ RNIFV02.00_3B2V01.01.xml	BCG_GlobalCountryCode.xsd BCG_GlobalTrackingReferenceType Code.xsd BCG_BusinessDescription_Types.xsd BCG_GlobalPartnerClassification Code.xsd BCG_string_len_0.xsd BCG_xml.xsd

Tabelle 11. Inhalt der PIP-Dokumentenflusspakete (Forts.)

PIP 3B12ShippingOrder Request		
BCG_Package_ RNIF1.1_3B12V01.01.zip	BCG_RNIF1.1_3B12V01.01.xml	BCG_3B12ShippingOrderRequest_V01.01.xsd BCG_3B12ShippingOrderConfirmation_V01.01.xsd BCG_common.xsd BCG_ContactInformation_Types.xsd BCG_ContactInformation_Types_V422.xsd BCG_PhysicalAddress_Types.xsd BCG_PartnerDescription_Types.xsd BCG_PartnerDescription_Types_V422.xsd BCG_BusinessTaxIdentifier_Types.xsd BCG_GlobalPartnerClassificationCode.xsd BCG_GlobalProductUnitOfMeasureCode.xsd BCG_GlobalCurrencyCode.xsd BCG_GlobalDocumentReferenceTypeCode.xsd BCG_GlobalShippingServiceLevelCode.xsd BCG_GlobalSpecialHandlingCode.xsd BCG_GlobalIncotermsCode.xsd BCG_GlobalPackageTypeCode.xsd BCG_GlobalCountryCode.xsd BCG_GlobalPartnerRoleClassificationCode.xsd BCG_GlobalPhysicalUnitOfMeasureCode.xsd BCG_GlobalShipDateCode.xsd BCG_common_V422.xsd BCG_string_len_0.xsd BCG_xml.xsd
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	

Tabelle 11. Inhalt der PIP-Dokumentenflusspakete (Forts.)

PIP 3B13ShippingOrder ConfirmationNotification		
BCG_Package_ RNIF1.1_3B13V01.01.zip	BCG_RNIF1.1_3B13V01.01.xml	BCG_3B13ShippingOrderConfirmation Notification_V01.01.xsd BCG_common_V422.xsd BCG_ContactInformation_Types.xsd BCG_BusinessTaxIdentifier_Types.xsd BCG_GlobalPartnerRoleClassification Code.xsd
BCG_Package_ RNIFV02.00_3B13V01.01.zip	BCG_RNIFV02.00_3B13V01.01.xml	BCG_GlobalProductUnitOfMeasure Code.xsd BCG_GlobalDocumentReferenceType Code.xsd BCG_GlobalCurrencyCode.xsd BCG_PartnerDescription_Types.xsd BCG_GlobalSpecialHandlingCode.xsd
BCG_Package_RNSC1.0_ RNIF1.1_3B13V01.01.zip	BCG_RNSC1.0_ RNIF1.1_3B13V01.01.xml	BCG_GlobalShippingServiceLevelCode.xsd BCG_GlobalPhysicalUnitOfMeasure Code.xsd BCG_GlobalShipDateCode.xsd BCG_GlobalTrackingReferenceType Code.xsd
BCG_Package_RNSC1.0_ RNIFV02.00_3B13V01.01.zip	BCG_RNSC1.0_ RNIFV02.00_3B13V01.01.xml	BCG_common.xsd BCG_BusinessDescription_Types.xsd BCG_GlobalCountryCode.xsd BCG_GlobalPartnerClassificationCode.xsd BCG_PhysicalAddress_Types.xsd BCG_string_len_0.xsd BCG_xml.xsd

Tabelle 11. Inhalt der PIP-Dokumentenflusspakete (Forts.)

PIP 3B18ShippingDocumentation		
Notification		
BCG_Package_ RNIF1.1_3B18V01.00.zip	BCG_RNIF1.1_3B18V01.00.xml	BCG_3B18ShippingDocumentation Notification_V01.00.xsd BCG_common_V422.xsd BCG_BusinessDescription_Types.xsd BCG_BusinessDescription_Types_V422.xsd BCG_PhysicalAddress_Types.xsd BCG_ContactInformation_Types.xsd BCG_InvoiceChargeTypeCode_V422.xsd BCG_NationalExportControl ClassificationCode.xsd BCG_GlobalPartnerRoleClassification Code_V422.xsd
BCG_Package_ RNIFV02.00_3B18V01.00.zip	BCG_RNIFV02.00_3B18V01.00.xml	BCG_GlobalPartnerClassification Code_V422.xsd BCG_GlobalShippingDocument Code_V422.xsd BCG_GlobalDocumentReferenceType Code.xsd BCG_GlobalOrderAdminCode_V422.xsd BCG_GlobalCountryCode.xsd BCG_GlobalPhysicalUnitOfMeasure Code_V422.xsd
BCG_Package_RNSC1.0_ RNIF1.1_3B18V01.00.zip	BCG_RNSC1.0_ RNIF1.1_3B18V01.00.xml	BCG_GlobalCurrencyCode.xsd BCG_GlobalMonetaryAmountType Code.xsd BCG_GlobalIncotermsCode.xsd BCG_GlobalPaymentTermsCode.xsd BCG_GlobalTrackingReferenceType Code.xsd BCG_GlobalSpecialHandling Code_V422.xsd BCG_GlobalProductUnitOfMeasure Code.xsd
BCG_Package_RNSC1.0_ RNIFV02.00_3B18V01.00.zip	BCG_RNSC1.0_ RNIFV02.00_3B18V01.00.xml	BCG_GlobalPackageTypeCode_V422.xsd BCG_GlobalPortTypeCode_V422.xsd BCG_GlobalPortIdentifierAuthority Code_V422.xsd BCG_GlobalShipDateCode.xsd BCG_GlobalFreeOnBoardCode_V422.xsd BCG_GlobalFreightPaymentTerms Code_V422.xsd BCG_GlobalShipmentModeCode.xsd BCG_GlobalShippingServiceLevel Code.xsdBCG_string_len_0.xsd

Table 11. Inhalt der PIP-Dokumentenflusspakete (Forts.)

