WebSphere®

# IBM WebSphere Partner Gateway Enterprise und Advanced Edition

Version 6.2.1

# *Hubkonfiguration*

IBM

**Hinweis**

Vor Verwendung dieser Informationen und des darin beschriebenen Produkts sollten die Informationen im Abschnitt „Bemerkungen" auf Seite 473 gelesen werden.

**Februar 2011**

Diese Veröffentlichung ist eine Übersetzung des Handbuchs
*IBM WebSphere Partner Gateway Enterprise and Advanced Editions Hub Configuration Guide Version 6.2.1*,
herausgegeben von International Business Machines Corporation, USA
(c) Copyright International Business Machines Corporation 2010, 2011
(c) Copyright IBM Deutschland GmbH 2011

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.

Werden an IBM Informationen eingesandt, gewährt der Einsender IBM ein nicht ausschließliches Recht zur beliebigen Verwendung oder Verteilung dieser Informationen, ohne dass eine Verpflichtung gegenüber dem Einsender entsteht.

Herausgegeben von:
SW TSC Germany
Kst. 2877
Februar 2011

# Inhaltsverzeichnis

# Kapitel 1. Zu diesem Handbuch

In dieser Dokumentation wird beschrieben, wie Sie den IBM(R) WebSphere(R) Partner Gateway-Server konfigurieren.

## Zielgruppe

WebSphere Partner Gateway wird von Administratoren verwaltet. Dieses Handbuch geht von zwei Arten von Administratoren aus:

- Hubadministrator
- Kontenadministrator

Der Hubadministrator ist der Superuser in der Community. Der Hubadministrator ist für die Konfiguration und Verwaltung der Hub-Community insgesamt verantwortlich. Dazu gehört auch die Konfiguration der Partner und die Verbindungsaktivierung. Der Kontenadministrator hat Zugriff auf eine Untergruppe der Funktionen des Hubadministrators und ist der wichtigste Benutzer mit Verwaltungsaufgaben für interne und externe Partner.

**Anmerkung:** Die Konsolen des Hubadministrators, der externen Partner und der internen Partner unterscheiden sich abhängig von der jeweiligen Zugriffssteuerung bzw. Zugriffsberechtigung.

## Typografische Konventionen

Diese Dokumentation verwendet die folgenden Konventionen.

*Tabelle 1. Typografische Konventionen*

| Konvention | Beschreibung |
|---|---|
| `Monospaceschrift` | Text in dieser Schriftart gibt von Ihnen einzugebenden Text, Werte für Argumente oder Befehlsoptionen, Beispiele oder Codebeispiele oder Informationen, die das System in der Anzeige druckt (Nachrichtentext oder Eingabeaufforderungen), an. |
| **Fettdruck** | In Fettdruck dargestellter Text kennzeichnet Steuerelemente der grafischen Benutzerschnittstelle (z. B. die Namen von Schaltflächen, Menüs oder Menüoptionen) und Spaltenüberschriften in Tabellen und im Fließtext. |
| *Kursivschrift* | In Kursivdruck dargestellter Text kennzeichnet Hervorhebungen, Buchtitel, neue Termini und Termini, die im Text definiert werden. Darüber hinaus werden in Kursivdruck Variablennamen und alphabetische Zeichen dargestellt, die als Literalwerte benutzt werden. |
| *`Kursive Monospaceschrift`* | In kursiv gedruckter Monospaceschrift dargestellter Text kennzeichnet Variablennamen innerhalb von Textsegmenten, die in Monospaceschrift gedruckt sind. |
| *Produktverz* | *Produktverz* steht für das Verzeichnis, in dem das Programm installiert ist. Alle IBM WebSphere Partner Gateway-Programmpfadnamen beziehen sich auf das Verzeichnis, in dem das Programm IBM WebSphere Partner Gateway auf Ihrem System installiert ist. |

*Tabelle 1. Typografische Konventionen (Forts.)*

| Konvention | Beschreibung |
|---|---|
| *%text%* und *$text* | Text in Prozentzeichen (%) gibt den Wert für den Text der Windows(R)-Systemvariablen bzw. Benutzervariablen an. Die entsprechende Notation in einer UNIX(R)-Umgebung ist $*text*. Sie gibt den Wert für den *text* der UNIX-Umgebungsvariablen an. |
| Unterstrichener farbiger Text | Unterstrichener farbiger Text gibt einen Querverweis an. Klicken Sie auf den Text, um das Objekt des Verweises aufzurufen. |
| Text in einem blauen Rahmen | (Nur in PDF-Dateien) Ein Rahmen um ein Textelement kennzeichnet einen Querverweis. Klicken Sie auf den umrandeten Text, um das Objekt des Verweises aufzurufen. Diese Konvention in PDF-Dateien entspricht der in der vorliegenden Tabelle bereits erläuterten Textkonvention für den unterstrichenen farbigen Text. |
| " " (Anführungszeichen) | (Nur in PDF-Dateien) Anführungszeichen umgeben Querverweise auf andere Abschnitte in der Dokumentation. |
| { } | In einer Zeile mit Syntaxelementen wird in geschweiften Klammern eine Gruppe von Optionen dargestellt, von der genau eine Option ausgewählt werden muss. |
| [ ] | In einer Zeile mit Syntaxelementen wird in eckigen Klammern ein optionaler Parameter dargestellt. |
| < > | Spitze Klammern umgeben variable Elemente eines Namens, um sie voneinander zu unterscheiden. Beispiel: <*servername*><*connectorname*>tmp.log. |
| / oder \ | Backslashes (\) werden in Windows-Installationen zur Trennung der einzelnen Elemente eines Verzeichnispfads verwendet. In UNIX-Installationen müssen Sie an Stelle der Backslashes Schrägstriche (/) angeben. |

## Referenzliteratur

Die gesamte, zum vorliegenden Produkt bereitgestellte Dokumentation enthält umfassende Informationen zur Installation, Konfiguration, Verwaltung und Verwendung von WebSphere Partner Gateway Enterprise Edition und Advanced Edition.

Sie können diese Dokumentation von der folgenden Site herunterladen oder sie dort direkt online lesen:

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

**Hinweis:** Wichtige Informationen zum vorliegenden Produkt, die erst nach der Veröffentlichung des vorliegenden Dokuments verfügbar wurden, werden bei Bedarf in technischen Hinweisen (TechNotes) der technischen Unterstützungsfunktion und in Aktualisierungen bereitgestellt. Diese können von der Unterstützungswebsite für WebSphere Business Integration heruntergeladen werden:

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

Wählen Sie dort den Bereich mit den für Sie relevanten Informationen aus, und durchsuchen Sie den Abschnitt mit den verfügbaren technischen Hinweisen und Aktualisierungen.

## Neuerungen in Release 6.2.1

WebSphere Partner Gateway Version 6.2.1 unterstützt die folgenden neuen Funktionen:

- Web Mail Box stellt webbasierte Unterstützung für B2B-Interaktionen bereit. Partner, Kunden und Lieferanten interagieren einfach über einen Internet-Browser mit dem WebSphere Partner Gateway-Hub.
- Neben dem integrierten FTP-Server wird nun auch ein integrierte SFTP-Server unterstützt.
- OpenPGP-Zertifikate werden in WebSphere Partner Gateway unterstützt.
- Unterstützung für WebSphere Application Server ND V7.0.0.13, WebSphere Messaging Queue 7.0 und WTX 8.3 wurde hinzugefügt.
- Plattformunterstützung für Windows 2008, Windows 7 und SLES 11.
- Unterstützung für Power 7 im Toleranzmodus (P6/P6+-kompatibler Modus).
- Unterstützung für Virtualisierung - VMware® ESX unter Windows und Linux, Power VM unter AIX.

# Kapitel 2. Einführung in die Hubkonfiguration

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

Dieses Kapitel behandelt die folgenden Themen:



## Übersicht über die Hubkonfiguration

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

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

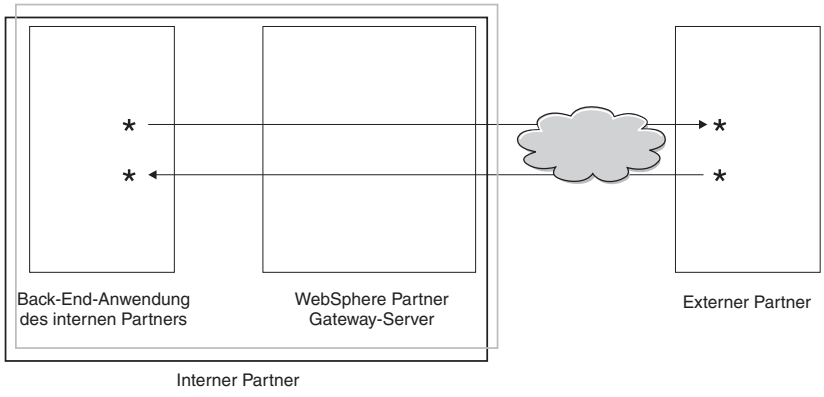



*Abbildung 1. Dokumentenfluss durch den Hub*

In diesem Handbuch erfahren Sie, wie Sie den Hub und anschließend die Partner konfigurieren. Sie erfahren außerdem, wie Sie die Sicherheit für den Hub konfigurieren.

In Abb. 1 auf Seite 5 sehen Sie, dass der interne Partner der Eigner des WebSphere Partner Gateway-Servers und der Back-End-Anwendung des internen Partners ist. Der interne Partner ist das Unternehmen, das Eigner des Hubs ist. Wie Sie in späteren Kapiteln feststellen werden, können Sie für interne Partner genauso ein Profil definieren wie für externe Partner.

**Anmerkung:** In dieser Dokumentation wird dargestellt, wie Sie Verbindungen erstellen, die von der Back-End-Anwendung des internen Partners zu einem Partnerziel und von einem externen Partner zum Ziel des internen Partners fließen. Nachdem die Dokumente am Ziel des internen Partners angekommen sind, möchten Sie diese wahrscheinlich in eine Back-End-Anwendung, wie WebSphere InterChange Server oder WebSphere MQ Broker, integrieren. Die erforderlichen Aufgaben für die Integration zwischen WebSphere Partner Gateway und solchen Back-End-Anwendungen werden im Handbuch *WebSphere Partner Gateway Unternehmensintegration* definiert.

## Für die Hubkonfiguration benötigte Informationen

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

- Welche Dokumenttypen (z. B. EDI-X12 oder angepasste XML) werden von den internen Partnern und ihren externen Partnern durch den Hub gesendet?
- Welche Transporttypen (z. B. HTTP oder FTP) verwenden die internen Partner und ihre externen Partner zum Senden der Dokumente?
- Muss ein auf dem Hub eingehendes Dokument in mehrere Dokumente aufgeteilt werden oder müssen einzelne auf dem Hub eingehende Dokumente gruppiert werden, bevor sie weitergesendet werden?
- Werden die Dokumente vor ihrer Zustellung transformiert?
- Werden die Dokumente vor ihrer Zustellung geprüft?
- Werden die Dokumente vor ihrer Zustellung geprüft, um festzustellen, ob Duplikate vorhanden sind?
- Werden die Dokumente verschlüsselt oder digital signiert, oder wird eine andere Sicherheitstechnik verwendet?

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

Nachdem Sie den Hub definiert haben, können Sie Ihre externen Partner mit den Informationen (wie z. B. IP-Adresse und DUNS-Nummern) definieren, die Sie von den externen Partnern erhalten haben. Wie zuvor angemerkt, definieren Sie auch den internen Partner als einen speziellen Typ von Hubpartner.

## Übersicht über Transporte

Dokumente können von Partnern an WebSphere Partner Gateway (den Hub) über eine Vielzahl von Transporten gesendet werden. Ein Partner kann Dokumente über öffentliche Netze unter Verwendung von HTTP, HTTPS, JMS, FTP, FTPS, FTP-Scripting, SMTP, SFTP oder eines Dateiverzeichnisses senden. Ein Partner kann Do-

kumente unter Verwendung des FTP-Scripting-Transports über VAN (Value Added Network - Mehrwertnetz), einem privaten Netz, senden. Sie können auch Ihren eigenen Transport erstellen.

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

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

Abb. 2 zeigt die Transporte HTTP, HTTPS, JMS und Dateiverzeichnis.

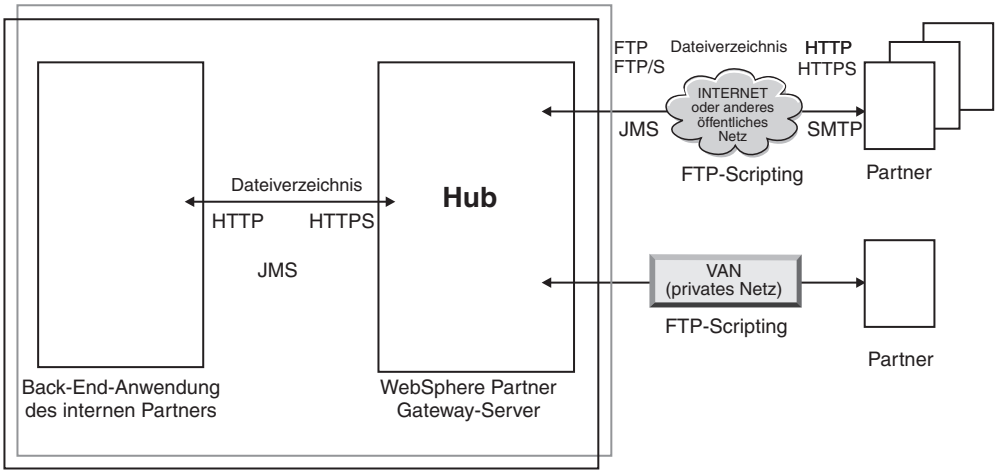



*Abbildung 2. Die am häufigsten verwendeten Transporte, die von WebSphere Partner Gateway unterstützt werden*

Der Transporttyp, mit dem Dokumente gesendet und empfangen werden, beeinflusst die Konfiguration von Empfängern und Zielen. Ein *Empfänger* ist ein Einstiegspunkt in den Hub. Es ist der Ort, an dem Dokumente, die von Partnern oder Back-End-Anwendungen gesendet wurden, auf dem Hub empfangen werden. Ein *Ziel* ist ein Einstiegspunkt in den Computer des Partners oder des Back-End-Systems. Es ist der Ort, an den der Hub Dokumente sendet. Sie müssen eine Reihe von Konfigurationsaufgaben ausführen, wie in Kapitel 4, „Konfiguration des Hubs vorbereiten", auf Seite 35 beschrieben, um die Verwendung der Transporte FTP, FTPS, FTP-Scripting, JMS und Dateiverzeichnis vorzubereiten.

## Übersicht über Dokumentdefinitionen

Wenn Sie den Austausch von Dokumenten zwischen externen Partnern und internen Partnern definieren, geben Sie mehrere Informationen bezüglich des Dokuments an:

- Das *Paket*, das das Dokument umgibt.
- Das *Geschäftsprotokoll*, das eine Klasse von Dokumenten definiert, die einige allgemeine Merkmale gemeinsam haben.
- Den *Dokumenttyp*, der eines der Dokumente identifiziert, die vom Geschäftsprotokoll bereitgestellt werden.

Das Paket des Dokuments, das Protokoll des Dokuments und der Dokumenttyp bilden gemeinsam die *Dokumentdefinition*. Nehmen wir an, Sie verwenden die folgende, vom Produkt bereitgestellte Dokumentdefinition:

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

Wird ein Dokument empfangen, das dieser Routing-Definition entspricht, geschieht Folgendes: Nachdem der Hub das Dokument empfangen hat, stellt der Entpackschritt des festen Eingangsarbeitsablauf fest, das der Pakettyp AS vom Dokument verwendet wird. Dies liegt daran, dass Transportheader vorhanden sind, die für das Paket AS angegeben wurden. Andere Pakettypen werden vom Hub in ähnlicher Weise erkannt, in der Regel durch Überprüfung der Transportheader, die mit dem Dokument eingehen. Liegt keine Übereinstimmung mit einem Pakettyp vor, wird dem Dokument der Pakettyp **None** zugeordnet. Bei AS-Paketen werden die Geschäfts-IDs von Absender und Empfänger über die Transportheader der Nachricht ermittelt. Die AS-Transportheader enthalten zudem weitere Header, die angeben können, ob die Nachricht verschlüsselt, komprimiert oder signiert ist.

Nach der Identifizierung des Pakets ermittelt der Parsingschritt des Protokolls für festen Eingangsarbeitsablauf für den Hub das Protokoll und den Dokumenttyp des Dokuments. Dazu wird der tatsächliche Nachrichteninhalt überprüft und in dem Dokument nach Merkmalen gesucht, die das Protokoll und den Dokumenttyp angeben. Darüber hinaus extrahiert der Parsingschritt des Protokolls für den Arbeitsablauf in Abhängigkeit des verwendeten Protokolls weitere Informationen aus dem Dokument.

Nachdem das Paket, das Protokoll und der Dokumenttyp für ein Dokument bekannt sind, kann der Hub die Verarbeitung des Dokuments fortsetzen. An diesem Punkt sind zusätzlich zu den Informationen zu Paket, Protokoll und Dokumenttyp die Geschäfts-IDs von Absender und Empfänger bekannt. Anhand dieser Informationen kann der Hub nach einer Verbindung zwischen Absender- und Empfängerpartner suchen, die das eingehende Paket, das Protokoll und den Dokumenttyp aufweist.

Sobald die Verbindung gefunden wurde, weiß der Hub, wie das Dokument weitergeleitet und verarbeitet werden muss, da Zugriff auf die folgenden zusätzlichen Informationen besteht:

- Zertifikate für Absender- und Empfängerpartner (sofern erforderlich)
- Attributeinstellungen für Absender- und Empfänger-Routing
- Die Aktion, die bei der Weiterleitung des Dokuments ausgeführt werden muss
- Die anwendbare Transformationszuordnung (sofern vorhanden)
- Die anwendbare Validierungszuordnung (sofern vorhanden)

## Paket

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

Abb. 3 auf Seite 9 zeigt die Pakettypen, die für Dokumente festgelegt werden können, die zwischen dem Hub und einem externen Partner und zwischen dem Hub und einer Back-End-Anwendung ausgetauscht werden.

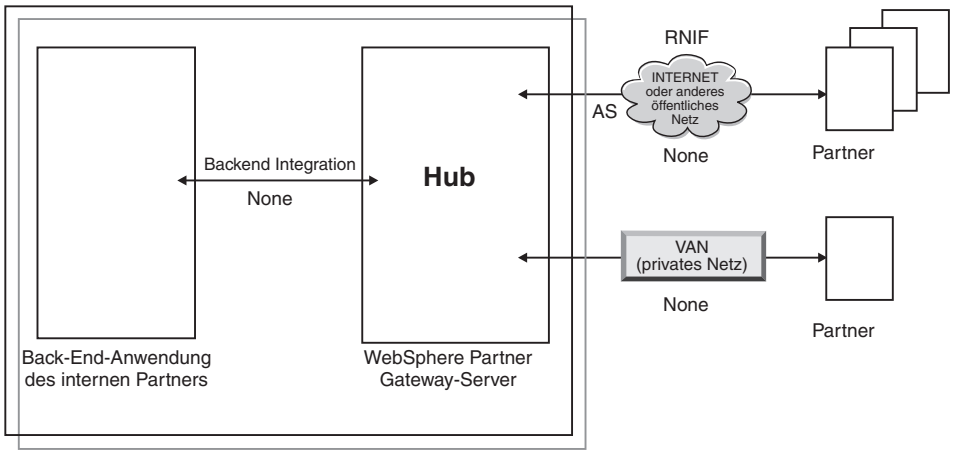



*Abbildung 3. Pakettypen für Dokumente*

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

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

**AS:** Das Paket **AS** wird am häufigsten zwischen Partnern und dem Hub verwendet. Das Paket **AS** kann für Dokumente verwendet werden, die mit den Standards AS1, AS2 oder AS3 konform sind. AS1 ist ein Standard, der für das sichere Übertragen von Dokumenten über SMTP verwendet wird, und AS2 ist ein Standard, der für das sichere Übertragen von Dokumenten über HTTP oder HTTPS verwendet wird. AS3 ist ein neuer Standard, der für das sichere Übertragen von Dokumenten über FTP oder FTPS verwendet wird. Dokumente, die von einem Partner mit dem Paket **AS** gesendet werden, haben entweder AS1-, AS2- oder AS3-Headerinformationen. An einen Partner gesendete Dokumente, der AS1-, AS2- oder AS3-Header erwartet, müssen (auf dem Hub) als Paket **AS** gepackt werden.

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

**RNIF:** Das Paket **RNIF** wird auf dem Installationsdatenträger bereitgestellt. Sie laden das Paket **RNIF** (zusammmen mit den PIPs, die Sie austauschen wollen) wie im Abschnitt „RosettaNet-Dokumente" auf Seite 114 beschrieben hoch. Das Paket **RNIF** wird verwendet, um RosettaNet-Dokumente vom Partner an den Hub bzw. vom Hub an den Partner zu senden.

**ebMS:** Der ebMS-Mechanismus (ebMS - ebXML Message Service) bietet eine standardisierte Möglichkeit für den Austausch von Geschäftsnachrichten zwischen ebXML-Handelspartnern. Mit ebMS können Geschäftsnachrichten zuverlässig aus-

getauscht werden, ohne auf proprietäre Technologien und Lösungen angewiesen zu sein. Eine ebXML-Nachricht enthält Strukturen für einen Nachrichtenheader (erforderlich für Routing und Zustellung), sowie einen Abschnitt mit Nutzdaten.

ebMS bietet eine standardisierte Möglichkeit für den Austausch von Geschäftsnachrichten zwischen ebXML-Handelspartnern. Eine ebXML-Nachricht ist ein vom Kommunikationsprotokoll unabhängiger MIME/Multipart-Nachrichtenumschlag.

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

Bei den meisten Übertragungen in einer Richtung zwischen einem externen Partner und dem internen Partner (oder umgekehrt) empfängt WebSphere Partner Gateway ein Dokument vom externen Partner und sendet es an den internen Partner. Wenn Sie in WebSphere Partner Gateway die Partnerverbindung erstellen, geben Sie das Paket an, in dem WebSphere Partner Gateway das Dokument empfangen wird, sowie das Paket, das WebSphere Partner Gateway verwenden wird, um das Dokument zu senden. In Abb. 4 fließt ein als AS gepacktes Dokument von einem externen Partner zur Back-End-Anwendung des internen Partners. Das Dokument wird an das Ziel des internen Partners ohne Transportheader zugestellt. In Abb. 4 ist dem Austausch von Dokumenten genau eine Aktivität zugeordnet.

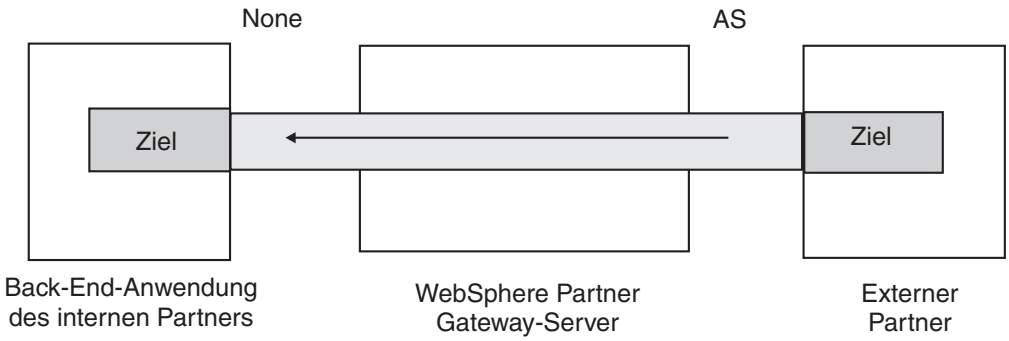



*Abbildung 4. Typische Einwegverbindung*

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

Der Prozess für das Definieren der Dokumentdefinitionen, die für einen EDI-Austausch erforderlich sind, wird in Kapitel 10, „EDI-Dokumentenflüsse konfigurieren", auf Seite 173 beschrieben.

## Protokolle

Die folgenden Protokolle werden vom System bereitgestellt:

- Binary

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

- EDI-X12, EDI-Consent, EDI-FACT

  Diese EDI-Protokolle können mit den Paketen **AS** oder **None** verwendet werden. Wie im Abschnitt „ N/A" auf Seite 10 beschrieben, geben Sie das Paket **N/A** an, falls die EDI-Transaktion oder der EDI-Austausch vom Hub stammt bzw. dort endet. X12 und EDIFACT sind EDI-Standards, die für den Austausch von Daten verwendet werden. EDI-Consent bezieht sich auf Inhaltstypen, die in der Spezifikation "EDI-Consent" angegeben sind.

- Web Service

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

- cXML

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

- XMLEvent

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

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

Bei der Transformation von EDI-Transaktionen oder XML- bzw. ROD-Dokumenten werden zur Erstellung von Transformationszuordnungen der DIS-Client (DIS - Data Interchange Services) oder WTX Design Studio verwendet.

Im DIS-Client werden Wörterverzeichnisse für das Protokoll definiert, das dieser Transformation zugeordnet ist. Ein Wörterverzeichnis enthält Informationen zu allen EDI-Dokumentdefinitionen, EDI-Segmenten, zusammengesetzten EDI-Datenelementen und EDI-Datenelementen, die den EDI-Standard ausmachen. Die Definitionen der Quellendokumente für EDI werden von WDI bereitgestellt, bei ROD und XML müssen sie im DIS-Client erstellt werden. Ab Version 6.2.1 können die Standard- und die Transformationszuordnungen separat kompiliert werden. Detaillierte Informationen zu einem bestimmten EDI-Standard finden Sie in den entsprechenden Handbüchern der jeweiligen EDI-Standards. Informationen zum Data Interchange Services-Client finden Sie im *WebSphere Partner Gateway Mapping Guide* oder in der Onlinehilfe, die mit dem Data Interchange Services-Client bereitgestellt wird.

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

Sie können angepasste Protokolle erstellen, um genau zu definieren, wie ein Dokument strukturiert sein soll. Bei XML-Dokumenten können Sie ein XML-Format definieren, wie in „Angepasste XML-Dokumentverarbeitung" auf Seite 159 beschrieben.

## Dokumenttyp

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

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

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

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

Sie können auch Ihre eigenen Dokumenttypen erstellen, wie in „Angepasste XML-Dokumentverarbeitung" auf Seite 159 beschrieben.

## Übersicht über die Dokumentverarbeitung

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

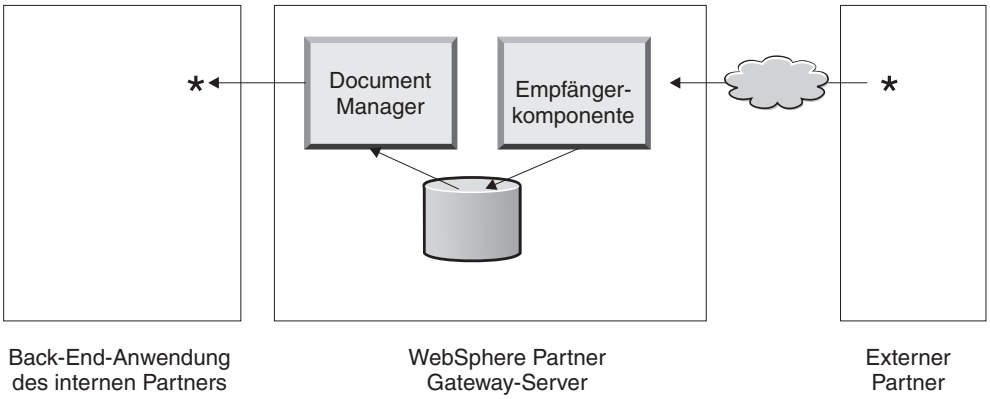



*Abbildung 5. Die Komponenten "Empfänger" und "Document Manager"*

Abb. 5 ist ein Beispiel dafür, wie ein Dokument von einem Partner gesendet, vom Hub empfangen, auf dem Hub verarbeitet und an eine Back-End-Anwendung des internen Partners gesendet wird.

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

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

Empfängerinstanzen sind transportspezifisch. Sie konfigurieren einen Empfänger für jeden Transporttyp, den der Hub unterstützt. Wenn Partner z. B. Dokumente über HTTP senden, konfigurieren Sie einen HTTP-Empfänger, um diese zu empfangen.

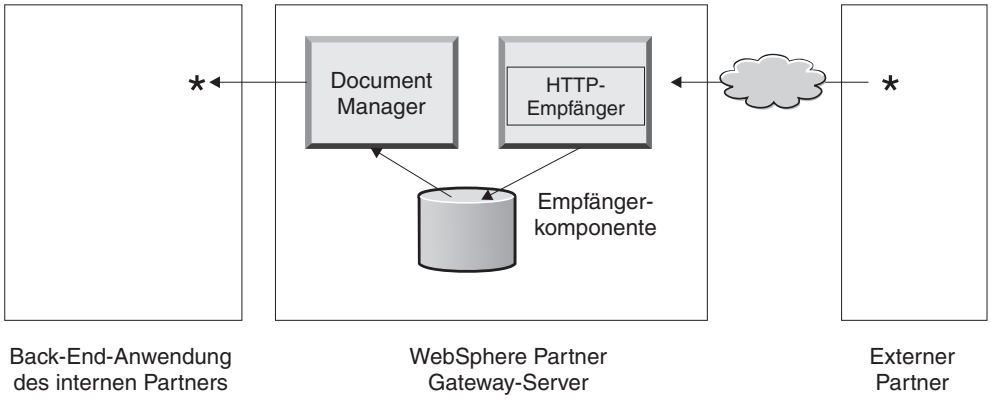



*Abbildung 6. Ein HTTP-Empfänger*

Wenn die Back-End-Anwendung des internen Partners Dokumente über JMS senden wird, konfigurieren Sie einen JMS-Empfänger auf dem Hub, um diese zu empfangen.

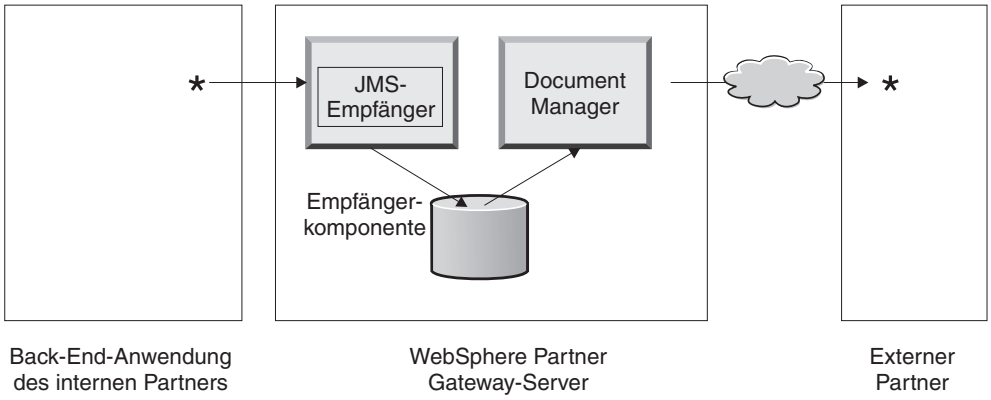



*Abbildung 7. Ein JMS-Empfänger*

Wie in „Übersicht über Transporte" auf Seite 6 beschrieben, unterstützt WebSphere Partner Gateway eine Vielzahl von Transporten, aber Sie können auch Ihren eigenen benutzerdefinierten Transport hochladen, um einen Empfänger zu definieren (wie in „ Empfänger für benutzerdefinierten Transport konfigurieren" auf Seite 76 beschrieben).

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

Der interne Partner könnte z. B. ein EDI-X12-Dokument im Paket **None** an den Hub senden, das an einen Partner gesendet werden soll, der das EDI-X12-Dokument in einem Paket **AS2** erwartet. Der Partner stellt die HTTP-URL bereit, an die das Dokument im Paket **AS2** gesendet werden soll, und Document Manager packt das Dokument wie vom Partner erwartet.

Document Manager verwendet die Zielkonfiguration für diesen Partner (der für die HTTP-URL konfiguriert worden sein muss, von der der Partner den Empfang der AS2-Dokumente erwartet), um das Dokument an den Partner zu senden.

## Dokumentverarbeitungskomponenten mit Handler konfigurieren

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

Sie verwenden *Handler*, um das vom Produkt bereitgestellte Verhalten von Empfängern, Destiantionen, Schritten für feste Arbeitsabläufe und Aktionen zu ändern. Es gibt zwei Handlertypen: die von WebSphere Partner Gateway bereitgestellten Handler und die benutzerdefinierten Handler. Informationen zur Erstellung von Handlern finden Sie im *WebSphere Partner Gateway Programmer Guide*.

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

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

### Empfänger

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

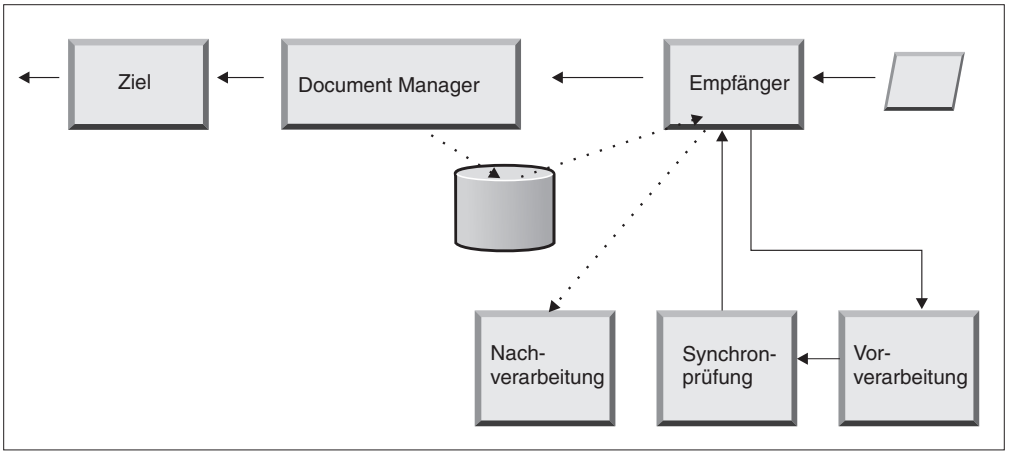



*Abbildung 8. Konfigurationspunkte für Empfänger*

Die Verarbeitung findet in der folgenden Reihenfolge statt:

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

Die Schritte werden in den folgenden Abschnitten beschrieben:

- Vorverarbeitung

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

  Informationen darüber, wie Sie den Vorverarbeitungs-Konfigurationspunkt konfigurieren, finden Sie in „ Vorverarbeitung" auf Seite 77.

- Synchronprüfung

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

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

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

  Informationen darüber, wie Sie den Synchronprüfungs-Konfigurationspunkt konfigurieren, finden Sie in „ Synchronprüfung" auf Seite 80.

- Nachverarbeitung

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

  Informationen darüber, wie Sie den Nachverarbeitungs-Konfigurationspunkt konfigurieren, finden Sie in „ Nachverarbeitung" auf Seite 82.

## Document Manager

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

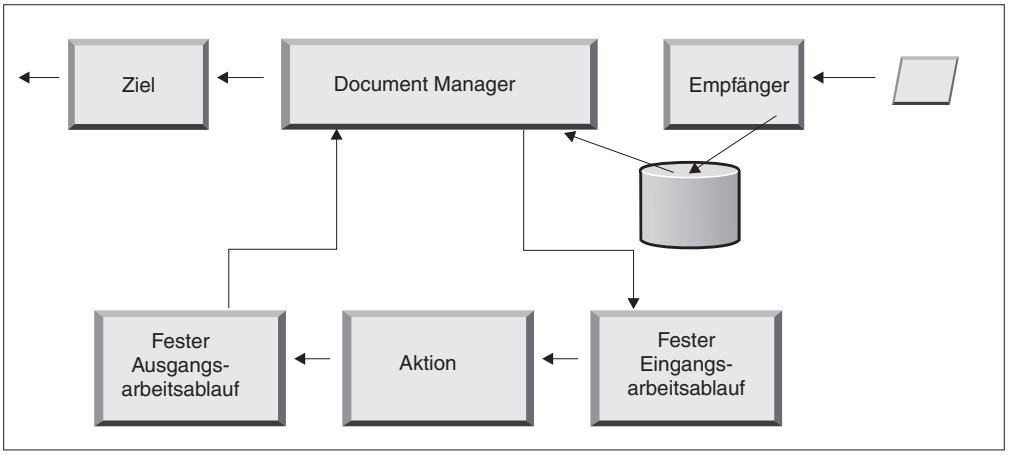



*Abbildung 9. Feste Arbeitsabläufe und Aktionen*

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

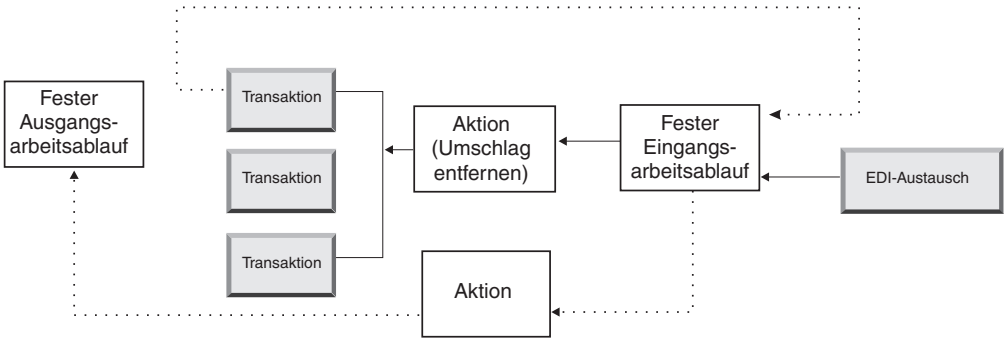



*Abbildung 10. Feste Arbeitsabläufe und Aktionen für einen EDI-Austauschvorgang*

## Fester Eingangsarbeitsablauf

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

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

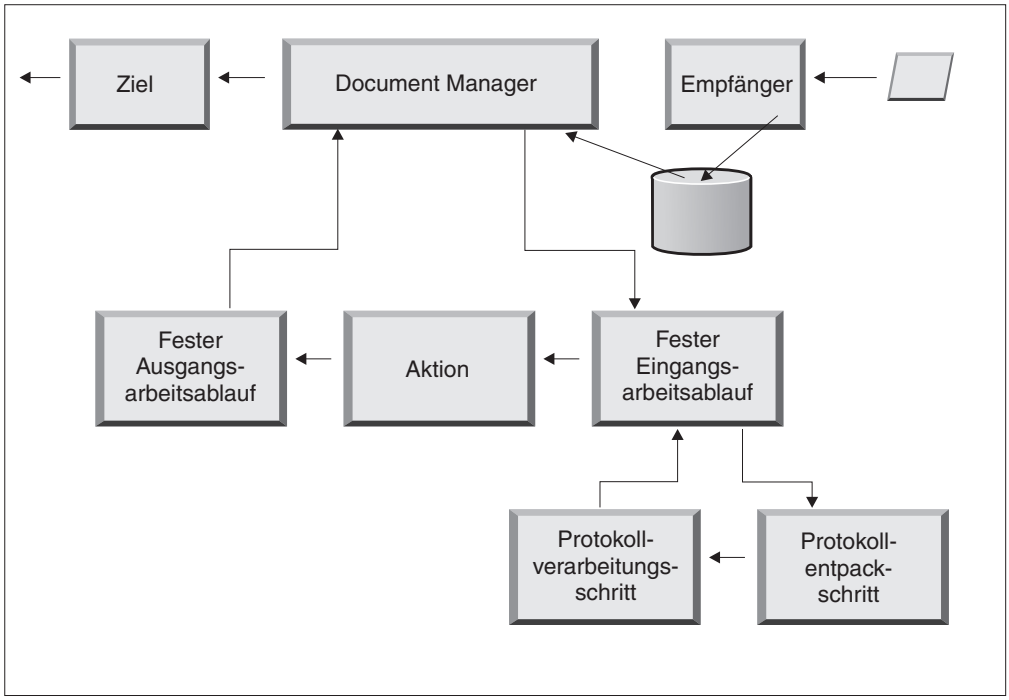



*Abbildung 11. Schritte für festen Eingangsarbeitsablauf*

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

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

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

Informationen darüber, wie Sie diesen Schritt konfigurieren, finden Sie in „Feste Arbeitsabläufe konfigurieren” auf Seite 84.

**Protokollverarbeitungsschritt:** Die Protokollverarbeitung bezieht das Ermitteln protokollspezifischer Informationen mit ein, wozu das Parsing der Nachricht gehören kann, um Route-Informationen (wie z. B. die Absender-ID und die Empfänger-ID), Protokollinformationen und Dokumenttypinformationen zu ermitteln. WebSphere Partner Gateway bietet die Verarbeitung für eine Vielzahl von Protokollen, wie in „ Handler für das Verarbeiten des Protokolls” auf Seite 85 aufgelistet. Die Verarbeitung anderer Protokolle, z. B. CSV (durch Kommata getrennter Wert), kann mit einem Benutzerexit bereitstellt werden.

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

Informationen darüber, wie Sie diesen Schritt konfigurieren, finden Sie in „Feste Arbeitsabläufe konfigurieren” auf Seite 84.

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

## Aktionen

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

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

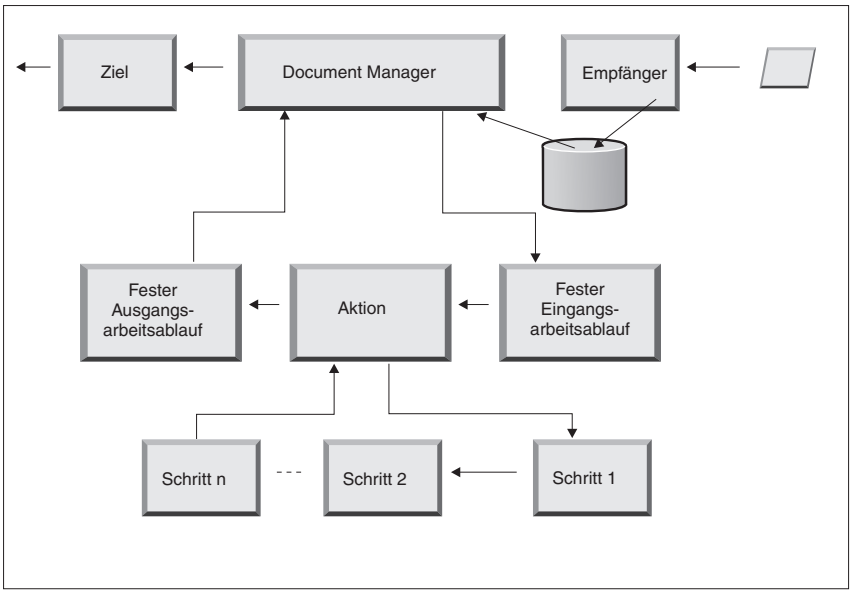



*Abbildung 12. Aktionsschritte*

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

Informationen zum Erstellen oder Kopieren einer vom Produkt bereitgestellten Aktion oder zum Konfigurieren einer benutzerdefinierten Aktion finden Sie in „Aktionen konfigurieren" auf Seite 86.

## Fester Ausgangsarbeitsablauf

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

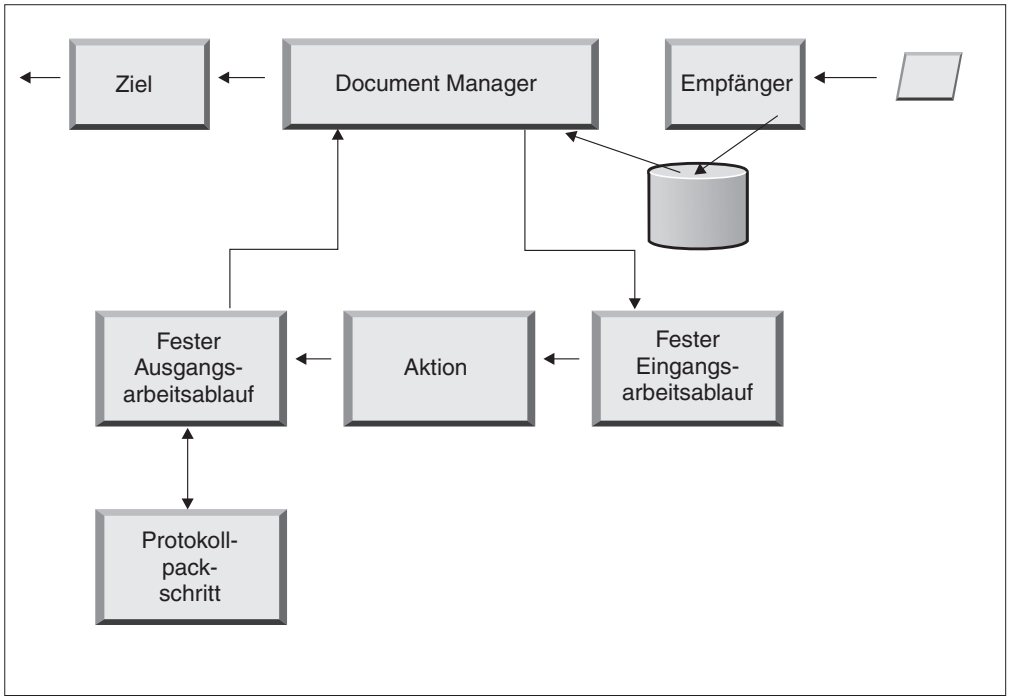



*Abbildung 13. Schritte für festen Ausgangsarbeitsablauf*

WebSphere Partner Gateway bietet Handler für eine Vielzahl von Paketen und Protokollen, wie in „Ausgangsarbeitsablauf" auf Seite 85 aufgelistet. Wenn weitere Pakethandler erforderlich sind, können sie als Benutzerexitschritte gestaltet werden. Normalerweise decken diese Schritte mindestens einen der folgenden Prozesse ab:

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

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

Informationen darüber, wie Sie diesen Arbeitsablaufschritt konfigurieren, finden Sie in „Feste Arbeitsabläufe konfigurieren" auf Seite 84.

## Ziele

Ziele werden in der Konsole für jeden Partner konfiguriert, an den Sie Nachrichten senden wollen. Die Konfiguration eines Ziels umfasst den Transport, der zum Senden von Nachrichten verwendet wird, sowie die hierfür benötigte Konfiguration, wie z. B. die URL für den Empfangsprozess des Partners.

Nachdem das Dokument Document Manager verlassen hat, wird es unter Verwendung eins Ziels an den beabsichtigten Empfänger gesendet. Das Ziel hat zwei Konfigurationspunkte: die Vorverarbeitung und die Nachverarbeitung.

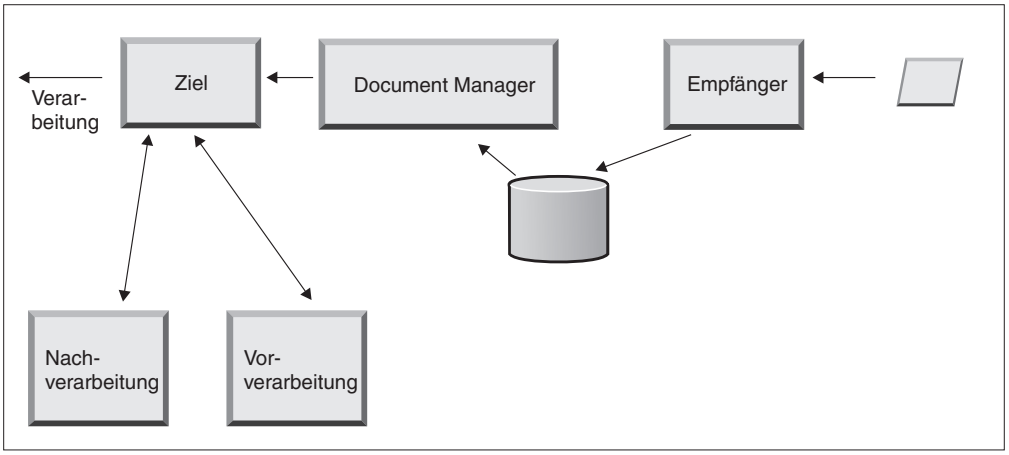



*Abbildung 14. Konfigurationspunkte des Ziels*

- Vorverarbeitung

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

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

Informationen darüber, wie Sie die Vorverarbeitungs- und Nachverarbeitungsschritte konfigurieren, finden Sie in „Handler konfigurieren" auf Seite 248.

# Übersicht über die Hubkonfiguration

Nachdem Sie Ihre Geschäftsanforderungen analysiert haben (siehe Abschnitt „Für die Hubkonfiguration benötigte Informationen" auf Seite 6), konfigurieren Sie den Hub und erstellen Ihre Partnerprofile. Dieser Abschnitt bietet eine Übersicht der zugehörigen Aufgaben auf höchster Ebene.

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

## Hub konfigurieren

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

1. Führen Sie jede vorläufige Konfiguration (sofern erforderlich) für die verwendeten Transporte aus. Die vorläufige Konfiguration wird in Kapitel 4, „Konfiguration des Hubs vorbereiten", auf Seite 35 beschrieben.
2. Passen Sie optional die Konsole an, und ändern Sie das Standardkennwort und die Berechtigungsrichtlinie. Diese Aufgaben werden in Kapitel 6, „Community Console konfigurieren", auf Seite 53 beschrieben.

3. Erstellen Sie Empfänger für die Transporttypen, mit denen Dokumente auf dem Hub (vom internen Partner und von externen Partnern) empfangen werden. Das Erstellen von Empfängern wird in Kapitel 7, „Empfänger definieren", auf Seite 59 beschrieben.

   **Anmerkung:** Wenn Sie den Empfänger mit benutzerdefinierten Handlern konfigurieren, müssen Sie die Handler hochladen, bevor Sie den Empfänger erstellen. Das Hochladen von Handlern wird in „ Benutzerdefinierte Handler hochladen" auf Seite 60 beschrieben.
4. Konfigurieren Sie beliebige Schritte für Eingangsarbeitsablauf oder Aktionen. Dies ist ein *optionaler* Schritt. Er wird nur dann benötigt, wenn bestimmte Anforderungen an die Dokumentverarbeitung gestellt werden, die WebSphere Partner Gateway nicht bereitstellt. Wenn Sie das vom Produkt bereitgestellte Verhalten von Arbeitsabläufen oder Aktionen nicht ändern müssen, überspringen Sie diesen Schritt. Das Konfigurieren der Arbeitsablaufschritte und Aktionen wird in Kapitel 8, „Schritte und Aktionen für feste Arbeitsabläufe konfigurieren", auf Seite 83 beschrieben.

   **Anmerkung:** Sie müssen die benutzerdefinierten Handler hochladen, bevor Sie Arbeitsabläufe oder Aktionen konfigurieren. Das Hochladen von benutzerdefinierten Handlern wird im Abschnitt „ Handler hochladen" auf Seite 83 beschrieben.
5. Erstellen Sie Dokumentdefinitionen (oder prüfen Sie, ob die von Ihnen benötigten Dokumentdefinitionen bereits verfügbar sind), um die Dokumenttypen zu definieren, die Sie auf dem Hub senden und empfangen können.
6. Erstellen Sie Interaktionen, um die gültige Kombination von zwei Dokumentdefinitionen anzuzeigen.

   Das Erstellen von Dokumentdefinitionen und das Erstellen von Interaktionen wird in Kapitel 9, „Dokumenttypen konfigurieren", auf Seite 107 und Kapitel 10, „EDI-Dokumentenflüsse konfigurieren", auf Seite 173 beschrieben.
7. Erstellen Sie ein Profil für den internen Partner, und stellen Sie Informationen zum internen Partner bereit. Erstellen Sie ferner die Dokumenttypen, die der interne Partner senden und empfangen kann (die B2B-Funktionalität des internen Partners). Das Erstellen des Profils wird in Kapitel 3, „Partner erstellen und definieren", auf Seite 25 beschrieben.

## Partner erstellen

Nachdem Sie den Hub konfiguriert haben, erstellen Sie ein Profil für jeden externen Partner, der mit dem internen Partner Dokumente austauschen wird. Nur der Hubadministrator kann Partner erstellen.

Als Hubadministrator können Sie außerdem die B2B-Funktionalität der Partner konfigurieren, die Ziele der Partner erstellen und Sicherheitsprofile für die Partner konfigurieren. Diese Schritte können alternativ von den Partnern selbst ausgeführt werden.

Das Erstellen von Partnern wird in Kapitel 3, „Partner erstellen und definieren", auf Seite 25beschrieben. Das Erstellen von Zielen wird in Kapitel 11, „Ziele erstellen", auf Seite 227 beschrieben. Die Konfiguration von Sicherheitsprofilen wird in Kapitel 13, „Sicherheit für Dokumentenaustauschvorgänge aktivieren", auf Seite 255 beschrieben.

## Dokumentverbindungen aufbauen

Nachdem Sie den Hub konfiguriert und Partnerprofile erstellt haben, können Sie nun Verbindungen konfigurieren. Verbindungen zeigen die gültigen Kombinationen von Absendern und von Empfängern sowie die Dokumente an, die sie austauschen können. Das Verwalten von Verbindungen wird in Kapitel 12, „Verbindungen verwalten", auf Seite 251 beschrieben.

# Übersicht über OpenPGP-Zertifikate

OpenPGP wird in WebSphere Partner Gateway unterstützt. OpenPGP verwendet eine Kombination aus starker Verschlüsselung mit einem öffentlichen Schlüssel und symmetrischer Verschlüsselung, um Sicherheitsservices bereitzustellen. OpenPGP umfasst die folgenden Funktionen, die in diesem Release enthalten sind:

- Gepackte Nachrichten gemäß RFC 4880.

  **Anmerkung:** RFC 2440 und RFC 3156 werden in diesem Release nicht unterstützt.
- Verschlüsselung, Verschlüsselung mit Änderungserkennung und Komprimierung.

  **Anmerkung:** In diesem Release unterstützt WebSphere Partner Gateway das Signieren mit OpenPGP nicht.
- Die folgenden Verschlüsselungsalgorithmen werden unterstützt: CAST5 (128-Bit-Schlüssel), TripleDES (168-Bit-Schlüssel), Blowfish (128-Bit-Schlüssel), Twofish (256-Bit-Schlüssel), AES (128, 192 & 256-Bit-Schlüssel).

  **Anmerkung:** Für Twofish, TripleDES und AES (192 & 256-Bit-Schlüssel) sind Standortrichtliniendateien für die uneingeschränkte Verschlüsselung erforderlich.
- Die folgenden Komprimierungsalgorithmen werden unterstützt: ZIP, ZLIB und BZip2.
- Nachrichten im Format ASCII-Armored.
- Die Funktion für die Partnermigration und die FIPS-Konformität wurde geändert, um OpenPGP zu unterstützen.
- Die teilweise Verarbeitung von Dokumenten wird von OpenPGP nicht unterstützt.

Bevor Sie mit OpenPGP-Zertifikaten arbeiten können, müssen einige Voraussetzungen erfüllt sein.

Laden Sie die folgenden Bibliotheksdateien von einer externen Quelle herunter und kopieren Sie sie in den Ordner 'HUB_INSTALLATIONSPOSITION>/lib/openpgp':

- BouncyCastle OpenPGP-Bibliothek Version 1.45 für JDK 1.5
- BouncyCastle JCE-Bibliothek Version 1.45 für JDK 1.5

  **Wichtig:** Beziehen Sie diese Bibliotheksdateien von einer externen Quelle, da sie nicht von IBM bereitgestellt werden. Weitere Informationen zum Beziehen der Bibliotheksdateien finden Sie auf der Homepage von Bouncy Castle unter http://www.bouncycastle.org. Die zu entpackenden JAR-Dateien sind http://www.bouncycastle.org/download/bcpg-jdk15-145.jar und http://www.bouncycastle.org/download/bcprov-jdk15-145.jar. Im verteilten Modus müssen Sie die JAR-Dateien auf allen Computern installieren, auf denen Document Manager und die Konsole installiert sind.

Starten Sie den Server erneut, nachdem Sie die Dateien an die angegebene Position kopiert haben.

# Kapitel 3. Partner erstellen und definieren

Es gibt zwei Partnertypen: interne Partner und externe Partner. Der interne Partner ist normalerweise das Unternehmen, das Eigner des WebSphere Partner Gateway-Servers ist und mithilfe des Servers mit anderen Unternehmen kommuniziert. Der interne Partner ist Eigner der Back-End-Anwendungen (interne Anwendungen des Unternehmens, das Eigner ist). Es können beliebig viele interne Partner vorhanden sein; der Standardpartner ist jedoch im Allgemeinen der erste definierte Partner. Die anderen Unternehmen, mit denen der interne Partner kommuniziert, sind die externen Partner.

Für jeden Partner, mit dem Sie Dokumente austauschen, müssen Sie ein Partnerprofil erstellen. Zusätzlich zum Erstellen von Profilen müssen diese definiert werden; dieser Prozess umfasst mehrere erforderliche und optionale Schritte.

In diesem Kapitel werden die grundlegenden Schritte zum Erstellen und Konfigurieren eines Partnerprofils beschrieben. Detaillierte Informationen zu einem bestimmten Schritt finden Sie in der Referenz, die am Ende des jeweiligen Schritts oder Abschnitts angegeben ist. Dieses Kapitel ist in die folgenden Abschnitte unterteilt:



**Anmerkung:** Verwenden Sie stets die Browserinstanz, mit der Sie sich an Community Console angemeldet haben, wenn Sie Konfigurationsänderungen an WebSphere Partner Gateway vornehmen. Die gleichzeitige Verwendung mehrerer Browserinstanzen kann dazu führen, dass die Konfigurationsänderungen aufgehoben werden.

## Partnerprofile erstellen

Dies ist der erste Schritt beim Definieren eines Partners in WebSphere Partner Gateway. In diesem Schritt werden Basisinformationen für den Partner definiert, wie beispielsweise Name, Anmeldename und Geschäfts-IDs.

Zum Erstellen eines Partners müssen die folgenden Informationen zu diesem Partner bekannt sein:

- Die Geschäfts-ID, die der Partner 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 Partner auswählt, um mit ihr die Firma anzugeben.

Gehen Sie für jeden Partner, den Sie der Hub-Community hinzufügen möchten, wie folgt vor:

1. Klicken Sie auf **Kontenadmin > Profile > Partner**.
2. Klicken Sie auf **Erstellen**.
3. Geben Sie einen Wert im Feld **Anmeldename des Unternehmens** ein. Dies ist der Namen, den der Partner im Unternehmensfeld beim Anmelden am Hub verwendet. Der Anmeldename des Unternehmens darf keine Leerzeichen enthalten.
4. Geben Sie unter **Anzeigename des Partners** den Firmennamen oder einen anderen beschreibenden Namen für den Partner ein. Dies ist der Name, der in der Liste **Partnersuche** angezeigt wird.
5. Wählen Sie den Partnertyp aus. Wenn es sich um den ersten Partner handelt, konfigurieren Sie vermutlich das Unternehmen, das Eigner von WebSphere Partner Gateway ist. Wählen Sie in diesem Fall **Interner Partner** aus. Wählen Sie in der Anzeige für die Partnerkonfiguration das Kontrollkästchen **Interner Standardpartner** aus, wenn der aktuelle interne Partner als Standardpartner definiert werden soll. Wenn Sie dieses Kontrollkästchen für einen anderen Partner auswählen, wird die Auswahl als Standardpartner automatisch vom bisherigen internen Standardpartner entfernt. Auf dieser Seite kann die Auswahl nicht gelöscht werden. Für den ersten erstellten internen Partner wird dieses Kontrollkästchen automatisch ausgewählt.
6. Geben Sie optional den Benutzernamen für den Administrator ein. Der Benutzername für den Administrator muss für alle Partner eindeutig sein. Der Administrator des Partners kann Verwaltungsaktivitäten für diesen Partner, wie beispielsweise die Verwaltung von Zielen, B2B-Funktionalität und Benutzern, ausführen. Der Hubbetreiber hat stets vollständigen Zugriff auf die Partnerverwaltung.
7. Wählen Sie den Status für den Partner aus. Wählen Sie **Aktiviert** aus, wenn der Status des Partners **Inaktiviert** ist. **Aktiviert** ist der Standardstatus des Partners.
8. Geben Sie optional den Firmentyp in das Feld **Lieferantentyp** ein.
9. Geben Sie optional die Website des Partners ein.
10. Klicken Sie auf **Geschäfts-ID** > **Neu**.
11. Geben Sie einen Typ aus der Liste an und geben Sie die entsprechende Kennung ein. WebSphere Partner Gateway verwendet die von Ihnen hier eingegebene Nummer, um das Dokument zum Partner und vom Partner 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 Partner mehr als eine Geschäfts-ID zuordnen. In einigen Fällen ist mehr als eine Geschäfts-ID erforderlich. Wenn z. B. der Hub EDI-X12- und EDIFACT-Dokumente sendet und empfängt, verwendet er sowohl DUNS- als auch unformatierte IDs während des Dokumentenaustauschs.

Sowohl der interne Partner als auch die externen Partner, die an diesen Dokumentenflusstypen beteiligt sind, sollten jeweils über eine DUNS-ID und eine unformatierte ID verfügen. Die unformatierte ID wird verwendet, um EDI-IDs darzustellen, die über eine Kennung und ein Qualifikationsmerkmal verfügen. Angenommen, das EDI-Qualifikationsmerkmal lautet z. B. "ZZ" und die EDI-Kennung lautet "810810810". Dann könnte die unformatierte ID wie folgt angegeben werden: ZZ-810810810.
Wenn Sie auf **Neu** klicken, wird auch das Textfeld "E-Mail-ID" aktiviert und angezeigt, damit Sie eine E-Mail-ID erstellen können.

12. Klicken Sie auf **Neu**, um eine neue E-Mail-ID zu erstellen, und geben Sie die E-Mail-ID im Feld "E-Mail-Kennung" ein. Wenn Sie auf **Neu** klicken, können Sie auch mehrere E-Mail-IDs erstellen.
13. Geben Sie optional eine IP-Adresse für den Partner ein. Die IP-Adresse wird in Verbindung mit einem Ziel verwendet, wenn **Client-IP prüfen** konfiguriert ist. Geben Sie eine IP-Adresse ein, indem Sie die folgenden Schritte ausführen:
    a. Klicken Sie unter **IP-Adresse** auf **Neu**.
    b. Geben Sie den Betriebsmodus an.
    c. Geben Sie die IP-Adresse des Partners ein.
14. Klicken Sie auf **Speichern**.
15. Wenn Sie eine Der Benutzernamen für den Administrator eingegeben haben, wird Ihnen ein Kennwort übermittelt, das der Partner verwendet, um sich beim Hub anzumelden. Notieren Sie sich dieses Kennwort. Stellen Sie es dem Administrator des Partners zur Verfügung.

## Ziele erstellen

Nachdem Sie ein Profil für einen Partner erstellt haben, müssen Sie die Ziele erstellen, die der Hub zum Senden von Dokumenten an den Partner verwendet.

Gehen Sie wie folgt vor, um Ziele für einen Partner zu erstellen:

1. Stellen Sie sicher, dass das Partnerprofil, für das Sie Ziele erstellen wollen, ausgewählt ist.
   Wenn Sie gerade ein Profil erstellt haben, ist dieses Profil bereits ausgewählt. Wenn es nicht ausgewählt ist, führen Sie die folgenden Schritte aus:
    a. Klicken Sie auf **Kontenadmin** > **Profile** > **Partner**.
    b. Geben Sie Suchkriterien ein und klicken Sie auf **Suchen**. Sie können auch auf **Suchen** klicken, ohne Suchkriterien einzugeben, um eine Liste aller Partner anzuzeigen.
    c. Klicken Sie auf das Symbol **Details anzeigen**, um das Profil des Partners anzuzeigen.
2. Klicken Sie auf **Ziele** .
3. Klicken Sie auf **Erstellen**.
4. Geben Sie einen Namen des Ziels ein, um das Ziel zu identifizieren.
5. Geben Sie optional den Status des Ziels an.
6. Geben Sie optional an, ob das Ziel **online** oder **offline** ist.
7. Geben Sie optional eine **Beschreibung** für das Ziel ein.
8. Wählen Sie einen **Transport** aus.

9. Nachdem Sie einen Transport ausgewählt haben, wird der Abschnitt **Zielkonfiguration** auf dieser Seite bezogen auf diesen Transport angezeigt. Informationen zum Ausfüllen dieses Abschnitts für die einzelnen Transporte finden Sie in den folgenden Abschnitten:
   - „Globale Transportwerte konfigurieren" auf Seite 229

     **Anmerkung:** Diese Werte beziehen sich nur auf das FTP-Scripting-Ziel.
   - „HTTP-Ziel einrichten" auf Seite 231
   - „HTTP-Ziel einrichten" auf Seite 233
   - „FTP-Ziel einrichten" auf Seite 234
   - „SMTP-Ziel einrichten" auf Seite 236
   - „JMS-Ziel einrichten" auf Seite 237
   - „Dateiverzeichnisziel einrichten" auf Seite 239
   - „FTPS-Ziel einrichten" auf Seite 241
   - „FTP-Scripting-Ziel einrichten" auf Seite 244
   - „SFTP-Ziel einrichten" auf Seite 242

## B2B-Funktionalität konfigurieren

Jeder Partner verfügt über B2B-Funktionalität, die die Dokumenttypen definiert, die der Partner senden und empfangen kann.

Als Hubadministrator können Sie die B2B-Funktionalität Ihrer Partner konfigurieren bzw. die Partner können diese Aufgabe selbst ausführen. Sie verwenden diese Funktion, um die B2B-Funktionalität eines Partners einer Dokumentdefinition zuzuordnen.

Gehen Sie wie folgt vor, um die B2B-Funktionalität für jeden Partner zu konfigurieren:

1. Stellen Sie sicher, dass das Partnerprofil, für das Sie die B2B-Funktionalität konfigurieren möchten, ausgewählt ist. Das ausgewählte Profil wird oben auf der Seite nach der Zeichenfolge **Profil** angezeigt.

   Wenn Sie gerade ein Profil erstellt haben, ist dieses Profil bereits ausgewählt. Wenn kein Profil ausgewählt ist, führen Sie die folgenden Schritte aus:
   a. Klicken Sie auf **Kontenadmin**.
   b. Geben Sie Suchkriterien ein und klicken Sie auf **Suchen**. Sie können auch auf **Suchen** klicken, ohne Suchkriterien einzugeben, um eine Liste aller Partner anzuzeigen.
   c. Klicken Sie auf das Symbol **Details anzeigen**, um das Profil des Partners anzuzeigen.
2. Klicken Sie auf **B2B-Funktionalität**. Die Seite **B2B-Funktionalität** wird angezeigt. Auf der Seite werden rechts die Pakete, Protokolle und Dokumente angezeigt, die vom System als Dokumentdefinitionen unterstützt werden.
3. Klicken Sie auf das Symbol **Rolle ist nicht aktiv** unter der Spalte **Quelle festlegen** für die Pakete. Das Paket enthält Dokumente, die die externen Partner an den internen Partner senden.
4. Wählen Sie sowohl **Quelle festlegen** als auch **Ziel festlegen** aus, wenn die Partner dieselben Dokumente senden und empfangen. Die Konsole zeigt ein Häkchen an, wenn die Dokumentdefinition aktiviert ist.

**Anmerkung:** Die Auswahl von **Quelle festlegen** ist für alle Aktionen in einem Zweiwege-PIP gleich, ungeachtet der Tatsache, dass die Anforderung von einem Partner und die entsprechende Bestätigung von einem anderen Partner stammt. Dies gilt auch für **Ziel festlegen**.

5. Klicken Sie auf das Symbol **Erweitern** auf der Ebene **Paket**, um einen einzelnen Knoten auf die entsprechende Ebene der Dokumentdefinition zu erweitern, oder wählen Sie eine Zahl zwischen **0-4** oder **Alle** aus, um alle angezeigten Dokumentdefinitionen auf die ausgewählte Ebene zu erweitern.
6. Wählen Sie erneut **Quelle festlegen**, **Ziel festlegen** oder beide Rollen für die unteren Ebenen von **Protokoll** und **Dokumenttyp** für jede Dokumentdefinition aus, die Ihr System unterstützt.

   Wenn eine Definition auf der Ebene **Dokumenttyp** aktiviert ist, werden die Definitionen **Aktion** und **Aktivität**, sofern vorhanden, automatisch aktiviert.
7. Klicken Sie optional auf **Aktiviert** in der Spalte **Aktiviert**, um eine Dokumentdefinition offline zu setzen. (Wenn Sie **Quelle festlegen** oder **Ziel festlegen** auswählen, ist der Eintrag automatisch aktiviert.) Klicken Sie auf **Inaktiviert**, um die Definition online zu setzen.

   Wenn ein Paket inaktiviert ist, sind alle Dokumentdefinitionen der unteren Ebene im selben Knoten ebenfalls inaktiviert, ungeachtet dessen, ob sie individuell aktiviert waren. Wenn eine Dokumentdefinition der unteren Ebene inaktiviert wird, bleiben alle Definitionen der höheren Ebenen im selben Kontext aktiviert. Wenn eine Dokumentdefinition inaktiviert wird, funktionieren alle zuvor vorhandenen Verbindungen und Attribute nicht mehr.
8. Klicken Sie optional auf das Symbol **Bearbeiten**, wenn Sie beliebige Attribute eines Protokolls, eines Pakets, eines Dokumenttyps, einer Aktion, einer Aktivität oder eines Signals bearbeiten wollen. Anschließend werden die Einstellungen für die Attribute angezeigt (sofern Attribute vorhanden sind). Sie können die Attribute ändern, indem Sie einen Wert eingeben oder einen Wert in der Spalte **Aktualisieren** auswählen und dann auf **Speichern** klicken.

## Zertifikate laden

Mit Zertifikaten können Partner unter Verwendung der folgenden Methoden sichere Dokumente senden und empfangen: Verschlüsselung, digitale Signatur oder SSL. Wenn ein Partner ein Zertifikat von einem anderen Partner empfangen hat, kann dieser Partner eine beliebige dieser Methoden verwenden, um das Dokument zu senden.

Verwenden Sie die im Abschnitt „Zertifikate mit dem Assistenten hochladen" auf Seite 290 beschriebenen Schritte, um Zertifikate für einen Partner hochzuladen.

Weitere Informationen zur Verwendung von Zertifikaten finden Sie in Kapitel 13, „Sicherheit für Dokumentenaustauschvorgänge aktivieren", auf Seite 255.

## Benutzer erstellen

Benutzer sind Personen, die sich zur Ausführung von Verwaltungsaufgaben für den Partner anmelden. Neue Benutzer, die zum LDAP-Server und zur WAS-Verwaltungskonsole hinzugefügt werden, müssen auch in der WebSphere Partner Gateway-Konsole hinzugefügt werden, damit sie aktiv werden können.

Gehen Sie wie folgt vor, um Benutzer für einen Partner zu erstellen:

1. Stellen Sie sicher, dass das Partnerprofil, für das Sie Benutzer erstellen möchten, ausgewählt ist. Das ausgewählte Profil wird oben auf der Seite nach der Zeichenfolge **Profil >** angezeigt. Wenn kein Profilname ausgewählt ist, können Sie die folgenden Schritte ausführen, um ein Profil zu erstellen:
   a. Klicken Sie auf **Kontenadmin > Profile > Partner**.
   b. Geben Sie Suchkriterien ein und klicken Sie auf **Suchen**. Sie können auch auf **Suchen** klicken, ohne Suchkriterien einzugeben, um eine Liste aller Partner anzuzeigen.
   c. Klicken Sie auf das Symbol **Details anzeigen**, um das Profil des Partners anzuzeigen.
2. Klicken Sie auf **Benutzer**.
3. Klicken Sie auf **Erstellen**.
4. Geben Sie den Namen des Benutzers ein.

   **Anmerkung:** Benutzernamen müssen für alle Partner im System eindeutig sein.
5. Stellen Sie sicher, dass der Status auf **Aktiviert** gesetzt ist.
6. Geben Sie optional den Vornamen, den Nachnamen und weitere persönliche Informationen für den Benutzer ein.
7. Wählen Sie **Sprache**, **Formatlocale** und **Zeitzone** für den Benutzer aus.
8. Ändern Sie den Alertstatus des Benutzerstatus in **Aktiviert**.
9. Wählen Sie die subskribierte Sichtbarkeit für den Benutzer aus.
10. Klicken Sie entweder auf **Kennwort autom. generieren**, um ein Kennwort für den Benutzer zu erstellen, oder geben Sie ein Kennwort ein und wiederholen Sie anschließend die Eingabe.
11. Klicken Sie auf **Speichern**.

**Anmerkung:**

1. Da für einen LDAP-Server eindeutige Benutzernamen erforderlich sind, müssen die Benutzernamen für WebSphere Partner Gateway ebenfalls eindeutig sein. Wenn Sie einen neuen Benutzer erstellen und der Benutzername bereits im selben oder in einem anderen Partner vorhanden ist, wird die folgende Fehlernachricht angezeigt: `Ein Benutzer mit diesem Namen ist bereits vorhanden.`
2. Wenn Sie von einer früheren Version, in der es keine Einschränkungen für Benutzernamen gab, auf WebSphere Partner Gateway migrieren, werden neben jedem doppelten Benutzernamen zwei Sterne (**) angezeigt, die darauf hinweisen, dass dieser Name im betreffenden oder einem anderen Partnerprofil bereits vorhanden ist. Ändern Sie einen der Benutzernamen, sodass beide eindeutig sind. Neue Benutzer und Gruppen, die zum LDAP-Server und zur WAS-Verwaltungskonsole hinzugefügt werden, müssen auch in der WebSphere Partner Gateway-Konsole hinzugefügt werden, damit sie aktiv werden können.

Zum Aktivieren von LDAP für WebSphere Partner Gateway müssen Sie die LDAP-Serverauthentifizierung unter Verwendung von WebSphere Application Server Console und die LDAP-Benutzerberechtigung unter Verwendung von WebSphere Partner Gateway Community Console konfigurieren. Informationen zum Konfigurieren der LDAP-Authentifizierung finden Sie im Handbuch *WebSphere Partner Gateway Installation*. Informationen zum Verwalten von Benutzern und zum Konfigurieren der LDAP-Benutzerberechtigung finden Sie im Handbuch *WebSphere Partner Gateway Verwaltung*.

Weitere Informationen zur Verwaltung von Benutzern finden Sie im Kapitel zur Benutzerverwaltung im *WebSphere Partner Gateway Partnerhandbuch*.

## FTP-Konfiguration

Führen Sie die Schritte in einem der folgenden Abschnitte aus, um einen FTP- oder SFTP-Benutzer zu erstellen:

- „FTP- und SFTP-Benutzer erstellen" - Einen Benutzer über die Anzeige für die FTP-Verwaltung der Konsole erstellen.
- „Vorhandene Benutzer für FTP und SFTP aktivieren" auf Seite 32

### FTP- und SFTP-Benutzer erstellen

In diesem Schritt werden Benutzer erstellt und beim Erstellen als FTP- oder SFTP-Benutzer konfiguriert.

Sie können FTP- und SFTP-Benutzer auf der Seite **FTP-Benutzerverwaltung** der Konsole erstellen.

1. Klicken Sie auf **Kontenadmin > FTP-Benutzerverwaltung**.
2. Klicken Sie auf **Erstellen**.
3. Geben Sie die Details des Benutzers ein und klicken Sie auf **Speichern**. Weitere Informationen zum Erstellen von Benutzen finden Sie im Abschnitt „Benutzer erstellen" auf Seite 29. Die Informationen für den erfolgreich erstellten Benutzer werden im Nur-Lese-Modus angezeigt.
4. Klicken Sie auf den Link **FTP-Konfiguration**.
5. Wählen Sie in der Anzeige `FTP-Konfiguration` für die Option **FTP-Benutzer aktiviert** oder **SFTP-Benutzer aktiviert** den Eintrag `Aktiviert` aus. Sie können einen Benutzer für den FTP- und den SFTP-Server aktivieren.
6. Geben Sie die folgenden Details der FTP-Konfiguration ein:
   a. Geben Sie das **Ausgangsverzeichnis** ein. Hierbei handelt es sich um den relativen Pfad zu dem für "bcg.ftp.config.rootdirectory" angegebenen Wert.
   b. Aktivieren oder inaktivieren Sie die **Schreibberechtigung** für das Ausgangsverzeichnis.
   c. Aktivieren oder inaktivieren Sie die Berechtigung **Verzeichnis erstellen/entfernen**.
   d. Wählen Sie einen Wert für **Maximale Anzahl Anmeldungen** aus. Dieser Wert gibt die maximale Anzahl der gleichzeitigen Anmeldungen an, die Sie ausführen können.
   e. Wählen Sie einen Wert für **Maximale Anzahl Anmeldungen von derselben IP** aus. Dieser Wert gibt die maximale Anzahl der gleichzeitigen Anmeldungen an, die Sie von derselben IP-Adresse aus ausführen können.
   f. Wählen Sie einen Wert für **Maximale Leerlaufzeit (Sekunden)** aus. Dies ist die maximale Leerlaufzeit der Verbindung in Sekunden, nach der die Benutzerverbindung gelöscht wird.
   g. Wählen Sie einen Wert für **Maximaler Upload (Byte/Sek.)** aus. Dies ist die maximale Geschwindigkeit für den Upload in Byte pro Sekunde.
   h. Wählen Sie einen Wert für **Maximaler Download (Byte/Sek.)** aus. Dies ist die maximale Geschwindigkeit für den Download in Byte pro Sekunde.

**Anmerkung:** Einige Felder enthalten den Wert `Angepasste Begrenzung` in der Dropdown-Liste. Wenn Sie in der Dropdown-Liste den Eintrag `Angepasste Begrenzung` auswählen, müssen Sie den angepassten Wert im Textfeld eingeben.

7. Geben Sie bei einer SFTP-Konfiguration **Schlüssel (nur SFTP)** ein. Die hochgeladene Datei wird für die schlüsselbasierte Authentifizierung verwendet. Das Ordnersymbol gibt an, dass bereits ein Schlüssel hochgeladen wurde. Sie können auch die Schaltfläche **Durchsuchen** verwenden, um einen Schlüssel hochzuladen.
8. Klicken Sie auf **Speichern**.

### Vorhandene Benutzer für FTP und SFTP aktivieren

In diesem Schritt können Sie einen vorhandenen Benutzer als FTP- oder SFTP-Benutzer festlegen.

Um einen FTP- oder SFTP-Benutzer zu konfigurieren, müssen Sie die FTP- oder SFTP-Eigenschaften für einen vorhandenen Benutzer aktivieren.

1. Klicken Sie auf **Kontenadmin > Profile > Benutzer**.
2. Geben Sie die Suchkriterien ein und klicken Sie auf **Suchen**.
3. Ist in den Suchergebnissen die Spalte **Status** für den Kontakt inaktiviert, klicken Sie auf das Symbol zum Aktivieren. Das Symbol wechselt zwischen den Status **Aktiviert** und **Inaktiviert** hin und her.
4. Klicken Sie auf das Symbol **Details anzeigen** für den Benutzer, um den FTP-Zugriff zu konfigurieren.
5. Klicken Sie in der Anzeige mit den Benutzerdetails auf den Link **FTP-Konfiguration**.
6. Wählen Sie in der Anzeige **FTP-Konfiguration** die Option `Aktiviert` für den eintrag **FTP-Benutzer aktiviert** oder **SFTP-Benutzer aktiviert** aus. Ein Benutzer kann für den FTP- und den SFTP-Server aktiviert werden.
7. Geben Sie die Details der FTP- oder der SFTP-Konfiguration ein. Einzelheiten zu den Details der FTP- oder SFTP-Benutzer finden Sie im Abschnitt „FTP- und SFTP-Benutzer erstellen” auf Seite 31.
8. Klicken Sie auf **Speichern**.

## Gruppen erstellen

Durch das Zusammenfassen von Benutzern in Gruppen können Sie eine große Anzahl von Benutzerberechtigungen gleichzeitig verwalten. Neue Gruppen, die zum LDAP-Server und zur WebSphere Application Server-Verwaltungskonsole hinzugefügt werden, müssen auch in der WebSphere Partner Gateway-Konsole hinzugefügt werden, damit sie aktiv werden können.

Gehen Sie wie folgt vor, um Gruppen für jeden Partner zu erstellen:

1. Stellen Sie sicher, dass das Partnerprofil, für das Sie Gruppen erstellen wollen, ausgewählt ist.

   Wenn Sie gerade ein Profil erstellt haben, ist dieses Profil bereits ausgewählt. Wenn kein Profil ausgewählt ist, führen Sie die folgenden Schritte aus:

   a. Klicken Sie auf **Kontenadmin** > **Profile** > **Partner**.
   b. Geben Sie Suchkriterien ein und klicken Sie auf **Suchen**. Sie können auch auf **Suchen** klicken, ohne Suchkriterien einzugeben, um eine Liste aller Partner anzuzeigen.
   c. Klicken Sie auf das Symbol **Details anzeigen**, um das Profil des Partners anzuzeigen.
2. Klicken Sie auf **Gruppen**.
3. Klicken Sie auf **Erstellen**.

4. Geben Sie den Namen der Gruppe ein.
5. Klicken Sie auf **Speichern**.
6. Klicken Sie auf den Link **Zugehörigkeiten**, um der Gruppe Benutzer hinzuzufügen.

   Benutzer, die diesem Partner zugeordnet sind, werden unter **Benutzer nicht in Gruppe** oder **Benutzer in Gruppe** angezeigt. Gehen Sie wie folgt vor, um einer Gruppe einen Benutzer hinzuzufügen:

   a. Klicken Sie auf das Symbol zum Bearbeiten des Datensatzes neben der Gruppe.
   b. Wählen Sie den gewünschten Benutzer aus und klicken Sie auf **Der Gruppe hinzufügen**.
   c. Klicken Sie auf **Speichern**.
7. Klicken Sie auf den Link **Berechtigungen**, um die Berechtigungen der Benutzer in dieser Gruppe zu ändern.

   Die Berechtigungen für die Benutzer in dieser Gruppe werden nach Modul angezeigt. Gehen Sie wie folgt vor, um die Berechtigungen für diese Gruppe zu ändern:

   a. Klicken Sie auf das Symbol zum Bearbeiten des Datensatzes neben der Gruppe.
   b. Klicken Sie auf ein Optionsfeld rechts neben einem Modul, um **Kein Zugriff**, **Lesezugriff** oder **Lese-/Schreibzugriff** für die Berechtigung anzugeben.
   c. Klicken Sie auf **Speichern**.

   **Anmerkung:** Benutzer können mehreren Gruppen angehören. Wenn die Berechtigungen in diesen Gruppen unterschiedlich sind, übernimmt der Benutzer die höchste Berechtigungsebene, die den Benutzern in allen Gruppen zugeordnet ist.

**Anmerkung:** Alle Mitglieder der Gruppe "hubadmin" können über Berechtigungen als Superuser verfügen. Auf diese Weise können zahlreiche Benutzer die Aufgaben eines Hubadministrators übernehmen, während der Kennwortschutz aufrecht erhalten wird.

Weitere Informationen zur Verwaltung von Gruppen finden Sie im Kapitel zur Verwaltung von Gruppen im *WebSphere Partner Gateway Partnerhandbuch*.

## Kontakte erstellen

WebSphere Partner Gateway ermöglicht die Erstellung von Kontakten, die benachrichtigt werden können, wenn bestimmte Ereignisse auftreten. Gehen Sie wie folgt vor, um Kontakte für einen Partner zu erstellen:

1. Stellen Sie sicher, dass das Partnerprofil, für das Sie Kontakte erstellen möchten, ausgewählt ist. Das ausgewählte Profil wird oben auf der Seite nach der Zeichenfolge **Profil >** angezeigt.

   Führen Sie die folgenden Schritte aus, wenn das Profil nicht ausgewählt ist:

   a. Klicken Sie auf **Kontenadmin > Profile > Partner**.
   b. Geben Sie Suchkriterien ein und klicken Sie auf **Suchen**. Sie können auch auf **Suchen** klicken, ohne Suchkriterien einzugeben, um eine Liste aller Partner anzuzeigen.

c. Klicken Sie auf das Symbol **Details anzeigen**, um das Profil des Partners anzuzeigen.

2. Klicken Sie auf **Kontakte**.
3. Klicken Sie auf **Erstellen**.
4. Geben Sie den Vor- und Nachnamen für den Kontakt ein.
5. Geben Sie optional die Adresse des Kontakts ein.
6. Wählen Sie optional den Kontakttyp aus.
7. Geben Sie optional die E-Mail-Adresse, die Telefonnummer und die Faxnummer des Kontakts ein.
8. Wählen Sie **Sprache**, **Locale für das Format** und **Zeitzone** für den Kontakt aus.
9. Ändern Sie den Alertstatus des Benutzerstatus in **Aktiviert**.
10. Wählen Sie die subskribierte Sichtbarkeit für den Benutzer aus.
11. Klicken Sie auf **Speichern**.

Weitere Informationen zur Verwaltung von Kontakten finden Sie im Kapitel zur Verwaltung von Kontakten im *WebSphere Partner Gateway Partnerhandbuch*.

## Adressen erstellen

WebSphere Partner Gateway ermöglicht die Erstellung von Partneradressen. Gehen Sie wie folgt vor, um eine Adresse für einen Partner zu erstellen:

1. Stellen Sie sicher, dass das Partnerprofil, für das Sie Adressen erstellen möchten, ausgewählt ist. Das ausgewählte Profil wird oben auf der Seite nach der Zeichenfolge **Profil >** angezeigt.

   Wenn Sie gerade ein Profil erstellt haben, ist dieses Profil bereits ausgewählt. Wenn kein Profil ausgewählt ist, führen Sie die folgenden Schritte aus:

   a. Klicken Sie auf **Kontenadmin > Profile > Partner**.
   b. Geben Sie Suchkriterien ein und klicken Sie auf **Suchen**. Sie können auch auf **Suchen** klicken, ohne Suchkriterien einzugeben, um eine Liste aller Partner anzuzeigen.
   c. Klicken Sie auf das Symbol **Details anzeigen**, um das Profil des Partners anzuzeigen.

2. Klicken Sie auf **Adressen**.
3. Klicken Sie auf **Neue Adresse erstellen**.
4. Wählen Sie einen Adresstyp aus.
5. Geben Sie optional die Adresse ein.
6. Klicken Sie auf **Speichern**.

Weitere Informationen zur Verwaltung von Adressen finden Sie im Kapitel zur Verwaltung von Adressen im *WebSphere Partner Gateway Partnerhandbuch*.

# Kapitel 4. Konfiguration des Hubs vorbereiten

In den nächsten Kapiteln werden Sie die in Kapitel 2, „Einführung in die Hubkonfiguration", auf Seite 5 beschriebenen Empfänger und Ziele konfigurieren. Konfigurieren Sie die Empfänger und Ziele abhängig von den zum Senden und Empfangen von Dokumenten verwendeten Transporttypen.

Dieses Kapitel behandelt die folgenden Themen:

- „ Dateiverzeichnisziel erstellen"
- „FTP-Server für das Empfangen von Dokumenten konfigurieren"
- „Hub für das JMS-Transportprotokoll konfigurieren" auf Seite 39
- „RNIF-Komprimierung konfigurieren" auf Seite 46

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

- „FTP-Scripts für FTP-Scripting-Empfänger und -Ziele verwenden" auf Seite 46
- „Zuordnungen vom Data Interchange Services-Client verwenden" auf Seite 47

Wenn Sie nicht beabsichtigen, einen der vorgenannten Empfänger- oder Zieltypen zu konfigurieren, überspringen Sie dieses Kapitel, und fahren Sie mit Kapitel 5, „Server starten und Community Console anzeigen", auf Seite 49 fort.

## Dateiverzeichnisziel erstellen

Das Verzeichnis, das Sie für ein Dateiverzeichnisziel angeben, wird bei Bedarf automatisch erstellt. Wenn das Verzeichnis bereits vorhanden ist, wird es vom Ziel verwendet.

## FTP-Server für das Empfangen von Dokumenten konfigurieren

**Anmerkung:** Dieser Abschnitt gilt nur für das Empfangen von Dokumenten von Partnern über FTP oder FTPS. Das Senden von Dokumenten an Partner wird in „FTP-Ziel einrichten" auf Seite 234 und „FTPS-Ziel einrichten" auf Seite 241 beschrieben.

Wenn Sie FTP oder FTPS als Transport für Eingangsdokumente verwenden, müssen Sie einen FTP-Server installieren. Wenn Sie vorhaben, FTP zu verwenden, und momentan noch keinen Server installiert haben, dann installieren Sie jetzt einen, bevor Sie fortfahren. Stellen Sie sicher, dass eines der folgenden Szenarios auf Ihre Installation zutrifft:

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

**Anmerkung:** Befindet sich die Installation auf mehreren Maschinen, muss der FTP-Server auf der Maschine installiert werden, auf der der Empfänger installiert ist.

## Erforderliche Verzeichnisstruktur auf dem FTP-Server konfigurieren

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

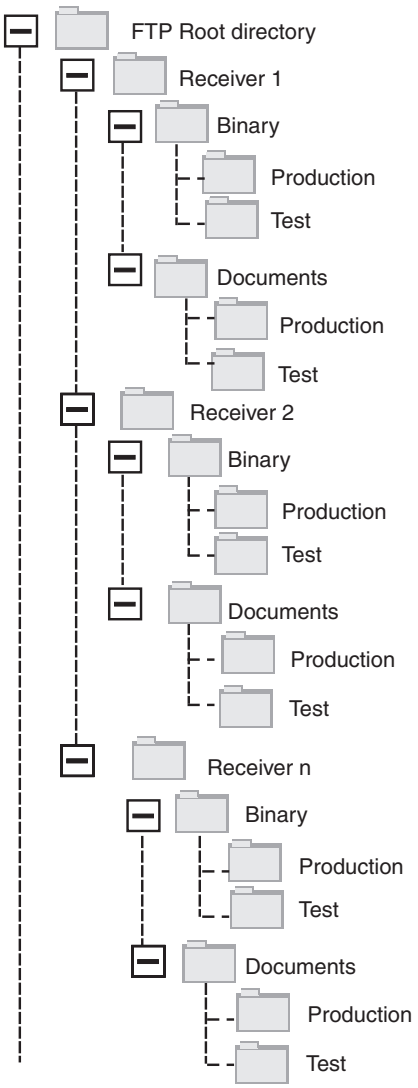



*Abbildung 15. FTP-Verzeichnisstruktur*

Jedes Partnerverzeichnis 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 Partner ein XML-Dokument, das die vollständigen Route-Informationen (unter Verwendung von FTP) enthält, an den Hub sendet. Dazu ist das Erstellen einer angepassten XML-Definition erforderlich. EDI-Dokumente (EDI - Electronic Data Interchange) können ebenfalls über dieses Verzeichnis gesendet werden.