PIP 3C3 Notify of Invoice		
BCG_Package_ RNIF1.1_3C3V01.01.zip	BCG_RNIF1.1_3C3V01.01.xml	BCG_3C3InvoiceNotification_V01.01.xsd BCG_common.xsd BCG_ContactInformation_Types.xsd BCG_PhysicalAddress_Types.xsd BCG_PartnerDescription_Types.xsd BCG_BusinessTaxIdentifier_Types.xsd BCG_GlobalCountryCode.xsd
BCG_Package_ RNIFV02.00_3C3V01.01.zip	BCG_RNIFV02.00_3C3V01.01.xml	BCG_GlobalCurrencyCode.xsd BCG_GlobalDocumentTypeCode.xsd BCG_GlobalMonetaryAmountType Code.xsd BCG_GlobalPartnerRoleClassification Code.xsd BCG_GlobalPaymentTermsCode.xsd BCG_GlobalProductUnitOfMeasure Code.xsd BCG_GlobalSaleTypeCode.xsd BCG_GlobalShipmentTermsCode.xsd BCG_GlobalShippingServiceLevelCode.xsd BCG_GlobalSpecialHandlingCode.xsd
BCG_Package_RNSC1.0_ RNIF1.1_3C3V01.01.zip	BCG_RNSC1.0_ RNIF1.1_3C3V01.01.xml	BCG_InvoiceChargeTypeCode.xsd BCG_NationalExportControl ClassificationCode.xsd BCG_BusinessDescription_Types.xsd BCG_GlobalPartnerClassificationCode.xsd BCG_string_len_0.xsd BCG_xml.xsd
BCG_Package_RNSC1.0_ RNIFV02.00_3C3V01.01.zip	BCG_RNSC1.0_ RNIFV02.00_3C3V01.01.xml	
PIP 3C4 Notify of Invoice Reject		
BCG_Package_ RNIF1.1_3C4V01.00.zip	BCG_RNIF1.1_3C4V01.00.xml	BCG_3C4InvoiceReject Notification_V01.00.xsd BCG_common.xsd BCG_ContactInformation_Types.xsd BCG_PhysicalAddress_Types.xsd BCG_PartnerDescription_Types.xsd BCG_GlobalInvoiceRejectionCode.xsd BCG_GlobalMonetaryAmountType Code.xsd BCG_BusinessDescription_Types.xsd BCG_BusinessTaxIdentifier_Types.xsd BCG_GlobalCountryCode.xsd BCG_GlobalPartnerClassificationCode.xsd BCG_string_len_0.xsd BCG_xml.xsd
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	

Tabelle 11. Inhalt der PIP-Dokumentenflusspakete (Forts.)

PIP 3C6 Notify of Remittance Advice		
BCG_Package_RNIF1.1_3C6V01.00.zip	BCG_RNIF1.1_3C6V01.00.xml	BCG_3C6RemittanceAdviceNotification_V01.00.xsd BCG_common.xsd BCG_ContactInformation_Types.xsd BCG_PhysicalAddress_Types.xsd BCG_PartnerDescription_Types.xsd
BCG_Package_RNIFV02.00_3C6V01.00.zip	BCG_RNIFV02.00_3C6V01.00.xml	BCG_GlobalCurrencyCode.xsd BCG_GlobalFinancialAdjustmentReasonCode.xsd BCG_GlobalInvoiceRejectionCode.xsd
BCG_Package_RNSC1.0_RNIF1.1_3C6V01.00.zip	BCG_RNSC1.0_RNIF1.1_3C6V01.00.xml	BCG_GlobalMonetaryAmountTypeCode.xsd BCG_GlobalPaymentMethodCode.xsd BCG_GlobalDocumentTypeCode.xsd
BCG_Package_RNSC1.0_RNIFV02.00_3C6V01.00.zip	BCG_RNSC1.0_RNIFV02.00_3C6V01.00.xml	BCG_BusinessTaxIdentifier_Types.xsd BCG_GlobalCountryCode.xsd BCG_GlobalPartnerClassificationCode.xsd BCG_string_len_0.xsd BCG_xml.xsd
PIP 3C7SelfBillingInvoice Notification		
BCG_Package_RNIF1.1_3C7V01.00.zip	BCG_RNIF1.1_3C7V01.00.xml	BCG_3C7SelfBillingInvoiceNotification_V01.00.xsd BCG_common_V422.xsd BCG_ContactInformation_Types.xsd BCG_PhysicalAddress_Types.xsd BCG_PartnerDescription_Types.xsd BCG_BusinessTaxIdentifier_Types.xsd BCG_NationalExportControlClassificationCode.xsd
BCG_Package_RNIFV02.00_3C7V01.00.zip	BCG_RNIFV02.00_3C7V01.00.xml	BCG_BusinessDescription_Types.xsd BCG_BusinessDescription_Types_V422.xsd BCG_InvoiceChargeTypeCode.xsd BCG_GlobalPartnerClassificationCode.xsd BCG_GlobalProductUnitOfMeasureCode.xsd BCG_GlobalCurrencyCode.xsd
BCG_Package_RNSC1.0_RNIF1.1_3C7V01.00.zip	BCG_RNSC1.0_RNIF1.1_3C7V01.00.xml	BCG_GlobalMonetaryAmountTypeCode.xsd BCG_GlobalDocumentTypeCode.xsd BCG_GlobalDocumentTypeCode_V422.xsd BCG_GlobalPaymentTermsCode.xsd BCG_GlobalSaleTypeCode.xsd BCG_GlobalShipmentTermsCode.xsd BCG_GlobalCountryCode.xsd
BCG_Package_RNSC1.0_RNIFV02.00_3C7V01.00.zip	BCG_RNSC1.0_RNIFV02.00_3C7V01.00.xml	BCG_GlobalShippingServiceLevelCode.xsd BCG_GlobalPartnerRoleClassificationCode.xsd BCG_GlobalDocumentReferenceTypeCode.xsd BCG_common.xsd BCG_string_len_0.xsd BCG_xml.xsd

Tabelle 11. Inhalt der PIP-Dokumentenflusspakete (Forts.)