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

Für jeden Partner, 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 Partner.

   **Anmerkung:** Der Name des Ordners sollte mit dem Namen übereinstimmen, den Sie bei der Erstellung des Partners als Anmeldenamen des Unternehmens angegeben haben. Das Erstellen von Partnern wird in „Partnerprofile erstellen" auf Seite 25 beschrieben.
2. Erstellen Sie unter dem Partnerordner die Unterordner namens `Binary` und `Documents`.
3. Erstellen Sie unter den Ordnern `Binary` und `Documents` die Unterordner namens `Production` und `Test`.

## Über FTP gesendete Dateien verarbeiten

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

### Binärdateien

Binärdateien müssen eine bestimmte Dateinamensstruktur verwenden, da die Dateien von Document Manager nicht überprüft werden.

Die Dateinamensstruktur lautet wie folgt: *<zielpartner-ID>.<eindeutiger_dateiname>*

Wenn die Empfängerkomponente eine Binärdatei ermittelt, wird diese Datei in den gemeinsam genutzten Speicher geschrieben und zur Verarbeitung an Document Manager übergeben.

Der Name des Verzeichnisses, in dem die Datei gefunden wurde, wird verwendet, um den Namen des Absenderpartners auszuwerten, und der erste Teil des Dateinamens wird verwendet, um den Namen des Zielpartners auszuwerten. 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` gefunden. Document Manager verfügt über die folgenden Informationen:

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

**Anmerkung:** An dieser Stelle und im ganzen Handbuch sind die verwendeten DUNS-Nummern nur als Beispiele zu verstehen. Bei WebSphere Partner Gateway ist es erforderlich, dass die <zielpartner-ID> mit der DUNS des empfangenden Partners übereinstimmt. Wenn die DUNS-ID nicht gefunden wird, schlägt die Kanalsuche fehl.

- Der Transaktionstyp ist **Produktion**.

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

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

Anschließend verarbeitet Document Manager die Datei.

Binärdateien können auch mit FTP übertragen werden, wobei der generische Vorverarbeitungshandler oder der Handler "FileNamePartnerId" verwendet wird. Weitere Informationen finden Sie im Abschnitt „Vorverarbeitungs-Konfigurationspunkt ändern" auf Seite 79.

### XML-Dateien

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

Wenn die Empfängerkomponente eine XML-Datei ermittelt, wird sie in den gemeinsam benutzten Speicher geschrieben und zur Verarbeitung an Document Manager übermittelt.

Document Manager vergleicht die XML-Datei mit den XML-Formaten, die definiert wurden, und wählt das erforderliche XML-Format aus. (Die Konfiguration von XML-Formaten wird in „Angepasste XML-Dokumentverarbeitung" auf Seite 159 beschrieben.) Der Name des Absenderpartners und des Zielpartners 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 Partnerverbindung zu finden, bevor die Datei verarbeitet wird.

## Zusätzliche FTP-Serverkonfiguration

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

1. Fügen Sie eine neue Gruppe hinzu (z. B. Partner).
2. Fügen Sie der neu erstellten Gruppe für jeden Partner, der Dokumente über FTP senden oder empfangen wird, einen Benutzer hinzu.

3. Konfigurieren Sie für jeden Partner den FTP-Server so, dass der eingehende Partner der Verzeichnisstruktur zugeordnet wird, die Sie im obigen Abschnitt „ Erforderliche Verzeichnisstruktur auf dem FTP-Server konfigurieren” auf Seite 36 erstellt haben. Zusätzliche Informationen finden Sie in der Dokumentation Ihres FTP-Servers.

### Sicherheitsaspekte für den FTPS-Server

Wenn Sie einen FTPS-Server zum Empfangen von Eingangsdokumenten verwenden, werden die Sicherheitserwägungen für SSL-Sitzungen ausschließlich vom FTPS-Server und dem vom Partner verwendeten Client verarbeitet. Es gibt keine spezielle Sicherheitskonfiguration für WebSphere Partner Gateway bei FTPS-Eingangsdokumenten. WebSphere Partner Gateway ruft die Dokumente vom FTP-Empfänger ab (dies wird in „ FTP-Empfänger konfigurieren” auf Seite 64 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 Partner kontaktieren kann.

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

## Hub für das JMS-Transportprotokoll konfigurieren

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

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

Dieser Abschnitt bezieht sich zwar auf WebSphere MQ, andere JMS-Provider erfordern jedoch ähnliche Prozeduren. Lesen Sie für WebSphere Platform Messaging den Abschnitt "JMS konfigurieren, wenn WebSphere Partner Gateway auf WebSphere Application Server installiert ist" in Kapitel 5 "Integration von WebSphere Process Server mit JMS als Transportmethode" im Handbuch *WebSphere Partner Gateway Unternehmensintegration*.

In späteren Abschnitten dieser Dokumentation erfahren Sie, wie Sie JMS-Empfänger oder -Ziele (oder beides) konfigurieren. Diese Aufgaben werden in „ JMS-Empfänger konfigurieren” auf Seite 66 und „JMS-Ziel einrichten” auf Seite 237 beschrieben.

## Verzeichnis für JMS erstellen

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

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

## Standard-JMS-Konfiguration ändern

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

1. Navigieren Sie zum Verzeichnis `Java\bin` von WebSphere MQ. In einer Windows-Installation navigieren Sie z. B. zu 'C:\IBM\MQ\Java\bin'.
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” definiert haben. Wenn Sie z. B. das Verzeichnis `c:/temp/JMS` definieren, würde die Zeile wie folgt aussehen:

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

6. Speichern Sie die Datei.

## Warteschlangen und den Kanal erstellen

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

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

   ```
   strmqcsv <name_des_warteschlangenmanagers>
   ```

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

   ```
   runmqsc <name_des_warteschlangenmanagers>
   ```

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

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

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

```
def ql(JMSIN)
```

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

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

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

   ```
   def ql(JMSOUT)
   ```

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

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

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

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

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

   ```
   end
   ```

## Java-Laufzeit zur Umgebung hinzufügen

Geben Sie den folgenden Befehl ein, um dem Systempfad eine Java™(TM)-Laufzeit hinzuzufügen:

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

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

## JMS-Konfiguration definieren

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

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

   ```
   JMSAdmin
   ```

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

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

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

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

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

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

```
define q(<name>) queue(<warteschlangenname>) qmgr(<name_des_warteschlangenmanagers>)
define q(<name>) queue(<warteschlangenname>) qmgr(<name_des_warteschlangenmanagers>)
end
```

**Anmerkung:**

- Sind MQ und WebSphere Partner Gateway auf zwei verschiedenen Systemen installiert, müssen Sie den Transporttyp **CLIENT** auswählen.
- Sind MQ und WebSphere Partner Gateway auf demselben System installiert, muss der Transporttyp **BINDINGS** sein.

Die vorherigen Schritte haben die .bindings-Datei erstellt, die sich in einem Unterordner des Ordners befindet, den Sie in Schritt 5 auf Seite 40 angegeben haben. Der Name des Unterordners ist der Name, den Sie für Ihren JMS-Kontext angegeben haben.

Als Beispiel wird die folgende JMSAdmin-Sitzung verwendet, um die Verbindungsfactory für Warteschlangen als `Hub` mit einer IP-Adresse von `sample.ibm.com` zu definieren, in der sich der MQ-Warteschlangenmanager (*<name_des_warteschlangenmanagers>* von `sample.queue.manager`) befindet. Das Beispiel verwendet die JMS-Warteschlangennamen und den Kanalnamen, die Sie in „Warteschlangen und den Kanal erstellen" auf Seite 40 erstellt haben.Beachten Sie, dass die Benutzereingabe an der Eingabeaufforderung > erfolgt.

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

In diesem Beispiel befindet sich die `.bindings`-Datei im folgenden Verzeichnis: `c:/temp/JMS/JMS`. Dabei steht `c:/temp/JMS` für die PROVIDER_URL und `JMS` für den Kontextnamen.

## Laufzeitbibliotheken konfigurieren

Für den JMS-Empfänger bzw. das JMS-Ziel sind mehrere WebSphere MQ-JAR-Dateien vorhanden, die für WebSphere Partner Gateway sichtbar sein müssen. Diese JAR-Dateien werden sichtbar, wenn sie in den Klassenpfad gestellt werden. Wenn Sie für den Zugriff auf MQ den MQ-Bindungsmodus verwenden, müssen die nativen MQ-Bibliotheken ebenfalls in dem Pfad vorhanden sein. Weitere Informationen zu den MQ-JAR-Dateien und den nativen Bibliotheken für JMS finden Sie in der WebSphere MQ-Dokumentation.

Es gibt mehrere Möglichkeiten, um die JAR-Dateien dem WebSphere Partner Gateway-Klassenpfad hinzuzufügen. Sie können die Dateien entweder in das Verzeichnis für Benutzerexits stellen oder sie über die gemeinsam genutzten WebSphere Application Server-Bibliotheken zuordnen.

### Verzeichnis für Benutzerexits verwenden

Zur Verwendung dieser Methode müssen die angegebenen JAR-Dateien in das entsprechende Verzeichnis für Benutzerexits gestellt werden:

- Für den JMS-Empfänger ist dies das Verzeichnis <WPG-Installationsstammverzeichnis>/receiver/lib/userexits
- Für das JMS-Ziel ist dies das Verzeichnis <WPG-Installationsstammverzeichnis>/router/lib/userexits

## Gemeinsam genutzte WebSphere Application Server-Bibliotheken verwenden

Zur Verwendung dieser Methode erstellen Sie eine Variable für gemeinsam genutzte Bibliotheken und ordnen diese Variable dem Empfänger oder der Document Manager-Anwendung zu, wie es in den nachfolgenden Schritten kurz beschrieben wird. Weitere Informationen zu dieser Vorgehensweise finden Sie in der WebSphere Application Server-Dokumentation.

1. Melden Sie sich an der Administrationskonsole von WebSphere Application Server an.
2. Gehen Sie wie folgt vor, um die Variable für gemeinsam genutzte Bibliotheken zu erstellen:
   a. Navigieren Sie zu **Umgebung** > **Gemeinsame Bibliotheken**.
   b. Wählen Sie einen Bereich aus (im Allgemeinen einen Knoten), und klicken Sie auf **Neu**.
   c. Geben Sie den Namen der Variablen ein (z. B. MQ_LIBRARIES), geben Sie die Klassenpfadeinträge für die MQ-JAR-Dateien ein, und klicken Sie auf **OK**.
3. Gehen Sie wie folgt vor, um die erstellte Variable für gemeinsam genutzte Bibliotheken den WebSphere Partner Gateway-Komponenten zuzuordnen:
   a. Navigieren Sie zu **Anwendungen** > **Enterprise-Anwendungen**.
   b. Wählen Sie entweder **BCGReceiver** (für JMS-Empfänger) oder **BCGDocMgr** (für JMS-Ziele) aus.
   c. Wählen Sie **Referenzen auf gemeinsam genutzte Bibliotheken** aus.
   d. Wählen Sie die Anwendung aus, und klicken Sie auf **Gemeinsam genutzte Bibliotheken angeben**.
   e. Wählen Sie in der Liste **Verfügbar** die erstellte Variable für gemeinsam genutzte Bibliotheken (z. B. MQ_LIBRARIES) aus, und verschieben Sie die Variable in die Liste **Ausgewählt**. Klicken Sie dann auf **OK**.

## JMS-Gateway und -Empfänger mit externem MQ konfigurieren

Im Folgenden werden die Schritte aufgelistet, mit denen eine Kommunikationsbrücke zwischen WebSphere Partner Gateway und MQ über die Administrationskonsole von WebSphere Application Server erstellt wird:

1. Erstellen Sie die JMS-Warteschlangenverbindungsfactory.
   a. Melden Sie sich an der Administrationskonsole von WebSphere Application Server an.
   b. Rufen Sie **Ressourcen > JMS > Verbindungs-Factory für Warteschlangen** auf.
   c. Wählen Sie einen **Bereich** aus und klicken Sie auf **Neu**.
      - Wählen Sie für die Gatewaykonfiguration den Bereich des Document Manager-Servers bzw. -Knotens aus. (Der Knotenbereich ist im Fall von Clustern hilfreich. Wählen Sie für den einfachen Modus einen Serverbereich aus.)

- Wählen Sie für die Empfängerkonfiguration den Bereich des Empfängerservers bzw. -knotens aus. (Der Knotenbereich ist im Fall von Clustern hilfreich. Wählen Sie für den einfachen Modus einen Serverbereich aus.)

d. Wählen Sie die Option **WebSphere-MQ-Messaging-Provider** aus und klicken Sie auf **OK**.

e. Geben Sie Werte für **Name** und **JNDI-Name** ein. Diese Angaben sind erforderlich.

f. Geben Sie korrekte Werte für **Queue Manager**, **Host** (IP des Systems, auf dem Queue Manager ausgeführt wird), **Port**, **Channel** und **Transporttyp** ein. Die übrigen Felder sind optional.

**Anmerkung:**

- Sind MQ und WebSphere Partner Gateway auf zwei verschiedenen Systemen installiert, müssen Sie den Transporttyp **CLIENT** auswählen.
- Sind MQ und WebSphere Partner Gateway auf demselben System installiert, muss der Transporttyp **BINDINGS** sein.

Weitere Informationen hierzu finden Sie im Information Center für WebSphere Application Server unter der folgenden Adresse: http://publib.boulder.ibm.com/infocenter/wasinfo/v6r1/index.jsp?topic=/com.ibm.websphere.nd.multipla...

2. Erstellen Sie die JMS-Warteschlange.
   a. Melden Sie sich an der Administrationskonsole von WebSphere Application Server an.
   b. Rufen Sie **Ressourcen > JMS > Warteschlangen** auf.
   c. Wählen Sie einen **Bereich** aus und klicken Sie auf **Neu**.
      - Wählen Sie für die Gatewaykonfiguration den Bereich des Document Manager-Servers bzw. -Knotens aus. (Der Knotenbereich ist im Fall von Clustern hilfreich. Wählen Sie für den einfachen Modus einen Serverbereich aus.)
      - Wählen Sie für die Empfängerkonfiguration den Bereich des Empfängerservers bzw. -knotens aus. (Der Knotenbereich ist im Fall von Clustern hilfreich. Wählen Sie für den einfachen Modus einen Serverbereich aus.)
   d. Geben Sie Werte für **Name** und **JNDI-Name** ein. Diese Angaben sind erforderlich.
   e. Geben Sie korrekte Werte für **Queue Manager**, **Host** (IP des Systems, auf dem Queue Manager ausgeführt wird), **Port**, **Channel** und **Transporttyp** ein. Die übrigen Felder sind optional.
   f. Starten Sie alle Server, für die Änderungen vorgenommen wurden, neu. Bei einer einfachen verteilten Installation ist dies beispielsweise DocumentManager/Receiver/bcgserver.
3. Konfigurieren Sie das JMS-Gateway auf WebSphere Partner Gateway.
   a. Melden Sie sich an der Administrationskonsole von WebSphere Partner Gateway an.
   b. Klicken Sie auf **Kontenadmin > Profile > Ziele**.
   c. Klicken Sie auf **Erstellen**.
   d. Geben Sie einen Wert für **Zielname** ein. Dies ist ein erforderliches Feld.
   e. Wählen Sie im Feld **Transport** die Option **JMS** aus.

f. Geben Sie Werte für die folgenden Pflichtfelder ein:
   - Adresse: Geben Sie die Zieladresse an, indem Sie den korrekten Hostnamen und Port für die in WebSphere Application Server erstellte Warteschlangenverbindungsfactory oder die erstellten Warteschlangenobjekte eingeben. Die Adresse muss das folgende Format aufweisen: corbaloc:iiop:<hostname>:<bootprogramm_portnummer>. Hierbei gilt Folgendes:
     – corbaloc:iiop - Gibt das Protokoll an, das für die Kommunikation zwischen der Client- (WebSphere Partner Gateway) und der Serversuchfunktion (WebSphere Application Server) verwendet wird.
     – <hostname> - Der Hostname oder die IP-Adresse des Systems, auf dem der WebSphere Application Server installiert ist, für den die Warteschlangenverbindungsfactory und die Warteschlangenobjekte erstellt wurden.
     – <bootprogramm_portnummer> - Die Bootprogramm-Portnummer des Servers, auf dem die Warteschlangenverbindungsfactory und die Warteschlangenobjekte gebunden sind. Zur Ermittlung der Bootprogramm-Portnummer können Sie sich an der Administrationskonsole von WebSphere Application Server anmelden, zu **Server > Application Server > <servername>-Ports** navigieren und die Bootstrap-Adresse prüfen. Im verteilten Modus unterscheiden sich die Portnummern für den Empfänger und das Gateway. Greifen Sie auf den entsprechenden Server ("bcg-receiver" für den Empfänger und "bcgdocmgr" für das Gateway) zu, um die Bootstrap-Portnummer zu ermitteln.
   - JMS-Factory-Name: Der für die JMS-Warteschlangenverbindungsfactory bereitgestellte JNDI-Name.
   - JMS-Warteschlangenname: Der für die JMS-Warteschlange bereitgestellte JNDI-Name.
   - JMS-JNDI-Factory-Name: Dies ist die für die JNDI-Kommunikation zu verwendende Factory. Da Sie WebSphere Application Server verwenden, können Sie den Wert als com.ibm.websphere.naming.WsnInitialContextFactory eingeben.

4. Konfigurieren Sie den JMS-Empfänger auf WebSphere Partner Gateway.
   a. Melden Sie sich an der Administrationskonsole von WebSphere Partner Gateway an.
   b. Klicken Sie auf **Hubadmin > Hubkonfiguration > Empfänger**.
   c. Klicken Sie auf **Empfänger erstellen**.
   d. Geben Sie einen Wert für **Empfängername** ein. Dies ist ein erforderliches Feld.
   e. Wählen Sie im Feld **Transport** die Option **JMS** aus.
   f. Geben Sie die korrekten Werte für die Pflichtfelder ein. Dies wird in Schritt 3f beschrieben.

## RNIF-Komprimierung konfigurieren

RosettaNet-Geschäftsnachrichten und ihre Anhänge werden mithilfe eines S/MIME-Umschlags komprimiert und gepackt, damit große Dokumente übertragen werden können. Darüber hinaus wird für RosettaNet-Geschäftsnachrichten Unterstützung für die Dekomprimierung bereitgestellt. Sie haben die Möglichkeit, die Nutzdaten separat oder mit Anhängen zu komprimieren. Um die Leistung zu verbessern, sollten Sie laut der RosettaNet 2.0 Technical Advisory Specification die Servicekomponente und ihre Anhänge komprimieren, bevor Sie sie verschlüsseln, signieren oder für die Übertragung codieren. Wählen Sie unter dem entsprechenden RosettaNet-WebSphere Partner Gateway-Kanal einen der folgenden Werte für das Attribut für die Komprimierung des Routingobjekts aus:

- Kein(e)
- Nutzdaten
- Nutzdaten und Anhang

Neben der ausgewählten Komprimierungsoption können Sie auch weitere Attribute für Filterkriterien auswählen, wie beispielsweise **Inhaltstyp für Komprimierung** oder **Größe für Komprimierung**. Durch die Verwendung der Filterkriterien können Sie auswählen, welche Nutzdaten oder Anhänge aus dem Pool der Anhänge komprimiert werden sollen. Für die Option **Inhaltstyp für Komprimierung** muss entweder "Alle" oder eine Reihe gültiger, durch Kommas getrennter MIME-Typen angegeben werden. Wenn Sie für die Basiskomprimierung die Option **Nutzdaten** ausgewählt haben, werden die Nutzdaten unabhängig von dem für das Routingobjektattribut **Inhaltstyp für Komprimierung** angegebenen Wert komprimiert. Nur Anhänge werden auf der Basis von angegebenen Inhaltstypen für die Komprimierung ausgewählt. Für das Routingobjektattribut **Größe für Komprimierung** muss entweder "Alle" oder eine gültige Größenbegrenzung angegeben werden. Die gültige Größenbegrenzung gibt die Mindestgröße an, für die die Komprimierung verwendet werden soll.

Wird ein komprimiertes RosettaNet-Dokument gesendet, wird die S/MIME-Dekomprimierung für den Serviceinhalt und seine anhänge ausgeführt.

## FTP-Scripts für FTP-Scripting-Empfänger und -Ziele verwenden

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

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

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

Informationen zum Erstellen eines FTP-Scripts für einen FTP-Scripting-Empfänger finden Sie in „ FTP-Scripting-Empfänger konfigurieren" auf Seite 69. Informationen zum Erstellen eines FTP-Scripts für ein FTP-Scripting-Ziel finden Sie in „FTP-Scripting-Ziel einrichten" auf Seite 244.

## Zuordnungen vom Data Interchange Services-Client verwenden

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

Der Data Interchange Services-Zuordnungsexperte erstellt Zuordnungen, die beschreiben, wie bestimmte Dokumente transformiert und validiert werden sollen.

Zur Erstellung einer beliebigen Zuordnung werden die Definitionen der Quellen- und Zieldokumente benötigt. Die Definitionen der Quellendokumente für EDI werden von WDI bereitgestellt, bei ROD und XML müssen sie mithilfe des DIS-Clients erstellt werden. Für EDI importieren Sie die .EIF-Datei (Standarddatei) in den DIS-Client. Für ROD erstellen Sie die Standarddatei mithilfe des DIS-Clients. Importieren Sie die DTD/XSD-Datei, um eine Standarddatei für XML zu erstellen. Die Standard- und die Transformationszuordnung können separat kompiliert werden.

Möglicherweise verfügen Sie zum Beispiel über eine Bestellung, die von einer Back-End-Anwendung erstellt wurde und die Sie transformieren und einem externen Partner als Standard-EDI-X12-Bestellung (850) zusenden wollen. Der Data Interchange Services-Zuordnungsexperte schreibt in diesem Fall eine Zuordnung, die detailliert beschreibt, wie jedes Feld oder Datenstück von Ihrem Programm in das X12-Format transformiert werden soll. Die Zuordnung wird dann direkt nach WebSphere Partner Gateway exportiert, oder sie wird in eine Datei exportiert, die Sie dann mit einem Befehlsscript importieren.

Detaillierte Informationen zum Importieren von Zuordnungen vom Data Interchange Services-Client finden Sie im Abschnitt „ Zuordnungen manuell importieren” auf Seite 212.

**Anmerkung:** Der DIS-Client verfügt über eine eigene Datenbank. Nachdem Sie eine Zuordnung in einem DIS-Client beenden, können Sie sie als EIF-Datei exportieren. Importieren Sie diese EIF-Datei über die Konsole von WebSphere Partner Gateway. Die Informationen werden in der WebSphere Partner Gateway-Datenbank gespeichert.

## Konfigurationstasks nach der Installation ausführen

Nachdem Sie WebSphere Partner Gateway installiert haben, müssen Sie das Produkt konfigurieren. Dazu gehört normalerweise auch die Konfiguration des Hubs über die Administrationskonsole von WebSphere Partner Gateway. In Abhängigkeit von den Anforderungen der jeweiligen Handelsgemeinschaft müssen Sie möglicherweise auch die WebSphere Application Server-Infrastruktur konfigurieren, in der sich die WebSphere Partner Gateway-Komponenten befinden. Einige dieser Tasks sind hier aufgelistet. Über die Links finden Sie detaillierte Anweisungen dazu, wie Sie diese Tasks ausführen können.

- „Verschlüsselungsstärke ändern” auf Seite 265
- „SSL mit konfigurierter Clientauthentifizierung” auf Seite 267

# Kapitel 5. Server starten und Community Console anzeigen

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

- „WebSphere Partner Gateway-Komponenten starten”
- „ Anmeldung an der Community Console” auf Seite 51

Informationen zum Starten der Cluster über die Administrationskonsole von WebSphere Application Server Network Deployment finden Sie in Kapitel 1. "Komponentenanwendungen von WebSphere Partner Gateway verwalten" des Handbuchs *WebSphere Partner Gateway Verwaltung*.

## WebSphere Partner Gateway-Komponenten starten

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

Im einfachen Modus werden alle Komponenten von WebSphere Partner Gateway auf derselben Instanz von WebSphere Application Server installiert. Sie starten und stoppen alle Komponenten mithilfe von Scripts oder der WebSphere Application Server-Administrationskonsole. Führen Sie das folgende Script aus, um die Komponenten von WebSphere Partner Gateway auf einem im einfachen Modus installierten System zu starten:

```
<INSTALL DIR>/bin/bcgStartServer.sh
```

Führen Sie das folgende Script aus, um die Komponenten von WebSphere Partner Gateway auf einem im einfachen Modus installierten System zu stoppen:

```
<INSTALL DIR>/bin/bcgStopServer.sh
```

**Anmerkung:** Bei einer Installation im einfachen Modus müssen Sie keinen Servernamen angeben. Bei der Installation im einfachen Modus ist der Servername stets "server1".

**Anmerkung:** Wird das Installationsprogramm ausgeführt, während das Verzeichnis **temp** über nur wenig Speicherplatz verfügt, kann das Installationsprogramm das Produkt nicht korrekt installieren. Vergrößern Sie den Speicherplatz im Verzeichnis **temp**, deinstallieren Sie das Produkt und installieren Sie es erneut.

1. Geben Sie "http://<computername_oder_IP-adresse>:58080/console" ein. Daraufhin zeigt der Web-Browser die Begrüßungsseite an. Melden Sie sich mit den folgenden Informationen bei WebSphere Partner Gateway an:
   - Geben Sie im Feld **Benutzername** Folgendes ein:

     ```
     hubadmin
     ```
   - Geben Sie im Feld **Kennwort** Folgendes ein:

     ```
     Pa55word
     ```
   - Geben Sie im Feld **Anmeldename des Unternehmens** Folgendes ein:

     ```
     Operator
     ```

   Klicken Sie auf **Anmelden**.

2. Wenn Sie sich zum ersten Mal anmelden, müssen Sie ein neues Kennwort erstellen. Geben Sie ein neues Kennwort ein und geben Sie anschließend das neue Kennwort ein zweites Mal im Feld **Kennwort bestätigen** ein.
3. Klicken Sie auf **Speichern**. Das System zeigt die erste Eingabeanzeige der Community Console an.

Bei der Installation von WebSphere Partner Gateway werden die Anwendungen **Erste Schritte** und IVT (Installation Verification Test) standardmäßig installiert. Diese bleiben installiert, bis die letzte WebSphere Partner Gateway-Komponente auf der Maschine installiert wurde. Die Seite **Erste Schritte** wird mit den Daten der installierten Komponenten gefüllt, um für jede Komponente einen separaten IVT ausführen zu können.

Die Seite **Erste Schritte** kann über den Befehl **bcgFirstSteps.sh** aufgerufen werden, der sich im Ordner <install_dir>/FirstSteps/bin befindet.

Auf der Seite **Erste Schritte** der Konsole kann für alle installierten Komponenten zwischen der Option **Start** und der Option **Stopp** hin- und hergewechselt werden. Wenn beispielsweise der Hub aktiv ist, wird die Option **Stopp** angezeigt. Andernfalls wird die Option **Start** angezeigt. Im Folgenden sind die Optionen **Start** und **Stopp** für die Komponenten basierend auf der jeweiligen Topologie aufgeführt:

- Die Optionen **Start** und **Stopp** für WebSphere Process Gateway stehen für einfache und einfache verteilte Topologien zur Verfügung.
- Die Optionen **Start** und **Stopp** für MAS stehen für einfache verteilte und vollständig verteilte Topologien zur Verfügung.
- Die Optionen **Start** und **Stopp** für Deployment Manager stehen für einfache und vollständig verteilte Topologien zur Verfügung.

  **Anmerkung:** Diese Optionen sind nur dann verfügbar, wenn Deployment Manager mit dem WebSphere Partner Gateway-Installationsprogramm installiert wird.
- Die Optionen **Start** und **Stopp** für die Konsole, den Empfänger und den Router stehen für vollständig verteilte Topologien zur Verfügung.
- Die Optionen **Start** und **Stopp** für FTP-Management stehen für alle Topologien zur Verfügung.

Die obigen Optionen stehen für die aufgelisteten Topologien zur Verfügung, sofern diese auf der jeweiligen Maschine installiert sind. Überprüfen Sie die Serverprotokolle, um zu ermitteln, ob die Aktion erfolgreich ausgeführt wurde. Sie können den Status auch über das Befehlszeilenfenster überprüfen. Wenn Sie auf den Link **WPG starten** in der Anzeige **Erste Schritte** klicken, wird der Startbefehl in einer DOS-Eingabeaufforderung ausgegeben. Die Anzeige **Erste Schritte** informiert nicht über die erfolgreiche (bzw. nicht erfolgreiche) Ausführung des Befehls.

Wenn Sie die Option für den Funktionstest für die Installation (Install Verification Test - IVT) aufrufen, wird die Gültigkeit der auf der Maschine installierten WebSphere Partner Gateway-Komponenten überprüft. Der IVT kann alternativ auch über die Befehlszeile mithilfe des Befehls **LaunchIVT.sh** aufgerufen werden. Dieser Befehl befindet sich im Ordner <install_dir>/FirstSteps/ivt/bin. Nach Abschluss der Prüfung erstellt der IVT einen Bericht mit den Details zu allen installierten WebSphere Partner Gateway-Komponenten. Darüber hinaus werden die während dieser Operation erstellten temporären Dateien bereinigt und die Server/Knoten gestoppt, die für diese Operation gestartet wurden. Wenn eine Komponente fehlschlägt, werden die erforderlichen Protokolldateien im Ordner "<install_dir>/FirstSteps/ivt/logs" generiert.

**Anmerkung:** In verteilten Topologien wird für Komponenten, die auf unterschiedlichen Maschinen installiert sind, kein IVT durchgeführt.

Wenn Sie Zertifikate mit stärkerer Verschlüsselung als die Standardverschlüsselung hochladen möchten, kann das Hochladen der Zertifikate fehlschlagen.

## Anmeldung an der Community Console

In diesem Abschnitt werden die Schritte zum Anzeigen und Anmelden bei der Community Console beschrieben. Als Bildschirmauflösung wird 1024x768 empfohlen.

**Anmerkung:** Für die Community Console von WebSphere Partner Gateway muss die Cookie-Unterstützung aktiviert werden, um die Sitzungsdaten zu verwalten. In den Cookies werden keine persönlichen Daten gespeichert; sie verfallen beim Schließen des Browsers.

1. Öffnen Sie einen Web-Browser, und geben Sie zum Anzeigen der Community Console die folgende URL ein:

   http://<*hostname*>.<*domäne*>:58080/console (nicht gesichert)

   https://<*hostname*>.<*domäne*>:58443/console (sicher)

   Hierbei stehen <*hostname*> und <*domäne*> für den Namen und den Standort des Computers, auf dem sich die Komponente Community Console befindet.

   **Anmerkung:** Diese URLs setzen die Verwendung der standardmäßigen Portnummern voraus. Wenn Sie die standardmäßigen Portnummern geändert haben, ersetzen Sie die Standardnummern durch die von Ihnen angegebenen Werte.

In den meisten Fällen sendet Ihnen der Hubadministrator den Benutzernamen, das Anfangskennwort und den Anmeldenamen des Unternehmens für die Anmeldung an der Community Console. Sie benötigen diese Informationen für die folgende Prozedur. Sollten Sie diese Informationen nicht erhalten haben, wenden Sie sich an den zuständigen Hubadministrator.

Gehen Sie wie folgt vor, um sich an der Community Console anzumelden (diese Anweisungen gelten sowohl für die internen als auch für die externen Partner):

1. Geben Sie den **Benutzernamen** für Ihr Unternehmen ein.
2. Geben Sie das **Kennwort** für Ihr Unternehmen ein.
3. Geben Sie den **Anmeldenamen des Unternehmens** ein, z. B. IBM.
4. Klicken Sie auf **Anmelden**. Wenn Sie sich das erste Mal anmelden, müssen Sie ein neues Kennwort erstellen.
5. Geben Sie ein neues Kennwort ein und wiederholen Sie anschließend die Eingabe des neuen Kennworts im Bestätigungsfeld.
6. Klicken Sie auf **Speichern**. Das System zeigt die erste Eingabeanzeige der Community Console an.

**Anmerkung:** Wird WebSphere Partner Gateway mithilfe von LDAP (Lightweight Directory Access Protocol) konfiguriert, müssen Sie den Benutzernamen und das Kennwort für LDAP eingeben. In diesem Fall ist der Anmeldename des Unternehmens nicht relevant; Sie werden daher nicht zur Eingabe dieser Informationen aufgefordert. Außerdem fordert das System Sie nicht auf, Ihr Kennwort zu ändern.

# Kapitel 6. Community Console konfigurieren

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

- „Locale-Informationen und Konsolbranding angeben"
- „Kennwortrichtlinie konfigurieren" auf Seite 55
- „Berechtigungen konfigurieren" auf Seite 56
- „Zeitlimitüberschreitungswert für die Konsole festlegen" auf Seite 57

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

**Anmerkung:** Verwenden Sie stets die Browserinstanz, mit der Sie sich an Community Console angemeldet haben, wenn Sie Konfigurationsänderungen an WebSphere Partner Gateway vornehmen. Die gleichzeitige Verwendung mehrerer Browserinstanzen kann dazu führen, dass die Konfigurationsänderungen aufgehoben werden.

## Locale-Informationen und Konsolbranding angeben

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

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

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

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

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

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

### Konsolbranding durchführen

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

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

Die Bilder müssen in Dateien im JPG-Format vorliegen und bestimmten Vorgaben entsprechen, damit sie in das Fenster von Community Console eingefügt werden können.

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

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

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

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

## Style-Sheet ändern

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

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

## Konsoldaten lokalisieren

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

- **Konsolbezeichnung**. Enthalten die Zeichenfolgen, die den gesamten Text der Schnittstelle darstellen
- **Ereignisbeschreibungen**. Enthalten die Zeichenfolgen zur Anzeige von Ereignisdetail (z. B. "Es wurde versucht, eine doppelte Verbindung zu erstellen")
- **Ereignisnamen**. Enthalten die Zeichenfolgen, die für Ereignisnamen stehen (z. B. "Verbindung besteht bereits")
- **EDI-Ereignisbeschreibungen**. Enthalten die Zeichenfolgen zur Anzeige von EDI-Ereignisdetail (z. B. "Fehler bei der FA-Abstimmung. Für die Konvertierungen in der EDI-Bestätigung wurden keine Aktivitäts-IDs gefunden.")
- **EDI-Ereignisnamen**. Enthalten die Zeichenfolgen, die für EDI-Ereignisnamen stehen (z. B. "Fehler bei der FA-Abstimmung")
- **Erweiterter Ereignistext**. Enthält die Zeichenfolgen, die zusätzliche Informationen zu Ereignissen bereitstellen (z. B. den Grund des Ereignisses und Informationen zur Fehlerbehebung)

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

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

## Kennwortrichtlinie konfigurieren

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

Sie können die folgenden Elemente der Kennwortrichtlinie ändern:

- **Mindestlänge**. Stellt die Mindestanzahl Zeichen dar, die der Partner 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 Partner kann kein altes Kennwort verwenden, wenn es in der Protokolldatei vorhanden ist. Der Standardwert ist 10 Kennwörter.
- **Sonderzeichen**. Gibt an, wenn ausgewählt, dass Kennwörter mindestens drei der folgenden Typen von Sonderzeichen enthalten müssen:
  - Großbuchstaben
  - Kleinbuchstaben
  - Numerische Zeichen
  - Sonderzeichen

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

Zu den vom System unterstützten Sonderzeichen gehören: '#', '@', '$', '&', '+'.

- **Prüfung auf Namensvariationen**. Verhindert, wenn ausgewählt, die Verwendung von Kennwörtern, die sich aus einer leicht zu erratenden Kombination des Anmeldenamens oder des vollständigen Namens vom Benutzer zusammensetzen. Dieses Feld ist standardmäßig ausgewählt.

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

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

# Berechtigungen konfigurieren

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

## Benutzern Berechtigungen erteilen

Bevor Sie Berechtigungen konfigurieren, ist es hilfreich zu verstehen, wie einzelnen Benutzern Berechtigungen erteilt werden. Alle drei Entitätstypen in der Hub-Community, der Hubadministrator, der interne Partner und die externen Partner, verfügen über einen Administrator. Wenn Sie einen internen Partner oder einen Partner erstellen, können Sie auch den Administrator für diese Entität erstellen.

**Anmerkung:** Für den Hubbetreiber werden während der Installation zwei Benutzer mit Verwaltungsaufgaben automatisch erstellt: ein Administrator und ein Hubadministrator.

Wenn Sie den Partner erstellen (wie in „Partnerprofile erstellen” auf Seite 25 definiert), stellen Sie für den Partner Anmeldeinformationen bereit, wie z. B. den Anmeldenamen und das Kennwort. Nachdem sich der Partner angemeldet hat, erstellt der Partner zusätzliche Benutzer innerhalb des Unternehmens. Der Partner erstellt auch Gruppen und ordnet diesen Gruppen Benutzer zu. Ein Unternehmen will z. B. unter Umständen über eine Gruppe für Personen verfügen, die das Dokumentvolumen überwachen. Der Partner würde eine Gruppe **Volumen** erstellen und ihr Benutzer hinzufügen.

**Anmerkung:** Als Hubadministrator können Sie ebenfalls die Benutzer und Gruppen für einen Partner definieren.

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

Die Einstellung, die Sie als Hubadministrator 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. die Hubadministratoren). Selbst wenn Sie eines dieser Module für die Verwendung durch einen Partner aktivieren, wird das Modul daher nicht auf der Seite **Gruppendetails** für den Partner angezeigt.

### Berechtigungen aktivieren oder inaktivieren

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

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

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

## Zeitlimitüberschreitungswert für die Konsole festlegen

Der Standardwert für das Sitzungszeitlimit, der 30 Minuten beträgt, ist in den folgenden Fällen möglicherweise unzureichend:

- Für Benutzer in sicheren Umgebungen sind möglicherweise kürzere Zeiträume für das Sitzungszeitlimit erforderlich, um die Sicherheit zu gewährleisten. Dies trifft beispielsweise zu, wenn sich die Benutzer von ihrer Maschine entfernen und vergessen, sich von der Konsole abzumelden.
- Für Benutzer sind möglicherweise längere Zeiträume für das Sitzungszeitlimit erforderlich, wenn Sie aus Gründen der behindertengerechten Bedienung langsamer als normale Benutzer antworten.

Führen Sie die folgenden Schritte aus, um das Zeitlimit für die WebSphere Partner Gateway-Konsole festzulegen:

1. Öffnen Sie die Konsole von WebSphere Application Server.
2. Navigieren Sie zu **Server** > **Application Server** > **bcgserver** > **Einstellungen für Webcontainer** > **Webcontainer** > **Sitzungsverwaltung**.
3. Wählen Sie auf der Seite **Sitzungsverwaltung** die Option **Zeitlimit festlegen** in Abschnitt **Sitzungszeitlimit** aus.
4. Geben Sie den gewünschten Wert in Minuten ein. Der Standardwert ist 30 Minuten.
5. Klicken Sie auf **Anwenden**.

# Kapitel 7. Empfänger definieren

In diesem Kapitel wird beschrieben, wie Sie Empfänger in WebSphere Partner Gateway konfigurieren. Es behandelt die folgenden Themen:



**Anmerkung:** Verwenden Sie stets die Browserinstanz, mit der Sie sich an Community Console angemeldet haben, wenn Sie Konfigurationsänderungen an WebSphere Partner Gateway vornehmen. Die gleichzeitige Verwendung mehrerer Browserinstanzen kann dazu führen, dass die Konfigurationsänderungen aufgehoben werden.

## Übersicht über Empfänger

Wie in „Übersicht über die Dokumentverarbeitung" auf Seite 13 beschrieben, ist der *Empfänger* für das Akzeptieren eingehender Dokumente von einem bestimmten Transport verantwortlich. Eine Empfängerinstanz wird für eine bestimmte Implementierung konfiguriert.

Dokumente, die von einem Empfänger auf dem Hub empfangen werden, können von externen Partnern (zur letztendlichen Zustellung an den internen Partner) oder von einer Back-End-Anwendung des internen Partners (zur letztendlichen Zustellung an externe Partner) stammen.

Abb. 16 auf Seite 60 zeigt einen WebSphere Partner Gateway-Server mit vier konfigurierten Empfängern. Zwei der Empfänger (HTTP/S und FTP/S) sind für Dokumente, die von Partnern gesendet werden. Diese beiden Empfänger stellen eine HTTP-URI und ein FTP-Verzeichnis dar. Sie stellen Ihren Partnern Informationen zu diesen Empfängern zur Verfügung, um anzugeben, wohin sie Ihnen Dokumente senden sollen. Die anderen beiden Empfänger (JMS und Dateiverzeichnis) sind für Dokumente, die von der Back-End-Anwendung des internen Partners stammen. Diese Empfänger stellen eine Warteschlange und ein Verzeichnis dar.

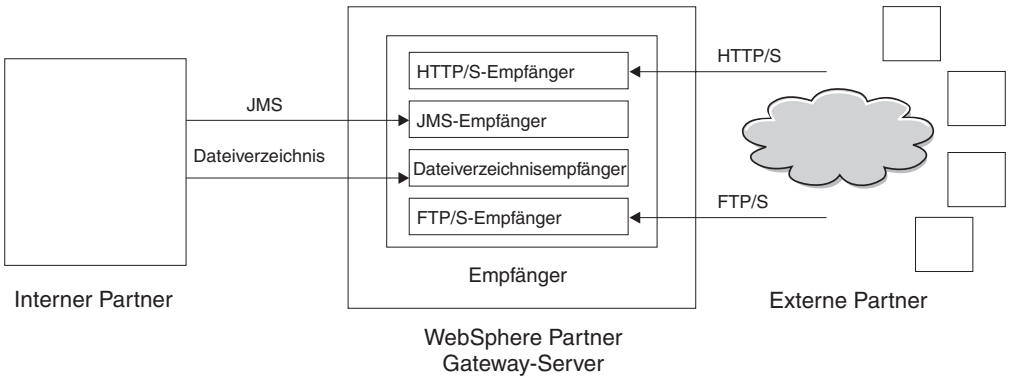



*Abbildung 16. Transporte und zugeordnete Empfänger*

Sie konfigurieren mindestens einen Empfänger für jeden Transporttyp, über den Dokumente an den Hub gesendet werden. Sie verfügen beispielsweise über einen HTTP-Empfänger, um beliebige Dokumente zu empfangen, die über den HTTP- oder HTTPS-Transport gesendet werden. Wenn Ihre externen Partner Dokumente über FTP senden, konfigurieren Sie einen FTP-Empfänger.

Wenn für einige der empfangenen Dokumente spezielle Anforderungen gelten, müssen für einen bestimmten Transport möglicherweise mehrere Empfänger konfiguriert werden. In einem solchen Fall teilen Sie Ihren Partnern diese Anforderungen mit und bitten Sie sie, diese Dokumente an spezielle Adressen zu senden, damit die korrekte Empfängerverarbeitung erfolgen kann.

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

## Benutzerdefinierte Handler hochladen

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

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

1. Klicken Sie im Hauptmenü auf **Hubadmin > Hubkonfiguration > Handler**.
2. Klicken Sie auf **Empfänger**.

   Die Liste der Handler, die derzeit für Empfänger definiert sind, wird angezeigt. Beachten Sie, dass die von WebSphere Partner Gateway bereitgestellten Handler die Provider-ID **Produkt** haben.
3. Klicken Sie auf der Seite **Handler-Liste** auf **Importieren**.

4. Geben Sie auf der Seite **Handler importieren** den Pfad zur XML-Datei an, die den Handler beschreibt, oder verwenden Sie **Durchsuchen**, um nach dieser XML-Datei zu suchen.

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

## Generische Vorverarbeitungshandler

Der Vorverarbeitungs-Konfigurationshandler ist auf allen Empfängertypen verfügbar, er kann jedoch nicht für SMTP-Empfänger verwendet werden. In der folgenden Tabelle werden die Attribute beschrieben, die Sie für einen generischen Vorverarbeitungshandler festlegen können.