PIP 3D8 Distribute Work in Process		
BCG_Package_ RNIF1.1_3D8V01.00.zip	BCG_RNIF1.1_3D8V01.00.xml	BCG_3D8WorkInProgress Notification_V01.00.xsd BCG_common.xsd BCG_ContactInformation_Types.xsd BCG_PhysicalAddress_Types.xsd BCG_PartnerDescription_Types.xsd
BCG_Package_ RNIFV02.00_3D8V01.00.zip	BCG_RNIFV02.00_3D8V01.00.xml	BCG_BusinessTaxIdentifier_Types.xsd BCG_GlobalPriorityCode.xsd BCG_GlobalWorkInProgressLocation Code.xsd BCG_GlobalProductUnitOfMeasure Code.xsd BCG_GlobalDocumentReferenceType Code.xsd
BCG_Package_RNSC1.0_ RNIF1.1_3D8V01.00.zip	BCG_RNSC1.0_ RNIF1.1_3D8V01.00.xml	BCG_GlobalWorkInProgressPartType Code.xsd BCG_GlobalLotCode.xsd BCG_GlobalLotStatusCode.xsd BCG_GlobalLotQuantityClassification Code.xsd
BCG_Package_RNSC1.0_ RNIFV02.00_3D8V01.00.zip	BCG_RNSC1.0_ RNIFV02.00_3D8V01.00.xml	BCG_GlobalPartnerClassificationCode.xsd BCG_BusinessDescription_Types.xsd BCG_GlobalCountryCode.xsd BCG_string_len_0.xsd BCG_xml.xsd
PIP 4A1 Notify of Strategic Forecast		
BCG_Package_ RNIF1.1_4A1V02.00.zip	BCG_RNIF1.1_4A1V02.00.xml	BCG_4A1StrategicForecast Notification_V02.00.xsd BCG_common.xsd BCG_ContactInformation_Types.xsd BCG_PhysicalAddress_Types.xsd BCG_PartnerDescription_Types.xsd
BCG_Package_ RNIFV02.00_4A1V02.00.zip	BCG_RNIFV02.00_4A1V02.00.xml	BCG_GlobalCurrencyCode.xsd BCG_GlobalForecastEventCode.xsd BCG_GlobalForecastTypeCode.xsd BCG_GlobalPartnerReferenceType Code.xsd
BCG_Package_RNSC1.0_ RNIF1.1_4A1V02.00.zip	BCG_RNSC1.0_ RNIF1.1_4A1V02.00.xml	BCG_GlobalProductUnitOfMeasure Code.xsd BCG_StrategicForecastQuantityType Code.xsd BCG_GlobalForecastIntervalCode.xsd
BCG_Package_RNSC1.0_ RNIFV02.00_4A1V02.00.zip	BCG_RNSC1.0_ RNIFV02.00_4A1V02.00.xml	BCG_BusinessDescription_Types.xsd BCG_BusinessTaxIdentifier_Types.xsd BCG_GlobalCountryCode.xsd BCG_GlobalPartnerClassificationCode.xsd BCG_string_len_0.xsd BCG_xml.xsd

Tabelle 11. Inhalt der PIP-Dokumentenflusspakete (Forts.)

PIP 4A3 Notify of Threshold Release Forecast		
BCG_Package_ RNIF1.1_4A3V02.00.zip	BCG_RNIF1.1_4A3V02.00.xml	BCG_4A3ThresholdRelease ForecastNotification_V02.00.xsd BCG_common.xsd BCG_ContactInformation_Types.xsd BCG_PhysicalAddress_Types.xsd BCG_PartnerDescription_Types.xsd
BCG_Package_ RNIFV02.00_4A3V02.00.zip	BCG_RNIFV02.00_4A3V02.00.xml	BCG_GlobalCurrencyCode.xsd BCG_GlobalForecastEventCode.xsd BCG_GlobalPartnerReferenceType Code.xsd BCG_GlobalProductUnitOfMeasure Code.xsd
BCG_Package_RNSC1.0_ RNIF1.1_4A3V02.00.zip	BCG_RNSC1.0_ RNIF1.1_4A3V02.00.xml	BCG_GlobalForecastIntervalCode.xsd BCG_GlobalForecastReferenceType Code.xsd BCG_GlobalForecastInventoryType Code.xsd
BCG_Package_RNSC1.0_ RNIFV02.00_4A3V02.00.zip	BCG_RNSC1.0_ RNIFV02.00_4A3V02.00.xml	BCG_OrderForecastQuantityTypeCode.xsd BCG_BusinessDescription_Types.xsd BCG_BusinessTaxIdentifier_Types.xsd BCG_GlobalCountryCode.xsd BCG_GlobalPartnerClassificationCode.xsd BCG_string_len_0.xsd BCG_xml.xsd
PIP 4A4 Planning Release Forecast Notification		
BCG_Package_ RNIF1.1_4A4R02.00A.zip	BCG_RNIF1.1_4A4R02.00A.xml	BCG_4A4PlanningReleaseForecast Notification_R02.00A.xsd BCG_common.xsd BCG_ContactInformation_Types.xsd BCG_PhysicalAddress_Types.xsd BCG_PhysicalAddress_Types_V422.xsd
BCG_Package_ RNIFV02.00_4A4R02.00A.zip	BCG_RNIFV02.00_4A4R02.00A.xml	BCG_PartnerDescription_Types.xsd BCG_BusinessTaxIdentifier_Types.xsd BCG_BusinessDescription_Types.xsd BCG_GlobalForecastReferenceType Code.xsd BCG_GlobalPartnerReference TypeCode.xsd
BCG_Package_RNSC1.0_ RNIF1.1_4A4R02.00A.zip	BCG_RNSC1.0_ RNIF1.1_4A4R02.00A.xml	BCG_GlobalPartnerClassificationCode.xsd BCG_GlobalProductUnitOfMeasure Code.xsd BCG_GlobalIntervalCode.xsd BCG_GlobalTransportEventCode.xsd BCG_GlobalForecastQuantityType Code_V422.xsd
BCG_Package_RNSC1.0_ RNIFV02.00_4A4R02.00A.zip	BCG_RNSC1.0_ RNIFV02.00_4A4R02.00A.xml	BCG_GlobalCurrencyCode.xsd BCG_GlobalForecastInventoryType Code.xsd BCG_GlobalCountryCode.xsd BCG_string_len_0.xsd BCG_xml.xsd

Tabelle 11. Inhalt der PIP-Dokumentenflusspakete (Forts.)

PIP 4A5 Notify of Forecast Reply		
BCG_Package_ RNIF1.1_4A5V02.00.zip	BCG_RNIF1.1_4A5V02.00.xml	BCG_4A5ForecastReply Notification_V02.00.xsd BCG_common.xsd BCG_ContactInformation_Types.xsd BCG_PhysicalAddress_Types.xsd BCG_PartnerDescription_Types.xsd BCG_GlobalCurrencyCode.xsd BCG_GlobalForecastEventCode.xsd BCG_GlobalPartnerReferenceType Code.xsd BCG_GlobalProductUnitOfMeasure Code.xsd BCG_GlobalForecastIntervalCode.xsd BCG_GlobalForecastReferenceType Code.xsd BCG_GlobalForecastResponseCode.xsd BCG_GlobalForecastInventoryType Code.xsd BCG_GlobalForecastRevisionReason Code.xsd BCG_GlobalPartnerClassificationCode.xsd BCG_ForecastReplyQuantityTypeCode.xsd BCG_BusinessDescription_Types.xsd BCG_BusinessTaxIdentifier_Types.xsd BCG_GlobalCountryCode.xsd BCG_string_len_0.xsd BCG_xml.xsd
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_4A5V02.00.xml	
BCG_Package_RNSC1.0_ RNIFV02.00_4A5V02.00.zip	BCG_RNSC1.0_ RNIFV02.00_4A5V02.00.xml	
PIP 4B2 Notify of Shipment Receipt		
BCG_Package_ RNIF1.1_4B2V01.00.zip	BCG_RNIF1.1_4B2V01.00.xml	BCG_4B2ShipmentReceipt Notification_V01.00.xsd BCG_common.xsd BCG_ContactInformation_Types.xsd BCG_PhysicalAddress_Types.xsd BCG_PartnerDescription_Types.xsd BCG_BusinessTaxIdentifier_Types.xsd BCG_GlobalCountryCode.xsd BCG_GlobalDocumentReferenceType Code.xsd BCG_GlobalLotDiscrepancyReason Code.xsd BCG_GlobalPartnerRoleClassification Code.xsd BCG_GlobalProductUnitOfMeasure Code.xsd BCG_GlobalReceivingDiscrepancyReason Code.xsd BCG_GlobalReceivingDiscrepancy Code.xsd BCG_GlobalSpecialFulfillmentRequest Code.xsd BCG_GlobalSpecialHandlingCode.xsd BCG_GlobalTrackingReferenceType Code.xsd BCG_BusinessDescription_Types.xsd BCG_GlobalPartnerClassification Code.xsd BCG_string_len_0.xsd BCG_xml.xsd
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	

Tabelle 11. Inhalt der PIP-Dokumentenflusspakete (Forts.)

PIP 4C1 Distribute Inventory Report		
BCG_Package_ RNIF1.1_4C1V02.03.zip	BCG_RNIF1.1_4C1V02.03.xml	BCG_4C1InventoryReport Notification_V02.03.xsd BCG_common.xsd BCG_ContactInformation_Types.xsd BCG_PhysicalAddress_Types.xsd BCG_BusinessDescription_Types.xsd BCG_BusinessTaxIdentifier_Types.xsd BCG_GlobalCountryCode.xsd BCG_GlobalDocumentReferenceType Code.xsd BCG_GlobalInventoryCode.xsd BCG_GlobalPartnerRoleClassification Code.xsd BCG_GlobalProductUnitOfMeasure Code.xsd BCG_GlobalPartnerClassification Code.xsd BCG_string_len_0.xsd BCG_xml.xsd
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	
PIP 4C1Inventory ReportNotification		
BCG_Package_ RNIF1.1_4C1V02.01.zip	BCG_RNIF1.1_4C1V02.01.xml	BCG_4C1InventoryReport Notification_V02.01.xsd BCG_common_V422.xsd BCG_ContactInformation_Types.xsd BCG_ContactInformation_Types_V422.xsd BCG_PhysicalAddress_Types_V422.xsd BCG_BusinessDescription_Types.xsd BCG_BusinessTaxIdentifier_Types.xsd BCG_GlobalCountryCode.xsd BCG_GlobalDocumentReferenceType Code.xsd BCG_GlobalInventoryCode.xsd BCG_GlobalPartnerRoleClassification Code.xsd BCG_GlobalProductUnitOfMeasure Code.xsd BCG_common.xsd BCG_GlobalPartnerClassificationCode.xsd BCG_PhysicalAddress_Types.xsd BCG_string_len_0.xsd BCG_xml.xsd
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	

Tabelle 11. Inhalt der PIP-Dokumentenflusspakete (Forts.)