*Tabelle 2. Generischer Vorverarbeitungshandler*

| Attribut | Beschreibung |
|---|---|
| From Packaging Name | Dieses Attribut gibt das Paket an, das dem Dokument zugeordnet ist. Dieser Wert muss mit dem Paket übereinstimmen, das in der Dokumentdefinition angegeben ist. |
| From Packaging Version | Dieses Attribut gibt die Version des Pakets an, das in **From Packaging Name** angegeben ist. Wenn für das Dokument beispielsweise das Paket **None** festgelegt ist, ist dieser Wert **N/A**. |
| From Protocol Name | Dieses Attribut gibt das Protokoll an, das dem Dokument zugeordnet ist. Dieser Wert muss mit dem Protokoll übereinstimmen, das in der Dokumentdefinition angegeben ist. |
| From Protocol Version | Dieses Attribut gibt die Version des Protokolls an, das in **From Protocol Name** angegeben ist. |
| From Process Code | Dieses Attribut gibt den Prozess (Dokumenttyp) an, der diesem Dokument zugeordnet ist. Dieser Wert muss mit dem Dokumenttyp in der Dokumentdefinition übereinstimmen. |
| From Process Version | Dieses Attribut gibt die Version des Prozesses an, der in **From Process Code** angegeben ist. |
| METADICTIONARY | Dieses Attribut gibt den Namen des Wörterverzeichnisses an, dem die Dokumentdefinition zugeordnet ist. Dieser Wert muss mit dem Protokoll übereinstimmen, das im Feld **From Protocol Name** angegeben ist. |
| METADOCUMENT | Dieses Attribut gibt den Namen der Dokumentdefinition an, die diesem Dokument zugeordnet ist. Dieser Wert muss mit dem Prozess übereinstimmen, der im Feld **From Process Code** angegeben ist. |
| METASYNTAX | Dieses Attribut gibt die Syntax des Dokuments an, das in diesem Empfänger verarbeitet wird. Zulässige Werte sind "ediIchg" (EDI-Austausch), "xml" und "rod" (Flachdatei). |
| ENCODING | Dieses Attribut gibt die Zeichencodierung des Dokuments an. Der Standardwert ist ASCII. |
| BCG_BATCHDOCS | Dieses Attribut wird auf **ON** festgelegt, wenn die Dokumente in einem Batch (Stapel) verarbeitet werden sollen. |
| SenderId, ReceiverId | Dieses Attribut gibt die Empfänger-ID und die Sender-ID an. Dies sind die Geschäfts-IDs der Partner, die in ihren Profilen konfiguriert sind. |

## Globale Transportwerte konfigurieren

Definieren Sie globale Transportattribute, die für alle FTP-Scripting-Empfänger gelten. Wenn Sie keine FTP-Scripting-Empfänger definieren, können Sie diesen Abschnitt überspringen.

1. Klicken Sie auf **Hubadmin > Hubkonfiguration > Empfänger**, um die Empfängerliste anzuzeigen.
2. Klicken Sie auf den Link **Globale Transportattribute**.
3. Wenn die Standardwerte für Ihre Konfiguration geeignet sind, klicken Sie auf **Abbrechen**. Fahren Sie andernfalls mit den übrigen Schritten in diesem Abschnitt fort.
4. Klicken Sie auf das Symbol **Bearbeiten** neben **Globale Attribute, nach Kategorie aufgelistet**.
5. Prüfen und ändern Sie gegebenenfalls die Werte von **FTP-Scripting-Transport** und **FTP-Scripting - Empfänger und Ziele**.

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

   - Werte für **FTP-Scripting-Transport**
     - **Wiederholungszähler für Sperren**. Gibt an, wie oft der Empfänger versucht, eine Sperre zu erhalten, wenn die Sperre gerade verwendet wird. Der Standardwert ist 3.
     - **Wiederholungsintervall für Sperren (Sekunden)**. Gibt an, wie viel Zeit zwischen den Versuchen, eine Sperre zu erhalten, verstreichen wird. Der Standardwert ist 260 Sekunden.
   - Werte für **FTP-Scripting - Empfänger und Ziele**
     - **Maximale Sperrenzeit (Sekunden)**. Gibt an, wie lange der Empfänger die Sperre beibehalten kann. Der Standardwert ist 240 Sekunden.
     - **Höchstalter der Warteschlange (Sekunden)**. Gibt an, wie lange der Empfänger in einer Warteschlange warten wird, um die Sperre zu erhalten. Der Standardwert ist 740 Sekunden.
6. Klicken Sie auf **Speichern**.

## HTTP/S-Empfänger konfigurieren

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

Die folgenden Schritte beschreiben, was Sie für einen HTTP/S-Empfänger angeben müssen.

1. Klicken Sie auf **Hubadmin > Hubkonfiguration > Empfänger**, um die Seite **Empfängerliste** anzuzeigen.
2. Klicken Sie auf der Seite **Empfängerliste** auf **Empfänger erstellen**.

## Empfängerdetails

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

1. Geben Sie einen Namen für den Empfänger ein. Sie könnten den Empfänger z. B. 'HttpEmpfänger1' nennen. Dies ist ein erforderliches Feld. Der Name, den Sie hier eingeben, wird in der Empfängerliste angezeigt.
2. Geben Sie optional den Status des Empfängers an. **Aktiviert** ist die Standardeinstellung. Ein aktivierter Empfänger ist für das Akzeptieren von Dokumenten bereit. Ein inaktivierter Empfänger kann keine Dokumente akzeptieren.
3. Geben Sie optional eine Beschreibung für den Empfänger ein.
4. Wählen Sie **HTTP/S** in der Liste **Transport** aus.

## Empfängerkonfiguration

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

1. Geben Sie optional den Betriebsmodus an. Der Betriebsmodus definiert die Art der Übertragung. Wenn Sie z. B. einen Dokumentenaustausch testen wollen, bevor Sie ihn in die Produktion einreihen, müssen Sie **Test** eingeben. Die Standardeinstellung ist **Produktion**.
2. Geben Sie die URI für den HTTP/S-Empfänger ein. Der Name muss mit **bcgreceiver** beginnen. Geben Sie beispielsweise /bcgreceiver/Receiver ein. Dokumente, die beim Server über HTTP/S eingehen, werden dann an der Position /bcgreceiver/Receiver empfangen.
3. Setzen Sie die Option **Basisauthentifizierung aktivieren** auf "true", um die Authentifizierung eines HTTP/S-Empfängers mithilfe des Headerattributs zu ermöglichen. Der Standardwert ist "false".
4. Prüfen Sie und, falls notwendig, ändern Sie die Werte für **HTTP/S-Transport**. Sie können Folgendes ändern:
   - **Zeitlimit für max. synchrone Verbindungen (Sekunden)**. Um die Anzahl Sekunden anzugeben, die eine synchrone Verbindung geöffnet bleiben kann. Der Standardwert ist 300 Sekunden.
   - **Max. gleichzeitige synchrone Verbindungen**. Um anzugeben, wie viele synchrone Verbindungen das System zulässt. Der Standardwert ist 100 Verbindungen.

**Anmerkung:** Die Werte für **Synchronrouting** können bearbeitet werden.

## Handler

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

Wenn Sie bestimmte Geschäftsdokumenttypen (RosettaNet, cXML, SOAP und AS2) über einen synchronen Austausch senden oder empfangen, geben Sie einen Handler für das zugeordnete Protokoll am Konfigurationspunkt **Synchronprüfung** an.

Darüber hinaus können Sie die Nachverarbeitungs-Konfigurationspunkte für den Empfänger ändern.

In „ Konfigurationspunkte ändern” auf Seite 77 erfahren Sie, wie Sie einen Konfigurationspunkt ändern. Ansonsten klicken Sie auf **Speichern**.

# FTP-Empfänger konfigurieren

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

Die folgenden Schritte beschreiben, was Sie für einen FTP-Empfänger angeben müssen.

1. Klicken Sie auf **Hubadmin > Hubkonfiguration > Empfänger**, um die Seite **Empfängerliste** anzuzeigen.
2. Klicken Sie auf der Seite **Empfängerliste** auf **Empfänger erstellen**.

## Empfängerdetails

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

1. Geben Sie einen Namen für den Empfänger ein. Sie könnten den Empfänger z. B. 'FTPEmpfänger1' nennen. Dies ist ein erforderliches Feld. Der Name, den Sie hier eingeben, wird in der Empfängerliste angezeigt.
2. Geben Sie optional den Status des Empfängers an. **Aktiviert** ist die Standardeinstellung. Ein aktivierter Empfänger ist für das Akzeptieren von Dokumenten bereit. Ein inaktivierter Empfänger kann keine Dokumente akzeptieren.
3. Geben Sie optional eine Beschreibung für den Empfänger ein.
4. Wählen Sie **FTP-Verzeichnis** in der Liste **Transport** aus.

## Empfängerkonfiguration

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

1. Geben Sie im Feld **FTP-Stammverzeichnis** das Stammverzeichnis des FTP-Servers ein. Document Manager fragt automatisch die Unterverzeichnisse der Partner innerhalb des FTP-Stammverzeichnisses nach Dokumentweiterleitungen ab. Dieses Feld ist erforderlich. Informationen zum Konfigurieren des Verzeichnisses für einen FTP-Server finden Sie in „FTP-Server für das Empfangen von Dokumenten konfigurieren" auf Seite 35.

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

**fügen**. Die Erweiterung wird dann der Liste mit Dateierweiterungen hinzugefügt, die ignoriert werden sollen. Die Standardeinstellung ist, dass keine Dateitypen ausgeschlossen werden.

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

### Handler

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

Im Abschnitt „ Konfigurationspunkte ändern" auf Seite 77 erfahren Sie, wie Sie den Konfigurationspunkt **Vorverarbeitung** ändern. Ansonsten klicken Sie auf **Speichern**.

## SMTP-Empfänger (POP3) konfigurieren

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

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

1. Klicken Sie auf **Hubadmin > Hubkonfiguration > Empfänger**, um die Seite **Empfängerliste** anzuzeigen.
2. Klicken Sie auf der Seite **Empfängerliste** auf **Empfänger erstellen**.

### Empfängerdetails

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

1. Geben Sie einen Namen für den Empfänger ein. Sie könnten den Empfänger z. B. 'POP3Empfänger1' nennen. Dies ist ein erforderliches Feld. Der Name, den Sie hier eingeben, wird in der Empfängerliste angezeigt.
2. Geben Sie optional den Status des Empfängers an. **Aktiviert** ist die Standardeinstellung. Ein aktivierter Empfänger ist für das Akzeptieren von Dokumenten bereit. Ein inaktivierter Empfänger kann keine Dokumente akzeptieren.
3. Geben Sie optional eine Beschreibung für den Empfänger ein.
4. Wählen Sie **POP3** in der Liste **Transport** aus.

### Empfängerkonfiguration

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

1. Geben Sie optional den Betriebsmodus an. Der Betriebsmodus definiert die Art der Übertragung. Wenn Sie z. B. einen Dokumentenaustausch testen wollen, bevor Sie ihn in die Produktion einreihen, müssen Sie **Test** eingeben. Die Standardeinstellung ist **Produktion**.
2. Geben Sie die Position des POP3-Servers ein, an den E-Mails zugestellt werden. Sie können beispielsweise eine IP-Adresse eingeben.
3. Geben Sie optional eine Portnummer ein. Wenn Sie nichts eingeben, wird der Wert 110 verwendet.

4. Geben Sie die Benutzer-ID und das Kennwort ein, die erforderlich sind, um auf den E-Mail-Server zuzugreifen, falls eine Benutzer-ID und ein Kennwort benötigt werden.
5. Das Feld **Anzahl Threads** ist schreibgeschützt. Durch diesen Wert wird angegeben, wie viele Dokumente Document Manager gleichzeitig verarbeiten kann.

### Zeitplan

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

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

### Handler

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

Im Abschnitt „ Konfigurationspunkte ändern” auf Seite 77 erfahren Sie, wie Sie den Konfigurationspunkt **Vorverarbeitung** ändern. Ansonsten klicken Sie auf **Speichern**.

## JMS-Empfänger konfigurieren

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

Die folgenden Schritte beschreiben, was Sie für einen JMS-Empfänger angeben müssen.

1. Klicken Sie auf **Hubadmin > Hubkonfiguration > Empfänger**, um die Seite **Empfängerliste** anzuzeigen.
2. Klicken Sie auf der Seite **Empfängerliste** auf **Empfänger erstellen**.

**Anmerkung:** Informationen zum Konfigurieren der Laufzeitbibliotheken, um die erforderlichen WebSphere MQ-JAR-Dateien für WebSphere Partner Gateway sichtbar zu machen, finden Sie in „Laufzeitbibliotheken konfigurieren" auf Seite 42.

## Empfängerdetails

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

1. Geben Sie einen Namen für den Empfänger ein. Sie könnten den Empfänger z. B. 'JMSReceiver1' nennen. Dies ist ein erforderliches Feld. Der Name, den Sie hier eingeben, wird in der Liste **Empfänger** angezeigt.
2. Geben Sie optional den Status des Empfängers an. **Aktiviert** ist die Standardeinstellung. Ein aktivierter Empfänger ist für das Akzeptieren von Dokumenten bereit. Ein inaktivierter Empfänger kann keine Dokumente akzeptieren.
3. Geben Sie optional eine Beschreibung für den Empfänger ein.
4. Wählen Sie in der Liste **Transport** den Eintrag **JMS** aus.

## Empfängerkonfiguration

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

1. Geben Sie optional den **Operationstyp** an. Der Operationstyp definiert die Art der Übertragung. Wenn Sie z. B. einen Dokumentenaustausch testen wollen, bevor Sie ihn in die Produktion einreihen, müssen Sie **Test** eingeben. Die Standardeinstellung ist *Produktion*.
2. Geben Sie die **JMS-Provider-URL** ein. Diese sollte mit dem Wert übereinstimmen, den Sie eingegeben haben (der Dateisystempfad zur .bindings-Datei), als Sie WebSphere Partner Gateway für JMS konfiguriert haben (Schritt 5 auf Seite 40). Sie können den Unterordner für den JMS-Kontext auch als Teil der JMS-Provider-URL angeben.

   Geben Sie ohne den JMS-Kontext beispielsweise `c:/temp/JMS` ein. Geben Sie mit dem JMS-Kontext beispielsweise `c:/temp/JMS/JMS` ein.
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 **JMS-Warteschlangenname** ein. Dies ist ein erforderliches Feld. Dieser Name sollte mit dem Namen übereinstimmen, den Sie mit dem Befehl `define q` angegeben haben, als Sie die Bindungdatei erstellt haben (Schritt 4 auf Seite 41).

   Wenn Sie den Unterordner für den JMS-Kontext in Schritt 2 eingegeben haben, geben Sie hier nur den Namen der Warteschlange ein, z. B. `inQ`. Wenn Sie den Unterordner für den JMS-Kontext nicht in der JMS-Provider-URL eingegeben haben, geben Sie den Unterordner vor dem Factory-Namen ein (z. B. `JMS/inQ`).
5. Geben Sie einen Wert für **JMS-Factory-Name** ein. Dies ist ein erforderliches Feld. Dieser Name sollte mit dem Namen übereinstimmen, den Sie mit dem Befehl `define qcf` angegeben haben, als Sie die Bindungsdatei erstellt haben (Schritt 4 auf Seite 41).

   Wenn Sie den Unterordner für den JMS-Kontext in Schritt 2 eingegeben haben, geben Sie hier nur den Factory-Namen ein (z. B. `Hub`). Wenn Sie den Unterordner für den JMS-Kontext nicht in der JMS-Provider-URL eingegeben haben, geben Sie den Unterordner vor dem Factory-Namen ein (z. B. `JMS/Hub`).
6. Geben Sie optional das **Provider-URL-Paket** ein.

7. Geben Sie einen Wert für **JNDI-Factory-Name** ein. Dies ist ein erforderliches Feld. Sie werden wahrscheinlich den Wert com.sun.jndi.fscontext.RefFSContextFactory verwenden, wenn Sie Ihre JMS-Konfiguration, wie in „Hub für das JMS-Transportprotokoll konfigurieren" auf Seite 39 beschrieben, für WebSphere MQ einrichten.
8. Geben Sie einen Wert für **JMS-Benutzername** und **JMS-Kennwort** ein.
9. Geben Sie optional einen Wert für **Zeitlimit** ein, um die Anzahl Sekunden anzugeben, die der Empfänger die JMS-Warteschlange auf Dokumente hin überwacht. Dieses Feld ist optional.
10. Geben Sie optional einen Wert für **Anzahl Threads** ein, um die Anzahl der Dokumente anzugeben, die Document Manager gleichzeitig verarbeiten kann. Der Standardwert 1 wird hier empfohlen.

Wenn Sie z. B. einen JMS-Empfänger konfigurieren wollen, der mit dem JMS-Konfigurationsbeispiel in „Hub für das JMS-Transportprotokoll konfigurieren" auf Seite 39 übereinstimmt, gehen Sie wie folgt vor:

1. Geben Sie im Feld **Empfängername** den Wert **JMSReceiver** ein.
2. Geben Sie im Feld **JMS-Provider-URL** einen der folgenden Werte ein:
   - **file:///C:/TEMP/JMS/JMS** (unter Windows)
   - **file:///opt/temp** in (unter UNIX)
3. Geben Sie im Feld **JMS-Warteschlangenname** den Wert **inQ** ein.
4. Geben Sie im Feld **JMS-Factory-Name** den Wert **Hub** ein.

### Handler

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

In „ Konfigurationspunkte ändern" auf Seite 77 erfahren Sie, wie Sie Konfigurationspunkte für diesen Empfänger ändern. Ansonsten klicken Sie auf **Speichern**.

## Dateiverzeichnisempfänger konfigurieren

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

Die folgenden Schritte beschreiben, welche Angaben für einen Dateiverzeichnisempfänger erforderlich sind.

1. Klicken Sie auf **Hubadmin > Hubkonfiguration > Empfänger**, um die Seite **Empfängerliste** anzuzeigen.
2. Klicken Sie auf der Seite **Empfängerliste** auf **Empfänger erstellen**.

### Empfängerdetails

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

1. Geben Sie einen Namen für den Empfänger ein. Sie könnten den Empfänger z. B. 'DateiEmpfänger1' nennen. Dies ist ein erforderliches Feld. Der Name, den Sie hier eingeben, wird in der Liste **Empfänger** angezeigt.
2. Geben Sie optional den Status des Empfängers an. **Aktiviert** ist die Standardeinstellung. Ein aktivierter Empfänger ist für das Akzeptieren von Dokumenten bereit. Ein inaktivierter Empfänger kann keine Dokumente akzeptieren.

3. Geben Sie optional eine Beschreibung für den Empfänger ein.
4. Wählen Sie in der Liste **Transport** den Eintrag **Dateiverzeichnis** aus.

### Empfängerkonfiguration

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

1. Geben Sie einen Wert für **Dokumentstammverzeichnispfad** ein, um das Verzeichnis anzugeben, in dem die Dokumente empfangen werden.

   Ist das Stammverzeichnis nicht vorhanden, wird für den Empfänger ein neues Verzeichnis erstellt. Ist das Stammverzeichnis jedoch bereits vorhanden, verwendet der Empfänger das vorhandene Verzeichnis. Dies gilt nur für WebSphere Partner Gateway 6.1.1 und neuere Versionen.

   Das Präfix `file://` ist optional.

   Wenn Sie zum Beispiel das Verzeichnis `c:\wpg\empfänger\datei1` als Dokumentstammverzeichnispfad angeben möchten, geben Sie `c:\wpg\empfänger\datei1` oder `file://c:\wpg\empfänger\datei1` ein.
2. 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.
3. Geben Sie optional einen Wert für **Nichtänderungsintervall für Datei** ein, um die Anzahl Sekunden anzugeben, die die Dateigröße unverändert bleiben muss, bevor Document Manager das Dokument zur Verarbeitung abruft. Dieser Nichtänderungszeitraum stellt sicher, dass ein Dokument vollständig übertragen wurde (und sich nicht mitten in der Übertragung befindet), wenn es von Document Manager abgerufen wird. Der Standardwert ist 3 Sekunden.
4. Geben Sie optional einen Wert für **Threadanzahl** ein, um die Anzahl der Dokumente anzugeben, die Document Manager gleichzeitig verarbeiten kann. Der Standardwert 1 wird hier empfohlen.

### Handler

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

Im Abschnitt „ Konfigurationspunkte ändern” auf Seite 77 erfahren Sie, wie Sie den Konfigurationspunkt **Vorverarbeitung** ändern. Ansonsten klicken Sie auf **Speichern**.

## FTP-Scripting-Empfänger konfigurieren

Ein FTP-Scripting-Empfänger ist ein Abfrageempfänger, der entsprechend dem von Ihnen festgelegten Zeitplan ausgeführt wird. Das Verhalten eines FTP-Scripting-Empfängers wird von einem FTP-Befehlsscript geregelt.

Der FTP-Empfänger fragt ein Verzeichnis auf Ihrem FTP-Server ab; im Gegensatz dazu fragt der FTP-Scripting-Empfänger Verzeichnisse auf einem anderen Server ab (z. B. einem VAN).

**Anmerkung:**

1. Wenn die Datenbank inaktiv und **Benutzer sperren** auf "Ja" gesetzt ist, funktioniert der FTP-Scripting-Empfänger möglicherweise nicht, weil er die Sperre nicht aus der Datenbank abrufen kann.
2. Der Partner muss sicherstellen, dass das Dokument vollständig ist, damit es vom FTP-Scripting-Empfänger empfangen werden kann. Dazu gibt es zwei Möglichkeiten: Der FTP-Server kann das Dokument entweder so lange sperren, bis es vollständig ist, oder der Partner kann das Dokument in ein temporäres Verzeichnis schreiben und dann das vollständige Dokument in ein Verzeichnis verschieben, das vom FTP-Scripting-Empfänger verwendet wird.

## FTP-Script erstellen

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

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

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

   Die Platzhalter (z. B. %BCGSERVERIP%) werden ersetzt, wenn der Empfänger durch die Werte aktiviert wird, die Sie eingeben, wenn Sie eine bestimmte Instanz eines FTP-Scripting-Empfängers erstellen. %BCGOPTION% ist in diesem Beispiel der Name des Verzeichnisses im Befehl `cd`. Die Scriptparameter und ihre zugeordneten Felder des FTP-Scripting-Empfängers werden in Tabelle 3 gezeigt:

*Tabelle 3. Zuordnung der Scriptparameter zu den Feldeinträgen für den FTP-Scripting-Empfänger*

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

2. Speichern Sie die Datei.

## FTP-Scripting-Befehle

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

- ascii, binary, passive, epsv

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

- cd

  Dieser Befehl wechselt zum angegebenen Verzeichnis.

- delete

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

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

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

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

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

  Dieser Befehl erstellt ein Verzeichnis auf dem FTP-Server.
- mputren

  Dieser Befehl ist eine Kombination der Befehle "mput" und "rename". Mit dem Befehl **mputren * *.tmp /destination/*** wird die Datei beispielsweise mit der Erweiterung **.tmp** vom Ziel auf den FTP-Server kopiert. Nach Abschluss des Downloadprozesses für das Dokument wird die Datei umbenannt und in das Verzeichnis **/destination** auf dem FTP-Server kopiert.
- open

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

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

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

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

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

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

  Dieser Befehl entfernt ein Verzeichnis vom FTP-Server.

- site

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

## Empfängerdetails

Die folgenden Schritte beschreiben, was Sie für einen FTP-Scripting-Empfänger angeben müssen.

1. Klicken Sie auf **Hubadmin > Hubkonfiguration > Empfänger**, um die Seite **Empfängerliste** anzuzeigen.
2. Klicken Sie auf der Seite **Empfängerliste** auf **Empfänger erstellen**.

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

1. Geben Sie einen Namen für den Empfänger ein. Sie könnten den Empfänger z. B. 'FTPScriptingEmpfänger1' nennen. Dies ist ein erforderliches Feld. Der Name, den Sie hier eingeben, wird in der Liste **Empfänger** angezeigt.
2. Geben Sie optional den Status des Empfängers an. **Aktiviert** ist die Standardeinstellung. Ein aktivierter Empfänger ist für das Akzeptieren von Dokumenten bereit. Ein inaktivierter Empfänger kann keine Dokumente akzeptieren.
3. Geben Sie optional eine Beschreibung für den Empfänger ein.
4. Wählen Sie **FTP-Scripting** in der Liste **Transport** aus.

## Empfängerkonfiguration

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

1. Geben Sie optional den **Operationstyp** an. Der Operationstyp definiert die Art der Übertragung. Wenn Sie z. B. einen Dokumentenaustausch testen wollen, bevor Sie ihn in die Produktion einreihen, müssen Sie **Test** eingeben. Die Standardeinstellung ist **Produktion**.
2. Geben Sie die Server-IP-Adresse (**Server IP**) des FTP-Servers ein, zu dem Sie eine Verbindung herstellen. Der hier eingegebene Wert ersetzt bei der Ausführung des FTP-Scripts den Wert %BCGSERVERIP%.
3. Geben Sie die **Benutzer-ID** und das **Kennwort** ein, mit denen Sie auf den Server zugreifen. Die Werte, die Sie hier eingeben, werden %BCGUSERID% und %BCGPASSWORD% ersetzen, wenn das FTP-Script ausgeführt wird.
4. Wählen Sie für For **FTPS-Modus** den Wert *Ja* oder *Nein* aus, um anzugeben, ob der Empfänger im SSL-Modus (Secure Sockets Layer) betrieben wird. Falls Sie *Ja* angeben, müssen Sie Zertifikate mit Ihren Partnern austauschen, wie in Kapitel 13, „Sicherheit für Dokumentenaustauschvorgänge aktivieren", auf Seite 255 beschrieben.
5. Laden Sie die Scriptdatei hoch, indem Sie die folgenden Schritte befolgen:
   a. Klicken Sie auf **Scriptdatei hochladen**.
   b. Geben Sie den Namen der Datei ein, die das Script für die Verarbeitung von Dokumenten enthält, oder navigieren Sie mit **Durchsuchen** zu der Datei.
   c. Wählen Sie den Codierungstyp für die Scriptdatei aus.
   d. Klicken Sie auf **Datei laden**, um die Scriptdatei in das Textfeld **Momentan geladene Scriptdatei** zu laden.
   e. Wenn es sich um die gewünschte Scriptdatei handelt, klicken Sie auf **Speichern**.

f. Klicken Sie auf **Fenster schließen**.

6. Geben Sie für **Verbindungszeitlimit** die Anzahl Sekunden ein, die ein Socket ohne Datenverkehr geöffnet bleibt.
7. Geben Sie im Feld **Benutzer sperren** an, ob der Empfänger eine Sperre anfordern wird, sodass keine anderen Instanzen eines FTP-Scripting-Empfängers gleichzeitig auf dasselbe FTP-Serververzeichnis zugreifen können.

**Anmerkung:** Die Werte für **Attribute des globalen FTP-Scripting** sind bereits ausgefüllt und Sie können diese über diese Seite nicht bearbeiten. Verwenden Sie die Seite **Globale Transportattribute**, um diese Werte zu ändern, wie im Abschnitt „ Globale Transportwerte konfigurieren" auf Seite 62 beschrieben.

## Benutzerdefinierte Attribute

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

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

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

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

%BCGOPTION% wäre in diesem Fall ein Verzeichnisname.

## Zeitplan

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

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

### Handler

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

Im Abschnitt „ Konfigurationspunkte ändern” auf Seite 77 erfahren Sie, wie Sie den Konfigurationspunkt **Vorverarbeitung** ändern. Ansonsten klicken Sie auf **Speichern**.

## SFTP-Empfänger konfigurieren

Dieser Abschnitt enthält Einzelheiten über die Verwendung von SFTP (SSH-FTP) als Protokoll zur Weiterleitung von Geschäftsdokumenten. Dieses Protokoll stellt die Vertraulichkeit, Authentifizierung und Nachrichtenintegrität der Daten sicher.

Der SFTP-Empfänger fragt den SFTP-Server ab, ruft Dateien vom SFTP-Server ab und speichert sie im lokalen Verzeichnis. Das abgefragte Verzeichnis auf dem SFTP-Server wird als "fernes Ereignisverzeichnis" bezeichnet. Das Verzeichnis, in dem die abgerufenen Dateien gespeichert werden, wird als "lokales Ereignisverzeichnis" bezeichnet.

Die folgenden Schritte beschreiben, was Sie für einen SFTP-Empfänger angeben müssen.

1. Klicken Sie auf **Hubadmin > Hubkonfiguration > Empfänger**, um die Seite **Empfängerliste** anzuzeigen.
2. Klicken Sie auf der Seite **Empfängerliste** auf **Empfänger erstellen**.

### SFTP-Empfänger auf für die WAS-Verwaltungssicherheit aktivierten Systemen erstellen

WebSphere Partner Gateway V6.2.1 unterstützt das Erstellen eines SFTP-Empfängers auf Systemen, die für die WAS-Verwaltungssicherheit aktiviert sind. In diesem Abschnitt werden die Schritte beschrieben, die zum Erstellen eines SFTP-Empfängers auf einem für die WAS-Verwaltungssicherheit aktivierten System erforderlich sind.

1. Navigieren Sie in der Konsole von WebSphere Partner Gateway Console zu **Systemverwaltung** > **Konsolenverwaltung** > **Sicherheit für WAS-Administration**.
2. Setzen Sie in dieser Anzeige den Wert für das Attribut **bcg.RMIConnector.security.enabled** auf "true". Standardmäßig ist der Wert für dieses Attribut auf "false" festgelegt.
3. Legen Sie die übrigen Attribute in dieser Anzeige auf die im Folgenden dargestellten Werte fest:
   a. **bcg.RMIConnector.security.enabled**: Setzen Sie dieses Attribut nur dann auf "true", wenn **Sicherheit für WAS-Administration** aktiviert ist. Wenn Sie diese Eigenschaft nicht auf "true" setzen, können Sie keinen SFTP-Empfänger erstellen.
   b. **bcg.RMIConnector.security.enabled**: Ist dieses Attribut auf "true" gesetzt, müssen die folgenden Attribute obligatorisch festgelegt werden:
      - **bcg.RMIConnector.host.name**: Geben Sie den Hostnamen oder die IP-Adresse von Deployment Manager ein.

- **bcg.RMIConnector.portNumber**: Geben Sie den Wert für den Bootstrap-Port von Deployment Manager an.
- **bcg.RMIConnector.admin.userId**: Legen Sie dieses Attribut auf die Benutzer-ID fest, die für die WAS-Verwaltungssicherheit verwendet wird.
- **bcg.RMIConnector.admin.password**: Legen Sie dieses Attribut auf das Kennwort fest, das für die WAS-Verwaltungssicherheit verwendet wird.

4. Klicken Sie auf **Speichern**.

## Empfängerdetails

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

1. Geben Sie einen Namen für den Empfänger ein. Sie könnten den Empfänger z. B. 'SFTPEmpfänger1' nennen. Dies ist ein erforderliches Feld. Der Name, den Sie hier eingeben, wird in der Empfängerliste angezeigt.
2. Geben Sie optional den Status des Empfängers an. **Aktiviert** ist die Standardeinstellung. Ein aktivierter Empfänger ist für das Akzeptieren von Dokumenten bereit. Ein inaktivierter Empfänger kann keine Dokumente akzeptieren.
3. Geben Sie optional eine Beschreibung für den Empfänger ein.
4. Wählen Sie in der Liste **Transport** den Eintrag **SFTP** aus.

## Empfängerkonfiguration

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

1. Geben Sie den **Betriebsmodus** ein. Wählen Sie eine Option aus der Dropdown-Liste aus oder klicken Sie auf **Neu**, um einen Modus zu erstellen.
2. Geben Sie in das Feld **IP für SFTP-Host** den Hostnamen des SFTP-Servers ein. Es sind maximal 100 Zeichen zulässig. Ferner können Sie IP-Adressen, IPv4- und IPv6-Adressen eingeben.
3. Geben Sie den Wert für die **Portnummer** ein.Der Standardwert ist 22.
4. **Fernes Ereignisverzeichnis** ist das Verzeichnis, aus dem der Adapter Ereignisdateien von der SFTP-Site herunterlädt.
5. Wählen Sie im Feld **Authentifizierungstyp** die Option **Benutzername/ Kennwort** oder **Authentifizierung über privaten Schlüssel** aus.
6. Geben Sie für Benutzername/Kennwort einen Wert für **Benutzername** und **Kennwort** ein. Ist als Authentifizierungstyp die Authentifizierung über einen privaten Schlüssel ausgewählt, müssen Sie die Felder **Benutzername**, **Datei mit privatem Schlüssel** und **Verschlüsselungstext** ausfüllen. Die Datei mit dem privaten Schlüssel muss im Format OpenSSH vorliegen.
7. Geben Sie in das Feld **Abfrageintervall für SFTP** die Wartezeit des Adapters (in Millisekunden) ein. Dieser wert gibt an, wie lange der Adapter wartet, während er das lokale Ereignisverzeichnis abfragt. Diese Zeitdauer wird zusammen mit der Zeitdauer für die Verarbeitung der Dokumente im lokalen Ereignisverzeichnis als "Abfragezyklus" bezeichnet.
8. **Anzahl Abfragen** gibt die Anzahl der Ereignisse (Dokumente) an, die der Empfänger während jedes einzelnen Abfragezyklus verarbeitet.
9. **Wiederholungsintervall** gibt die Länge des Zeitraums (in Millisekunden) an, in dem der Adapter nach einem Fehler bei eingehenden Operationen zwischen den Versuchen, eine neue Verbindung herzustellen, wartet.
10. **Wiederholungslimit** gibt an, wie oft der Adapter versucht, eine eingehende Verbindung nach einem Fehler erneut herzustellen.

11. **EIS-Codierung** ist die Codierung des FTP-Servers. Anhand dieses Werts können Sie die Codierung für die Steuerverbindung des FTP-Servers festlegen.
12. Die Option **Serverauthentifizierung aktivieren** kann ausgewählt werden, um den Server, zu dem eine Verbindung hergestellt wird, zu authentifizieren. Ist die Serverauthentifizierung aktiviert, müssen Sie den Pfad für die Hostschlüsseldatei angeben. Die Hostschlüsseldatei muss im Format OpenSSH vorliegen.
13. Konfigurieren Sie gegebenenfalls die Handler.
14. Klicken Sie auf **Speichern**, um die Konfiguration zu speichern.

### Handler

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

Im Abschnitt „ Konfigurationspunkte ändern" auf Seite 77 erfahren Sie, wie Sie den Konfigurationspunkt **Vorverarbeitung** ändern. Ansonsten klicken Sie auf **Speichern**.

## Empfänger für benutzerdefinierten Transport konfigurieren

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

Führen Sie die folgenden Schritte aus:

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

   **Anmerkung:** Sie können aus der Empfängerliste auch einen benutzerdefinierten Transporttyp löschen. Sie können keinen Transport löschen, der von WebSphere Partner Gateway bereitgestellt wurde. Ebenfalls können Sie keinen benutzerdefinierten Transport löschen, nachdem er zum Erstellen eines Empfängers verwendet wurde.
5. Klicken Sie auf **Empfänger erstellen**.
6. Geben Sie einen Namen für den Empfänger ein. Dies ist ein erforderliches Feld. Der Name, den Sie hier eingeben, wird in der Liste **Empfänger** angezeigt.
7. Geben Sie optional den Status des Empfängers an. **Aktiviert** ist die Standardeinstellung. Ein aktivierter Empfänger ist für das Akzeptieren von Dokumenten bereit. Ein inaktivierter Empfänger kann keine Dokumente akzeptieren.
8. Geben Sie optional eine Beschreibung für den Empfänger ein.
9. Wählen Sie den benutzerdefinierten Transport in der Liste aus.
10. Füllen Sie die Felder aus, die für jeden benutzerdefinierten Transport eindeutig sind.
11. Wenn Sie Konfigurationspunkte für diesen Empfänger ändern wollen, lesen Sie „ Konfigurationspunkte ändern" auf Seite 77. Ansonsten klicken Sie auf **Speichern**.

## Konfigurationspunkte ändern

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

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

Um einen benutzerdefinierten Handler auf diese Konfigurationspunkte anzuwenden, müssen Sie zuerst den Handler hochladen, wie in „ Benutzerdefinierte Handler hochladen" auf Seite 60 beschrieben. Sie können auch einen vom Produkt bereitgestellten Handler verwenden, der bereits verfügbar ist und nicht mehr hochgeladen werden muss.

## Vorverarbeitung

Der Vorverarbeitungs-Konfigurationshandler ist auf allen Empfängertypen verfügbar, er ist jedoch nicht auf SMTP-Empfänger anwendbar.

### Vorverarbeitungsattribute

Tabelle 4 beschreibt die Attribute, die Sie für einen Vorverarbeitungshandler festlegen können und listet die Verteilerhandler auf, auf die die Attribute angewendet werden.

Die ROD-Attribute, die in dieser Tabelle als Beispiele verwendet werden, entsprechen denen, die in „ Beispiel: ROD zu EDI" auf Seite 372 verwendet wurden. Im Beispiel sind die ROD-Attribute in der Zuordnung **S_DT_ROD_TO_EDI.eif** enthalten, welche die folgende Dokumentdefinition einschließt:

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

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

*Tabelle 4. Attribute für Verteilerhandler*

| Attribut | Beschreibung | Verteiler-handler |
|---|---|---|
| Encoding | Die Zeichencodierung des Dokuments. Der Standardwert ist ASCII. | ROD Generic XML EDI |

*Tabelle 4. Attribute für Verteilerhandler (Forts.)*

| Attribut | Beschreibung | Verteiler-handler |
|---|---|---|
| BATCHDOCS | Wenn BCG_BATCHDOCS aktiv ist, fügt der Verteiler den Dokumenten Stapel-IDs hinzu, nachdem die Dokumente aufgeteilt wurden. Wenn die Dokumente in EDI-Transaktionen transformiert werden, die mit einem Umschlag versehen werden sollen, verwendet das Programm zur Umschlagsgenerierung die Stapel-IDs, um sicherzustellen, dass die Transaktionen, wenn möglich, in denselben EDI-Austausch gestellt werden, bevor sie zugestellt werden. Beachten Sie, dass für das Stapelattribut des Programms zur Umschlagsgenerierung der Standardwert **On** (Ein) festgelegt sein muss. Siehe „Stapelbetrieb" auf Seite 196. | ROD Generic XML |
| From Packaging Name | Das Paket, das dem Dokument zugeordnet ist. Dieser Wert muss mit dem Paket übereinstimmen, das in der Dokumentdefinition angegeben ist. Für ein Dokument im Paket **None** sollte dieser Wert z. B. **None** sein. | ROD Generic |
| From Packaging Version | Die Version des Pakets, das in **From Packaging Name** angegeben ist. Wenn für das Dokument beispielsweise das Paket **None** festgelegt ist, ist dieser Wert **N/A**. | ROD Generic |
| From Protocol Name | Das Protokoll, das dem Dokument zugeordnet ist. Dieser Wert muss mit dem Protokoll übereinstimmen, das in der Dokumentdefinition angegeben ist. Für ein ROD-Dokument könnte dieser Wert z. B. **ROD-TO-EDI_DICT** sein. | ROD Generic |
| From Protocol Version | Die Version des Protokolls, das in **From Protocol Name** angegeben ist. Für das Protokoll ROD-TO-EDI_DICT ist der Wert beispielsweise **ALL**. | ROD Generic |
| From Process Code | Der Prozess (Dokumenttyp), der diesem Dokument zugeordnet ist. Dieser Wert muss mit dem Dokumenttyp in der Dokumentdefinition übereinstimmen. Für ein ROD-Dokument könnte dieser Wert z. B. **DTROD-TO-EDI_ROD** sein. | ROD Generic |
| From Process Version | Die Version des Prozesses, der in **From Process Code** angegeben ist. Für DTROD-TO-EDI_ROD ist dieser Wert beispielsweise **ALL**. | ROD Generic |
| Metadictionary | Das Metawörterbuch stellt Informationen bereit, mit denen WebSphere Partner Gateway die Daten interpretieren kann. Für ein ROD-Dokument könnte dieser Wert z. B. **ROD-TO-EDI_DICT** sein. | ROD Generic |
| Metadocument | Das Metadokument stellt Informationen bereit, mit denen WebSphere Partner Gateway die Daten interpretieren kann. Für ein ROD-Dokument könnte dieser Wert z. B. **DTROD-TO-EDI_ROD** sein. | ROD Generic |
| Metasyntax | Die Metasyntax beschreibt das Format des Dokuments, das aufgeteilt wird. Der Standardwert ist **rod**. | ROD Generic |
| SenderId | Die ID des sendenden Partners. | Generic |
| ReceiverId | Die ID des empfangenden Partners. | Generic |

**Hinweise:**

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

## Vorverarbeitungs-Konfigurationspunkt ändern

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

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

   Standardmäßig werden die folgenden fünf Vorverarbeitungshandler bereitgestellt und in der **Verfügbarkeitsliste** angezeigt:

   - com.ibm.bcg.edi.receiver.preprocesshandler.EDISplitterHandler
   - com.ibm.bcg.edi.receiver.preprocesshandler.XMLSplitterHandler
   - com.ibm.bcg.edi.receiver.preprocesshandler.RODSplitterHandler
   - com.ibm.bcg.edi.receiver.preprocesshandler.GenericDocumentFlowHandler
   - com.ibm.bcg.server.receiver.preprocesshandler.FileNamePartnerId

   **Anmerkung:** Die Vorverarbeitungshandler werden nicht auf SMTP-Empfänger angewendet.
2. Wenn Sie mehrere EDI-Austauschvorgänge oder XML- oder ROD-Dokumente empfangen, die aufgeteilt werden müssen, stellen Sie sicher, dass Sie die entsprechenden Verteilerhandler auswählen. Führen Sie die folgenden Schritte aus, um den Vorverarbeitungsschritt zu konfigurieren:
   a. Wählen Sie einen Handler in der **Verfügbarkeitsliste** aus, und klicken Sie auf **Hinzufügen**. Beachten Sie, dass der Handler von der **Verfügbarkeitsliste** in die **Konfigurationsliste** versetzt wird, wie in Abb. 17 dargestellt:

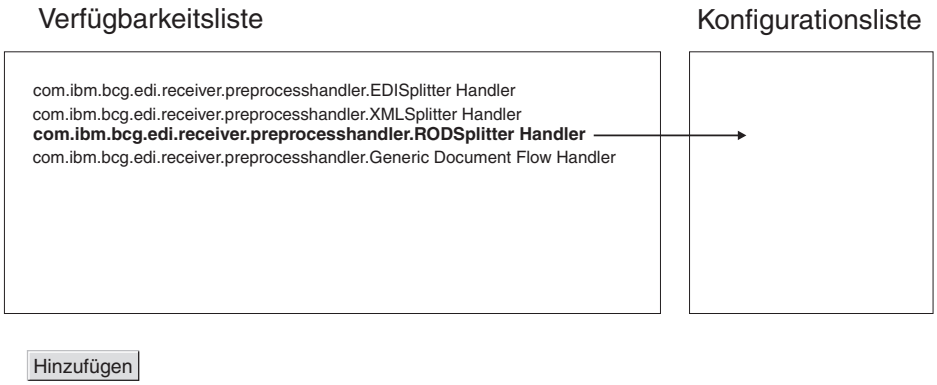



*Abbildung 17. Vorverarbeitungsschritt für einen Empfänger konfigurieren*

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

      Denken Sie daran, dass die Handler für Empfänger in der Reihenfolge aufgerufen werden, in der sie in der Konfigurationsliste angezeigt werden. Der erste anwendbare Handler verarbeitet die Anforderung, und die in der Liste nachfolgenden Handler werden nicht aufgerufen.
   c. Konfigurieren Sie den Handler, indem Sie ihn auswählen und auf **Konfigurieren** klicken:
      - Wenn Sie EDISplitterHandler hinzugefügt haben, können Sie sein Attribut **Encoding** ändern. Die Standardcodierung ist ASCII.
      - Wenn Sie XMLSplitterHandler hinzugefügt haben, können Sie sein Attribut **BCGBATCHDOCS** ändern. Die Standardeinstellung ist **ON**. Informationen zu diesem Attribut finden Sie in „Vorverarbeitungsattribute" auf Seite 77.

- Wenn Sie RODSplitterHandler hinzugefügt haben, können Sie Werte für 11 Attribute angeben. **Encoding**, **BATCHDOCS** und **Metasyntax** haben Standardwerte. Für die anderen Attribute müssen Sie einen Wert für **From Packaging Name**, **From Packaging Version**, **From Protocol Name**, **From Protocol Version**, **From Process Code**, **From Process Version**, **Metadictionary** und **Metadocument** eingeben. Informationen zu diesen Attributen finden Sie in „Vorverarbeitungsattribute" auf Seite 77.
- Wenn Sie GenericDocumentFlowHandler hinzugefügt haben, können Sie Werte für 13 Attribute angeben. **Encoding** und **BATCHDOCS** verfügen über Standardwerte. Die Attribute "SenderId" und "ReceiverId" sind für den Handler "GenericDocumentFlowHandler" vorkonfiguriert und verwenden keine Standardwerte. Für die anderen Attribute müssen Sie einen Wert für **From Packaging Name**, **From Packaging Version From Protocol Name**, **From Protocol Version**, **From Process Code**, **From Process Version**, **Metadictionary**, **Metadocument** und **Metasyntax** eingeben. Informationen zu diesen Attributen finden Sie in „Vorverarbeitungsattribute" auf Seite 77.
- Wenn Sie FileNamePartnerId hinzugefügt haben, werden keine Konfigurationsparameter erwartet. Die empfangene Datei muss die folgende Namenskonvention aufweisen:

  ```
  <beliebige_zeichenfolge>bcgrcv<Empfänger-ID>bcgsdr
  <Absender-ID>bcgend<beliebige_zeichenfolge>
  ```

  Dabei gilt Folgendes:

  *Empfänger-ID*, *Absender-ID*
  : Die Geschäfts-IDs der Partner, wie in den zugehörigen Profilen definiert.

  **bcgrcv, bcgsdr**
  : Die Zeichenfolgekonstanten, die angeben, dass die Geschäfts-IDs von Empfänger und Absender folgen.

  **bcgend**
  : Die Zeichenfolgekonstante, die das Ende der Zeichenfolge gemäß Namenskonvention festlegt.

  *beliebige_zeichenfolge*
  : Ein beliebiges alphanumerisches Zeichen, das vom Benutzer ausgewählt wird.

  Dieser Handler kann nur für FTP-Scripting- oder Dateiverzeichnisempfänger konfiguriert werden. Sie können den Handler für den Empfänger konfigurieren, um Binärdateien über FTP-Scripting oder das Dateiverzeichnis zu empfangen.

## Synchronprüfung

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

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

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

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

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

Wenn Sie z. B. einen HTTP/S-Empfänger konfigurieren, sieht die Verfügbarkeitsliste wie folgt aus:

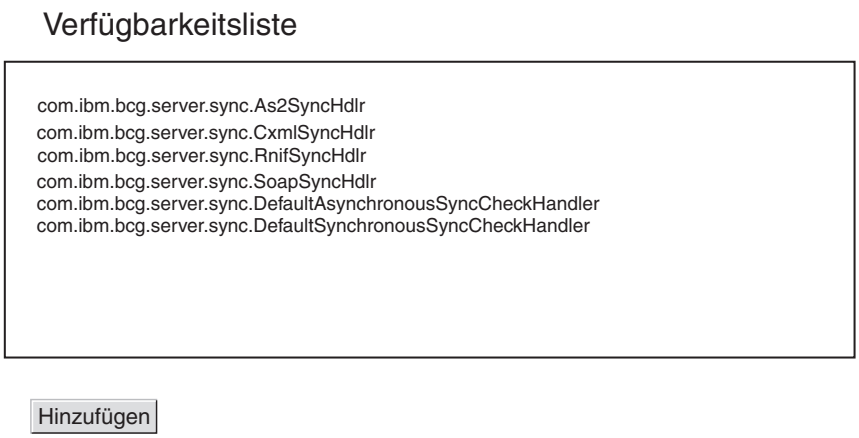



*Abbildung 18. Liste verfügbarer Handler für einen HTTP/S-Synchronprüfungs-Konfigurationspunkt*

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

'DefaultAsynchronousSyncCheckHandler' und 'DefaultSynchronousSyncCheckHandler' können mit anderen Empfängern, wie z. B. einem JMS-Empfänger, verwendet werden.

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

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

## Nachverarbeitung

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

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

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

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

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

## Konfigurationsliste ändern

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

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

# Kapitel 8. Schritte und Aktionen für feste Arbeitsabläufe konfigurieren

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

Dieses Kapitel behandelt die folgenden Themen:

- „ Handler hochladen"
- „Feste Arbeitsabläufe konfigurieren" auf Seite 84
- „Aktionen konfigurieren" auf Seite 86

**Anmerkung:** Verwenden Sie stets die Browserinstanz, mit der Sie sich an Community Console angemeldet haben, wenn Sie Konfigurationsänderungen an WebSphere Partner Gateway vornehmen. Die gleichzeitige Verwendung mehrerer Browserinstanzen kann dazu führen, dass die Konfigurationsänderungen aufgehoben werden.

## Handler hochladen

Wenn Sie Komponenten modifizieren, laden Sie zuerst die Handler für diese Komponenten hoch, bevor Sie die Komponenten erstellen oder konfigurieren. Sie müssen nur die benutzerdefinierten Handler für die Komponenten hochladen, die sie benötigen. Wenn Sie z. B. Ihren eigenen Validierungsschritt hinzufügen, müssen Sie den Handler von der Seite **Aktionen** der Seite **Handler** hochladen (wie in den Schritten 1 bis 4 auf Seite 84 beschrieben).

**Anmerkung:** Wie in „Dokumentverarbeitungskomponenten mit Handler konfigurieren" auf Seite 15 erwähnt, laden Sie nur benutzerdefinierte Handler hoch. Die Handler, die von WebSphere Partner Gateway bereitgestellt wurden, sind bereits verfügbar.

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

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

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

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

   Die Liste der Handler, die derzeit für die bestimmte Komponente definiert sind, wird angezeigt. Beachten Sie, dass die von WebSphere Partner Gateway bereitgestellten Handler aufgelistet werden. Sie haben die Provider-ID **Produkt**.
3. Klicken Sie auf der Seite **Handler-Liste** auf **Importieren**.

4. Geben Sie auf der Seite **Handler importieren** den Pfad zur XML-Datei an, die den Handler beschreibt, oder verwenden Sie **Durchsuchen**, um nach dieser XML-Datei zu suchen.
5. Klicken Sie auf **Hochladen**.

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

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

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

## Feste Arbeitsabläufe konfigurieren

In Kapitel 2, „Einführung in die Hubkonfiguration", auf Seite 5 wurden die zwei Schritte für festen Eingangsarbeitsablauf beschrieben, die Sie konfigurieren können: Ein Schritt für das Entpacken eines Protokolls und einen Schritt für das Parsing des Protokolls. Für Ausgangsarbeitsabläufe ist ein Schritt für das Packen des Protokolls vorhanden.

Wenn Sie einen benutzerdefinierten Handler verwenden, um einen Arbeitsablaufschritt zu konfigurieren, laden Sie den Handler hoch, wie in „ Handler hochladen" auf Seite 83 beschrieben.

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

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

   Der Schritt wird zusammen mit einer Liste der Handler aufgelistet, die bereits für diesen Schritt konfiguriert wurden. Eine Liste der Standardhandler finden Sie in „Eingangsarbeitsabläufe" auf Seite 85 und „Ausgangsarbeitsablauf" auf Seite 85.
4. Klicken Sie auf das Symbol **Bearbeiten**, um die Liste der Handler zu bearbeiten.
5. Führen Sie mindestens eine der folgenden Aufgaben für jeden Schritt aus, den Sie ändern wollen.
   a. Fügen Sie einen Handler hinzu, indem Sie den Handler in der **Verfügbarkeitsliste** auswählen, und klicken Sie auf **Hinzufügen**. (Ein Handler wird in der **Verfügbarkeitsliste** angezeigt, wenn Sie einen benutzerdefinierten Handler hochgeladen haben, oder wenn Sie zuvor einen Handler aus der **Konfigurationsliste** entfernt haben.) Der Handler wird in die **Konfigurationsliste** versetzt.
   b. Entfernen Sie einen Handler, indem Sie den Handler in der **Konfigurationsliste** auswählen, und klicken Sie auf **Entfernen**. Der Handler wird in die **Verfügbarkeitsliste** versetzt.
   c. Ändern Sie die Reihenfolge, in der die Handler aufgerufen werden, indem Sie den Handler auswählen und auf **Nach oben** oder **Nach unten** klicken.

Handler werden in der Reihenfolge aufgerufen, in der sie in der **Konfigurationsliste** aufgelistet sind. Der erste verfügbare Handler, der die Anforderung verarbeiten kann, ist derjenige, der die Anforderung bearbeitet. Wenn Sie erwarten, eine große Anzahl von Dokumenten eines bestimmten Typs (z. B. ROD-Dokumente) zu empfangen, können Sie den Handler, der diesem Dokumenttyp (in diesem Beispiel: com.ibm.bcg.edi.business.process.RODScannerHandler) zugeordnet ist, an den Anfang der Liste setzen.

6. Klicken Sie auf **Speichern**.

## Eingangsarbeitsabläufe

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

### Handler für das Entpacken des Protokolls

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

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

### Handler für das Verarbeiten des Protokolls

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

- com.ibm.bcg.server.RNOChannelParseHandler
- com.ibm.bcg.server.RNSignalChannelParseHandler
- com.ibm.bcg.server.RNSCChannelParseHandler
- com.ibm.bcg.server.BinaryChannelParseHandler
- com.ibm.bcg.cxml.cXMLChannelParseHandler
- com.ibm.bcg.soap.SOAPChannelParseHandler
- com.ibm.bcg.server.XMLRouterBizProcessHandler
- com.ibm.bcg.edi.EDIRouterBizProcessHandler
- com.ibm.bcg.edi.business.process.RODScannerHandler
- com.ibm.bcg.edi.business.process.NetworkAckHandler
- com.ibm.bcg.server.EBMSProtocolParseHandler
- com.ibm.bcg.server.BackendChannelParseHandler

Das Attribut "Content-Types" ist BinaryChannelParseHandler, XMLRouterBizHandler, EDIRouterBizProcessHandler und cXMLChannelParseHandler zugeordnet. Diese Handler sind bereits mit der Standardliste der Inhaltstypen ausgefüllt. Wenn das empfangene Dokument über einen "Content-Type"-Header verfügt, der für einen der obigen Handler konfiguriert ist, wird dieser Handler angewendet.

## Ausgangsarbeitsablauf

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

- com.ibm.bcg.server.pkg.NullPackagingHandler
- com.ibm.bcg.ediint.ASPackagingHandler
- com.ibm.bcg.edi.server.EDITransactionHandler
- com.ibm.bcg.rosettanet.pkg.RNOPPackagingHandler

- com.ibm.bcg.server.pkg.RNPassThruPackagingHandler
- com.ibm.bcg.cxml.cXMLPackagingHandler
- com.ibm.bcg.soap.SOAPPackagingHandler
- com.ibm.bcg.eai.EAIPackagingHandler

# Aktionen konfigurieren

In Kapitel 2, „Einführung in die Hubkonfiguration", auf Seite 5 wird ersichtlich, dass Aktionen aus mindestens einem Schritt bestehen können. WebSphere Partner Gateway stellt eine Reihe von Standardaktionen bereit. Sie können der Liste der Aktionen etwas hinzufügen, indem Sie mindestens einen Aktionshandler (dies sind Schritte in der Aktion) hochladen, den Sie dann in einer Aktion verwenden können. Sie können ebenfalls neue Aktionen erstellen, wie in „Aktionen erstellen" auf Seite 103 beschrieben.

**Anmerkung:** Sie können die Aktionen nicht ändern, die von WebSphere Partner Gateway bereitgestellt wurden, obwohl Sie eine dieser Aktionen kopieren und ändern können, wie in „Aktion kopieren" auf Seite 104 beschrieben.

Wenn Sie einen benutzerdefinierten Handler verwenden, um eine Aktion zu konfigurieren, laden Sie den Handler hoch, wie in „ Handler hochladen" auf Seite 83 beschrieben.

## Vom Produkt bereitgestellte Aktionen

In diesem Abschnitt werden die Aufgaben der von WebSphere Partner Gateway bereitgestellten Aktionen sowie die eventuell erforderlichen Konfigurationsmaßnahmen beschrieben. Kapitel 9, „Dokumenttypen konfigurieren", auf Seite 107 enthält weitere Einzelheiten zur Verwendung einiger dieser Aktionen.

Im Namen einiger Aktionen ist das Wort "bidirektional" enthalten. *Bidirektional* bedeutet in diesem Zusammenhang, dass Quellen- und Zielformat ausgetauscht werden können und die Aktion weiterhin verwendbar ist. Zum Beispiel kann für die Aktion "Bidirektionale Konvertierung von RosettaNet und XML mit Validierung" das Quellendokument RosettaNet-Format und das Zieldokument XML-Format oder das Quellendokument XML-Format und das Zieldokument RosettaNet-Format haben.

WebSphere Partner Gateway stellt die folgenden Aktionen bereit:

- „Pass-Through" auf Seite 87
- „Abbruch des RosettaNet-Prozesses durch den internen Partner (Internal Partner Cancellation of RosettaNet Process)" auf Seite 87
- „RosettaNet-Pass-Through mit Prozessprotokollierung" auf Seite 88
- „Bidirektionale Konvertierung von RosettaNet und RosettaNet Service Content mit Validierung" auf Seite 89
- „Bidirektionale Konvertierung von RosettaNet und RosettaNet Service Content ohne Inhaltsvalidierung" auf Seite 90
- „Bidirektionale Konvertierung von angepasster XML des internen Partners in RosettaNet mit Inhaltsduplikatprüfung und Validierung" auf Seite 91
- „Bidirektionale Konvertierung von RosettaNet und XML mit Validierung" auf Seite 90
- „Bidirektionale Konvertierung von angepasster XML mit Validierung" auf Seite 92

- „Bidirektionale Konvertierung von angepasster XML mit Duplikatprüfung und Validierung" auf Seite 93
- „Pass-Through von angepasster XML mit Duplikatprüfung und Validierung" auf Seite 94
- „Pass-Through von angepasster XML mit Duplikatprüfung" auf Seite 95
- „Pass-Through von angepasster XML mit Validierung" auf Seite 95
- „EDI - Umschlag entfernen" auf Seite 96
- „EDI validieren und EDI konvertieren" auf Seite 96
- „ROD (FlatFile) konvertieren und EDI validieren" auf Seite 97
- „XML konvertieren und EDI validieren" auf Seite 97
- „ebMS - Teilen und parsen" auf Seite 98
- „Validierung des SOAP-Umschlags" auf Seite 101
- „Validierung des SOAP-Hauptteils" auf Seite 101
- „Aus SOAP-Umschlag entfernen" auf Seite 101
- „EDI-Austausch validieren" auf Seite 99
- „WTX-Transformation" auf Seite 99
- „EDI-ReEnveloper" auf Seite 100

## Pass-Through

Diese Aktion wird verwendet, wenn keine speziellen Verarbeitungsaktivitäten (z. B. Validierung oder Transformation) für das Dokument ausgeführt werden müssen. Das Quellendokument wird unverändert an die Zielposition gesendet.

### Konfiguration

Keine erforderlich.

### Änderung

Diese Aktion kann in eine neue Aktion kopiert werden. Neue Schritte können den vorhandenen Schritten vorangestellt werden. Zum Beispiel ein angepasster Validierungsschritt, der das Quellendokument validiert, oder andere angepasste Verarbeitungsaktivitäten.

### Schritte

Diese Aktion enthält die folgenden Schritte, die nacheinander ausgeführt werden:

1. **com.ibm.bcg.passthrough.No_op** - Gibt an, dass der Inhaltstyp des Zieldokuments nicht vom Dokumentinhalt abgeleitet werden soll.
2. **com.ibm.bcg.outbound.OutboundDocFactory** - Immer erforderlich. Führt von WebSphere Partner Gateway geforderte Verarbeitungsaktivitäten für das Zieldokument aus. Dies ist der letzte Schritt, und die Konsole fügt diesen Schritt automatisch zu vorhandenen oder neu erstellten Aktionen hinzu. Dieser Schritt wird in der Liste der konfigurierten Handler nicht angezeigt.

## Abbruch des RosettaNet-Prozesses durch den internen Partner (Internal Partner Cancellation of RosettaNet Process)

### Zweck

Diese Aktion bezieht sich auf den Abbruch eines RosettaNet-RNIF-Prozesses durch den internen Partner (Back-End). Wenn die Back-End-Anwendung (interner Part-

ner) ein XMLEvent-Dokument mit dem Ereigniscode 800/801 sendet, wird in diesem Schritt ein 0A1-Dokument für den Versand an den externen Partner erstellt, und der entsprechende PI-Prozess wird abgebrochen.

### Konfiguration

Der RNIF-Prozess, der abgebrochen wird, muss bereits in WebSphere Partner Gateway konfiguriert worden sein. Außerdem muss WebSphere Partner Gateway bereits das RosettaNet-Dokument empfangen haben, das den Prozess gestartet hat, der abgebrochen wird.

### Änderung

Diese Aktion kann nicht geändert oder kopiert werden, da sie sich speziell auf den Abbruch des RosettaNet-PI-Prozesses bezieht.

### Schritte

Diese Aktion enthält die folgenden Schritte, die nacheinander ausgeführt werden:

1. **com.ibm.bcg.server.pkg.UnPackagingFactory** - Ermittelt die korrekte Klasse für das Entpacken von RNIF-Dokumenten fest oder nimmt an, dass es sich um kein RNIF-Dokument handelt und das Entpacken entfällt.
2. **com.ibm.bcg.validation.ValidationFactory** - Prüft das RN-Quellendokument auf den korrekten RNIF Service Content.
3. **com.ibm.bcg.outbound.OutboundDocFactory** - Immer erforderlich. Führt von WebSphere Partner Gateway geforderte Verarbeitungsaktivitäten für das Zieldokument aus. Dies ist der letzte Schritt, und die Konsole fügt diesen Schritt automatisch zu vorhandenen oder neu erstellten Aktionen hinzu. Dieser Schritt wird in der Liste der konfigurierten Handler nicht angezeigt.

## RosettaNet-Pass-Through mit Prozessprotokollierung

Diese Aktion wird verwendet, wenn das RosettaNet-RNIF-Quellendokument in WebSphere Partner Gateway ein Pass-Trough-Dokument ist. Verwenden Sie diesen Schritt, wenn der Service Content des RNIF-Dokuments nicht extrahiert oder transformiert werden kann. Obwohl es sich um ein Pass-Through-Dokument handelt, erfolgt die RNIF-Verarbeitung dennoch, und die Empfangsbestätigungen werden generiert.

### Konfiguration

Keine erforderlich

### Änderung

Diese Aktion kann kopiert und geändert werden. Für zusätzliche angepasste Verarbeitungsaktivitäten können den vorhandenen Schritten neue Schritte vorangestellt werden.

### Schritte

Diese Aktion enthält die folgenden Schritte, die nacheinander ausgeführt werden:

1. **com.ibm.bcg.rosettanet.passthru.ProcessLoggingFactory** - Dieser Schritt speichert die Metadaten des RosettaNet-Dokuments im Geschäftsdokumentobjekt (Business Document Object - BDO).

2. **com.ibm.bcg.passthrough.No_op** - Gibt an, dass der Inhaltstyp des Zieldokuments nicht vom Dokumentinhalt abgeleitet werden soll.
3. **com.ibm.bcg.outbound.OutboundDocFactory** - Immer erforderlich. Führt von WebSphere Partner Gateway geforderte Verarbeitungsaktivitäten für das Zieldokument aus. Dies ist der letzte Schritt, und die Konsole fügt diesen Schritt automatisch zu vorhandenen oder neu erstellten Aktionen hinzu. Dieser Schritt wird in der Liste der konfigurierten Handler nicht angezeigt.

## Bidirektionale Konvertierung von RosettaNet und RosettaNet Service Content mit Validierung

Diese Aktion wird für RosettaNet-RNIF-Dokumente verwendet. Beim Empfang eines RNIF-Dokuments vom externen Partner werden die Nutzdaten (RNSC - RosettaNet Service Content) aus dem Dokument im Paket **RNIF** extrahiert und an die Back-End-Anwendung (interner Partner) gesendet. Die Validierung erfolgt für das RNIF-Dokument, das den RNSC enthält. Ist der Absender die Back-End-Anwendung (interner Partner), wird das RNSC-Dokument validiert.

### Konfiguration

Das RosettaNet-PIP-Paket für das RosettaNet-Dokument muss geladen sein.

### Änderung

Diese Aktion kann nicht kopiert oder geändert werden.

### Schritte

Diese Aktion enthält die folgenden Schritte, die nacheinander ausgeführt werden:

1. **com.ibm.bcg.server.pkg.UnPackagingFactory** - Ermittelt die korrekte Klasse für das Entpacken von RNIF-Dokumenten fest oder nimmt an, dass es sich um kein RNIF-Dokument handelt und das Entpacken entfällt.
2. **com.ibm.bcg.validation.ValidationFactory** - Führt die Validierung durch und verwendet die folgenden Geschäftsprozesse, um RNIF 1.1-, RNIF 2.0- und RNSC-Dokumente zu validieren:
   - RNSignal0A1Validation (validiert die von WebSphere Partner Gateway generierten RNIF-Signale bzw. die generierte 0A1-Nachricht)
   - ValidationNoOp (gibt nur das Geschäftsdokument zurück, ohne Verarbeitungsaktivitäten auszuführen; wird aufgerufen, wenn WBIC Wiederholungen für RNIF-Signale oder die 0A1-Nachricht veranlasst)
   - RN11Validation (validiert die RNIF 1.1-Nachricht)
   - RN20Validation (validiert die RNIF 2.0-Nachricht)
   - RNSCValidation (validiert XMLEvent- und RNSC-Nachricht)
3. **com.ibm.bcg.translation.protocol.StdRNandRNSCProtFactory** - Wird verwendet, um den RNSC aus dem RNIF-Dokument zu extrahieren oder die RNIF-Informationen für den RNSC zu erstellen.
4. **com.ibm.bcg.sponsor.SponsorBusProcessFactory** - Wird bei der Verarbeitung von RosettaNet-0A1-Dokumenten zum Aktualisieren der RosettaNet-Statusengine verwendet.
5. **com.ibm.bcg.outbound.OutboundDocFactor** - Immer erforderlich. Führt von WebSphere Partner Gateway geforderte Verarbeitungsaktivitäten für das Zieldokument aus. Dies ist der letzte Schritt, und die Konsole fügt diesen Schritt auto-

matisch zu vorhandenen oder neu erstellten Aktionen hinzu. Dieser Schritt wird in der Liste der konfigurierten Handler nicht angezeigt.

## Bidirektionale Konvertierung von RosettaNet und XML mit Validierung

Diese Aktion wird für RosettaNet-RNIF-Dokumente verwendet, die in ein angepasstes XML-Dokument (oder umgekehrt) transformiert werden müssen. Beim Empfang eines RNIF-Dokuments vom externen Partner werden die Nutzdaten (RNSC - RNIF Service Content) aus dem RNIF-Paket extrahiert, validiert und in ein XML-Dokument transformiert, wobei die transformierten Zieldokumente für den Versand an die Back-End-Anwendung (interner Partner) validiert werden. Ist der Absender die Back-End-Anwendung (interner Partner), wird die XML validiert und in den RNSC transformiert, der ebenfalls validiert wird.

### Konfiguration

- Das RosettaNet-PIP-Paket für das RosettaNet-Dokument muss geladen sein.
- Die Validierungszuordnung (XML-SCHEMA) muss im XML-Quellendokument oder im XML-Zieldokument konfiguriert werden.
- Eine XSLT-Transformationszuordnung muss für diese Aktion konfiguriert werden.

### Änderung

Diese Aktion kann nicht kopiert oder geändert werden.

### Schritte

Diese Aktion enthält die folgenden Schritte, die nacheinander ausgeführt werden:

1. **com.ibm.bcg.server.pkg.UnPackagingFactory** - Ermittelt die korrekte Klasse für das Entpacken von RNIF-Dokumenten fest oder nimmt an, dass es sich um kein RNIF-Dokument handelt und das Entpacken entfällt.
2. **com.ibm.bcg.validation.ValidationFactory** - Validiert das RNIF- oder XML-Quellendokument.
3. **com.ibm.bcg.translation.protocol.RNXsltProtFactory** - Transformiert den RNSC in das bzw. aus dem XML-Format.
4. **com.ibm.bcg.validation.OutboundValidationFactory** - Validiert das sich daraus ergebende, transformierte XML-Dokument.
5. **com.ibm.bcg.sponsor.SponsorBusProcessFactory** - Wird bei der Verarbeitung von RosettaNet-0A1-Dokumenten zum Aktualisieren der RosettaNet-Statusengine verwendet.
6. **com.ibm.bcg.outbound.OutboundDocFactory** - Immer erforderlich. Führt von WebSphere Partner Gateway geforderte Verarbeitungsaktivitäten für das Zieldokument aus. Dies ist der letzte Schritt, und die Konsole fügt diesen Schritt automatisch zu vorhandenen oder neu erstellten Aktionen hinzu. Dieser Schritt wird in der Liste der konfigurierten Handler nicht angezeigt.

## Bidirektionale Konvertierung von RosettaNet und RosettaNet Service Content ohne Inhaltsvalidierung

Diese Aktion wird für RosettaNet-Dokumente (RNIF-Dokumente) verwendet. Beim Empfang eines RNIF-Dokuments von einem externen Partner werden die Nutzdaten (RNSC - RNIF Service Content) aus dem RNIF-Paket extrahiert. Die extrahierten Nutzdaten werden validiert und in ein XML-Dokument transformiert, das an

die Back-End-Anwendung (interne Partner) gesendet wird. Wenn ein XML-Dokument von der Back-End-Anwendung (dem internen Partner) empfangen wird, werden die folgenden Schritte für das Dokument ausgeführt:

1. Prüfung auf doppelte IDs
2. Validierung
3. Transformation in RNSC
4. Validierung des RNSC

### Konfiguration

Das RosettaNet-PIP-Paket für das RosettaNet-Dokument muss geladen sein.

### Änderung

Diese Aktion kann nicht kopiert oder geändert werden.

### Schritte

Diese Aktion enthält die folgenden Schritte, die nacheinander ausgeführt werden:

1. **com.ibm.bcg.server.pkg.UnPackagingFactory** - Ermittelt die korrekte Klasse für das Entpacken von RNIF-Dokumenten fest oder nimmt an, dass es sich um kein RNIF-Dokument handelt und das Entpacken entfällt.
2. **com.ibm.bcg.validation.ValidationWithoutContentFactory** - Führt die Validierung (jedoch nicht für den RNSC) durch.
3. **com.ibm.bcg.translation.protocol.StdRNandRNSCProtFactory** - Wird verwendet, um den RNSC aus dem RNIF-Dokument zu extrahieren oder die RNIF-Informationen für den RNSC zu erstellen.
4. **com.ibm.bcg.sponsor.SponsorBusProcessFactory** - Wird bei der Verarbeitung von RosettaNet-0A1-Dokumenten zum Aktualisieren der RosettaNet-Statusengine verwendet.
5. **com.ibm.bcg.outbound.OutboundDocFactory** - Immer erforderlich. Führt von WebSphere Partner Gateway geforderte Verarbeitungsaktivitäten für das Zieldokument aus. Dies ist der letzte Schritt, und die Konsole fügt diesen Schritt automatisch zu vorhandenen oder neu erstellten Aktionen hinzu. Dieser Schritt wird in der Liste der konfigurierten Handler nicht angezeigt.

## Bidirektionale Konvertierung von angepasster XML des internen Partners in RosettaNet mit Inhaltsduplikatprüfung und Validierung

Diese Aktion wird für RosettaNet-RNIF-Dokumente verwendet, die in ein angepasstes XML-Dokument (oder umgekehrt) transformiert werden müssen. Beim Empfang eines RNIF-Dokuments vom externen Partner werden die Nutzdaten (RNSC - RNIF Service Content) aus dem RNIF-Paket extrahiert, validiert und in ein XML-Dokument transformiert, das an die Back-End-Anwendung (interner Partner) gesendet wird. Ist der Absender die Back-End-Anwendung (interner Partner), wird die XML auf doppelte IDs überprüft; dann wird die XML validiert und in den RNSC transformiert, der ebenfalls validiert wird. Entspricht der Aktion "Bidirektionale Konvertierung von RosettaNet und XML mit Validierung", jedoch mit einer zusätzlichen Duplikatprüfung für das XML-Quellendokument.

### Konfiguration

- Für das XML-Format des Quellendokuments müssen die Duplikatprüfschlüssel konfiguriert werden.

- Das RosettaNet-PIP-Paket für das RosettaNet-Dokument muss geladen sein.
- Die Validierungszuordnung (XML-SCHEMA) muss im XML-Quellendokument oder im XML-Zieldokument konfiguriert werden.
- Eine XSLT-Transformationszuordnung muss für diese Aktion konfiguriert werden.

### Änderung

Diese Aktion kann nicht kopiert oder geändert werden, da sie sich speziell auf RNIF-Dokumente bezieht.

### Schritte

Diese Aktion enthält die folgenden Schritte, die nacheinander ausgeführt werden:

1. **com.ibm.bcg.duplicate.ContentDuplicateProcessFactory** - Führt für eine empfangene angepasste XML eine Prüfung auf doppelte IDs durch.
2. **com.ibm.bcg.server.pkg.UnPackagingFactory** - Ermittelt die korrekte Klasse für das Entpacken von RNIF-Dokumenten fest oder nimmt an, dass es sich um kein RNIF-Dokument handelt und das Entpacken entfällt.
3. **com.ibm.bcg.validation.ValidationFactory** - Validiert das RNIF- oder XML-Quellendokument.
4. **com.ibm.bcg.translation.protocol.RNXsltProtFactory** - Transformiert den RNSC in das bzw. aus dem XML-Format.
5. **com.ibm.bcg.validation.OutboundValidationFactory** - Validiert das sich daraus ergebende, transformierte XML-Dokument.
6. **com.ibm.bcg.sponsor.SponsorBusProcessFactory** - Wird bei der Verarbeitung von RosettaNet-0A1-Dokumenten zum Aktualisieren der RosettaNet-Statusengine verwendet.
7. **com.ibm.bcg.outbound.OutboundDocFactory** - Immer erforderlich. Führt von WebSphere Partner Gateway geforderte Verarbeitungsaktivitäten für das Zieldokument aus. Dies ist der letzte Schritt, und die Konsole fügt diesen Schritt automatisch zu vorhandenen oder neu erstellten Aktionen hinzu. Dieser Schritt wird in der Liste der konfigurierten Handler nicht angezeigt.

## Bidirektionale Konvertierung von angepasster XML mit Validierung

Diese Aktion wird für angepasste XML-Dokumente verwendet, die von einem externen oder von den internen Partners stammen. Das Quellendokument wird validiert und in das Zieldokument transformiert, das ebenfalls validiert wird.

### Konfiguration

- Die Validierungszuordnung (XML-SCHEMA) muss im Quellendokument konfiguriert werden.
- Eine XSLT-Transformationszuordnung muss für diese Aktion konfiguriert werden.
- Die Validierungszuordnung (XML-SCHEMA) muss im Zieldokument konfiguriert werden.

### Änderung

Diese Aktion kann kopiert und geändert werden. Die Transformations- oder Validierungsschritte können durch benutzerdefinierte Schritte ersetzt werden, oder es können zusätzlich benutzerdefinierte Schritte hinzugefügt werden.

### Schritte

Diese Aktion enthält die folgenden Schritte, die nacheinander ausgeführt werden:

1. **com.ibm.bcg.validation.ValidationFactory** - Dieser Schritt validiert das empfangene angepasste XML-Dokument.
2. **com.ibm.bcg.translation.protocol.translators.xslt.XSLTranslationFactory** - Führt die Transformation durch.
3. **com.ibm.bcg.validation.OutboundValidationFactory** - Validiert das sich daraus ergebende, transformierte XML-Dokument.
4. **com.ibm.bcg.outbound.OutboundDocFactory** - Immer erforderlich. Führt von WebSphere Partner Gateway geforderte Verarbeitungsaktivitäten für das Zieldokument aus. Dies ist der letzte Schritt, und die Konsole fügt diesen Schritt automatisch zu vorhandenen oder neu erstellten Aktionen hinzu. Dieser Schritt wird in der Liste der konfigurierten Handler nicht angezeigt.

## Bidirektionale Konvertierung von angepasster XML mit Duplikatprüfung und Validierung

Diese Aktion wird für angepasste XML-Dokumente verwendet. Sie kann für Dokumente verwendet werden, die von externen Partnern oder vom internen Partner stammen. Die folgenden Schritte werden ausgeführt: Prüfung auf doppelte IDs für das Quellendokument, Validierung für das Quellendokument, Transformation des Quellendokuments in das Zieldokument und Validierung des Zieldokuments. Diese Aktion entspricht der Aktion "Bidirektionale Konvertierung von angepasster XML mit Validierung" mit Ausnahme der zusätzlichen Duplikatprüfung.

### Konfiguration

- Für das XML-Format des Quellendokuments müssen die Duplikatprüfschlüssel konfiguriert werden.
- Die Validierungszuordnung (XML-SCHEMA) muss im Quellendokument konfiguriert werden.
- Eine XSLT-Transformationszuordnung muss für diese Aktion konfiguriert werden.
- Die Validierungszuordnung (XML-SCHEMA) muss im Zieldokument konfiguriert werden.

### Änderung

Diese Aktion kann kopiert und geändert werden. Die folgenden Schritte können durch benutzerdefinierte Schritte ersetzt werden: ValidationFactory, XSLTTranslationFactory und OutboundValidationFactory; es können auch zusätzliche benutzerdefinierte Schritte hinzugefügt werden.

### Schritte

Diese Aktion enthält die folgenden Schritte, die nacheinander ausgeführt werden:

1. **com.ibm.bcg.duplicate.ContentDuplicateProcessFactory** - Sucht nach einem doppelten Dokument basierend auf der Dokument-ID.
2. **com.ibm.bcg.validation.ValidationFactory** - Dieser Schritt validiert das empfangene angepasste XML-Dokument.

3. **com.ibm.bcg.translation.protocol.translators.xslt.XSLTranslationFactory** - Dieser Schritt transformiert das empfangene angepasste XML-Dokument in das XML-Zielformat.
4. **com.ibm.bcg.validation.OutboundValidationFactory** - Dieser Schritt validiert das transformierte XML-Zieldokument aus dem vorherigen Transformationsschritt.
5. **com.ibm.bcg.outbound.OutboundDocFactory** - Immer erforderlich. Führt von WebSphere Partner Gateway geforderte Verarbeitungsaktivitäten für das Zieldokument aus. Dies ist der letzte Schritt, und die Konsole fügt diesen Schritt automatisch zu vorhandenen oder neu erstellten Aktionen hinzu. Dieser Schritt wird in der Liste der konfigurierten Handler nicht angezeigt.

## Pass-Through von angepasster XML mit Duplikatprüfung und Validierung

### Zweck

Diese Aktion wird für angepasste XML-Dokumente verwendet. Sie kann für Dokumente verwendet werden, die von einem externen Partner oder vom internen Partner stammen. Die Prüfung auf doppelte IDs wird ausgeführt, und das Quellendokument wird validiert. Diese Aktion entspricht der Aktion "Pass-Through von angepasster XML mit Duplikatprüfung" mit der Ausnahme, dass eine zusätzliche Validierungsprüfung für das Quellendokument erfolgt.

### Konfiguration

- Für das XML-Format des Quellendokuments müssen die Duplikatprüfschlüssel konfiguriert werden.
- Die Validierungszuordnung (XML-SCHEMA) muss im XML-Quellendokument konfiguriert werden.

### Änderung

Diese Aktion kann kopiert und geändert werden. Der Schritt ValidationFactory kann durch einen benutzerdefinierten Schritt ersetzt werden, oder es können zusätzliche benutzerdefinierte Schritte hinzugefügt werden.

### Schritte

Diese Aktion enthält die folgenden Schritte, die nacheinander ausgeführt werden:

1. **com.ibm.bcg.duplicate.ContentDuplicateProcessFactory** - Sucht nach einem doppelten Dokument basierend auf der Dokument-ID. Das XML-Format für dieses Quellendokument muss die Konfiguration für doppelte IDs haben.
2. **com.ibm.bcg.validation.ValidationFactor** - Dieser Schritt validiert das angepasste XML-Quellendokument.
3. **com.ibm.bcg.passthrough.No_op** - Gibt an, dass der Inhaltstyp des Zieldokuments nicht vom Dokumentinhalt abgeleitet werden soll.
4. **com.ibm.bcg.outbound.OutboundDocFactory** - Immer erforderlich. Führt von WebSphere Partner Gateway geforderte Verarbeitungsaktivitäten für das Zieldokument aus. Dies ist der letzte Schritt, und die Konsole fügt diesen Schritt automatisch zu vorhandenen oder neu erstellten Aktionen hinzu. Dieser Schritt wird in der Liste der konfigurierten Handler nicht angezeigt.

## Pass-Through von angepasster XML mit Duplikatprüfung

Diese Aktion wird für angepasste XML-Dokumente verwendet. Sie kann für Dokumente verwendet werden, die von einem externen Partner oder vom internen Partner stammen. Prüfung auf doppelte IDs erfolgt für das Quellendokument.

### Konfiguration

Für das XML-Format des Quellendokuments müssen die Duplikatprüfschlüssel konfiguriert werden.

### Änderung

Diese Aktion kann nicht in eine neue Aktion kopiert werden, da eine mögliche Änderung einen Validierungsschritt hinzufügt, der in der Aktion "Pass-Through von angepasster XML mit Duplikatprüfung und Validierung" definiert ist.

### Schritte

Diese Aktion enthält die folgenden Schritte, die nacheinander ausgeführt werden:

1. **com.ibm.bcg.duplicate.ContentDuplicateProcessFactory** - Sucht nach einem doppelten Dokument basierend auf der Dokument-ID. Das XML-Format für dieses Quellendokument muss die Konfiguration für doppelte IDs haben.
2. **com.ibm.bcg.passthrough.No_op** - Gibt an, dass der Inhaltstyp des Zieldokuments nicht vom Dokumentinhalt abgeleitet werden soll.
3. **com.ibm.bcg.outbound.OutboundDocFactory** - Immer erforderlich. Führt von WebSphere Partner Gateway geforderte Verarbeitungsaktivitäten für das Zieldokument aus. Dies ist der letzte Schritt, und die Konsole fügt diesen Schritt automatisch zu vorhandenen oder neu erstellten Aktionen hinzu. Dieser Schritt wird in der Liste der konfigurierten Handler nicht angezeigt.

## Pass-Through von angepasster XML mit Validierung

Diese Aktion wird für angepasste XML-Dokumente verwendet, die von einem externen Partner oder vom internen Partner stammen. Das Quellendokument wird validiert.

### Konfiguration

Die Validierungszuordnung (XML-SCHEMA) muss im XML-Quellendokument konfiguriert werden.

### Änderung

Diese Aktion kann kopiert und geändert werden. ValidationFactory kann durch einen benutzerdefinierten Schritt ersetzt werden, oder es können zusätzliche benutzerdefinierte Schritte hinzugefügt werden.

### Schritte

Diese Aktion enthält die folgenden Schritte, die nacheinander ausgeführt werden:

1. **com.ibm.bcg.validation.ValidationFactory** - Dieser Schritt validiert das angepasste XML-Quellendokument.
2. **com.ibm.bcg.passthrough.No_op** - Gibt an, dass der Inhaltstyp des Zieldokuments nicht vom Dokumentinhalt abgeleitet werden soll.

3. **com.ibm.bcg.outbound.OutboundDocFactory** - Immer erforderlich. Führt von WebSphere Partner Gateway geforderte Verarbeitungsaktivitäten für das Zieldokument aus. Dies ist der letzte Schritt, und die Konsole fügt diesen Schritt automatisch zu vorhandenen oder neu erstellten Aktionen hinzu. Dieser Schritt wird in der Liste der konfigurierten Handler nicht angezeigt.

## EDI - Umschlag entfernen

Diese Aktion wird für EDI-Austauschvorgänge verwendet, die von einem externen Partner stammen. Der Umschlag des EDI-Austauschs wird entfernt, d. h. die EDI-Transaktionen werden extrahiert. Diese EDI-Transaktionen werden erneut in WebSphere Partner Gateway eingeführt und einzeln verarbeitet. Das EDI-Austauschdokument wird in WebSphere Partner Gateway nicht weiter verarbeitet.

### Konfiguration

Optionale Konfiguration in den Dokumentdefinitionen.

### Änderung

Diese Aktion kann nicht kopiert oder geändert werden.

### Schritte

Diese Aktion enthält die folgenden Schritte, die nacheinander ausgeführt werden:

1. **com.ibm.bcg.edi.business.process.EDIDenvFactory** - Entfernt den Umschlag des EDI-Austauschs.
2. **com.ibm.bcg.outbound.OutboundDocFactory** - Immer erforderlich. Führt von WebSphere Partner Gateway geforderte Verarbeitungsaktivitäten für das Zieldokument aus. Dies ist der letzte Schritt, und die Konsole fügt diesen Schritt automatisch zu vorhandenen oder neu erstellten Aktionen hinzu. Dieser Schritt wird in der Liste der konfigurierten Handler nicht angezeigt.

## EDI validieren und EDI konvertieren

Diese Aktion wird für EDI-Transaktionen verwendet, für die der Umschlag eines EDI-Austauschs mithilfe der Aktion "EDI - Umschlag entfernen" entfernt wurde. Diese stammen von einem externen Partner. Die EDI-Transaktionsdokumente werden validiert und anschließend transformiert.

### Konfiguration

- Optionale Konfiguration in den Dokumentdefinitionen.
- Optionale Validierungszuordnungen für die EDI-Quellentransaktion vom DIS-Client oder von WTX Design Studio.
- Transformationszuordnungen vom DIS-Client oder von WTX Design Studio.
- Die Partnerverbindung von <beliebiges Paket> / EDI - Any / Any zu None / EDI - Any / Any muss mit einer als "EDI - Umschlag entfernen" definierten Aktion konfiguriert werden.

### Änderung

Diese Aktion kann kopiert und geändert werden, um zusätzliche Benutzerexitschritte hinzuzufügen.

### Schritte

Diese Aktion enthält die folgenden Schritte, die nacheinander ausgeführt werden:

1. **com.ibm.bcg.edi.business.process.EDISourceValidationFactory** - Validiert die EDI-Transaktion. Durch diesen Schritt wird außerdem die funktionale EDI-Bestätigung ausgegeben, nachdem alle EDI-Transaktionen des EDI-Austauschs verarbeitet wurden.
2. **com.ibm.bcg.edi.business.process.EDITranslatorFactory** - Transformiert die EDI-Transaktion in das Zieldokument.
3. **com.ibm.bcg.outbound.OutboundDocFactory** - Immer erforderlich. Führt von WebSphere Partner Gateway geforderte Verarbeitungsaktivitäten für das Zieldokument aus. Dies ist der letzte Schritt, und die Konsole fügt diesen Schritt automatisch zu vorhandenen oder neu erstellten Aktionen hinzu. Dieser Schritt wird in der Liste der konfigurierten Handler nicht angezeigt.

## XML konvertieren und EDI validieren

### Zweck

Diese Aktion wird für angepasste XML-Dokumente verwendet, die vom internen Partner stammen. Das XML-Quellendokument wird in eine EDI-Transaktion transformiert und validiert. Dann wird es entweder an das Back-End oder einen externen Partner gesendet. XML-Formate werden zum Angeben der Routing-Informationen verwendet.

### Konfiguration

- Optionale Konfiguration in den Dokumentdefinitionen.
- Optionale Validierungszuordnungen für die EDI-Zieltransaktion vom DIS-Client.
- Transformationszuordnungen vom DIS-Client oder von WDI Design Studio.

### Änderung

Diese Aktion kann kopiert und geändert werden, um EDITargetValidationFactory zu entfernen oder zusätzliche Benutzerexitschritte hinzuzufügen.

### Schritte

Diese Aktion enthält die folgenden Schritte, die nacheinander ausgeführt werden:

1. **com.ibm.bcg.edi.business.process.XMLTranslatorFactory** - Transformiert das XML-Quellendokument in die EDI-Zieltransaktion.
2. **com.ibm.bcg.edi.business.process.EDITargetValidationFactory** - Validiert die EDI-Zieltransaktion.
3. **com.ibm.bcg.outbound.OutboundDocFactory** - Immer erforderlich. Führt von WebSphere Partner Gateway geforderte Verarbeitungsaktivitäten für das Zieldokument aus. Dies ist der letzte Schritt, und die Konsole fügt diesen Schritt automatisch zu vorhandenen oder neu erstellten Aktionen hinzu. Dieser Schritt wird in der Liste der konfigurierten Handler nicht angezeigt.

## ROD (FlatFile) konvertieren und EDI validieren

Diese Aktion wird für ROD (FlatFile)-Dokumente (ROD - Record Oriented Documents) verwendet, die vom internen Partner stammen. Das ROD-Quellendokument wird in eine EDI-Transaktion transformiert und validiert.

### Konfiguration

- Optionale Konfiguration in den Dokumentdefinitionen.
- Optionale Validierungszuordnungen für die EDI-Zieltransaktion vom DIS-Client.
- Der ROD-Standard muss im DIS-Client definiert und anhand einer Pseudo-Transformationszuordnung kompiliert werden.
- Ein ROD-Verteiler/generischer Dokumentprozessor sollte als Handler für die einzelnen Prozesse in den Empfänger eingefügt werden. Auf diese Weise können das Wörterverzeichnisdokument und -format erkannt werden.

### Änderung

Diese Aktion kann kopiert und geändert werden, um EDITargetValidationFactory zu entfernen oder zusätzliche Benutzerexitschritte hinzuzufügen.

### Schritte

Diese Aktion enthält die folgenden Schritte, die nacheinander ausgeführt werden:

1. **com.ibm.bcg.edi.business.process.RODTranslatorFactory** - Transformiert das ROD-Quellendokument in die EDI-Zieltransaktion.
2. **com.ibm.bcg.edi.business.process.EDITargetValidationFactory** - Validiert die EDI-Zieltransaktion.
3. **com.ibm.bcg.outbound.OutboundDocFactory** - Immer erforderlich. Führt von WebSphere Partner Gateway geforderte Verarbeitungsaktivitäten für das Zieldokument aus. Dies ist der letzte Schritt, und die Konsole fügt diesen Schritt automatisch zu vorhandenen oder neu erstellten Aktionen hinzu. Dieser Schritt wird in der Liste der konfigurierten Handler nicht angezeigt.

## ebMS - Teilen und parsen

Diese Aktion wird für ebMS-Dokumente verwendet, die von einem externen Partner stammen. Die Anhänge mit den Nutzdaten werden extrahiert und erneut in WebSphere Partner Gateway eingeführt, wo sie einzeln verarbeitet werden. Das ebMS-Dokument wird in WebSphere Partner Gateway nicht weiter verarbeitet.

### Konfiguration

Es sind keine zusätzlichen Konfigurationsmaßnahmen erforderlich.

### Änderung

Diese Aktion kann nicht kopiert oder geändert werden.