PIP 5C1 Distribute Product List		
BCG_Package_ RNIF1.1_5C1V01.00.zip	BCG_RNIF1.1_5C1V01.00.xml	BCG_5C1ProductList Notification_V01.00.xsd BCG_common.xsd BCG_ContactInformation_Types.xsd
BCG_Package_ RNIFV02.00_5C1V01.00.zip	BCG_RNIFV02.00_5C1V01.00.xml	BCG_PartnerDescription_Types.xsd BCG_GlobalPartnerRoleClassification Code.xsd BCG_GlobalPartnerClassificationCode.xsd
BCG_Package_RNSC1.0_ RNIF1.1_5C1V01.00.zip	BCG_RNSC1.0_ RNIF1.1_5C1V01.00.xml	BCG_GlobalCountryCode.xsd BCG_GlobalPriceTypeCode.xsd BCG_GlobalCurrencyCode.xsd BCG_BusinessDescription_Types.xsd
BCG_Package_RNSC1.0_ RNIFV02.00_5C1V01.00.zip	BCG_RNSC1.0_ RNIFV02.00_5C1V01.00.xml	BCG_BusinessTaxIdentifier_Types.xsd BCG_PhysicalAddress_Types.xsd BCG_string_len_0.xsd BCG_xml.xsd
PIP 5C4 Distribute Registration Status		
BCG_Package_ RNIF1.1_5C4V01.02.zip	BCG_RNIF1.1_5C4V01.02.xml	BCG_5C4RegistrationStatus Notification_V01.02.xsd BCG_common.xsd BCG_ContactInformation_Types.xsd
BCG_Package_ RNIFV02.00_5C4V01.02.zip	BCG_RNIFV02.00_5C4V01.02.xml	BCG_PhysicalAddress_Types.xsd BCG_PartnerDescription_Types.xsd BCG_GlobalCountryCode.xsd BCG_GlobalRegistrationComplexity LevelCode.xsd
BCG_Package_RNSC1.0_ RNIF1.1_5C4V01.023.zip	BCG_RNSC1.0_ RNIF1.1_5C4V01.02.xml	BCG_GlobalRegistrationInvolvement LevelCode.xsd BCG_GlobalPartnerRoleClassification Code.xsd
BCG_Package_RNSC1.0_ RNIFV02.00_5C4V01.02.zip	BCG_RNSC1.0_ RNIFV02.00_5C4V01.02.xml	BCG_GlobalPartnerClassificationCode.xsd BCG_BusinessDescription_Types.xsd BCG_BusinessTaxIdentifier_Types.xsd BCG_string_len_0.xsd BCG_xml.xsd

Tabelle 11. Inhalt der PIP-Dokumentenflusspakete (Forts.)

PIP 5D1 Request Ship From Stock And Debit Authorization Status		
BCG_Package_ RNIF1.1_5D1V01.00.zip	BCG_RNIF1.1_5D1V01.00.xml	BCG_5D1ShipFromStockAnd DebitAuthorization Confirmation_V01.00.xsd BCG_5D1ShipFromStockAnd DebitAuthorizationRequest_V01.00.xsd BCG_common.xsd
BCG_Package_ RNIFV02.00_5D1V01.00.zip	BCG_RNIFV02.00_5D1V01.00.xml	BCG_BusinessDescription_Types.xsd BCG_ContactInformation_Types.xsd BCG_PhysicalAddress_Types.xsd BCG_PartnerDescription_Types.xsd BCG_GlobalCurrencyCode.xsd BCG_GlobalCountryCode.xsd BCG_GlobalPartnerRoleClassification Code.xsd
BCG_Package_RNSC1.0_ RNIF1.1_5D1V01.00.zip	BCG_RNSC1.0_ RNIF1.1_5D1V01.00.xml	BCG_GlobalProductUnitOfMeasure Code.xsd BCG_GlobalDocumentReferenceType Code.xsd BCG_GlobalPartnerClassificationCode.xsd
BCG_Package_RNSC1.0_ RNIFV02.00_5D1V01.00.zip	BCG_RNSC1.0_ RNIFV02.00_5D1V01.00.xml	BCG_GlobalPriceTypeCode.xsd BCG_GlobalShipFromStockAnd DebitAuthorizationRejectionCode.xsd BCG_BusinessTaxIdentifier_Types.xsd BCG_string_len_0.xsd BCG_xml.xsd

Tabelle 11. Inhalt der PIP-Dokumentenflusspakete (Forts.)

PIP 7B1 Distribute Work in Process		
BCG_Package_ RNIF1.1_7B1V01.00.zip	BCG_RNIF1.1_7B1V01.00.xml	BCG_7B1WorkInProgress Notification_V01.00.xsd BCG_common.xsd BCG_ContactInformation_Types.xsd BCG_PhysicalAddress_Types.xsd BCG_PartnerDescription_Types.xsd BCG_GlobalChangeReasonCode.xsd BCG_GlobalDocumentReferenceType Code.xsd
BCG_Package_ RNIFV02.00_37B1V01.00.zip	BCG_RNIFV02.00_7B1V01.00.xml	BCG_GlobalEquipmentTypeCode.xsd BCG_GlobalLotCode.xsd BCG_GlobalLotStatusCode.xsd BCG_GlobalLotQuantityClassification Code.xsd BCG_GlobalPartnerRoleClassification Code.xsd
BCG_Package_RNSC1.0_ RNIF1.1_7B1V01.00.zip	BCG_RNSC1.0_ RNIF1.1_7B1V01.00.xml	BCG_GlobalPriorityCode.xsd BCG_GlobalProductUnitOfMeasure Code.xsd BCG_GlobalWorkInProgressTypeCode.xsd BCG_GlobalWorkInProgressQuantity ChangeCode.xsd BCG_GlobalWorkInProgressLocation Code.xsd
BCG_Package_RNSC1.0_ RNIFV02.00_7B1V01.00.zip	BCG_RNSC1.0_ RNIFV02.00_7B1V01.00.xml	BCG_GlobalWorkInProgressPartType Code.xsd BCG_BusinessDescription_Types.xsd BCG_BusinessTaxIdentifier_Types.xsd BCG_GlobalCountryCode.xsd BCG_GlobalPartnerClassificationCode.xsd BCG_string_len_0.xsd BCG_xml.xsd

Tabelle 11. Inhalt der PIP-Dokumentenflusspakete (Forts.)