### Schritte

Diese Aktion enthält die folgenden Schritte, die nacheinander ausgeführt werden:

1. **com.ibm.bcg.server.EBMSSplitAndParse** - Die Anhänge mit den Nutzdaten werden in einzelne Dokumente extrahiert.
2. **com.ibm.bcg.outbound.OutboundDocFactory** - Immer erforderlich. Führt von WebSphere Partner Gateway geforderte Verarbeitungsaktivitäten für das Zieldokument aus. Dies ist der letzte Schritt, und die Konsole fügt diesen Schritt automatisch zu vorhandenen oder neu erstellten Aktionen hinzu. Dieser Schritt wird in der Liste der konfigurierten Handler nicht angezeigt.

## EDI-Austausch validieren

Die Validierung des EDI-Austauschs erfolgt während der asynchronen Integration mit WTX. Durch Entfernen des Umschlags vom Austausch werden die einzelnen Transaktionen aus dem Austausch extrahiert. Bei der Umschlagsentfernung werden alle Transaktionen aus dem Austausch extrahiert. Jede Transaktion erzeugt ein Dokument, das zu Validierungszwecken direkt weitergeleitet wird.

**Anmerkung:** Das Attribut "Umschlag bei Fehlern löschen" kann im Kontext "Validierung des EDI-Austauschs" nicht verwendet werden. Wenn Sie den Wert für die Verwendung dieses Attributs definieren, wird der Wert ignoriert.

### Konfiguration

- Die Partnerverbindung von <beliebiges Paket> / EDI – xxxx / XXX zu None / EDI – xxxx / XXX muss mit einer Aktion konfiguriert werden, die als "Validierung des EDI-Austauschs" definiert ist.
- FA-Benutzer können optional FA-Zuordnungen konfigurieren.
- Für die funktionale Bestätigung muss ein Kanal definiert werden.

## WTX-Transformation

EDI-, XML-, ROD- und Flachdateien werden mit WTX transformiert.

Die EDI-Transformation unter Verwendung von WTX kann im asynchronen oder synchronen Modus erfolgen. Der synchrone Modus wird zumeist dann verwendet, wenn eine Transaktion, deren Umschlag entfernt und die validiert wurde, zur Verarbeitung an WTX gesendet wird. In diesem Fall muss die Transaktion allerdings erneut mit einem Umschlag versehen werden, da dies für die Verarbeitung mit WTX erforderlich ist. Nach einer erfolgreichen Validierung der EDI-Transaktion wird diese an die Aktion "EDI-Transaktion mit WTX transformieren" weitergeleitet. Im asynchronen Modus werden EDI-Transaktionen im Back-End transformiert, wo WTX in WESB/WMB oder im WTX-Startprogramm implementiert ist.

Bei der Verwendung von EDI als Eingabe für die Transformation sollten die folgenden Aspekte bedacht werden:

**Wichtig:**

1. Verwenden Sie immer einen aus nur einem Zeichen bestehenden Begrenzer.
2. Wenn Sie eine Kombination der Zeichenbegrenzer "/r/n" verwenden und der Zeichenbegrenzer "/r" an der Position des Segmentbegrenzers im Austauschheader gefunden wird, wird der Zeichenbegrenzer "/n" ignoriert.
3. Ändern Sie die Typenbaumstruktur entsprechend.

### Konfiguration für synchronen Modus

- Die Partnerverbindung von <beliebiges Paket> / EDI – xxxx / XXX zu None / EDI – xxxx / XXX muss mit einer als "EDI - Umschlag entfernen" definierten Aktion konfiguriert werden.
- Die Partnerverbindung von <N/A> / XXXXXXX/ YYYYY zu None / ZZZZZZ / BBBBBBB muss mit einer als "EDI validieren" und "EDI-Transaktion mit WTX transformieren" definierten Aktion konfiguriert werden.
- Ferner sollte diesem Kanal eine WTX-Transformationszuordnung zugeordnet werden.

### Konfiguration für asynchronen Modus

- Die Partnerverbindung von <beliebiges Paket> / EDI – xxxx / XXX zu None / EDI – xxxx / XXX muss mit einer als "EDI - Umschlag entfernen" definierten Aktion konfiguriert werden.
- Die Partnerverbindung von <N/A> / <EDI-Version>/ Transaktion zu <N/A> / <EDI-Version> / Transaktion muss mit einer als "EDI validieren" definierten Aktion konfiguriert werden.
- Die Partnerverbindung von <N/A> / <EDI-Version> / Transaktion zu <BI> / <EDI-Austausch> / <ISA> / <UNB> / <UCS> muss mit einer als "EDI validieren" und "EDI-ReEnveloper" definierten Aktion konfiguriert werden.

### Konfiguration für ROD und XML

- ROD-Transformation - Die Partnerverbindung von <beliebiges Paket> / <beliebiges Protokoll (Flachdatei) > / <beliebige Flachdatei> zu <Any> / <ANY> / <Any>-Format sollte mit einer als "WTX-Transformation" definierten Aktion konfiguriert werden.
- XML-Transformation - Die Partnerverbindung von <beliebiges Paket> / <beliebiges Protokoll> / <beliebiges XML> zu <Any> / <ANY> / <Any>-Format sollte mit einer als "WTX-Transformation" definierten Aktion konfiguriert werden.

## WTX - Mit Umschlag versehen

### Zweck

Bei der Verwendung von WTX im asynchronen Modus werden EDI-Transaktionen nach der WTX-Transformation transformiert und erzeugt. Dann werden die Transaktionen an WebSphere Partner Gateway gesendet, um sie mit einem Umschlag zu versehen.

### Konfiguration

- Verbindung von <Back-End> / <EDI-Wörterverzeichnis> / <EDI-Dokument> {EDI Trx} zu <N/A> / <EDI X12/EDIFACT> / <EDI ISA/UNB> mit Pass-Through-Aktion: Profil für Programm zur Umschlagsgenerierung in Back-End-Zielsystem konfigurieren (Kanal-A).
- Verbindung von <NA> / <EDI-Austausch> / <EDI ISA/UNB> zu <BELIEBIGES PAKET> / <EDI X12/EDIFACT> / <EDI ISA/UNB> mit Pass-Through-Aktion: (Kanal-B).

## EDI-ReEnveloper

Mit ReEnveloper können einzelne Transaktionen mit einem Umschlag versehen werden. ReEnveloper greift auf die Header des Programms zur Umschlaggenerierung im Quellenumschlag zu und schließt die einzelnen Transaktionen, deren Umschlag entfernt wurde, in diese Header ein.

### Konfiguration

- Eine Verbindung zwischen Quelle (Transaktion) und Ziel (EDI-Austausch) mit einem konfigurierten Umschlagsprofil.
- Diese Aktion wird als "EDI-ReEnveloper" festgelegt.

## Validierung des SOAP-Umschlags

Die gesamte Web-Service-Anforderung wird anhand des SOAP 1.1-Schemas gemäß Industriestandard geprüft. Die Aktion für den SOAP-Umschlag enthält die folgenden Schritte, die nacheinander ausgeführt werden:

1. **com.ibm.bcg.validation.WebserviceFactory** – Führt die Validierung der Web-Service-Anforderung aus und gibt den Handler "WebserviceValidation" zurück.
2. **com.ibm.bcg.outbound.OutboundDocFactory** - Dieser Schritt ist immer erforderlich. Führt die Verarbeitung, die für WebSphere Partner Gateway erforderlich ist, auf dem Zieldokument aus. Dies ist der letzte Schritt, und die Konsole fügt diesen Schritt automatisch zu vorhandenen oder neu erstellten Aktionen hinzu. Dieser Schritt wird in der Liste der konfigurierten Handler nicht angezeigt.

## Validierung des SOAP-Hauptteils

Mit dieser Funktion werden der SOAP-Hauptteil oder die Nutzdaten, die innerhalb des SOAP-Umschlags verfügbar sind, validiert. Die Validierung der Nutzdaten wird nur für XML-Nutzdaten in einem SOAP-Umschlag unterstützt. Für die schemabasierte Validierung wird ein dem Branchenstandard entsprechender Schemapositionszeiger unter der Nutzdaten-XML verwendet. Darüber hinaus können Sie Ihr Schema optional der entsprechenden Web-Service-Verbindung zuordnen, um die Nutzdaten zu validieren. Das Schema, das Sie der Web-Service-Verbindung explizit zugeordnet haben, hat Vorrang vor dem Schema, das sich unter der Nutzdaten-XML befindet. Ist in einer Nutzdaten-XML kein Schemapositionszeiger vorhanden, müssen Sie ein Schema unter der Web-Service-Verbindung zuordnen. Die Attribute des Routingobjekts lauten für die Web-Service-Anforderung und -Antwort wie folgt:

- **ResponseValidation** – Legen Sie den Wert dieses Attributs auf der Zielseite auf "No" fest, wenn Antwortdokumente nicht validiert werden sollen. Der Standardwert für dieses Attribut ist "Yes".
- **ContentValidation** – Dieses Attribut ermöglicht es, die Inhaltsvalidierung über die Nutzdaten-XML zu aktivieren oder zu inaktivieren. Standardmäßig ist die Inhaltsvalidierung aktiviert. Wird das Attribut auf "No" festgelegt, wird eine Grammatikvalidierung durchgeführt.

Die Aktion für den SOAP-Hauptteil enthält die folgenden Schritte, die nacheinander ausgeführt werden:

1. **com.ibm.bcg.validation.ValidationFactory** - Führt die Validierung der Web-Service-Anforderung aus.
2. **com.ibm.bcg.outbound.OutboundDocFactory** - Dieser Schritt ist immer erforderlich. Führt die Verarbeitung, die für WebSphere Partner Gateway erforderlich ist, auf dem Zieldokument aus. Dies ist der letzte Schritt, und die Konsole fügt diesen Schritt automatisch zu vorhandenen oder neu erstellten Aktionen hinzu. Dieser Schritt wird in der Liste der konfigurierten Handler nicht angezeigt.

Informationen dazu, wie WebSphere Partner Gateway so aktualisiert wird, dass die Funktion für die Validierung von Nutzdaten unter einem SOAP-Umschlag verwendet wird, finden Sie im Handbuch *WebSphere Partner Gateway Verwaltung*.

## Aus SOAP-Umschlag entfernen

Für die weitere Verarbeitung muss der SOAP-Umschlag entfernt und der SOAP-Hauptteil eingeführt werden. Die Attribute des Routingobjekts zum Entfernen des SOAP-Umschlags lauten wie folgt:

- **SOAP-Umschlag entfernen** - Unterstützt nur die asynchrone Kommunikation. Da es sich um die Unterstützung des Basisprofils für unidirektionale Web-Services handelt, werden keine SOAP-Fehler oder SOAP-Antworten zurückgegeben. Bei synchroner Kommunikation schlägt das Entfernen des SOAP-Umschlags fehl, und ein Fehlerereignis wird protokolliert.
- **Dokument nach Entfernen des Umschlags weiterleiten** - Dies ist ein verknüpftes Attribut des Routingobjekts für die Aktion **SOAP-Umschlag entfernen**. Ist das Attribut dieses Routingobjekts auf "Yes" festgelegt, muss die Aktion **SOAP-Umschlag entfernen** den extrahierten SOAP-Hauptteil aus dem SOAP-Umschlag als neues Dokument in WebSphere Partner Gateway einführen. Darüber hinaus muss der Anhang ebenfalls als neues Dokument eingeführt werden. Alle neu eingeführten Dokumente verwenden das Paket N/A (nicht verfügbar). Um eine weitergehende Weiterleitung auszuführen, müssen Sie einen auf dem Paket N/A basierenden Kanal für die extrahierten Nutzdaten und angehängten Dokumente konfigurieren.
- **SOAP-Nutzdaten verarbeiten** - Dieses Attribut ist mit dem Attribut **Dokument nach Entfernen des Umschlags weiterleiten** verknüpft. Es wird dazu verwendet, die Nutzdaten nach der Extraktion zu komprimieren. Wenn der Wert für dieses Attribut und der Wert für **Dokument nach Entfernen des Umschlags weiterleiten** auf "Ja" gesetzt ist, werden die Nutzdaten nicht extrahiert und nicht vom SOAP-Umschlag weitergeleitet. Stattdessen werden nur die Anhänge weitergeleitet. Wenn dieses Attribut auf "Nein" und **Dokument nach Entfernen des Umschlags weiterleiten** auf "Ja" gesetzt ist, werden die Nutzdaten und die Anhänge separat weitergeleitet. Der Standardwert für dieses Attribut ist "Nein".

Die Aktion **SOAP-Umschlag entfernen** umfasst die folgenden Schritte, die nacheinander ausgeführt werden:

1. **com.ibm.bcg.validation.SOAPDeEnveloperFactory** – Führt die Validierung der Web-Service-Anforderung aus und gibt den Handler "SOAPDeEnveloper" zurück.
2. **com.ibm.bcg.outbound.OutboundDocFactory** - Dieser Schritt ist immer erforderlich. Führt die Verarbeitung, die für WebSphere Partner Gateway erforderlich ist, auf dem Zieldokument aus. Dies ist der letzte Schritt, und die Konsole fügt diesen Schritt automatisch zu vorhandenen oder neu erstellten Aktionen hinzu. Dieser Schritt wird in der Liste der konfigurierten Handler nicht angezeigt.

In Fällen, in denen der Umschlag von SOAP with attachment entfernt wird und nur die Anhänge und nicht die Nutzdaten unter dem SOAP-Hauptteil weitergeleitet werden sollen, lautet die Konfiguration wie folgt:

- bcg.soap.ConsumePayload = Y (dieser Wert ist standardmäßig auf "N" gesetzt)
- bcg.soap.Re-RouteDe-EnvelopedDocument = Y (dieser Wert ist standardmäßig auf "Y" gesetzt)

Wenn der Umschlag von SOAP with attachment entfernt wird und Nutzdaten und Anhänge separat weitergeleitet werden sollen, lautet die Konfiguration wie folgt:

- bcg.soap.ConsumePayload = N (dieser Wert ist standardmäßig auf "N" gesetzt)
- bcg.soap.Re-RouteDe-EnvelopedDocument = Y (dieser Wert ist standardmäßig auf "Y" gesetzt)

Informationen dazu, wie WebSphere Partner Gateway so aktualisiert werden kann, dass die Funktion zur Validierung von Nutzdaten unter einem SOAP-Umschlag verwendet wird, finden Sie im Handbuch *WebSphere Partner Gateway Verwaltung*.

## Benutzerdefinierte Aktion ändern

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

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

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

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

## Aktionen erstellen

Sie können eine Aktion auf eine der folgenden Weisen erstellen:

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

### Neue Aktion erstellen

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

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

Denken Sie daran, dass Handler von der Aktion in der Reihenfolge aufgerufen werden, in der sie in der **Konfigurationsliste** angezeigt werden. Stellen Sie sicher, dass Sie die Handler in der richtigen Reihenfolge anordnen. Sie können mit den Schaltflächen **Nach oben** oder **Nach unten** die Reihenfolge der Handler ändern oder mit der Schaltfläche **Wiederholen** bewirken, dass ein Handler mehr als einmal verarbeitet wird.

7. Konfigurieren Sie einen Handler, indem Sie ihn in der **Konfigurationsliste** auswählen und auf **Konfigurieren** klicken. Die Liste der Attribute, die konfiguriert werden können, wird angezeigt.
8. Klicken Sie auf **Speichern**.

## Aktion kopieren

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

1. Klicken Sie auf **Hubadmin > Hubkonfiguration > Aktionen**.
2. Klicken Sie in der Liste **Aktionen** auf das Symbol **Kopieren** neben der Aktion, die Sie kopieren wollen.
3. Geben Sie einen Namen für die Aktion ein. Dieses Feld ist erforderlich.
4. Geben Sie eine optionale Beschreibung der Aktion ein.
5. Geben Sie an, ob die Aktion zur Verwendung aktiviert ist.
6. Beachten Sie, dass schon mindestens ein Schritt in der **Konfigurationsliste** vorhanden ist. Dies sind die Schritte, die der kopierten Aktion zugeordnet sind. Wenn Sie beispielsweise die vom Produkt bereitgestellte Aktion **Abbruch des RosettaNet-Prozesses durch den internen Partner** geklont haben, enthält Ihre Verfügbarkeits- und Konfigurationsliste die folgenden Handler:

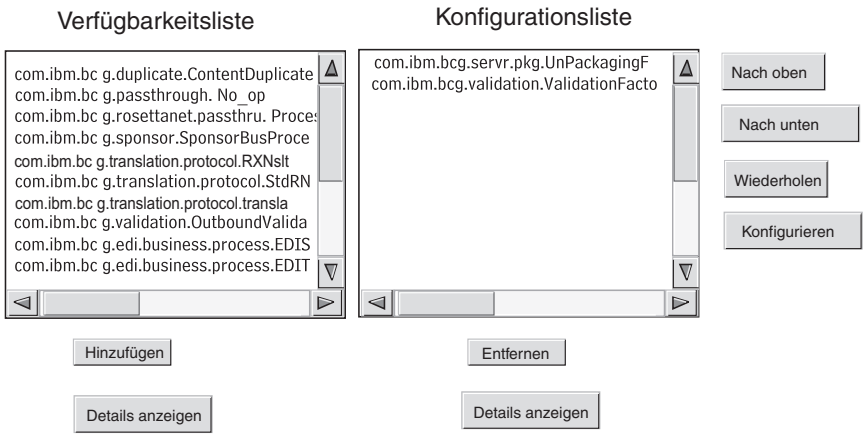



*Abbildung 19. Aktion klonen*

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

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

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

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

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

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

7. Klicken Sie auf **Speichern**.

# Kapitel 9. Dokumenttypen konfigurieren

In diesem Kapitel wird beschrieben, wie Sie die Nicht-EDI-Dokumente konfigurieren, die Sie mit Ihren externen Partnern und mit Ihren Back-End-Anwendungen austauschen werden. Das Konfigurieren von Dokumenttypen und Interaktionen für EDI-Dokumente (mit Ausnahme der EDI-Dokumente, die weitergeleitet werden), wird in Kapitel 10, „EDI-Dokumentenflüsse konfigurieren", auf Seite 173 beschrieben. Kapitel 10, „EDI-Dokumentenflüsse konfigurieren", auf Seite 173 beschreibt außerdem, wie Sie Dokumenttypen und Interaktionen für XML-Dokumente und satzorientierte Datendokumente (ROD-Dokumente) konfigurieren.

Das Kapitel behandelt die folgenden Themen:



**Anmerkung:** Verwenden Sie stets die Browserinstanz, mit der Sie sich an Community Console angemeldet haben, wenn Sie Konfigurationsänderungen an WebSphere Partner Gateway vornehmen. Die gleichzeitige Verwendung mehrerer Browserinstanzen kann dazu führen, dass die Konfigurationsänderungen aufgehoben werden.

## Übersicht über die Dokumenttypen

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

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

Die folgenden Abschnitte beschreiben kurz den Gesamtablauf für das Konfigurieren eines Dokumenttyps zwischen dem internen Partner und einem Partner.

### Schritt 1: Sicherstellen, dass die Dokumentdefinition verfügbar ist

Überprüfen Sie, ob eine der auf dem System vordefinierten Dokumentdefinitionen vorhanden ist. Wenn der Fluss nicht bereits vorhanden ist, erstellen Sie ihn, indem Sie die notwendigen Dateien hochladen oder indem Sie manuell eine angepasste Definition erstellen.

Im Rahmen der Erstellung der Dokumentdefinition können Sie bestimmte Attribute ändern. Attribute werden verwendet, um verschiedene Dokumentverarbeitungs- und Routing-Funktionen auszuführen, wie z. B. Validierung, Verschlüsselungsüberprüfung und Wiederholungszähler. Die Attribute, die Sie auf der Dokumentdefinitionsebene festlegen, liefern eine globale Einstellung für das zugeordnete Paket und Protokoll sowie den zugeordneten Dokumenttyp. Die Attribute, die zur Verfügung stehen, variieren je nach Dokumentdefinition. Die Attribute für EDI-Dokumentdefinitionen unterscheiden sich beispielsweise von den Attributen für RosettaNet-Dokumentdefinitionen.

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

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

Sie müssen den Dokumenttyp auf der Seite **Dokumentdefinitionen verwalten** auflisten, bevor Sie Interaktionen erstellen können. Weitere Informationen zum Verwalten von Dokumentdefinitionen finden Sie im Kapitel "Hubverwaltungstasks" des Handbuchs *IBM WebSphere Partner Gateway Verwaltung*.

## Schritt 2: Interaktionen erstellen

Erstellen Sie Interaktionen für die Dokumenttypen, die definiert worden sind. Die Interaktion teilt WebSphere Partner Gateway mit, welche Aktionen an einem Dokument ausgeführt werden sollen. Für einige Austauschvorgänge benötigen Sie nur zwei Dokumentenflüsse: Der eine beschreibt das Dokument, das auf dem Hub vom Partner oder vom internen Partner empfangen wird, und der andere beschreibt das Dokument, das vom Hub zum externen oder internen Partner gesendet wird. Wenn der Hub jedoch einen EDI-Austauschvorgang sendet oder empfängt, der in einzelne Transaktionen aufgeteilt wird bzw. in dem Bestätigungen erforderlich sind, dann erstellen Sie tatsächlich mehrere Interaktionen, um den Austausch auszuführen. Weitere Informationen zum Verwalten von Interaktionen finden Sie im Kapitel "Hubverwaltungstasks" des Handbuchs *IBM WebSphere Partner Gateway Verwaltung*.

## Schritt 3: Partnerprofile, Ziele und B2B-Funktionalität erstellen

Erstellen Sie Partnerprofile für den internen Partner und für externe Partner. Definieren Sie Ziele, die bestimmen, wohin Dokumente gesendet werden, und B2B-Funktionalität, die festlegt, welche Dokumente der interne Partner und die externen Partner senden und empfangen können. Die Seite **B2B-Funktionalität** listet alle Dokumenttypen auf, die definiert worden sind.

Sie können Attribute auf der B2B-Funktionalitätsebene festlegen. Jedes Attribut, das Sie auf dieser Ebene festlegen, überschreibt die auf der Dokumentdefinitionsebene festgelegten Attribute. Wenn Sie z. B. die Bestätigungszeit auf der Dokumentdefinitionsebene für das Paket **AS** auf 30 und auf der B2B-Funktionalitätsebene dann

aber auf 60 setzen, wird der Wert 60 verwendet. Wenn Sie ein Attribut auf der B2B-Ebene festlegen, können Sie das Attribut an einen bestimmten Partner anpassen.

## Schritt 4: Verbindungen aktivieren

Aktivieren Sie Verbindungen zwischen den internen Partnern und den externen Partnern. Welche Verbindungen verfügbar sind, hängt von den erstellten Interaktionen ab. Die Interaktionen basieren auf der B2B-Funktionalität. Die Interaktionen hängen von den Dokumentdefinitionen ab, die zur Verfügung stehen.

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

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

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

## Ein Beispieldokumentenfluss

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

1. Prüfen Sie auf der Seite **Dokumentdefinitionen verwalten**, ob die Dokumentdefinition aktiviert ist, die den Dokumenttyp beschreibt, welcher vom Partner in den Hub fließt.
   a. Klicken Sie auf **Hubadmin > Hubkonfiguration > Dokumentdefinition**.
   b. Klicken Sie auf das Symbol **Erweitern** neben **Paket: AS**. Beachten Sie, dass **EDI-X12** bereits aufgelistet ist.
   c. Klicken Sie auf das Symbol **Erweitern** neben **Protokoll: EDI-X12**. Beachten Sie, dass **Dokumenttyp: ISA** bereits aufgelistet ist.
2. Prüfen Sie, während die Seite **Dokumentdefinitionen verwalten** noch angezeigt ist, ob die zweite Dokumentdefinition aktiviert ist, die den Dokumenttyp beschreibt, welcher zur Back-End-Anwendung fließt.
   a. Klicken Sie auf das Symbol **Erweitern** neben **Paket: None**. Beachten Sie, dass **EDI-X12** bereits aufgelistet ist.
   b. Klicken Sie auf das Symbol **Erweitern** neben **Protokoll: EDI-X12**. Beachten Sie, dass **Dokumenttyp: ISA** bereits aufgelistet ist.

3. Erstellen Sie eine Interaktion, die beschreibt, ob der Dokumenttyp ein Quellen- oder ein Empfängertyp ist.
   a. Klicken Sie auf den Link **Interaktionen verwalten**, während die Seite **Dokumentdefinitionen verwalten** noch angezeigt wird.
   b. Erweitern Sie in der Spalte **Quelle** den Eintrag **Paket: AS**, **Protokoll: EDI-X12 (ALL)** und klicken Sie dann auf **Dokumenttyp: ISA**, sodass das Optionsfeld ausgewählt ist.
   c. Erweitern Sie in der Spalte **Ziel** den Eintrag **Paket: None**, **Protokoll: EDI-X12 (ALL)** und klicken Sie dann auf **Dokumenttyp: ISA**, sodass das Optionsfeld ausgewählt ist.
   d. In diesem Beispiel gibt es keine Transformation. Treffen Sie daher keine Auswahl in der Liste **Transformationszuordnung**.
   e. Wählen Sie in der Liste **Aktion** die Option **Pass-Through** aus.
   f. Klicken Sie auf **Speichern**.

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

*Tabelle 5. Vom Produkt bereitgestellte Interaktionen für OpenPGP*

| Diese Verbindung auf der Absenderseite festlegen | Diese Verbindung auf der Empfängerseite festlegen |
|---|---|
| None/EDI-X12/ISA zu None/EDI-X12/ISA | None/EDI-X12/ISA zu None/EDI-X12/ISA |
| Backend integration/EDI-X12/ISA zu None/EDI-X12/ISA | None/EDI-X12/ISA zu None/EDI-X12/ISA |

**Anmerkung:** EDI-X12 ist standardmäßig in "Backend Integration" nicht enthalten; daher müssen Sie "EDI-X12" zum Kontext von "Backend Integration" hinzufügen. Nachdem Sie "EDI-X12" zum Kontext von "Backend Integration" hinzugefügt haben, müssen Sie "ISA" zum Kontext von "Backend Integration - EDI-X12" hinzufügen.

Sie haben noch nicht angegeben, welcher Partner in der Lage ist, diesen Austauschtyp zum Hub zu senden. Sie definieren dies, wenn Sie das Partnerprofil und die B2B-Funktionalität des Partners konfigurieren. (Sie definieren außerdem ein Profil und die B2B-Funktionalität für das Back-End-System des internen Partners.) Nachdem Sie diese Aufgaben ausgeführt haben, erstellen Sie eine Verbindung zwischen dem Partner und der Back-End-Anwendung. Abb. 20 auf Seite 111 zeigt die Verbindung zwischen dem Partner und der Back-End-Anwendung des internen Partners für dieses Beispiel.

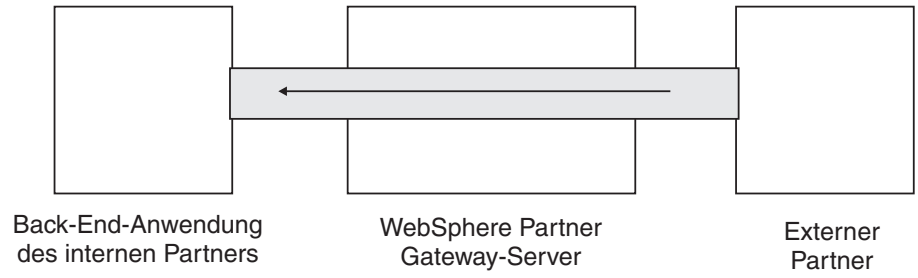



*Abbildung 20. Eine Einwegverbindung von einem Partner zum internen Partner*

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

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

## Binäre Dokumente

Binäre Dokumente sind Dokumente, die unverändert durch den Hub geleitet werden. Diese Dokumente werden zwischen einem externen Partner und einem internen Partner mithilfe der einer Back-End-Anwendung ausgetauscht. Sie müssen die Profile und die B2B-Funktionalität (B2B - Business-to-Business) der internen Partner und der externen Partner definiert haben, bevor Sie Verbindungen zwischen ihnen erstellen können. Wenn Sie nicht den internen Standardpartner verwenden, muss die Empfänger-ID (receiverID) des internen Partners explizit festgelegt werden. Wenn das binäre Dokument über den HTTP-Transport weitergeleitet wird und dafür die Basisauthentifizierung verwendet wird, kann die Empfänger-ID über das Attribut **X-aux-receiver-id** übergeben werden. Ein externer Partner kann über das FTP-Protokoll binäre Dokumente an den Hub senden. Das binäre Protokoll ist bereits für die Pakete **AS**, **None** und **Backend Integration** verfügbar. Daher ist „Schritt 1: Sicherstellen, dass die Dokumentdefinition verfügbar ist” auf Seite 107 bereits erledigt.

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

Standardmäßig werden für WebSphere Partner Gateway vier Interaktionen bereitgestellt, die binäre Dokumente einschließen. Drei Interaktionen werden neu für OpenPGP bereitgestellt. Für diese Interaktionen müssen Sie „Schritt 2: Interaktionen erstellen” auf Seite 108 nicht ausführen. Interaktionen werden für die folgenden Austauschvorgänge bereitgestellt:

*Tabelle 6. Vom Produkt bereitgestellte Interaktionen*

| Quellenpaket/Protokoll/Dokumenttyp | Zielpaket/Protokoll/Dokumenttyp |
|---|---|
| AS/Binary/Binary | Backend Integration/Binary/Binary |
| Backend Integration/Binary/Binary | AS/Binary/Binary |
| AS/Binary/Binary | None/Binary/Binary |
| None/Binary/Binary | AS/Binary/Binary |

Für OpenPGP müssen Sie die folgenden unterstützten Interaktionen über die Konsole von WebSphere Partner Gateway manuell aktivieren:

*Tabelle 7. Von OpenPGP unterstützte Interaktionen*

| Quellenpaket/Protokoll/Dokumenttyp | Zielpaket/Protokoll/Dokumenttyp |
|---|---|
| None/Binary/Binary | None/Binary/Binary |
| Backend Integration/Binary/Binary | None/Binary/Binary |

Für den Austausch binärer Dokumente müssen Sie noch Folgendes ausführen:

- „Schritt 3: Partnerprofile, Ziele und B2B-Funktionalität erstellen" auf Seite 108 wird in Kapitel 3, „Partner erstellen und definieren", auf Seite 25 und Kapitel 11, „Ziele erstellen", auf Seite 227 beschrieben.
- „Schritt 4: Verbindungen aktivieren" auf Seite 109 wird in Kapitel 12, „Verbindungen verwalten", auf Seite 251 beschrieben.

## EDI-Dokumente mit Pass-Through-Aktion

WebSphere Partner Gateway stellt für EDI-Austauschvorgänge die Funktion zum Entfernen des Umschlags und zum Transformieren bereit. Dieser Prozess wird in Kapitel 10, „EDI-Dokumentenflüsse konfigurieren", auf Seite 173 beschrieben.

Abb. 21 zeigt den Ablauf eines EDI-Austauschs, der von einem Partner an den internen Partner weitergeleitet wird.

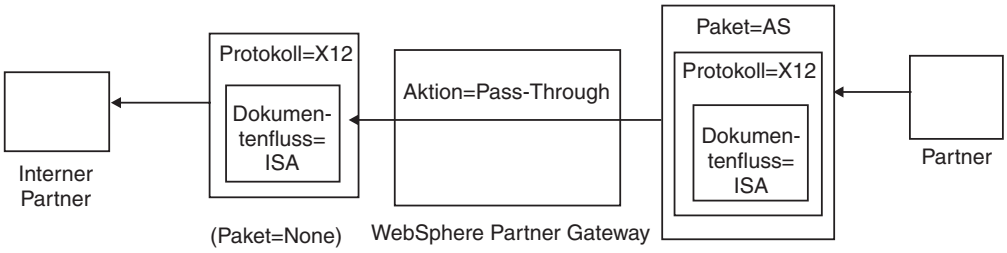



*Abbildung 21. Eingehender EDI-Austausch mit Pass-Through-Aktion*

In diesem Beispiel werden die AS2-Header entfernt; ansonsten wird der Austausch aber nicht verändert und fließt durch das System zum Ziel des internen Partners.

Erfolgt eine synchrone Transformation der EDI-Transaktion mit WTX (EDI zu Any) und sind für diese Transformation mehrere Ausgaben vorhanden, werden die untergeordneten Elemente basierend auf der Markierung für Weiterleitung (Reroute) direkt an den den Ausgangsarbeitsablauf übergeben oder an den festen Eingangsarbeitsablauf weitergeleitet, um durch einen neuen Kanal zu fließen. Bei einer asynchronen Transformation werden die EDI-Transaktionen von WTX an WPG ge-

sendet, um sie mit einem Umschlag zu versehen. Für die beiden Kanäle müssen Verbindungen konfiguriert werden: <None> / <EDI-Wörterverzeichnis> / <EDI-Dokument > {EDI Trx} mit Pass-Through-Aktion und <NA> / <EDI-Austausch> / <,EDI ISA / UNB> zu <beliebiges Paket> / <EDI X12 / FACT> / <EDI ISA / UNB> mit Pass-Through-Aktion.

## Dokumentdefinitionen erstellen

Der Dokumenttyp für EDI-Austauschvorgänge mit Pass-Through wird bereits standardmäßig auf der Seite **Dokumentdefinitionen verwalten** bereitgestellt, wie im Abschnitt „Ein Beispieldokumentenfluss" auf Seite 109 beschrieben. Wenn Sie ein Attribut mit Standardwert ändern oder ein Attribut ohne zugeordneten Wert festlegen wollen, können Sie die Seite **Dokumentdefinitionen verwalten** zur Ausführung dieser Aufgabe verwenden.

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

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

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

## Interaktionen erstellen

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

1. Klicken Sie auf **Hubadmin > Hubkonfiguration > Dokumentdefinition > Interaktionen verwalten**.
2. Klicken Sie in der Anzeige **Interaktionen verwalten** auf den Link **Interaktion erstellen**.
3. Erweitern Sie unter **Quelle** den Eintrag **Paket: AS** und **Protokoll: EDI-X12** und wählen Sie dann **Dokumenttyp: ISA** aus.
4. Erweitern Sie unter **Ziel** den Eintrag **Paket: None** und **Protokoll: EDI-X12** und wählen Sie dann **Dokumenttyp: ISA** aus.
5. Wählen Sie optional eine **Transformationszuordnung** aus.
6. Wählen Sie in der Liste **Aktion** die Option **Pass-Through** aus.

Mit den Schritten 1 bis 4 wurde WebSphere Partner Gateway aktiviert, um einen EDI-X12-Austausch im AS-Paket von einem Quellenpartner zu akzeptieren, einen EDI-X12-Austausch ohne Paket an den Zielpartner zu senden und den Austausch von der Quelle an das Ziel weiterzuleiten.

Wenn Sie eine Interaktion konfigurieren wollen, deren Quellendokument als **None/EDI-X12/ISA** gepackt und deren Zieldokument als **AS/EDI-X12/ISA** gepackt ist, erweitern Sie **Paket: None** in Schritt 3 (in der Spalte **Quelle**) und erweitern Sie **Paket: AS** in Schritt 4 (in der Spalte **Ziel**).

## RosettaNet-Dokumente

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

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

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

### RNIF- und PIP-Dokumenttyppakete

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

Für RNIF V1.1 gibt es folgende Pakete:

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

Für RNIF V02.00 gibt es folgende Pakete:

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

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

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

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

- PIP 0A1 Notification of Failure v1.0
- PIP 0A1 Notification of Failure V02.00.00
- PIP 2A1 Distribute New Product Information V02.00.00
- PIP 2A12 Distribute Product Master V01.03.00
- PIP 3A1 Request Quote V02.00.00
- PIP 3A2 Request Price and Availability R02.01.00
- PIP 3A4 Request Purchase Order V02.02.00
- PIP 3A4 Request Purchase Order V02.00
- PIP 3A5 Query Order Status R02.00.00
- PIP 3A6 Distribute Order Status V02.02.00
- PIP 3A7 Notify of Purchase OrderUpdate V02.02.00
- PIP 3A8 Request Purchase Order Change V01.02.00
- PIP 3A8 Request Purchase Order Change V01.03.00
- PIP 3A9 Request Purchase Order Cancellation V01.01.00
- PIP 3B2 Notify of Advance Shipment V01.01.00
- PIP 3B3 Distribute Shipment Status R01.00.00
- PIP 3B11 Notify of Shipping Order R01.00.00A
- PIP 3B12 Request Shipping Order V01.01.00
- PIP 3B13 Notify of Shipping Order Confirmation V01.01.00
- PIP 3B14 Request Shipping Order Cancellation V01.00.00
- PIP 3B18 Notify of Shipping Documentation V01.00.00
- PIP 3C1 Return Product V01.00.00
- PIP 3C3 Notify of Invoice V01.01.00
- PIP 3C4 Notify of Invoice Reject V01.00.00
- PIP 3C6 Notify of Remittance Advice V01.00.00
- PIP 3C7 Notify of Self-Billing Invoice V01.00.00
- PIP 3D8 Distribute Work in Process V01.00.00
- PIP 4A1 Notify of Strategic Forecast V02.00.00

- PIP 4A3 Notify of Threshold Release Forecast V02.00.00
- PIP 4A4 Notify of Planning Release Forecast R02.00.00A
- PIP 4A5 Notify of Forecast Reply V02.00.00
- PIP 4B2 Notify of Shipment Receipt V01.00.00
- PIP 4B3 Notify of Consumption V01.00.00
- PIP 4C1 Distribute Inventory Report V02.03.00
- PIP 4C1 Distribute Inventory Report V02.01
- PIP 5C1 Distribute Product List V01.00.00
- PIP 5C2 Request Design Registration V01.00.00
- PIP 5C4 Distribute Registration Status V01.02.00
- PIP 5D1 Request Ship From Stock And Debit Authorization V01.00.00
- PIP 6C1 Query Service Entitlement V01.00.00
- PIP 6C2 Request Warranty Claim V01.00.00
- PIP 7B1 Distribute Work in Process V01.00.00
- PIP 7B5 Notify of Manufacturing Work Order V01.00.00
- PIP 7B6 Notify of Manufacturing Work Order Reply V01.00.00

Für jeden PIP gibt es vier PIP-Dokumenttyppakete:

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

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

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

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

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

'BCG_Package_RNIF1.1_3A4V02.02.zip' ist z. B. für das Validieren der Dokumente für Version 02.02 des 3A4 PIP, die zwischen Partnern und WebSphere Partner Gateway mit dem RNIF 1.1-Protokoll gesendet werden. Bei PIP-Dokumenttyppaketen 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 *WebSphere Partner Gateway Unternehmensintegration*.

## Dokumentdefinitionen erstellen

Für die RosettaNet-Nachrichtenübermittlung benötigt WebSphere Partner Gateway die RNIF-Pakete für die Version von RNIF, mit der die Nachrichten gesendet wer-

den. Für jeden PIP, den WebSphere Partner Gateway unterstützt, benötigt es die zwei PIP-Dokumenttyppakete für die RNIF-Version. WebSphere Partner Gateway benötigt z. B. die folgenden Pakete, um den 3A4 PIP über RNIF 2.0 zu unterstützen:

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

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

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

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

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

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

   Die Pakete, die für die Kommunikation mit Partnern oder mit dem Back-End-System benötigt werden, sind jetzt auf dem System installiert. Wenn Sie die Seite **Dokumentdefinitionen verwalten** überprüfen, finden Sie einen Eintrag für **Paket: RNIF/Protokoll: RosettaNet**, der das Paket für die Kommunikation mit Partnern darstellt, und einen Eintrag für **Paket: Backend Integration/Protokoll: RNSC**, der das Paket für die Kommunikation mit Back-End-Anwendungen darstellt.
9. Laden Sie für jeden PIP, den Sie unterstützen wollen, das PIP-Dokumenttyppaket für den PIP und für die unterstützte RNIF-Version hoch. Führen Sie die folgenden Schritte aus, um z. B. den 3A6 PIP (Notify of Remittance Advice) hochzuladen, der zu einem Partner gesendet werden soll:
   a. Klicken Sie auf **Durchsuchen** und wählen Sie BCG_Package_RNIFV02.00_3C6V02.02 im Verzeichnis B2BIntegrate/Rosettanet aus.
   b. Stellen Sie sicher, dass **In Datenbank festschreiben** auf **Ja** gesetzt ist.
   c. Klicken Sie auf **Hochladen**.

   Der 3C6V02.02 PIP wird jetzt als Dokumenttyp unter **Paket:RNIF/Protokoll:RosettaNet** auf der Seite **Dokumentdefinitionen verwalten** ange-

zeigt. Darüber hinaus werden eine Aktivität, eine Aktion und zwei Signale angezeigt. Sie werden in den Upload des PIP einbezogen.

Führen Sie die folgenden Schritte aus, um den 3A6 PIP hochzuladen, der zu einer Back-End-Anwendung gesendet werden soll:

a. Klicken Sie auf **Durchsuchen** und wählen Sie BCG_Package_RNSC1.0_RNIFV02.00_3C6V02.02.zip aus.
b. Stellen Sie sicher, dass **In Datenbank festschreiben** auf **Ja** gesetzt ist.
c. Klicken Sie auf **Hochladen**.

Der 3C6V02.02 PIP wird jetzt als Dokumenttyp unter **Paket:Backend Integration/Protokoll:RNSC** auf der Seite **Dokumentdefinitionen verwalten** angezeigt. Wenn WebSphere Partner Gateway kein Paket für den PIP oder die PIP-Version bereitstellt, die Sie verwenden wollen, können Sie Ihre eigenen erstellen und hochladen. Weitere Informationen finden Sie in „PIP-Dokumentdefinitionspakete erstellen" auf Seite 381.

## Attributwerte konfigurieren

Für PIP-Dokumentdefinitionen sind die meisten Attributwerte bereits gesetzt und müssen nicht konfiguriert werden. Die folgenden Attribute müssen jedoch definiert werden:

RNIF (1.0)-Paket

- **Globaler Lieferkettencode** - Geben Sie den Typ der Lieferkette an, die vom Partner 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 Nutzdaten, einen verschlüsselten Container und verschlüsselte Nutzdaten oder keine Verschlüsselung haben müssen. Der Standardwert ist **Kein(e)**.
- **Sync-Bestätigung erforderlich** - Setzen Sie auf **Ja**, wenn der Partner die Empfangsbestätigung empfangen möchte. Setzen Sie auf **Nein**, wenn 200 angefordert wurden.
- **Sync unterstützt** - Legen Sie fest, ob der PIP Austauschvorgänge für Synchronnachrichten unterstützt. Der Standardwert ist **Nein**.

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

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

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

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

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

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

**Anmerkung:** Sie können auch RosettaNet-Attribute auf der Verbindungsebene aktualisieren, indem Sie für die Quelle oder das Ziel auf **Attribute** klicken und dann die Werte in die Spalte **Aktualisieren** eingeben oder dort ändern. Lesen Sie „Attribute angeben oder ändern" auf Seite 253.

## Interaktionen erstellen

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

Bevor Sie anfangen, stellen Sie sicher, dass die entsprechenden RNIF-Dokumentdefinitionen sowie die Pakete für den PIP, den Sie verwenden wollen, hochgeladen wurden. Wenn Sie über die Funktion zum Generieren eines 0A1 PIP (Notification of Failure) verfügen wollen, stellen Sie sicher, dass Sie den PIP hochgeladen haben, wie in Schritt 9 auf Seite 117 beschrieben.

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

1. Klicken Sie auf **Hubadmin > Hubkonfiguration > Dokumentdefinition > Interaktionen verwalten**.
2. Klicken Sie in der Anzeige **Interaktionen verwalten** auf den Link **Interaktion erstellen**.
3. Erweitern Sie die Baumstruktur **Quelle** auf die Ebene **Aktion** und erweitern Sie die Baumstruktur **Ziel** auf die Ebene **Aktion**.
4. Wählen Sie in den Baumstrukturen die Dokumentdefinitionen aus, die für den Quellenkontext und den Zielkontext verwendet werden sollen. Wenn z. B. der Partner der Initiator eines 3C6 PIP (eines PIP mit einer Aktion) ist, wählen Sie die folgenden Dokumentdefinitionen aus:

*Tabelle 8. 3C6 PIP von einem Partner initiiert*

| Quelle | Ziel |
|---|---|
| Paket: RNIF (V02.00) | Paket: Backend Integration (1.0) |

*Tabelle 8. 3C6 PIP von einem Partner initiiert (Forts.)*

| Quelle | Ziel |
|---|---|
| Protokoll: RosettaNet (V02.00) | Protokoll: RNSC (1.0) |
| Dokumenttyp: 3C6 (V01.00) | Dokumenttyp: 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 Dokumentdefinitionen aus:

*Tabelle 9. 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) |
| Dokumenttyp: 3C6 (V01.00) | Dokumenttyp: 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 Partner initiiert, wählen Sie die folgenden Dokumentdefinitionen für die erste Aktion aus:

*Tabelle 10. 3A4 PIP von einem Partner initiiert*

| Quelle | Ziel |
|---|---|
| Paket: RNIF (V02.00) | Paket: Backend Integration (1.0) |
| Protokoll: RosettaNet (V02.00) | Protokoll: RNSC (1.0) |
| Dokumenttyp: 3A4 (V02.02) | Dokumenttyp: 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 Dokumentdefinitionen für die erste Aktion aus:

*Tabelle 11. 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) |
| Dokumenttyp: 3A4 (V02.02) | Dokumenttyp: 3A4 (V02.02) |
| Aktivität: Request Purchase Order | Aktivität: Request Purchase Order |
| Aktion: Purchase Order Request Action | Aktion: Purchase Order Request Action |

5. Wählen Sie im Feld **Aktion** den Eintrag **Bidirektionale Konvertierung von RosettaNet und RosettaNet Service Content mit Validierung** aus.
6. Klicken Sie auf **Speichern**.
7. Wenn Sie einen Doppelaktions-PIP konfigurieren, wiederholen Sie die benötigten Schritte, um die Interaktion für die zweite Aktion zu erstellen. Wählen Sie

z. B. die folgenden Dokumentdefinitionen für die zweite Aktion für einen von einem Partner initiierten 3A4 PIP aus. Dies ist die Aktion, bei der das Back-End-System die Antwort sendet.

*Tabelle 12. 3A4 PIP von einem Partner initiiert (zweite Aktion)*

| **Quelle** | **Ziel** |
|---|---|
| Paket: Backend Integration (1.0) | Paket: RNIF (V02.00) |
| Protokoll: RNSC (1.0) | Protokoll: RosettaNet (V02.00) |
| Dokumenttyp: 3A4 (V02.02) | Dokumenttyp: 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 Dokumentdefinitionen aus:

*Tabelle 13. 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) |
| Dokumenttyp: 3A4 (V02.02) | Dokumenttyp: 3A4 (V02.02) |
| Aktivität: Request Purchase Order | Aktivität: Request Purchase Order |
| Aktion: Purchase Order Confirmation Action | Aktion: Purchase Order Confirmation Action |

8. Wenn Sie **0A1 Notification of Failure** generieren wollen, erstellen Sie eine Interaktion für XMLEvent.
   a. Klicken Sie auf **Hubadmin > Hubkonfiguration > Dokumentdefinition > Interaktionen verwalten**.
   b. Klicken Sie in der Anzeige **Interaktionen verwalten** auf den Link **Interaktion erstellen**.
   c. Erweitern Sie die Baumstruktur **Quelle** auf die Ebene **Dokumenttyp** und erweitern Sie die Baumstruktur **Ziel** auf die Ebene **Dokumenttyp**.
   d. Wählen Sie die folgenden Dokumentdefinitionen aus:

*Tabelle 14. Dokumentdefinition für XMLEvent*

| **Quelle** | **Ziel** |
|---|---|
| Paket: Backend Integration (1.0) | Paket: Backend Integration (1.0) |
| Protokoll: XMLEvent (1.0) | Protokoll: XMLEvent (1.0) |
| Dokumenttyp: XMLEvent (1.0) | Dokumenttyp: XMLEvent (1.0) |

   e. Wählen Sie im Feld **Aktion** die Option **Pass-Through** aus.
   f. Klicken Sie auf **Speichern**.
9. Erstellen Sie eine Interaktion für XMLEvent zu 0A1 RNSC.
   a. Klicken Sie auf **Hubadmin > Hubkonfiguration > Dokumentdefinition > Interaktionen verwalten**.
   b. Klicken Sie in der Anzeige **Interaktionen verwalten** auf den Link **Interaktion erstellen**.
   c. Erweitern Sie die Baumstruktur **Quelle** auf die Ebene **Dokumenttyp** und erweitern Sie die Baumstruktur **Ziel** auf die Ebene **Aktivität**.
   d. Wählen Sie die folgenden Dokumentdefinitionen aus:

*Tabelle 15. Dokumentdefinition für XMLEvent zu 0A1*

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

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

f. Klicken Sie auf **Speichern**.

**Anmerkung:** Informationen zum Aktivieren und Inaktivieren von XMLEvent finden Sie im Abschnitt *"XMLEvent aktivieren oder inaktivieren" des Handbuchs Unternehmensintegration*.

## RosettaNet-Dokumente anzeigen

Die RosettaNet-Anzeige zeigt Informationen zu RosettaNet-Dokumenten an. Sie können unformatierte Dokumente und zugeordnete Dokumentverarbeitungsdetails und Ereignisse mithilfe von bestimmten Suchkriterien anzeigen. Diese Informationen sind nützlich, wenn Sie zu ermitteln versuchen, ob ein Dokument erfolgreich zugestellt wurde bzw. worin die Ursache eines Fehlers besteht.

Gehen Sie wie folgt vor, um die RosettaNet-Anzeige zu öffnen:

1. Klicken Sie auf **Anzeigen > RosettaNet-Anzeige**.
2. Wählen Sie die passenden Suchkriterien in den Listen aus. Diese Kriterien werden in Tabelle 16 beschrieben.

*Tabelle 16. Suchkriterien für RosettaNet*

| Wert | Beschreibung |
|---|---|
| Startdatum und -zeit | Das Datum und die Zeit des eingeleiteten Prozesses. |
| Enddatum und -zeit | Das Datum und die Zeit des abgeschlossenen Prozesses. |
| Quellen- und Zielpartner | Gibt den Quellenpartner (den einleitenden Partner) und die Zielpartner (die empfangenden Partner) an (nur für interne Partner). |
| Partner | Gibt an, ob die Suche für alle Partner oder nur den internen Partner ausgeführt wird. |
| Meine Rolle ist | Gibt an, ob Dokumente gesucht werden sollen, in denen der Partner das Ziel oder die Quelle ist. |
| Quellengeschäfts-ID | Geschäfts-ID des einleitenden Partners, z. B. DUNS. |
| Betriebsmodus | Dieser Wert kann "Produktion" oder "Test" sein. Der Eintrag "Test" ist nur auf Systemen verfügbar, die den Betriebsmodus "Test" unterstützen. |
| Protokoll | Die für die Partner verfügbaren Protokolle. |
| Dokumenttyp | Der jeweilige Geschäftsprozess. |
| Prozessinstanz-ID | Die eindeutige Identifikationsnummer, die dem Prozess zugeordnet ist. Die Kriterien können einen Stern (*) als Platzhalterzeichen beinhalten. |
| Sortieren nach | Ergebnisse sortieren nach:<br>• Zielzeitmarke<br>• Dokumenttyp<br><br>Der Standardwert ist "Zielzeitmarke". |

*Tabelle 16. Suchkriterien für RosettaNet (Forts.)*

| Wert | Beschreibung |
|---|---|
| Absteigend oder Aufsteigend | "Absteigend" zeigt Einträge mit der neusten Zeitmarke oder beginnend am Anfang des Alphabets zuerst an.<br><br>"Aufsteigend" zeigt Einträge mit der ältesten Zeitmarke oder beginnend am Ende des Alphabets zuerst an.<br><br>Der Standardwert ist "Absteigend". |
| Ergebnisse pro Seite | Gibt die Anzahl der pro Seite angezeigten Ergebnisse an. |

3. Klicken Sie auf **Suchen**.

## CIDX-Dokumente

CIDX ist ein etablierter Fachverband und ein Standardisierungsgremium, dessen Ziel es ist, die elektronischen Geschäftsabläufe zwischen Chemieunternehmen und deren Handelspartnern zu vereinfachen, zu beschleunigen und kostengünstiger zu machen. Verschiedene CIDX-Initiativen geben Standards für die chemische Industrie vor. Die CIDX-Initiative Chem eStandards ist für das vorliegende Dokument von Interesse. Chem eStandards besteht aus einheitlichen Standards für den Datenaustausch im Zusammenhang mit dem Kauf, Verkauf und der Bereitstellung von Chemieprodukten. Chem eStandards setzt sich wie folgt zusammen:

- ChemXML/Chem eStandards Message Specifications: Version 2.0, Version 2.0.1, Version 2.0.2, Version 3.0 und Version 4.0.
- Chem eStandards Envelope and Security Specification: Version 2.0 und Version 3.0.

Für Pakete verwendet CIDX stets RNIF 1.1. Dabei muss beachtet werden, dass die Verarbeitung bei RNIF 1.1 immer asynchron erfolgt. Deshalb ist der CIDX-Dokumentenaustausch immer asynchron.

CIDX besteht aus Paketen und Transaktionen, während RosettaNet aus Paketen und PIPs (Partner Interchange Processes) besteht. CIDX verwendet RNIF 1.1-Pakete. Transaktionen sind gemäß dem ChemXML-Standard definiert. Jede Version des ChemXML-Standards definiert Transaktionen. Alle ChemXML-Transaktionen unter einer bestimmten Version des ChemXML-Standards verfügen über dieselbe Version wie der ChemXML-Standard. Im Gegensatz zu RosettaNet erfordert CIDX keine Konformität mit der Prozessdefinition. CIDX konzentriert sich mehr auf die Struktur der Transaktion und den sicheren Nachrichtenaustausch.

Des weiteren ist RosettaNet das Verwaltungsorgan für den RosettaNet-Standard, genauso wie CIDX das Verwaltungsorgan für den CIDX-Standard ist. RosettaNet definiert RNIF-Pakete und PIPs. RosettaNet-Nachrichten können RNIF 1.1 oder RNIF 2.0 verwenden. Mit RosettaNet definierte PIPs liefern den Nachrichtensatz und den Prozessablauf. CIDX verwendet RNIF 1.1 stets wie von RosettaNet definiert. Da CIDX das Verwaltungsorgan ist, muss der RNIF-Umschlag gemäß der Umschlags- und Sicherheitsspezifikation (Envelope and Security Specification) von Chem eStandards erstellt werden. Diese Spezifikation basiert auf der RosettaNet-Implementierung. CIDX verwendet KEINE von RosettaNet definierten PIPs. Stattdessen verwendet CIDX die Chem eStandards-Nachrichtenspezifikation (Message Specification).

Weitere Informationen zu CIDX finden Sie unter http://www.cidx.org. CIDX-Standards können von der Website http://www.cidx.org heruntergeladen werden.

Chem eStandards Envelope and Security Version 3.0 finden Sie unter http://www.cidx.org/Portals/0/Publications/Envelope_and_Security_v3.0.pdf.

WebSphere Partner Gateway unterstützt die folgenden Chem eStandards:

- Chem eStandards Envelope and Security Specification Version 3.0.
- ChemXML/Chem eStandards Message Specifications Version 4.0.

## RNIF- und PIP-Dokumenttyppakete für CIDX

CIDX verwendet RNIF 1.1. Zur Unterstützung von CIDX stellt WebSphere Partner Gateway zwei Gruppen von komprimierten Dateien, auch Pakete genannt, bereit. Die *RNIF-Pakete* bestehen aus Dokumentdefinitionen, die zur Unterstützung des RNIF-Protokolls erforderlich sind. Diese Pakete befinden sich im Verzeichnis 'B2BIntegrate'.

Für RNIF V1.1 gibt es folgende Pakete:

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

Das erste Paket bietet die Dokumentdefinitionen, die zur Unterstützung der CIDX-Kommunikation mit Partnern erforderlich sind, und das zweite Paket bietet die Dokumentdefinitionen, die zur Unterstützung der CIDX-Kommunikation mit Back-End-Systemen erforderlich sind.

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

Für CIDX stellt WebSphere Partner Gateway Dokumenttyppakete für E41 ChemXML Version 4.0 (Order Create) und E42 ChemXML Version 4.0 (Order Response) bereit.

Die Namenskonvention für die bereitgestellten CIDX-Pakete entspricht der Namenskonvention für die Pakete, die für RosettaNet bereitgestellt werden. 'BCG_Package_RNIF1.1_E414.0.zip' wird beispielsweise zum Validieren der Dokumente für Version 4.0 des E41 PIP für den Versand zwischen Partnern und WPG mit RNIF 1.1 verwendet.

## Dokumentdefinitionen erstellen

Für die CIDX-Nachrichtenübermittlung benötigt WebSphere Partner Gateway die RNIF-Pakete für die Version von RNIF, mit der die Nachrichten gesendet werden. Für jeden PIP, den WebSphere Partner Gateway unterstützt, benötigt es die zwei PIP-Dokumenttyppakete für die RNIF-Version. WebSphere Partner Gateway benötigt z. B. die folgenden Pakete, um den E41 PIP über RNIF 1.1 zu unterstützen:

- Package_RNIF_1.1.zip
- Package_RNSC_1.0_RNIF_1.1.zip
- BCG_Package_RNIF1.1_E414.0.zip

- BCG_Package_RNSC1.0RNIF1.1_E414.0.zip

Das erste Paket unterstützt die CIDX-Nachrichtenübermittlung mit Partnern, und das zweite Paket unterstützt die CIDX-Nachrichtenübermittlung mit Back-End-Systemen. Das dritte und vierte Paket aktivieren WebSphere Partner Gateway für das Übergeben von E41-Nachrichten zwischen Partnern und Back-End-Systemen.

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

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

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

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

   Die Pakete, die für die Kommunikation mit Partnern oder mit dem Back-End-System benötigt werden, sind jetzt auf dem System installiert. Wenn Sie die Seite **Dokumentdefinitionen verwalten** überprüfen, finden Sie einen Eintrag für **Paket: RNIF/Protokoll: Rosettanet**, der das Paket für die Kommunikation mit Partnern darstellt, und einen Eintrag für **Paket: Backend Integration/Protokoll: RNSC**, der das Paket für die Kommunikation mit Back-End-Anwendungen darstellt.
9. Laden Sie für jeden PIP, den Sie unterstützen wollen, das PIP-Dokumenttyppaket für den PIP und für die unterstützte RNIF-Version hoch.

   Führen Sie die folgenden Schritte aus, um z. B. den E41 CIDX PIP (Order Create) hochzuladen, der zu einem Partner gesendet werden soll:

   a. Klicken Sie auf **Durchsuchen** und wählen Sie **BCG_Package_RNIF1.1_E414.0.zip** im Verzeichnis B2BIntegrate/Rosettanet aus.
   b. Stellen Sie sicher, dass **In Datenbank festschreiben** auf **Ja** gesetzt ist.
   c. Klicken Sie auf **Hochladen**.

   Der E41 PIP wird jetzt als Dokumenttyp unter **Paket:RNIF/ Protokoll:RosettaNet** auf der Seite **Dokumentdefinitionen verwalten** angezeigt. Darüber hinaus werden eine Aktivität, eine Aktion und zwei Signale angezeigt. Sie werden in den Upload des PIP einbezogen.

   Führen Sie die folgenden Schritte aus, um den E41 PIP hochzuladen, der zu einer Back-End-Anwendung gesendet werden soll:

   a. Klicken Sie auf **Durchsuchen** und wählen Sie **BCG_Package_RNSC1.0RNIF1.1_E414.0.zip** aus.
   b. Stellen Sie sicher, dass **In Datenbank festschreiben** auf **Ja** gesetzt ist.

c. Klicken Sie auf **Hochladen**.

Der E41 PIP wird jetzt als Dokumenttyp unter **Paket:Backend Integration/ Protokoll:RNSC** auf der Seite **Dokumentdefinitionen verwalten** angezeigt.

## Attributwerte konfigurieren

Für RNIF-Dokumentdefinitionen sind die meisten Attributwerte bereits gesetzt und müssen nicht konfiguriert werden. Die folgenden Attribute müssen jedoch definiert werden:

RNIF (1.1)-Paket

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

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

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

**Anmerkung:** Sie können auch RosettaNet-Attribute auf der Verbindungsebene aktualisieren, indem Sie für die Quelle oder das Ziel auf **Attribute** klicken und dann die Werte in die Spalte **Aktualisieren** eingeben oder dort ändern. Lesen Sie „Attribute angeben oder ändern" auf Seite 253.

## Interaktionen erstellen

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

Bevor Sie anfangen, stellen Sie sicher, dass die entsprechenden RNIF-Dokumentdefinitionen sowie die Pakete für den PIP, den Sie verwenden wollen, hochgeladen wurden.

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

1. Klicken Sie auf **Hubadmin > Hubkonfiguration > Dokumentdefinition > Interaktionen verwalten**.
2. Klicken Sie in der Anzeige **Interaktionen verwalten** auf den Link **Interaktion erstellen**.

3. Erweitern Sie die Baumstruktur **Quelle** auf die Ebene **Aktion** und erweitern Sie die Baumstruktur **Ziel** auf die Ebene **Aktion**.
4. Wählen Sie in den Baumstrukturen die Dokumentdefinitionen aus, die für den Quellenkontext und den Zielkontext verwendet werden sollen. Wenn z. B. der Partner der Initiator eines E41 PIP ist, wählen Sie die folgenden Dokumentdefinitionen aus:

*Tabelle 17. 3C6 PIP von einem Partner initiiert*

| Quelle | Ziel |
|---|---|
| Paket: RNIF(1.1) | Paket: BackEnd Integration (1.1) |
| Protokoll: RosettaNet(1.1) | Protokoll: RNSC (1.0) |
| Dokumenttyp: E41 (4.0) | Dokumenttyp: E41 (4.0) |
| Aktivität: OrderCreate | Aktivität: OrderCreate |
| Aktion: Order Create | Aktion: Order Create |

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

*Tabelle 18. 3A4 PIP von einem Partner initiiert*

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

5. Wählen Sie im Feld **Aktion** den Eintrag **Bidirektionale Konvertierung von RosettaNet und RosettaNet Service Content mit Validierung** aus.
6. Klicken Sie auf **Speichern**.

## CIDX-Dokumente anzeigen

Die RosettaNet-Anzeige zeigt Informationen zu CIDX-Dokumenten an. Sie können unformatierte Dokumente und zugeordnete Dokumentverarbeitungsdetails und Ereignisse mithilfe von bestimmten Suchkriterien anzeigen. Diese Informationen sind nützlich, wenn Sie zu ermitteln versuchen, ob ein Dokument erfolgreich zugestellt wurde bzw. worin die Ursache eines Fehlers besteht.

Gehen Sie wie folgt vor, um die RosettaNet-Anzeige zu öffnen:

1. Klicken Sie auf **Anzeigen > RosettaNet-Anzeige**.
2. Wählen Sie die entsprechenden Suchkriterien aus.
3. Klicken Sie auf **Suchen**.

# ebMS-Dokumente

Der ebMS-Mechanismus bietet eine standardisierte Möglichkeit für den Austausch von Geschäftsnachrichten zwischen ebXML-Handelspartnern. Mit dem ebXML Messaging Service können Geschäftsnachrichten zuverlässig ausgetauscht werden, ohne auf proprietäre Technologien und Lösungen zurückgreifen zu müssen. Dieser Abschnitt zeigt Ihnen, wie Sie Dokumentdefinitionen und Interaktionen für diese Dokumente konfigurieren.

## Dokumentdefinitionen erstellen

Für die ebMS-Nachrichtenübermittlung muss eine CPA-XML-Datei (CPA - Collaboration Profile Agreement) hochgeladen werden, bevor Sie Dokumente definieren können.

Gehen Sie wie folgt vor, um eine CPA-XML-Datei hochzuladen:

1. Klicken Sie auf **Hubadmin** > **Hubkonfiguration** > **ebMS**.
2. Klicken Sie auf **CPA hochladen**.
3. Klicken Sie auf **Durchsuchen** und wählen Sie das entsprechende CPA-Paket aus.
4. Stellen Sie sicher, dass **ebMS Version** 2.0 ausgewählt ist.
5. Klicken Sie auf **Hochladen**.

Beim Hochladen werden Sie aufgefordert, aus den Partnern im CPA den internen Partner auszuwählen. Der interne Partner wird als Manager im ebMS-Fluss behandelt, und alle Ziele im ebMS-Fluss für den internen Partner verwenden das Paket **Backend Integration** oder **N/A**. Auf der Konsole wird der Partner jedoch nur als externer Partner angezeigt.

Der ebMS wird nun als Paket und Protokoll unter **ebMS** und **Paket: Backend Integration** auf der Seite **Dokumentdefinitionen verwalten** angezeigt.

Der ebMS-Fluss kann auch ohne CPA in WebSphere Partner Gateway konfiguriert werden. Erstellen Sie dazu ebMS-Dokumentdefinitionen und B2B-Funktionalität über WebSphere Partner Gateway Console, wie in „Übersicht über die Dokumenttypen" auf Seite 107 beschrieben. Beim Hochladen des CPA werden alle Konfigurationsoperationen automatisch ausgeführt. Ist kein CPA vorhanden, sollten Sie die in diesem Abschnitt beschriebenen Schritte ausführen.

## Attributwerte konfigurieren

Für ebMS-Dokumentdefinitionen sind die meisten Attributwerte bereits gesetzt und müssen nicht konfiguriert werden. Die folgenden Attribute müssen jedoch definiert werden:

**ebMS-Paket**

- **Zeit für Bestätigung (in Minuten)** - Gibt die Wartezeit für eine Bestätigung an, bevor die ursprüngliche Anforderung erneut gesendet wird. Dieses Attribut funktioniert in Verbindung mit **Wiederholungszähler**. Die Einheiten werden in Minuten angegeben. Der Standardwert ist 30.
- **Wiederholungszähler** - Gibt an, wie oft eine Anforderung gesendet werden soll, wenn keine Bestätigung empfangen wird. Dieses Attribut wird in Verbindung mit **Bestätigungszeit** verwendet. Der Standardwert ist 3.
- **Unbestreitbarkeit erforderlich** - Gibt an, ob das ursprüngliche Dokument im Unbestreitbarkeitsspeicher gespeichert werden soll. Der Standardwert ist **Ja**.

  **Anmerkung:** In WebSphere Partner Gateway 6.2 werden die Unbestreitbarkeitsinformationen aus den Parametern der Partnerverbindung abgerufen. Die Parameter der Partnerverbindung werden nach einer erfolgreichen Suche der Partnerverbindung ermittelt. Die Unbestreitbarkeit ist standardmäßig auf **Ja** gesetzt.

Dies bedeutet, dass das Dokument im Unbestreitbarkeitsspeicher abgelegt wird, wenn die Informationen aus irgendwelchen Gründen nicht aus der Partnerverbindung abgerufen werden können.

- **Nachrichtenspeicherung erforderlich** - Gibt an, ob das Dokument im Nachrichtenspeicher gespeichert werden soll. Der Standardwert ist **Ja**.

  **Anmerkung:** Die Informationen zum Nachrichtenspeicher werden aus den Parametern der Partnerverbindung abgerufen. Die Parameter der Partnerverbindung werden nach einer erfolgreichen Suche der Partnerverbindung ermittelt. Die Speicherung im Nachrichtenspeicher ist standardmäßig auf **Ja** gesetzt. Dies bedeutet, dass das Dokument im Nachrichtenspeicher bestehen bleibt.
- **Unbestreitbarkeit des Empfangs** - Gibt an, ob die Empfangsbestätigung im Unbestreitbarkeitsspeicher abgelegt wird. Der Standardwert ist **Ja**.
- **Wiederholungsintervall** - Gibt die Wartezeit des Systems zwischen Wiederholungsversuchen an. Dieses Attribut funktioniert in Verbindung mit **Wiederholungszähler**. Der Standardwert ist 5 Minuten.

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

1. Klicken Sie auf **Hubadmin > Hubkonfiguration > Dokumentdefinition**.
2. Klicken Sie auf das Symbol **Erweitern**, um einen Knoten individuell zur entsprechenden Dokumentdefinitionsebene zu erweitern, oder wählen Sie **Alle** aus, um alle angezeigten Dokumentdefinitionsknoten zu erweitern.
3. Klicken Sie in der Spalte **Aktionen** auf das Symbol **Attributwerte bearbeiten** für das Paket, das Sie bearbeiten wollen.
4. Gehen Sie im Abschnitt **Attribute für Dokumentdefinitionskontexte** in die Spalte **Aktualisieren** des Attributs, das Sie festlegen wollen, und wählen Sie den neuen Wert aus, bzw. geben Sie ihn dort ein. Wiederholen Sie dies für jedes Attribut, das Sie festlegen wollen.
5. Klicken Sie auf **Speichern**.

**Anmerkung:** Sie können auch ebMS-Attribute auf der Verbindungsebene aktualisieren, indem Sie für die Quelle oder das Ziel auf **Attribute** klicken und dann die Werte in die Spalte **Aktualisieren** eingeben oder dort ändern. Lesen Sie „Attribute angeben oder ändern” auf Seite 253.

## Interaktionen erstellen

Der folgende Prozess beschreibt, wie Sie eine Interaktion zwischen einem Back-End-System und einem Partner erstellen.

Bevor Sie anfangen, stellen Sie sicher, dass die entsprechenden ebMS-Dokumentdefinitionen hochgeladen wurden.

Führen Sie die folgenden Schritte aus, um eine Interaktion für einen bestimmten Partner zu erstellen:

1. Klicken Sie auf **Hubadmin > Hubkonfiguration > Dokumentdefinition > Interaktionen verwalten**.
2. Klicken Sie in der Anzeige **Interaktionen verwalten** auf den Link **Interaktion erstellen**.
3. Erweitern Sie die Baumstruktur **Quelle** auf die Ebene **Aktion** und erweitern Sie die Baumstruktur **Ziel** auf die Ebene **Aktion**.

4. Wählen Sie in den Baumstrukturen die Dokumentdefinitionen aus, die für den Quellenkontext und den Zielkontext verwendet werden sollen. Wenn z. B. der Partner der Initiator eines ebMS ist, wählen Sie die folgenden Dokumentdefinitionen aus:

*Tabelle 19. ebMS von einem Partner initiiert*

| **Quelle** | **Ziel** |
|---|---|
| Paket: ebMS | Paket: Backend Integration (1.0) |
| Protokoll: ebMS | Protokoll: ebMS |
| Dokumenttyp: ALMService | Dokumenttyp: ALMService |
| Aktivität: ALMService | Aktivität: ALMService |
| Aktion: Remittance ALMBusiness | Aktion: ALMBusiness |

Wenn das Back-End-System der Initiator des ebMS ist, wählen Sie die folgenden Dokumentdefinitionen aus:

*Tabelle 20. ebMS von einem Back-End-System initiiert*

| **Quelle** | **Ziel** |
|---|---|
| Paket: Backend Integration (1.0) | Paket: ebMS |
| Protokoll: ebMS | Protokoll: ebMS |
| Dokumenttyp: ALMService | Dokumenttyp: ALMService |
| Aktivität: ALMService | Aktivität: ALMService |
| Aktion: ALMBusiness | Aktion: Remittance ALMBusiness |

5. Wählen Sie im Feld **Aktion** optional **ebMS - Teilen und parsen** aus.

   Bei Auswahl dieses Handlers werden die Nutzdaten aus der ebMS-Nachricht extrahiert, die vom Partner gesendet wird; dann werden die Nutzdaten in den Fluss zurückgeführt, als ob der Partner sie gesondert gesendet hätte. Dieser Handler sollte nicht ausgewählt werden, wenn das Back-End-System die Nachricht initiiert. Wenn Sie diesen Handler nicht auswählen, wählen Sie die Option **Pass-Through** für das Feld **Aktion** aus.
6. Klicken Sie auf **Speichern**.

**Anmerkung:** In manchen ebMS-Flüssen, z. B. in STAR-Spezifikationen, ist das ebMS-Serviceelement (der ebMS-Servicewert entspricht dem Wert der Dokumentenflussdefinition für den WPG-Kanal) keine URI, sondern eine Zeichenfolge. In solchen Fällen muss gemäß ebMS 2.0-Spezifikation neben dem Serviceelement ein Typattribut in der ebMS-SOAP-Nachricht vorhanden sein. In einer STAR-Spezifikation muss das Typattribut beispielsweise den Wert "STARBOD" aufweisen. Ein solches Attribut kann auf der Zielseite der Dokumentdefinitionsattribute konfiguriert werden. (Siehe Tabelle 22 auf Seite 146).

## Zuordnung von ebMS-CPA zur WebSphere Partner Gateway-Konfiguration

In diesem Abschnitt wird die Zuordnung zwischen dem Collaboration Profile Agreement (CPA) und der WebSphere Partner Gateway-Konfiguration über die Benutzerschnittstelle dargestellt. Die einzelnen Funktionen werden zusammen mit den entsprechenden Elementen der WebSphere Partner Gateway-Konfiguration über die Benutzerschnittstelle aufgelistet.

**1.**

**Funktion**
**Element/Attribut**

**1.1 CPAId 1**

**Importiert/Manuell konfiguriert:** Importiert.

**WebSphere Partner Gateway-Konfiguration über die Benutzerschnittstelle:**

CPAID wird über die zwischen zwei Partnern zugeordneten Kanäle konfiguriert. Sie können den Wert anzeigen, indem Sie in WebSphere Partner Gateway Console den Wert **Hubadmin > ebMS** aufrufen. Klicken Sie auf das Symbol **Suchen** und anschließend in den angezeigten Suchergebnissen auf **Details anzeigen**.

**2.**

**Funktion**
**Element/Attribut**

**1.2. Status 1**

**Importiert/Manuell konfiguriert:** Importiert, aber nicht in WebSphere Partner Gateway gespeichert. Kann nicht manuell konfiguriert werden.

**WebSphere Partner Gateway-Konfiguration über die Benutzerschnittstelle:**

Dieses Attribut kann in WebSphere Partner Gateway nicht konfiguriert werden. Der Wert wird beim Importieren des CPA geprüft. Beim Importieren wird einer der folgenden Status angezeigt:

- Agreed: Das CPA kann importiert werden.
- Signed: Das CPA kann importiert werden. Vor dem Importieren wird die Signatur überprüft.
- Proposed: Das CPA kann nicht importiert werden.

**3.**

**Funktion**
**Element/Attribut**

**1.3 Start 1**

**Importiert/Manuell konfiguriert:** Importiert.

**WebSphere Partner Gateway-Konfiguration über die Benutzerschnittstelle:**

Dieses Attribut kann in WebSphere Partner Gateway nicht konfiguriert werden. Es kann nur über den CPA-Import definiert werden. Sie können den Wert anzeigen, indem Sie in WebSphere Partner Gateway Console den Wert **Hubadmin > ebMS** aufrufen. Klicken Sie auf das Symbol **Suchen** und anschließend in den angezeigten Suchergebnissen auf **Details anzeigen**.

**4.**

**Funktion**
**Element/Attribut**

**1.4 End 1**

**Importiert/Manuell konfiguriert:** Importiert.

**WebSphere Partner Gateway-Konfiguration über die Benutzerschnittstelle:**

Dieses Attribut kann in WebSphere Partner Gateway nicht konfiguriert werden. Es kann nur über den CPA-Import definiert werden. Sie können den Wert anzeigen, indem Sie in WebSphere Partner Gateway Console den Wert **Hubadmin > ebMS** aufrufen. Klicken Sie auf das Symbol **Suchen** und anschließend in den angezeigten Suchergebnissen auf **Details anzeigen**.

**5.**

**Funktion**
**Element/Attribut**

**1.5 Conversation Constraints 0, 1 (9.5) - invocationLimit 0,1 - concurrentConversations 0, 1**

**Importiert/Manuell konfiguriert:** Importiert.

**WebSphere Partner Gateway-Konfiguration über die Benutzerschnittstelle:**

Dieses Attribut kann in WebSphere Partner Gateway nicht konfiguriert werden. Es kann nur über den CPA-Import definiert werden. Sie können den Wert anzeigen, indem Sie in WebSphere Partner Gateway Console den Wert **Hubadmin > ebMS** aufrufen. Klicken Sie auf das Symbol **Suchen** und anschließend in den angezeigten Suchergebnissen auf **Details anzeigen**.

**6.**

**Funktion**
**Element/Attribut**

**1.6 PartyInfo 2**
partyName 1

**Importiert/Manuell konfiguriert:** Importiert.

**WebSphere Partner Gateway-Konfiguration über die Benutzerschnittstelle:**

Sie können die Werte anzeigen, indem Sie in die Option **Kontenadmin > Profile > Partner** aufrufen. Klicken Sie auf das Symbol **Suchen** und anschließend in den für die Partner im CPA angezeigten Suchergebnissen auf **Details anzeigen**.

**7.**

**Funktion**
**Element/Attribut**

**1.6 PartyInfo 2**
defaultMshChannelId 1

**Importiert/Manuell konfiguriert:** Importiert, aber nicht in WebSphere Partner Gateway gespeichert. Kann nicht manuell konfiguriert werden.

**WebSphere Partner Gateway-Konfiguration über die Benutzerschnittstelle:**

Diese Werte werden beim Importieren des CPA verwendet, um die Kanalattribute für Signalelemente von **Aktivität: MSHService (2.0)**, wie beispielsweise Ping, Sta-

tusanforderung, MessageError (Nachrichtenfehler) und Bestätigung, zu definieren. Diese Kanalwerte werden ihrerseits überschrieben, wenn im CPA ein Element "OverrideMshActionBinding" für ein bestimmtes Aktionselement vorhanden ist.

**8.**

**Funktion**
**Element/Attribut**

**1.6 PartyInfo 2**
defautMshPackageId 1

**Importiert/Manuell konfiguriert:** Importiert, aber nicht in WebSphere Partner Gateway gespeichert. Kann nicht manuell konfiguriert werden.

**WebSphere Partner Gateway-Konfiguration über die Benutzerschnittstelle:**

Diese Werte werden beim Importieren des CPA verwendet, um die Kanalattribute für Signalelemente von **Aktivität: MSHService (2.0)**, wie beispielsweise Ping, Statusanforderung, MessageError (Nachrichtenfehler) und Bestätigung, zu definieren. Diese Kanalwerte werden ihrerseits überschrieben, wenn im CPA ein Element "OverrideMshActionBinding" für ein bestimmtes Aktionselement vorhanden ist.

**9.**

**Funktion**
**Element/Attribut**

**1.6 PartyInfo 2**
PartyId 1, *

**Importiert/Manuell konfiguriert:** Importiert.

**WebSphere Partner Gateway-Konfiguration über die Benutzerschnittstelle:**

Sie können die Werte anzeigen, indem Sie in die Option **Kontenadmin > Profile > Partner** aufrufen. Klicken Sie auf das Symbol **Suchen** und anschließend in den für die Partner im CPA angezeigten Suchergebnissen auf **Details anzeigen**.

**10.**

**Funktion**
**Element/Attribut**

**1.6 PartyInfo 2**
type

**Importiert/Manuell konfiguriert:** Wird nicht importiert und kann nicht konfiguriert werden.

**11.**

**Funktion**
**Element/Attribut**

**1.6 PartyInfo 2**

```
PartyRef 1,*= (8.4.2)
- xlink:type F
- xlink:href 1
- type Fixed
- schemaLocation Implied
```

**Importiert/Manuell konfiguriert:** Wird nicht importiert und kann nicht konfiguriert werden.

**12.**

**Funktion**
**Element/Attribut**

**1.6 PartyInfo 2**
1.6.3 CollaborationRole 1,*

**Importiert/Manuell konfiguriert:** Importiert.

**WebSphere Partner Gateway-Konfiguration über die Benutzerschnittstelle:**

WebSphere Partner Gateway unterstützt mehrere CollaborationRole-Elemente.

**13.**

**Funktion**
**Element/Attribut**

**1.6 PartyInfo 2**

```
.6.3.1 ProcessSpecification 1
- name 1
- version 1
- xlink:type 1
- xlink:href
1 - uuid ImpliedReference 0,*  (8.4.4.6)
- URI 0, 1
 Transforms 1
  Transform
1 - Algorithm Fixed
 DigestMethod 1
  DigestValue 1
```

**Importiert/Manuell konfiguriert:** Wird nicht importiert.

**WebSphere Partner Gateway-Konfiguration über die Benutzerschnittstelle:**

Kann nicht konfiguriert werden.

**14.**

**Funktion**
**Element/Attribut**

**1.6 PartyInfo 2**

```
1.6.3.2 Role 1   (8.4.5)
- name 1
- xlink:type Fixed
- xlink:href 1
```

**Importiert/Manuell konfiguriert:** Das Attribut **xlink:href** wird importiert; andere Attribute werden nicht importiert.

**WebSphere Partner Gateway-Konfiguration über die Benutzerschnittstelle:**

Der Wert kann in den Kanalattributen konfiguriert werden. Rufen Sie **Kontenadmin > Verbindungen > Partnerverbindungen** auf. Suchen Sie die Kanäle, und greifen Sie auf das Kanalattribut **Rolle** zu.

**15.**

**Funktion**
**Element/Attribut**

**1.6 PartyInfo 2**
1.6.3.3 ApplicationCertificateRef 0,1 (8.4.6)

**Importiert/Manuell konfiguriert:** Importiert.

**WebSphere Partner Gateway-Konfiguration über die Benutzerschnittstelle:**

Der Wert kann nicht konfiguriert werden. Das für das Attribut **certId** angegebene Zertifikat wird in das Dateisystem, aber nicht in WebSphere Partner Gateway geladen.

**16.**

**Funktion**
**Element/Attribut**

**1.6 PartyInfo 2**
1.6.3.4 ApplicationSecurityDetailsRef 0, 1 (8.4.7)
- securityId 1

**Importiert/Manuell konfiguriert:** Wird nicht importiert.

**WebSphere Partner Gateway-Konfiguration über die Benutzerschnittstelle:**

Kann nicht konfiguriert werden.

**17.**

**Funktion**
**Element/Attribut**

**1.6.3.5 ServiceBinding 1**
1.6.3.5.1 Service 1 (8.4.9)
- type Implied

**Importiert/Manuell konfiguriert:** Importiert.

**WebSphere Partner Gateway-Konfiguration über die Benutzerschnittstelle:**

- **Service**: Dies ist der Name der Dokumentdefinition. Sie können den Wert anzeigen, indem Sie die Option **Hubadmin > Dokumentdefinitionen** aufrufen. Der Wert für **Service** wird als Dokumenttyp und Aktivität unter dem ebMS-Paket und dem Back-End-Integrationspaket angezeigt.
- **Type**: Der Typ wird als Kanalattribut unter **Kontenadmin > Verbindungen > Partnerverbindungen** verwendet. Suchen Sie die Kanäle und greifen Sie auf das Kanalattribut **Servicetyp** zu.

**18.**

**Funktion**
**Element/Attribut**

**1.6.3.5 ServiceBinding 1**
1.6.3.5.1 Service 1 (8.4.9)
- type  Implied

**Importiert/Manuell konfiguriert:** Importiert.

**WebSphere Partner Gateway-Konfiguration über die Benutzerschnittstelle:**

- **Service**: Dies ist der Name der Dokumentdefinition. Sie können den Wert anzeigen, indem Sie die Option **Hubadmin > Dokumentdefinitionen** aufrufen. Der Wert für **Service** wird als Dokumenttyp und Aktivität unter dem ebMS-Paket und dem Back-End-Integrationspaket angezeigt.
- **Type**: Der Typ wird als Kanalattribut unter **Kontenadmin > Verbindungen > Partnerverbindungen** verwendet. Suchen Sie die Kanäle und greifen Sie auf das Kanalattribut **Servicetyp** zu.

**19.**

**Funktion**
**Element/Attribut**

**1.6.3.5.2 CanSend 0, * (8.4.10)**
ThisPartyActionBinding 1
- action 1
- packageId 1
- xlink:href  Implied -
xlink:type Fixed
BusinessTransactionCharacteristics 1
- isNonRepudiationRequired
  All implied
isNonRepudiationReceiptRequired
- isConfidential
- isAuthenticated
- isAuthorizationRequired
- isTamperProof
- isIntelligibleCheckRequired
- timeToAcknowledgeReceipt
- timeToAcknowledgeAcceptance
- timeToPerform
- retryCountChannelId 1,*
ActionContext 0, 1
- binaryCollaboration 1
- businessTransactionActivity 1
- requestOrResponseAction 1
CollaborationActivity 0, 1
- name 1
OtherPartyActionBinding 0, 1
CanReceive 0, 1

**Importiert/Manuell konfiguriert:** Importiert.

**WebSphere Partner Gateway-Konfiguration über die Benutzerschnittstelle:**

- **CanSend**: Von **Backend Integration > ebMS >> Service name > Action of the partnerA** nach **ebMS > Service name > Action of partnerB** wird ein Kanal erstellt (wobei partnerB das Element **CanReceive** hat, das über das Element **OtherPartyActionBinding** gebunden wird).

- **Action**: Wird als Aktionselement in der Dokumentdefinition unter **Aktivität** importiert und erstellt.
- **packageId**: Die Attribute der referenzierenden Paket-ID werden als Kanalattribute gespeichert.
- **Xlink:href** und **xlink:type**: Werden nicht importiert und können nicht konfiguriert werden.
- **isNonRepudiationRequired, isNonRepudiationReceiptRequired, isIntelligibleCheckRequired, timeToAcknowledgeReceipt, timeToPerform**: Diese Attribute werden as Kanalattribute konfiguriert.
- **isConfidential, isAuthenticated, isTamperProof, isAuthorizationRequired, timeToAcknowledgeAcceptance, retryCount**: Werden nicht importiert und können nicht konfiguriert werden.
- **ChannelId** 1, *: Für WebSphere Partner Gateway wird nur ein Wert akzeptiert. Die referenzierenden Attribute werden als Kanalattribute definiert.
- **binaryCollaboration, businessTransactionActivity, requestOrResponseAction, CollaborationActivity**: Werden nicht importiert und können nicht konfiguriert werden.
- **OtherPartyActionBinding**: Wird importiert. Die Referenz wird verwendet, um den Kanal zu erstellen.
- **CanReceive**: Wird importiert und wird als synchron behandelt, wenn ein weiterer Kanal für dieselbe Verbindung vorhanden ist.

**20.**

**Funktion**
**Element/Attribut**

**1.6.3.5.2 CanSend 0, * (8.4.10)**
1.6.3.5.3 CanReceive 0, * (8.4.11)
ThisPartyActionBinding 1
OtherPartyActionBinding 0, 1
CanSend 0, 1

**Importiert/Manuell konfiguriert:** Importiert.

**WebSphere Partner Gateway-Konfiguration über die Benutzerschnittstelle:**
- **CanReceive**: Von **ebMS > Service name > Action of the partnerA** nach **Backend Integration > ebMS > Service name > Action of partnerB** wird ein Kanal erstellt (wobei partnerB das Element **CanSend** hat, das über das Element **OtherPartyActionBinding** gebunden wird).
- **OtherPartyActionBinding**: Wird importiert. Die Referenz wird verwendet, um den Kanal zu erstellen.
- **CanSend**: Wird importiert und wird als synchron behandelt, wenn ein weiterer Kanal für dieselbe Verbindung vorhanden ist.

**21.**

**Funktion**
**Element/Attribut**

**1.6.3.5.2 CanSend 0, * (8.4.10)**
1.6.4 Certificate 1, * (8.4.18)
- certId KeyInfo

**Importiert/Manuell konfiguriert:** Importiert.

**WebSphere Partner Gateway-Konfiguration über die Benutzerschnittstelle:**

Das Zertifikat wird im Dateisystem gespeichert und muss mithilfe der Option **Kontenadmin > Profile > Zertifikate** manuell in WebSphere Partner Gateway geladen werden.

**22.**

**Funktion**
**Element/Attribut**

**1.6.3.5.2 CanSend 0, * (8.4.10)**
1.6.5 SecurityDetails 0, * (8.4.18)
- securityId 1 TrustedAnchor 0, *
AnchorCertificateRef 1, *
SecurityPolicy 0, 1

**Importiert/Manuell konfiguriert:** Wird nicht importiert. Nur die Referenzzertifikate werden in das Dateisystem geladen.

**23.**

**Funktion**
**Element/Attribut**

**1.6.3.5.2 CanSend 0, * (8.4.10)**
1.6.6 DeliveryChannel 1, * (8.4.22)
- channelId 1
- transportId 1
- docExchangeId1
MessagingCharacteristics 1
- syncReplyMode All implied
- ackRequested attribute
- ackSignatureRequested
- duplicateElimination
- actor

**Importiert/Manuell konfiguriert:** Importiert.

**WebSphere Partner Gateway-Konfiguration über die Benutzerschnittstelle:**

- **channelId**: Die referenzierenden Attribute werden als Kanalattribute definiert.
- **transportId**: Die referenzierenden Attribute werden verwendet, um das Gateway zu erstellen und als Standardgateway für den Kanal zu definieren.
- **docExchangeId**: Die referenzierenden Attribute werden als Kanalattribute definiert.
- **syncReplyMode, ackRequested, ackSignatureRequested, duplicateElimination, actor**: Diese Attribute werden als Kanalattribute importiert und konfiguriert.

**24.**

**Funktion**
**Element/Attribut**

**1.6.3.5.2 CanSend 0, * (8.4.10)**
1.6.7 Transport 1, * (8.4.24)
- transportId 1
TransportSender 0, 1 (8.4.25)
TransportProtocol 1
- version 1
ImpliedAccessAuthentication 0, *
TransportClientSecurity 0, 1

```
TransportSecurityProtocol 1
- version 1
ImpliedClientCertificateRef  0, 1
- certId 1
ServerSecurityDetailsRef 0, 1
- securityId 1EncryptionAlgorithm 0, *
- minimumStrength All Implied
- oid
- w3c
- enumeratedType
```

**Importiert/Manuell konfiguriert:** Wird nicht importiert.

**25.**

**Funktion**
**Element/Attribut**

**1.6.3.5.2 CanSend 0, * (8.4.10)**

```
1.6.7 Transport 1, * (8.4.24)
TransportReceiver 0, 1 (8.4.33)
TransportProtocol 1
- version 1
ImpliedEndpoint 1, *
- uri 1
- type  ImpliedAccessAuthentication 0, *
TransportServerSecurity 0, 1
TransportSecurityProtocol 1
- version 1
ServerCertificateRef 1
- certId 1
ClientSecurityDetailsRef 0, 1
- SecurityId 1
EncryptionAlgorithm 0, *
- minimumStrength All Implied
- oid
- w3c
- enumeratedType
```

**Importiert/Manuell konfiguriert:** Importiert.

**WebSphere Partner Gateway-Konfiguration über die Benutzerschnittstelle:**

- **TransportProtocol**: Definiert das Gatewayprotokoll.
- **Version**: Definiert die Version des Gatewayprotokolls.
- **URL**: Definiert die URL des Gateways. Diese Werte können über **Kontenadmin > Profile > Partnersuche** angezeigt werden. Klicken Sie für alle Partner und für den ausgewählten Partner auf die Registerkarte **Ziele**. Die übrigen Attributwerte werden nicht importiert.