PIP 7B5NotifyOfManufacturing WorkOrder		
BCG_Package_ RNIF1.1_7B5V01.00.zip	BCG_RNIF1.1_7B5V01.00.xml	BCG_7B5NotifyOfManufacturing WorkOrder_V01.00.xsd BCG_common.xsd BCG_ContactInformation_Types.xsd BCG_PartnerDescription_Types.xsd BCG_GlobalPartnerClassificationCode.xsd BCG_GlobalProductUnitOfMeasure Code.xsd
BCG_Package_ RNIFV02.00_7B5V01.00.zip	BCG_RNIFV02.00_7B5V01.00.xml	BCG_GlobalDocumentReferenceType Code.xsd BCG_GlobalBusinessActionCode_V422.xsd BCG_GlobalAttachmentDescription Code_V422.xsd BCG_GlobalMimeType QualifierCode_V422.xsd BCG_GlobalDevicePackageType Code_V422.xsd
BCG_Package_RNSC1.0_ RNIF1.1_7B5V01.00.zip	BCG_RNSC1.0_ RNIF1.1_7B5V01.00.xml	BCG_GlobalPackageTypeCode.xsd BCG_GlobalChangeReasonCode.xsd BCG_GlobalLineItemStatusCode.xsd BCG_GlobalPartnerRoleClassification Code.xsd BCG_GlobalPhysicalUnitOfMeasure Code.xsd BCG_GlobalWorkInProgressLocation Code.xsd
BCG_Package_RNSC1.0_ RNIFV02.00_7B5V01.00.zip	BCG_RNSC1.0_ RNIFV02.00_7B5V01.00.xml	BCG_GlobalLotCode.xsd BCG_GlobalPriorityCode.xsd BCG_BusinessDescription_Types.xsd BCG_BusinessTaxIdentifier_Types.xsd BCG_GlobalCountryCode.xsd BCG_PhysicalAddress_Types.xsd BCG_string_len_0.xsd BCG_xml.xsd

Tabelle 11. Inhalt der PIP-Dokumentenflusspakete (Forts.)

PIP 7B6NotifyOfManufacturing WorkOrderReply		
BCG_Package_ RNIF1.1_7B6V01.00.zip	BCG_RNIF1.1_7B6V01.00.xml	BCG_7B6NotifyOfManufacturing WorkOrderReply_V01.00.xsd BCG_common.xsd BCG_ContactInformation_Types.xsd BCG_PartnerDescription_Types.xsd
BCG_Package_ RNIFV02.00_7B6V01.00.zip	BCG_RNIFV02.00_7B6V01.00.xml	BCG_GlobalProductUnitOfMeasure Code.xsd BCG_GlobalDocumentReferenceType Code.xsd BCG_GlobalPartnerRoleClassification Code.xsd
BCG_Package_RNSC1.0_ RNIF1.1_7B6V01.00.zip	BCG_RNSC1.0_ RNIF1.1_7B6V01.00.xml	BCG_GlobalChangeReasonCode.xsd BCG_GlobalLineItemStatusCode.xsd BCG_BusinessDescription_Types.xsd BCG_BusinessTaxIdentifier_Types.xsd
BCG_Package_RNSC1.0_ RNIF1.1_7B6V01.00.zip	BCG_RNSC1.0_ RNIFV02.00_7B6V01.00.xml	BCG_GlobalCountryCode.xsd BCG_GlobalPartnerClassificationCode.xsd BCG_PhysicalAddress_Types.xsd BCG_string_len_0.xsd BCG_xml.xsd
PIP 0A1 Notification of Failure v1.0		
BCG_Package_ RNIF1.1_0A11.0.zip	BCG_RNIF1.1_0A11.0.xml	0A1FailureNotification_1.0.xml BCG_0A1FailureNotification_1.0.xsd BCG_GlobalPartnerClassificationCode.xsd BCG_GlobalPartnerRoleClassification Code.xsd
BCG_Package_RNSC1.0_ RNIF1.1_0A11.0.zip	BCG_RNSC1.0_ RNIF1.1_0A11.0.xml	BCG_common.xsd BCG_string_len_0.xsd BCG_xml.xsd
PIP 0A1 Notification of Failure V02.00.00		
BCG_Package_ RNIF1.1_0A1V02.00.zip	BCG_RNIF1.1_0A1V02.00.xml	0A1FailureNotification_V02.00.xml BCG_0A1FailureNotification_V02.00.xsd
BCG_Package_ RNIFV02.00_0A1V02.00.zip	BCG_RNIFV02.00_0A1V02.00.xml	BCG_common.xsd BCG_GlobalPartnerClassificationCode.xsd BCG_GlobalPartnerRoleClassification Code.xsd
BCG_Package_RNSC1.0_ RNIF1.1_0A1V02.00.zip	BCG_RNSC1.0_ RNIF1.1_0A1V02.00.xml	BCG_string_len_0.xsd
BCG_Package_RNSC1.0_ RNIFV02.00_0A1V02.00.zip	BCG_RNSC1.0_ RNIFV02.00_0A1V02.00.xml	BCG_xml.xsd

Anhang C. Web-Serviceanforderungen konfigurieren

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 Business Integration Connect-Server auf, um den Web-Service zu erhalten. WebSphere Business Integration Connect 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 Anhang 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
- Die Teilnehmerverbindung aktivieren
- 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 Business Integration Connect, 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`).
 - Das Kennwort entspricht dem Kennwort des Konsolbenutzernamens.
2. Stellen Sie ein SSL-Clientzertifikat bereit, das zuvor in WebSphere Business Integration Connect 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://WBIChost/bcreceiver/Receiver?to=123456789`

Dadurch erfährt WebSphere Business Integration Connect, dass der Provider des Web-Services der Teilnehmer mit der Geschäfts-ID '123456789' ist.

Dokumentenflussdefinitionen für einen Web-Service konfigurieren

Um die Dokumentenflussdefinition zu konfigurieren, laden Sie die WSDL-Dateien (Web Service Definition Language) hoch, die den Web-Service definieren, wie in Kapitel 5, „Den Hub konfigurieren“ beschrieben. Alternativ hierzu können Sie die entsprechenden Dokumentenflussdefinitionen manuell über Community Console eingeben.

Um die entsprechenden Dokumentenflussdefinitionen manuell einzugeben, befolgen Sie die Prozeduren in „Dokumentenflussdefinition erstellen“ auf Seite 45. Sie müssen auch die Einträge **Dokumentenfluss**, **Aktivität** und **Aktion** einzeln unter dem Protokoll **Web Service** erstellen, wie unten beschrieben. Beachten Sie dabei besonders die Voraussetzungen 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 (Name und Code), Version N/A

Protokoll: Web Service (Name und Code), Version 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 für den WSDL-Namespace und -Namen typisch.

Aktivitäten: Eine Aktivität für jede Web-Service-Operation mit Name und Code:
'{<operations-namespace>:<operationsname>'

Aktionen: Eine Aktion für die Eingabenachricht jeder Operation mit Name und Code:

'{<namespace des angebenen xml-elements = erstes untergeordnetes element von soap:body>:<name des angebenen xml-elements = erstes untergeordnetes element von soap:body>'

Die Aktionen sind die kritischen Definitionen, da WebSphere Business Integration Connect 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 Namensbereich und Namen einer bekannten Aktion in den Dokumentenflussdefinitionen von WebSphere Business Integration Connect übereinstimmen.

Wenn z. B. eine Web-Serviceanforderungs-SOAP-Nachricht (für eine SOAP-Bindung **document-literal**) wie folgt aussieht:

```
<?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>
```

Dann würde WebSphere Business Integration Connect 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>
```

Bei der obigen Nachricht würde WebSphere Business Integration Connect nach einer definierten Web-Serviceaktion mit dem folgenden 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.

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 in jedem Attribut "location" des Importelements 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 ZIP-Datei gepackt sind, jede mit einem ZIP-Pfad, der dem Pfad (sofern vorhanden) im Importattribut "location" entspricht, wird das Hochladen der ZIP-Datei alle enthaltenen Primär- und Import-WSDL-Dateien hochladen.

Beispiel:

Inhalt der primären WSDL-Datei 'helloworldRPC.wsdl'

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

Inhalt der importierten WSDL-Datei 'bindingRPC.wsdl'

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

Die ZIP-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-Servicenachrichten werden nicht wirklich von WebSphere Business Integration Connect geprüft. Sie werden direkt mit dem ursprünglichen Serviceendpunkt-URL übergeben.) Dies wird als *private* WSDL bezeichnet.

Daneben wird eine *öffentliche* WSDL gespeichert, bei der der private URL durch einen Ziel-URL ersetzt wurde, welcher vom Benutzer in der Eingabe für die Dokumentenflusshochladeoperation bereitgestellt wurde. 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 Business Integration Connect wird dann die Web-Serviceanforderung an ein Gateway weiterleiten, das der private URL des ursprünglichen Web-Service-Providers ist. WebSphere Business Integration Connect 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

Business Integration Connect bietet die Möglichkeit, WSDL-Dateien zu importieren. 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 trifft zu, wenn Sie WSDL-Dateien innerhalb einer primären WSDL-Datei importiert haben), würden diese in einem ZIP-Archiv hochgeladen.

Wichtig: Die WSDL-Dateien in dem ZIP-Archiv müssen in einem Verzeichnis sein, das im WSDL-Importelement angegeben ist. Beim folgenden Importelement `<import namespace="http://www.helloworld.com/wsdl/helloRPC.wsdl" location="path1/bindingRPC.wsdl"/>` würde die Verzeichnisstruktur im ZIP-Archiv `path1/bindingRPC.wsdl` lauten. Im nächsten Beispiel `<import namespace="http://www.helloworld.com/wsdl/helloRPC.wsdl" location="bindingRPC.wsdl"/>`, würde sich die Datei `bindingRPC.wsdl` im ZIP-Archiv auf Rootebene befinden.

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

1. Klicken Sie auf **Hubadmin > Hubkonfiguration > Dokumentenflussdefinition**.
2. Klicken Sie auf **Pakete hoch-/herunterladen**.
3. Wählen Sie **Ja** für **WSDL-Paket** aus, um eine WSDL-Datei hochzuladen. Geben Sie für **Öffentliche Web-Service-URL-Adresse** die öffentliche URL-Adresse des Web-Services ein, der von Community Manager zur Verfügung gestellt wird (welcher von einem Teilnehmer aufgerufen wird). Beispiel: `http(s)://<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 Web-Service (der von Community Manager aufgerufen wird), der von einem Teilnehmer bereitgestellt wird, die öffentliche URL-Adresse des Teilnehmers mit einer Abfragezeichenfolge ein: Beispiel: `http(s)://<ziel host:port>/bcgreceiver/Receiver?to=<teilnehmergegeschäfts-ID>`.
4. Klicken Sie auf **Durchsuchen**, und wählen Sie die WSDL-Datei oder das ZIP-Archiv aus.
5. 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.
6. 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.
7. Klicken Sie auf **Hochladen**. Die WSDL-Datei wird auf dem System installiert.

Pakete mit Schemadateien prüfen

Eine Gruppe von XML-Schemata, die die XML-Dateien beschreiben, welche über die Konsole hochgeladen werden können, wird auf dem Business Integration Connect-Installationsdatenträger bereitgestellt. Hochgeladene Dateien werden mit diesen Schemata geprüft. 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`

Interaktion für einen neuen Web-Service konfigurieren

Der letzte Schritt bei der Erstellung der nötigen Dokumentenflussdefinitionen für einen neuen Web-Service besteht darin, eine Interaktion mit derselben Web-Service-dokumentenflussaktion als Quelle und Ziel zu konfigurieren.

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. Wählen Sie **Pass-Through** in der Dropdown-Liste **Aktion** unten in der Anzeige aus (**Pass-Through** ist die einzige gültige Option, die in WebSphere Business Integration Connect für einen Web-Service unterstützt wird).

Dokumentenflüsse der B2B-Funktionalität von Teilnehmern hinzufügen

Fügen Sie die Web-Servicedokumentenflüsse der B2B-Funktionalität von Quellen- und Zielteilnehmern hinzu, um eine Teilnehmerverbindung zwischen den Quellen- und Zielteilnehmern zu konfigurieren.

Bevor Sie eine Teilnehmerverbindung zwischen dem Web-Servicebenutzer und dem Web-Service-Provider konfigurieren, müssen Sie die Gateways konfigurieren, die in der Teilnehmerverbindung verwendet werden. Siehe „Gateways erstellen“ auf Seite 52.

Der Quellgateway-URL wird vom Web-Service nicht verwendet. Er kann ein Pseudo-URL sein. Mit dem Quellgateway können die Optionen **Client-IP prüfen** oder **Client-SSL-Zertifikat prüfen** auf der Absenderseite konfiguriert werden.

Geben Sie für das Zielgateway den privaten URL an, der vom Web-Service-Provider bereitgestellt wird. Dort wird WebSphere Business Integration Connect den Web-Service aufrufen, wenn er als Proxy-Server für den Web-Service-Provider agiert.

Die Teilnehmerverbindung aktivieren

Der neue Dokumentenfluss sollte als verfügbare Auswahlmöglichkeit für Teilnehmerverbindungen zwischen den zwei ausgewählten Teilnehmern angezeigt werden. Aktivieren Sie die Teilnehmerverbindung, um den Web-Service dem Quellenteilnehmer verfügbar zu machen. Siehe „Teilnehmerverbindungen aktivieren“ auf Seite 62.

Einschränkungen und Begrenzungen der Web-Serviceunterstützung

WebSphere Business Integration Connect 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.

Anhang D. cXML-Austauschvorgänge konfigurieren

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

cXML-Unterstützungsübersicht

WebSphere Business Integration Connect Document Manager gibt ein cXML-Dokument durch den Rootelementnamen des XML-Dokuments, der lautet "cXML", 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; Business Integration Connect stellt jedoch keine cXML-DTDs bereit. Sie können diese unter www.cxml.org herunterladen; und sie dann in Business Integration Connect 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 Kapitel 5, „Den Hub konfigurieren“.

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 unten stellt die Elemente **From** und **To** als die Quelle und das Ziel des cXML-Dokuments dar:

```
<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.

Business Integration Connect verwendet nicht die Informationen im Absender-element.

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 Business Integration Connect. 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 Business Integration Connect:

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

Antwort

Der Zielteilnehmer sendet eine cXML-Antwort, um den Quellteilnehmer 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 Status-Element enthalten. Ein Element **Response** kann auch Daten der Anwendungsebene enthalten. Während PunchOut sind z. B. die Daten der Anwendungsebene in einem Element **PunchOutSetup-Response** enthalten. Typische Antwortelemente:

- ProfileResponse
- PunchOutSetupResponse
- GetPendingResponse

Die folgende Tabelle zeigt die Beziehung zwischen den Elementen in einem cXML-Antwortdokument und den Dokumentenflussdefinitionen in Business Integration Connect:

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

Nachricht

Eine cXML-Nachricht enthält die Business Integration Connect-Dokumentenflussinformation im cXML-Nachrichtenelement. Es kann optional ein Statusselement enthalten, das mit dem im Antwortelement 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 des Elements <Message> entspricht dem Dokumentenfluss, der in Business Integration Connect erstellt wurde. In dem Beispiel darunter würde **SubscriptionChangeMessage** der Dokumentenfluss sein:

```
<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 Business Integration Connect:

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 Nachrichtenelement 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** wäre die **payloadID** einer Nachricht, die zuvor empfangen wurde. Diese würde für die Erstellung einer Zweiwege-Transaktion 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 unten aufgelisteten Header **Content-Type** 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 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

Business Integration Connect unterstützt die folgenden cXML-Dokumentenflussdefinitionsinteraktionen:

Quelle	Ziel	Quellenpaket	Zielpaket	Quellenprotokoll	Zielprotokoll	Pass-Through	Validierung	Konvertierung
Teilnehmer	Manager	Keins	Keins	cXML	cXML	x	x	
Manager	Teilnehmer	Keins	Keins	cXML	cXML	x	x	
Manager	Teilnehmer		Keins	XML	cXML	x	x	x

cXML-Dokumentenflussdefinition 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 Konsole zeigt die Anzeige **Dokumentenflussdefinitionen erstellen** an.
3. Wählen Sie **Dokumentenfluss** als Dokumentenflusstyp aus.
4. Geben Sie den Anforderungstyp, wie z. B. *OrderRequest*, in den Feldern **Code** und **Name** ein. Geben Sie für das Antwortdokument, falls das Antwortelement über keine untergeordneten Tags außer <Status> verfügt, *Response* ein. Andernfalls geben Sie den nächsten Tag-Namen auf <Status> folgend ein.

Beispiel:

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

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

5. 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 **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 das **Protokoll: cXML (1.2.009): cXML** aus.
12. Klicken Sie auf **Speichern**.

Sobald die Dokumentenflussdefinition erstellt ist, aktivieren Sie die Teilnehmerverbindungen nach Bedarf. Weitere Informationen finden Sie in „Teilnehmerverbindungen aktivieren“ auf Seite 62.

Bemerkungen und Marken

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 Quellsprache 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 Business Integration Connect 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 NUTZUNGS-AUSFALL, DATENVERLUST, GEWINNEINBUSSEN. DIES GILT UNABHÄNGIG VON DER HAFTUNGSGRUNDLAGE, SEI SIE VERSCHULDENSABHÄNGIG ODER VERSCHULDENSUNABHÄNGIG, SOFERN SIE IN IRGEND EINER 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:

IBM
Das IBM Logo
AIX
CrossWorlds
DB2
DB2 Universal Database
Domino
Lotus
Lotus Notes
MQIntegrator
MQSeries
Tivoli
WebSphere

Microsoft, Windows, Windows NT und das Windows-Logo sind in gewissen Ländern Marken oder eingetragene 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.

Andere Namen von Unternehmen, Produkten oder Services können Marken oder Servicemarken anderer Unternehmen sein.

WebSphere Business Integration Connect Enterprise und Advanced Edition enthält Software, die von Eclipse Project (www.eclipse.org) entwickelt wurde.



WebSphere Business Integration Connect Enterprise und Advanced Edition Version 4.2.2.

IBM