**26.**

**Funktion**
**Element/Attribut**

**1.6.3.5.2 CanSend 0, * (8.4.10)**

```
1.6.8 DocExchange (8.4.39)
- docExchangeId 1 1.6.8.2.1
ebXMLSenderBinding 0, 1 (8.4.40)
- version ReliableMessaging 0, 1
Retries 0, 1
RetryInterval 0, 1
MessageOrderSemantics 1
PersistDuration 0, 1
```

```
SenderNonRepudiation 0, 1
NonRepudiationProtocol 1
- version 1 Implied
HashFunction 1
SignatureAlgorithm 1
- oid All implied
- w3c
- enumeratedTypeSigningCertificateRef 1
- certId 1
SenderDigitalEnvelope 0, 1
DigitalEnvelopeProtocol 1
- version 1  EncryptionAlgorithm 1
- minimumStrength All Implied
- oid
- w3c
- enumeratedType
```

**Importiert/Manuell konfiguriert:** Importiert.

**WebSphere Partner Gateway-Konfiguration über die Benutzerschnittstelle:**

**Retries, RetryInterval, MessageOrderSemantics, PersistDuration, HashFunction, SignatureAlgorithm, DigitalEnvelopeProtocol, EncryptionAlgorithm**: Diese Werte werden als Kanalattribute importiert und gespeichert. Sie können über **Kontenadmin > Verbindungen > Partnerverbindungen** angezeigt werden. Suchen Sie die Kanäle, und rufen Sie **Kanalattribute** auf. Die übrigen Werte werden nicht importiert und können nicht konfiguriert werden.

**27.**

**Funktion**

**Element/Attribut**

**1.6.3.5.2 CanSend 0, * (8.4.10)**

```
1.6.8.2 ebXMLReceiverBinding 0, 1 (8.4.53)
- version 1
ReliableMessaging 0, 1
Retries 0, 1
RetryInterval 0, 1
MessageOrderSemantics 1
ReceiverNonRepudiation 0, 1
NonRepudiationProtocol 1
- version 1
HashFunction 1
SigningAlgorithm 1
- oid All Implied
- w3c
- enumeratedTypeSigningSecurityDetailsRef 1
- securityId 1ReceiverDigitalEnvelope 0, 1
DigitalEnvelopeProtocol 1
- version 1
EncryptionAlgorithm 1
- minimumStrength All Implied
- oid
- w3c
- enumeratedTypeEncryptionCertificateRef 1
- certId 1
NamespaceSupported 0, *
- location 1
- version Implied
```

**Importiert/Manuell konfiguriert:** Importiert.

**WebSphere Partner Gateway-Konfiguration über die Benutzerschnittstelle:**

**Retries, RetryInterval, MessageOrderSemantics, PersistDuration, HashFunction, SignatureAlgorithm, DigitalEnvelopeProtocol, EncryptionAlgorithm**: Diese Werte werden als Kanalattribute importiert und gespeichert. Sie können über **Kontenadmin > Verbindungen > Partnerverbindungen** angezeigt werden. Suchen Sie die Kanäle, und rufen Sie **Kanalattribute** auf. Die übrigen Werte werden nicht importiert und können nicht konfiguriert werden.

**28.**

**Funktion**
**Element/Attribut**

```
1.6.3.5.2 CanSend 0, * (8.4.10)
        1.6.9  OverrideMshActionBinding 0, *  (8.4.58)
        - action 1
        - channelId
```

**Importiert/Manuell konfiguriert:** Importiert.

**WebSphere Partner Gateway-Konfiguration über die Benutzerschnittstelle:**

Für die angegebene Aktion werden die Kanalattribute mithilfe der Referenzkanal-ID definiert.

**29.**

**Funktion**
**Element/Attribut**

```
1.6.3.5.2 CanSend 0, * (8.4.10)
        1.7 SimplePart (8.5)
        - id 1
        - mimetype 1
        - mimparameters  Implied
        - xlink:role
          ImpliedNamespaceSupported 0, *
```

**Importiert/Manuell konfiguriert:** Importiert.

**WebSphere Partner Gateway-Konfiguration über die Benutzerschnittstelle:**

**Mimetype**: Werte werden als Kanalattribute importiert und gespeichert. Die übrigen Werte werden nicht importiert und können nicht konfiguriert werden.

**30.**

**Funktion**
**Element/Attribut**

```
1.6.3.5.2 CanSend 0, * (8.4.10)
        1.8 Packaging (8.6)
        - id 1
        ProcessingCapabilities 1, *
        - parse 1
        - generate 1
        CompositeList 0, *
        Composite 0, *
        - mimetype 1
        - id 1
        - mimeparameters ImpliedConstituent 1, *
        - idref 1
        - excludeFromSignature Implied
```

```
- minOccurs Implied
- maxOccurs Implied
SignatureTransform 0, 1
Transform 1, *
EncryptionTransform 0, 1
Transform 1, *
```

**Importiert/Manuell konfiguriert:** Importiert.

**WebSphere Partner Gateway-Konfiguration über die Benutzerschnittstelle:**

**Composite : mimetype, mimeparameters, Constituent-idref, Constituent- excludeFromSignature, signatureTransform, encryptionTransform, Algorithm**: Diese Werte werden als Kanalattribute in **Kontenadmin > Verbindungen > Partnerverbindungen** importiert und gespeichert. Suchen Sie die Kanäle, und rufen Sie **Kanalattribute** auf. Die übrigen Werte werden nicht importiert und können nicht konfiguriert werden.

**31.**

**Funktion**
**Element/Attribut**

```
1.6.3.5.2 CanSend 0, * (8.4.10)
Encapsulation 0, *
- mimetype 1
- id 1
- mimeparameters  ImpliedConstituent 1
- idref 1
- excludeFromSignature Implied
- minOccurs Implied
- maxOccurs Implied
SignatureTransform 0, 1
Transform 1, *
EncryptionTransform 0, 1
Transform 1, *
```

**Importiert/Manuell konfiguriert:** Importiert.

**WebSphere Partner Gateway-Konfiguration über die Benutzerschnittstelle:**

**Encapsulation: mimetype, mimeparameters, Constituent-idref, Constituent- excludeFromSignature, signatureTransform, encryptionTransform, Algorithm**: Diese Werte werden als Kanalattribute in **Kontenadmin > Verbindungen > Partnerverbindungen** importiert und gespeichert. Suchen Sie die Kanäle, und rufen Sie **Kanalattribute** auf. Die übrigen Werte werden nicht importiert und können nicht konfiguriert werden.

**32.**

**Funktion**
**Element/Attribut**

```
1.6.3.5.2 CanSend 0, * (8.4.10)
1.9 Signature 0, 1 (8.7)
ds:Signature 1,3
SignedInfo 1
CanonicalizationMethod 0, 1
SignatureMethod 1
```

```
- AlgorithmReference 1, *
- URI FixedTransforms 1
Transform 1
- Algorithm Fixed
```

**Importiert/Manuell konfiguriert:** Wird nicht importiert.

**WebSphere Partner Gateway-Konfiguration über die Benutzerschnittstelle:**

Kann nicht konfiguriert werden.

**33.**

**Funktion**
**Element/Attribut**

**1.6.3.5.2 CanSend 0, * (8.4.10)**

```
1.10 Comments 0, * (8.8)
- xml:lang
```

**Importiert/Manuell konfiguriert:** Wird nicht importiert.

**WebSphere Partner Gateway-Konfiguration über die Benutzerschnittstelle:**

Kann nicht konfiguriert werden.

## Verbindungsattribute

In der folgenden Tabelle werden die Routingobjektattribute aufgelistet, die in den Geschäftskanälen der Nachricht in der ebMS-Verpackung angezeigt werden können.

Klicken Sie auf **Kontenadmin > Verbindungen > Partnerverbindungen** und wählen Sie die Quelle bzw. das Ziel aus. Klicken Sie auf **Attribute** auf der Quellenseite, wenn der Kanal für eingehende ebMS-Nachrichten verwendet wird; klicken Sie auf **Attribute** auf der Zielseite, wenn der Kanal für ausgehende ebMS-Nachrichten verwendet wird. Blättern Sie in der daraufhin angezeigten Anzeige nach unten und klicken Sie auf den Ordner **Aktion**.

*Tabelle 21. Verbindungsattribute*

| CPA-XML-Attribute | Standardwert | Mögliche Werte | Angezeigter Text in WebSphere Partner Gateway |
|---|---|---|---|
| isNonRepudiationRequired | False | True/false - Wird als Yes/No zugeordnet | Unbestreitbarkeit erforderlich |
| isNonRepudiationReceiptRequired | False | True/false - Wird als Yes/No zugeordnet | Unbestreitbarkeit des Empfangs |
| timeToAcknowledgeReceipt | | | Bestätigungszeit |
| Retries | 3 | Beliebige Zahl | Wiederholungszähler |
| MessageOrderSemantics | Not Guaranteed | "Guaranteed" "NotGuaranteed" | Semantik der Nachrichtenreihenfolge |
| PersistDuration | P1D | | Dauer der Persistenz |

*Tabelle 21. Verbindungsattribute (Forts.)*

| CPA-XML-Attribute | Standardwert | Mögliche Werte | Angezeigter Text in WebSphere Partner Gateway |
|---|---|---|---|
| syncReplyMode | None | "mshSignalsOnly"<br><br>"signalsOnly"<br><br>"responseOnly"<br><br>"signalsAndResponse"<br><br>"none"<br><br>(In Phase 2 versetzt) | Synchroner Antwortmodus |
| ackRequested | perMessage | "always" - Gibt an, dass eine Bestätigung immer angefordert werden soll.<br><br>"never" - Gibt an, dass nie eine Bestätigung angefordert werden soll.<br><br>“perMessage” - Gibt an, dass die Bestätigung abhängig vom Element "ack" im ebXML-Dokument angefordert oder nicht angefordert werden soll. | Bestätigung angefordert |
| ackSignatureRequested | perMessage | "always"<br><br>"never"<br><br>"perMessage" | Bestätigung mit Signatur angefordert |
| duplicateElimination | perMessage | "always"<br><br>"never"<br><br>"perMessage" | Doppelter Ausschluss |
| Actor | "urn:oasis:names: tc:ebxml-msg: actor:nextMSH" | "urn:oasis:names:tc: ebxml-msg:actor: nextMSH""urn:oasis: names:tc:ebxml-msg: actor:toPartyMSH" | Actor |
| PartyRole | - | Rolle in CPA | Rolle |
| Wiederholungsintervall | 270 | - | Wiederholungsintervall |
| NonRepudiationProtocol | - | http://www.w3.org/2000/09/ xmldsig# | Signaturprotokoll |
| SignatureAlgorithm | - | 1. http://www.w3.org.2000/ 09/xmldsig#dsa-sha1<br><br>2. http://www.w3.org/2000/ 09/xmldsig#rsa-sha1<br>**Anmerkung:** In ebMS wird 'hmac-sha1' nicht unterstützt. | Signaturalgorithmus |
| isEncryptionRequired | No | True/false - Wird als Yes/No zugeordnet | Verschlüsselung erforderlich |
| isCompressionRequired | No | True/false - Wird als Yes/No zugeordnet | Komprimierung erforderlich |
| /Packaging/CompositeList /Encapsulation/Constituent: mimetype | - | | MIME-Typ komprimieren |
| /tp:SenderDigitalEnvelope /tp:DigitalEnvelopeProtocol | - | SMIME XMLEncryption | Verschlüsselungsprotokoll |

*Tabelle 21. Verbindungsattribute (Forts.)*

| CPA-XML-Attribute | Standardwert | Mögliche Werte | Angezeigter Text in WebSphere Partner Gateway |
|---|---|---|---|
| /tp:SenderDigitalEnvelope /EncryptionAlgorithm | - | 3des-cbc, aes128-cbc, aes-256-cbc | Verschlüsselungsalgorithmus |
| /tp:ReceiverDigitalEnvelope /tp:DigitalEnvelopeProtocol | - | SMIME XMLEncryption | Verschlüsselungsprotokoll |
| /tp:ReceiverDigitalEnvelope /EncryptionAlgorithm | - | 3des-cbc, aes128-cbc, aes-256-cbc | Verschlüsselungsalgorithmus |
| /Packaging/CompositeList /Encapsulation tp:MimeType | - | text/xml application/pkcs7-mime | MIME-Typ für Verschlüsselung |
| /Packaging/CompositeList /Encapsulation- tp:mimeparameters | - | | MIME-Parameter für Verschlüsselung |
| /Packaging/CompositeList /Encapsulation/Constituent: mimetype | - | | Bestandteile verschlüsseln |
| /Packaging/CompositeList / Composite/ tp:mimeparameters | - | | MIME-Parameter für Paket |
| /Packaging/CompositeList / Composite /Constituent: mimetype | - | | Bestandteile verpacken |
| /Packaging/CompositeList /Composite/Contituent /excludeFromSignature: mimetype | - | | Von Signatur ausschließen |
| /Packaging/CompositeList / Composite/Contituent/ SignatureTransform | - | 1. BASE64<br>2. ENVELOPED<br>3. XPATH<br>4. XPATH2<br>5. XSLT | Algorithmus für Signaturtransformation |
| /Packaging/CompositeList /Composite/Contituent/ EncryptionTransform | - | 1. BASE64<br>2. ENVELOPED<br>3. XPATH<br>4. XPATH2<br>5. XSLT | Algorithmus für Verschlüsselungstransformation |

### Einschränkungen

Im Folgenden werden die Einschränkungen bei der Zuordnung des CPA (Collaboration Profile Agreement) zu WebSphere Partner Gateway aufgelistet:

1. Zertifikate aus dem CPA werden nicht in WebSphere Partner Gateway importiert. Sie werden im Dateisystem gespeichert und müssen vom Administrator manuell überprüft und in WebSphere Partner Gateway hochgeladen werden.
2. WebSphere Partner Gateway kann die synchronen und asynchronen Datenflüsse des CPA verarbeiten. Dies gilt jedoch nicht, wenn mehrere Bindungen denselben Aktionswert verwenden.
3. Nur neunstellige numerische DUNS-IDs werden unterstützt (freie Formate werden nicht unterstützt).

## ebMS-SOAP-Header zu WebSphere Partner Gateway-Headern zuordnen

Die ebMS-Spezifikation 2.0 definiert eine Reihe von verbindlichen Headern, die in einer ebMS-SOAP-Nachricht vorhanden sein müssen. Die folgende Tabelle zeigt die Zuordnung zwischen einigen dieser erforderlichen ebMS-Header und den WebSphere Partner Gateway-Headern, aus denen die diesbezüglichen Werte stammen.

*Tabelle 22. ebMS-SOAP-Header und entsprechende WebSphere Partner Gateway-Header*

| Laufende Nummer | Headername in ebMS-SOAP-Nachricht | Entsprechender Headername in WebSphere Partner Gateway |
|---|---|---|
| 1 | From PartyId | “x-aux-sender-id” (vom Back-End-System festgelegt) |
| 2 | From Role | Rollenattribut auf der Quellenseite der Dokumentdefinitionsattribute. |
| 3 | From PartyId Type | Kann vom Benutzer nicht konfiguriert werden. Wenn PartyId auf den Wert DUNS gesetzt ist, ist “type” auf “urn:duns” gesetzt. Ansonsten lautet der Wert “string”. |
| 4 | To PartyId | “x-aux-receiver-id” (vom Back-End-System festgelegt) |
| 5 | To Role | Rollenattribut auf der Zielseite der Dokumentdefinitionsattribute. |
| 6 | To PartyId Type | Kann vom Benutzer nicht konfiguriert werden. Wenn PartyId auf den Wert "duns" gesetzt ist, ist “type” auf “urn:duns” gesetzt. Ansonsten lautet der Wert “string”. |
| 7 | CPAId | Wenn die Datenbank ein CPA enthält, verwendet WebSphere Partner Gateway die im CPA enthaltene CPA-ID. Andernfalls kann der Benutzer das CPA-ID-Attribut konfigurieren, das auf der Zielseite der Dokumentdefinitionsattribute vorhanden ist. Wenn der Benutzer dieses Attribut nicht konfiguriert hat und kein CPA vorhanden ist, generiert WebSphere Partner Gateway eine CPA-ID, die auf den Partner-IDs basiert. |
| 8 | Conversation Id | “x-aux-process-instance-id” (vom Back-End-System festgelegt). Wenn das Back-End-System diese ID nicht festlegt, generiert WebSphere Partner Gateway eine eigene Dialog-ID (ConversationId). |
| 9 | Service | Der Dokumentdefinitionswert für die Zielpartnerverbindung.<br>**Anmerkung:** Die Dokumentdefinition und die Aktivität sind in einem ebMS-Fluss identisch. |
| 10 | Service Type | ServiceType-Attribut auf der Zielseite der Dokumentdefinitionsattribute. |
| 11 | Action | Der Aktionswert für die Zielpartnerverbindung. |
| 12 | MessageId | “x-aux-msg-id” (vom Back-End-System festgelegt). Wenn das Back-End-System diese ID nicht festlegt, generiert WebSphere Partner Gateway eine eigene Nachrichten-ID (MessageId). |

Wenn Sie eine synchrone ebMS-Antwort an ein ebMS-Anforderungsdokument senden, muss das Back-End-System den Header “x-aux-request-msg-id” für das Antwortdokument festlegen. Der Wert dieses Headers ist die Nachrichten-ID der Anforderungsnachricht. Darüber hinaus sollte sich das Antwortdokument im selben Dialog wie das Anforderungsdokument befinden. Dies bedeutet, dass “x-aux-process-instance-id” für die Antwort mit der Dialog-ID der Anforderung identisch sein sollte.

Die Dialog-ID und die Nachrichten-ID des Anforderungsdokuments werden als “x-aux-process-instance-id” bzw. “x-aux-msg-id” an das Back-End-System gesendet.

## ebMS-Dokumente anzeigen

Die RosettaNet-Anzeige zeigt Informationen zu ebMS-Dokumenten an. Sie können unformatierte Dokumente und zugeordnete Dokumentverarbeitungsdetails und Ereignisse mithilfe von bestimmten Suchkriterien anzeigen. Diese Informationen sind nützlich, wenn Sie zu ermitteln versuchen, ob ein Dokument erfolgreich zugestellt wurde bzw. worin die Ursache eines Fehlers besteht.

Gehen Sie wie folgt vor, um die ebMS-Anzeige zu öffnen:

1. Klicken Sie auf **Anzeigen > ebMS-Anzeige**.
2. Wählen Sie die entsprechenden Suchkriterien aus.
3. Klicken Sie auf **Suchen**.

In der ebMS-Anzeige sind Dokumente nach Dialog-ID organisiert. Dies bedeutet, dass alle Dokumente mit derselben Dialog-ID in einer Gruppe zusammengefasst werden und durch Klicken auf das Symbol für weitere Details auf der linken Seite einer Zeile mit der Dialog-ID angezeigt werden können. Wenn Sie auf das Symbol für weitere Details klicken, wird eine neue Seite mit allen Nachrichten in diesem Dialog angezeigt. Oben auf der Seite befindet sich das Attribut "Dialogstatus". Der Wert dieses Attributs ist die nächste Nachricht, die in diesem Dialog erwartet wird.

### Status für eine ebMS-Nachricht anfordern

Führen Sie die folgenden Schritte aus, um den Status einer ebMS-Nachricht anzufordern:

1. Nachdem Sie das gewünschte ebMS-Dokument gefunden haben, klicken Sie auf das Symbol **Details anzeigen**, das sich daneben befindet.
2. Klicken Sie auf **Status anfordern**. Daraufhin wird der Status dieses Dokuments angezeigt.

Klicken Sie auf **Status anzeigen**, um den Status zu aktualisieren.

Erfolgt die Konfiguration für ebMS Status Request- und ebMS Status Response-Dokumente (Statusanforderung/Statusantwort), müssen Sie Folgendes beachten:

- Nur die Status Request-Verbindung muss erstellt werden. Die Status Response-Verbindung verwendet die vorhandene Status Request-Verbindung.
- Für eine Status Request-Verbindung vom internen Partner zu einem externen Partner wird das Quellenziel der Verbindung nicht verwendet.
- Für eine Status Request-Verbindung von einem externen Partner zum internen Partner wird das Quellenziel der Verbindung zum Zurücksenden des Status Response-Antwortdokuments an den externen Partner verwendet.
- Verfügt ein Benutzer über kein CPA, muss er die B2B-Funktionalität aktivieren und einen Kanal für die ebMS Status Request-Nachricht wie folgt erstellen:
  - Für eine eingehende ebMS Status Request-Nachricht

    Die B2B-Funktionalität für die Quellenseite sollte wie folgt aussehen:

    Paket: N/A (N/A)
    Protokoll: ebMS (2.0)
    Dokumenttyp: MSHService (2.0)
    Aktivität: MSHService (2.0)
    Aktion: StatusRequest(N/A)

    Die B2B-Funktionalität für die Zielseite sollte wie folgt aussehen:

Paket: ebMS (2.0)
Protokoll: ebMS (2.0)
Dokumenttyp: MSHService (2.0)
Aktivität: MSHService (2.0)
Aktion: StatusRequest(N/A)

– Für eine ausgehende ebMS Status Request-Nachricht

Die B2B-Funktionalität für die Quellenseite sollte wie folgt aussehen:

Paket: ebMS (2.0)
Protokoll: ebMS (2.0)
Dokumenttyp: MSHService (2.0)
Aktivität: MSHService (2.0)
Aktion: StatusRequest(N/A)

Die B2B-Funktionalität für die Zielseite sollte wie folgt aussehen:

Paket: N/A (N/A)
Protokoll: ebMS (2.0)
Dokumenttyp: MSHService (2.0)
Aktivität: MSHService (2.0)
Aktion: StatusRequest(N/A)

Dann sollte der Benutzer den Kanal aktivieren und auf der Seite für die Partnerverbindungen Ziele festlegen.

**Anmerkung:** Diese Informationen gelten für ebMS-Fehler und -Bestätigungen. Die Aktion für diese Kanäle wird in MessageError (Nachrichtenfehler) bzw. Acknowledgment (Bestätigung) geändert.

## Pingsignal für ebMS-Partner absetzen

Über die Seite **Partnerverbindung testen** können Sie ebMS-Partner mit Ping überprüfen. Dies bedeutet, dass Sie eine Pingnachricht an einen Partner senden können, der mit einer Pongnachricht antwortet, sofern er aktiv und empfangsbereit ist. Sobald Sie ein CPA hochladen, wird der Kanal für die Ping- und Pongnachrichten erstellt.

Die Überprüfung mit Ping funktioniert nur, wenn mit dem beteiligten Partner entsprechende Verbindungen definiert wurden. Detaillierte Informationen finden Sie im Abschnitt zum Überprüfen von ebMS-Partnern mit Ping im Handbuch *WebSphere Partner Gateway Hubkonfiguration*.

Führen Sie die folgenden Schritte aus, um ein Pingsignal für einen ebMS-Partner abzusetzen:

1. Klicken Sie auf **Tools** > **Partnerverbindung testen**.
2. Wählen Sie für **Befehl** die Option **PING ebMS** aus.
3. Wählen Sie **Absenderpartner** und **Empfängerpartner** aus.
4. Wählen Sie optional ein **Ziel** aus, oder geben Sie eine **URL** an.
5. Klicken Sie auf **Testen**, um eine Pingnachricht zu senden.

Wenn Sie den Status der Pingnachricht ermitteln möchten, klicken Sie auf **Ping-Status**. Daraufhin wird der Status für die letzte Ping-Anforderung unter **Ergebnisse** angezeigt.

**Anmerkung:** Die letzte Pinganforderung wurde möglicherweise durch das erneute Senden eines vorhandenen Pingdokuments über **Partnerverbindung testen** oder über eine Dokumentanzeige eingeleitet.

# Web-Services

Ein Partner kann einen Web-Service aufrufen, der vom internen Partner bereitgestellt wird. In ähnlicher Weise kann der interne Partner einen Web-Service aufrufen, der von einem Partner bereitgestellt wird. Der Partner oder der interne Partner ruft den Web-Service über den WebSphere Partner Gateway-Server auf. WebSphere Partner Gateway agiert als Proxy-Server, der die Web-Serviceanforderung an den Web-Service-Provider übergibt und die Antwort synchron vom Provider an den Requester zurückgibt.

Dieser Abschnitt enthält die folgenden Informationen für das Konfigurieren eines Web-Service zur Verwendung durch einen Partner oder den internen Partner:

- Die Partner für einen Web-Service identifizieren.
- Dokumentdefinition für einen Web-Service konfigurieren.
- Dokumentdefinitionen der B2B-Funktionalität des Partners hinzufügen.
- Einschränkungen und Begrenzungen der Web-Serviceunterstützung.

## Die Partner für einen Web-Service angeben

Wenn ein Web-Service vom internen Partner zur Verwendung durch die Partner bereitgestellt wird, ist für WebSphere Partner Gateway erforderlich, dass der interne und die externen Partner identifiziert werden. In WebSphere Partner Gateway können Sie mehrere interne Partner erstellen, von denen einer als standardmäßiger interner Partner konfiguriert wird. Um den standardmäßigen internen Partner zu überschreiben und einen eigenen internen Partner auszuwählen, müssen Sie zusätzliche Parameter an den WebSphere Partner Gateway-Empfänger senden, wie beispielsweise **FromPartnerBusinessId** oder **ToPartnerBusinessId**, abhängig davon, ob es sich um einen ausgehenden (outbound) oder eingehenden (inbound) Datenfluss handelt. Wenn zwei unterschiedliche externe Partner-IDs über die Basisauthentifizierung und die URL angegeben werden, hat die Basisauthentifizierung Vorrang, was zu einem Fehler führen kann. Die verschiedenen möglichen Abfragezeichenfolgen für den ausgehenden Datenfluss lauten wie folgt: `<Receiver-URL>?to=<business id>` and `<Receiver-URL?to=<business id>&from=<business id>`. Die verschiedenen möglichen Abfragezeichenfolgen für den eingehenden Datenfluss lauten wie folgt: `<Receiver-URL` and `Receiver-URL?to=business id`. Bei einem eingehenden Datenfluss ist die **Basisauthentifizierung** obligatorisch.

## Dokumentdefinitionen erstellen

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

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

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

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

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

Die Datei sollte das Folgende enthalten:

```
Name                    Path

helloworldRPC.wsdl

bindingRPC.wsdl

porttypeRPC.wsdl                port\
```

Wenn eine WSDL-Dateidefinition eines Web-Services hochgeladen wird, wird die ursprüngliche WSDL als Validierungszuordnung gespeichert. (Web-Service-Nachrichten werden von WebSphere Partner Gateway gegenüber der WSDL nicht validiert.) Dies wird als *private* WSDL bezeichnet.

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

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

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

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

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

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

Sehen Sie sich jetzt dieses Beispiel an:

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

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

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

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

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

     Die URL-Adresse ist in der Regel dieselbe wie das HTTP-Produktionsziel, das in **Ziele** definiert ist.
   - Geben Sie für einen von einem Partner bereitgestellten Web-Service (der vom internen Partner aufgerufen wird) die öffentliche URL-Adresse des Partners mit einer Abfragezeichenfolge ein: Beispiel:

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

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

Die Dateien befinden sich in: `B2BIntegrate\packagingSchemas`

## Dokumentdefinition manuell erstellen

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

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

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

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

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

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

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

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

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

WebSphere Partner Gateway würde nach einer definierten Web-Serviceaktion mit diesem Code suchen:

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

Beispiel einer SOAP-Anforderungsnachricht im RPC-Bindungsstil:

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

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

WebSphere Partner Gateway würde nach einer definierten Web-Serviceaktion mit diesem Code suchen:

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

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

Bei einer Bindung **document-literal** sollte der Namespace und Name des ersten untergeordneten Elements vom `soap:body` einer SOAP-Anforderungsnachricht der Namespace und Name des XML-Attributs `element` im Element `part` der Eingabedefinition `message` für den Web-Service sein.

## Interaktionen erstellen

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

Verwenden Sie die folgende Prozedur, um Interaktionen zu erstellen.

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

## Einschränkungen und Begrenzungen der Web-Serviceunterstützung

WebSphere Partner Gateway unterstützt die folgenden Standards:

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

**Anmerkung:**
- WebSphere Partner Gateway bietet eine teilweise Unterstützung für Basic Profile 1.0.
- 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).

Weitere Informationen finden Sie in den Abschnitten „Validierung des SOAP-Umschlags" auf Seite 101 und „Aus SOAP-Umschlag entfernen" auf Seite 101.

## cXML-Dokumente

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

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

Document Manager führt die DTD-Validierung für cXML-Dokumente aus; WebSphere Partner Gateway stellt jedoch keine cXML-DTDs bereit. Sie können diese unter 'www.cxml.org' herunterladen, und sie dann in WebSphere Partner Gateway über das Validierungszuordnungsmodul in Community Console hochladen. Nachdem Sie die DTD hochgeladen haben, ordnen Sie diese dem cXML-Dokumenttyp zu. Weitere Informationen zum Zuordnen der DTD zum cXML-Dokumenttyp finden Sie in „Zuordnungen zu Dokumentdefinitionen zuordnen" auf Seite 170.

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

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

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

```
<Header>
<From>

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

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

WebSphere Partner Gateway verwendet nicht die Informationen im Absenderelement.

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

## cXML-Dokumenttypen

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

### Anforderung

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

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

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

**cXML-Element**
: **Dokumentdefinition**

**cXML-DOCTYPE**
: Protokoll

**DTD-Version**
: Protokollversion

**Anforderungstyp Beispiel: OrderRequest**
: Dokumenttyp

### Antwort

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

- ProfileResponse

- PunchOutSetupResponse
- GetPendingResponse

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

**cXML-Element**
**Dokumentdefinition**

**cXML-DOCTYPE**
Protokoll

**DTD-Version**
Protokollversion

**Antworttyp Beispiel: ProfileResponse**
Dokumenttyp

## Nachricht

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

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

```
<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 Dokumentdefinitionen in WebSphere Partner Gateway:

**cXML-Element**
**Dokumentdefinition**

**cXML-DOCTYPE**
Protokoll

**DTD-Version**
Protokollversion

**Nachricht**
Dokumenttyp

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

Eine Nachricht kann über die folgenden Attribute verfügen:

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

## Die Header "Content-Type" und angehängte Dokumente

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

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

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

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

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

## Gültige cXML-Interaktionen

WebSphere Partner Gateway unterstützt die folgenden cXML-Dokumentdefinitionsinteraktionen:

- Vom externen Partner zum internen Partner: None/cXML zu None/cXML mit Pass-Through und Validierung
- Vom internen Partner zum externen Partner:
  - None/cXML zu None/cXML mit Pass-Through und Validierung.
  - None/XML zu None/cXML mit Pass-Through, Validierung und Transformation.

## Dokumentdefinitionen erstellen

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

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

1. Klicken Sie auf **Hubadmin** > **Hubkonfiguration** > **Dokumentdefinition**.
2. Klicken Sie auf **Dokumentdefinition erstellen**. Die Seite **Dokumentdefinitionen erstellen** wird angezeigt.
3. Wählen Sie **Dokumenttyp** als Dokumenttyp aus.
4. Führen Sie eine der folgenden Aufgaben abhängig vom Dokumenttyp aus:
   - Geben Sie für Anforderungen den Anforderungstyp, z. B. `OrderRequest`, im Feld **Name** ein.

- Geben Sie für Antworten, falls das Element Response über keine untergeordneten Tags außer `<Status>` verfügt, `Response` ein. Geben Sie andernfalls den nächsten Tag-Namen ein, der auf `<Status>` folgt. Im nachfolgenden Beispiel würden Sie `Response` für das erste Element `Response` und `ProfileResponse` für das zweite Element eingeben.

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

5. Geben Sie **1.0** für **Version** ein.

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

## Interaktionen erstellen

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

Verwenden Sie die folgende Prozedur, um Interaktionen zu erstellen.

1. Klicken Sie auf **Hubadmin > Hubkonfiguration > Dokumentdefinition > Interaktionen verwalten**.
2. Klicken Sie in der Anzeige **Interaktionen verwalten** auf den Link **Interaktion erstellen**.
3. Wenn das cXML-Dokument die Quelle ist, erweitern Sie unter **Quelle** den Eintrag **Paket: None** und **Protokoll: cXML** und wählen Sie **Dokumenttyp:**<*dokumentenfluss*> aus. Wenn das cXML-Dokument das Ziel ist, erweitern Sie **Paket: None** und **Protokoll: cXML** und wählen Sie **Dokumenttyp:** <*dokumentenfluss*> in der Spalte **Ziel** aus.
4. Erweitern Sie die Quellen- bzw. Zielspalte für die andere Hälfte der Interaktion (das Dokument, das in cXML konvertiert wird, bzw. das Dokument, das von cXML transformiert wird), erweitern Sie sein Paket und Protokoll und wählen Sie seinen Dokumententyp aus.
5. Wählen Sie **Pass-Through** in der Liste **Aktion** unten auf der Seite aus. (**Pass-Through** ist die einzige gültige Option, die für cXML-Dokumente unterstützt wird.)

## Angepasste XML-Dokumentverarbeitung

In diesem Abschnitt wird beschrieben, wie Sie den Hub für das Weiterleiten von XML-Dokumenten konfigurieren können, die nicht von einem der anderen integrierten Routing-Protokolle verarbeitet werden.

*Angepasste XML* ist ein WebSphere Partner Gateway-Begriff, der sich auf XML-Dokumente bezieht, die nicht von einem der integrierten Protokolle verarbeitet werden.

Angepasste XML-Dokumente werden durch einen Eliminierungsprozess identifiziert. Basierend auf der Reihenfolge der Parsingschritte des Protokolls für festen Eingangsarbeitsablauf versucht der Hub, die XML-Dokumente mit den einzelnen Standardprotokollen abzugleichen, bevor der Parsingschritt des Protokolls für die Verarbeitung angepasster XML-Dokumente aufgerufen wird. Der angepasste XML-Handler wird für jedes XML-Dokument aufgerufen, das nicht mit einem der XML-Standarddokumenttypen übereinstimmt.

Zur Verarbeitung eines angepassten XML-Dokuments muss der Protokollparser Informationen aus dem Dokument extrahieren. Ihre Gruppe von XML-Formaten, Dokumentprotokolldefinitionen und Dokumenttypdefinitionen enthält die Informationen, die der Protokollparser für angepasste XML-Dokumente benötigt, um ein Dokument unter Verwendung Ihrer Konfiguration zu erkennen und zu verarbeiten.

Übersicht über die Funktionsweise des angepassten XML-Protokolls:

1. Das XML-Dokument wird geparst, um den DTD-Namen des Dokuments, den Namespace des Root-Tag und den Namen des Root-Tag abzurufen.
2. Basierend auf den im ersten Schritt ermittelten Kennungen wird eine Gruppe von Dokumentfamilien mit XML-Formaten als mögliche Übereinstimmung für das Dokument identifiziert. Informationen zur Erstellung von Dokumentfamilien und XML-Formaten finden Sie in „XML-Formate erstellen" auf Seite 160.
3. Jedes in Frage kommende XML-Format aus den Familien wird auf das Dokument angewendet, um festzustellen, ob es mit dem Dokument übereinstimmt. Übereinstimmungen werden später in diesem Abschnitt beschrieben.
4. Wird ein übereinstimmendes XML-Format gefunden, werden damit die Daten aus dem Dokument extrahiert, das der Hub zur Verarbeitung des Dokuments verwendet. Die Dokumentfamilie, zu der das übereinstimmende XML-Format gehört, legt das für das Routing verwendete Dokumentprotokoll fest. Das übereinstimmende XML-Format selbst wird durch den für das Routing verwendeten Dokumenttyp bestimmt.

Sie können mit der Seite **XML-Formate verwalten** Dokumentfamilien erstellen, die Dokumentprotokollen zugeordnet werden. Dann können Sie die Formatfamilien mit XML-Formaten füllen, die Dokumenttypen zugeordnet werden.

Ein XML-Format enthält zwei Arten von Informationen:

- XPath-Ausrücke, die zum Extrahieren von Informationen aus XML-Dokumenten verwendet werden.
- Literaldaten, die als konstanter Wert verwendet werden.

Mithilfe von XML-Formaten ruft Document Manager die Werte ab, die ein eingehendes Dokument eindeutig identifizieren, und greift auf die Informationen innerhalb des Dokuments zu, die für das ordnungsgemäße Routing und die korrekte Verarbeitung nötig sind.

Das Konfigurieren von angepasstem XML-Routing ist ein Prozess, der aus mehreren Schritten besteht. Gehen Sie dazu wie folgt vor:

1. Erstellen Sie ein Protokoll, das zum Weiterleiten einer Gruppe von zusammengehörigen Dokumenten verwendet wird, und ordnen Sie dieses Protokoll einem oder mehreren Paketen zu.
2. Erstellen Sie einen Dokumenttyp für das Format, und ordnen Sie ihn dem neu erstellten Protokoll zu.
3. Erstellen Sie eine Dokumentfamilie für eine Gruppe von XML-Formaten, die mit den Dokumenten übereinstimmen, die mit dem Protokoll weitergeleitet werden sollen.
4. Fügen Sie der Familie XML-Formate hinzu, die jeweils einem der Dokumenttypen für das Familienprotokoll zugeordnet werden.

Dann erstellen Sie Interaktionen zwischen den neuen Dokumenttypen, damit Verbindungen hergestellt werden können.

Diese Schritte werden in den folgenden Abschnitten beschrieben. Ein Beispiel für diese Schritte finden Sie auch in „Hub für angepasste XML-Dokumente konfigurieren" auf Seite 339.

## XML-Formate erstellen

Mit XML-Formaten werden Daten aus angepassten XML-Dokumenten für die Verarbeitung identifiziert und extrahiert. XML-Formate sind in Dokumentfamilien enthalten. Eine Dokumentfamilie ist eine Gruppe von zusammengehörigen XML-Formaten, die einen DTD-Namen, einen Tag für das Root-Element oder einen Namespace für das Root-Element gemeinsam nutzen. Deshalb gibt es drei Arten von Dokumentfamilien: DTD-Familien, Root-Tag-Familien und Namespace-Familien.

Dokumentfamilien haben zwei Aufgaben:

- Sie können festlegen, wie Dokumente weitergeleitet werden. Stimmt ein Dokument während der Laufzeit mit einem XML-Format überein, werden das Routing-Protokoll und die Routing-Version, die der Familie des Formats zugeordnet sind, zum Weiterleiten eines Dokuments verwendet.
- Sie können bei der Verwaltung der XML-Formate im System behilflich sein. Bei der Konfiguration des Systems können Sie die XML-Formate in Familien zusammenfassen. Sie könnten zum Beispiel Nachrichten zu Bestellungen in einer entsprechenden Familie gruppieren und dann nach einer Dokumentfamilie suchen, um auf die Formate in dieser Familie zuzugreifen.

### Dokumentfamilie erstellen

Zum Gruppieren zusammengehöriger XML-Formate müssen Sie zunächst eine Familie erstellen. Gehen Sie wie folgt vor, um eine Dokumentfamilie zu erstellen:

1. Klicken Sie auf **Hubadmin** > **Hubkonfiguration** > **XML-Formate**.
2. Klicken Sie auf **Dokumentfamilie erstellen**.
3. Geben Sie in der Sicht **Neue Dokumentfamilie** einen Familiennamen ein.

   **Anmerkung:** Mehrere Familien können dieselbe Kennung bzw. denselben Namen aufweisen. Die Kombination aus Kennungstyp und Name bildet einen eindeutigen Familienschlüssel. Angenommen, Sie möchten SOAP-Nachrichten mit dem angepassten XML-Handler weiterleiten. Sind mehrere Arten von SOAP-

Nachrichten vorhanden, können diese in Familien mit unterschiedlichen Namen klassifiziert werden, die alle die Kennung "Envelope" im Root-Tag aufweisen.

4. Wählen Sie aus der Liste der verfügbaren Protokolle im System ein Protokoll aus. Definieren Sie ein angepasstes Protokoll, bevor Sie die Familie definieren, die dieses Protokoll verwendet. Sie können das Protokoll für eine Familie nach deren Erstellung nicht mehr ändern, planen Sie also entsprechend voraus.
5. Wählen Sie eine Option für große Dateien aus: **Keine**, **Prozessor für große Dateien verwenden** oder **Namespace-abhängigen Prozessor für große Dateien verwenden**.

   **Keine** bedeutet, dass die XML-Formate in der Familie XPath Version 1.0-Ausdrücke verwenden können, die Größe der verarbeitbaren Dateien jedoch durch mehrere Faktoren eingeschränkt wird. Zu diesen Faktoren gehören die Hauptspeicherkonfiguration von Document Manager, die Auslastung von Document Manager und die Struktur der zu verarbeitenden Dokumente.

   **Prozessor für große Dateien verwenden** oder **Namespace-abhängigen Prozessor für große Dateien verwenden** bedeutet, dass die Dateigröße zwar keine Einschränkung darstellt, aber dass Sie nur einfache Elementpfadausdrücke in den XML-Formaten verwenden dürfen, die Mitglieder der Familie sind.

   Verwenden Sie eine Option für große Dateien beim Schreiben von XML-Formaten, die mit großen Dokumenten übereinstimmen sollen, die nicht mit dem vollständigen XPath-Prozessor verarbeitet werden können. Bei Auswahl der Option für Namespace-Abhängigkeit enthalten die Elementpfade Namespacepräfixe, wenn sie in einem Dokument erscheinen.
6. Wählen Sie einen Familientyp für das Dokument aus der Liste aus: **DTD**, **Root-Tag** oder **Namespace**.
7. Geben Sie für den erstellten Familientyp eine Familienkennung ein:

*Tabelle 23. Kennungen für Familientypen*

| Familientyp | Kennung |
|---|---|
| DTD | Der DTD-Name. |
| Root-Tag | Der Root-Tag der Nachrichten, die sich in dieser Familie befinden.<br>**Anmerkung:** Übergehen Sie das Namespacepräfix, falls eines vorhanden ist. |
| Namespace | Der Namespace des Root-Tag. |

   Mit dieser Kennung wird während der Laufzeit eine Familie von XML-Formaten ausgewählt. Eines dieser Formate kann mit dem Dokument in Übereinstimmung gebracht und zum Extrahieren von Verarbeitungsinformationen aus diesem Dokument verwendet werden. Wenn mehrere Familien dieselbe Kennung verwenden, werden die Formate in allen Familien anhand der Nachricht überprüft, bis eine Übereinstimmung gefunden wird.
8. Klicken Sie auf **Speichern**, um die neue Familie zu speichern, oder klicken Sie auf **Abbrechen**, um die Erstellung einer Dokumentfamilie zu stoppen. Klicken Sie auf **Zurückkehren**, um zur Eingangsanzeige zurückzukehren.

## Dokumentfamilie suchen

Bevor Sie eine Dokumentfamilie anzeigen können, müssen Sie diese suchen. Gehen Sie wie folgt vor, um eine Dokumentfamilie zu suchen:

1. Klicken Sie auf **Hubadmin** > **Hubkonfiguration** > **XML-Formate**.
2. Wählen Sie das Protokoll der Dokumentfamilie aus, das Sie anzeigen möchten.

3. Geben Sie den Familiennamen ein, falls dieser bekannt ist. Mithilfe eines Sterns (*) können Sie eine Platzhaltersuche durchführen.
4. Wählen Sie den Familientyp aus: **Beliebiger Typ**, **DTD**, **Namespace** oder **Root-Tag**.
5. Wählen Sie die Option für große Dateien aus: **Keine**, **Prozessor für große Dateien verwenden** oder **Namespace-abhängigen Prozessor für große Dateien verwenden**.
6. Klicken Sie auf **Suchen**. Alle Dokumentfamilien, die Ihren Suchkriterien entsprechen, werden unterhalb der Schaltfläche **Suchen** angezeigt.
7. Klicken Sie auf das Symbol **Details anzeigen** neben einer Dokumentfamilie, um die entsprechenden Details anzuzeigen.

## Dokumentfamilie bearbeiten

Im Fenster **Details** der Dokumentfamilie können die Merkmale für eine Familie geändert werden. Dazu müssen Sie die folgenden Schritte ausführen:

1. Klicken Sie auf die Schaltfläche mit dem Stift in der Anzeige **Details** der Familie, um eine Anzeige zum Bearbeiten der Dokumentfamilie aufzurufen. Beachten Sie, dass das Protokoll in dieser Anzeige nicht geändert werden kann. Der Grund dafür ist, dass möglicherweise Nachrichten unter Verwendung der Formate in dieser Familie weitergeleitet wurden und das Debugging schwierig ist, wenn das der Familie zugeordnete Protokoll geändert wird.
2. In der Anzeige zum Bearbeiten der Dokumentfamilie können Sie nun den Familiennamen, den Familientyp und die Familienkennung ändern.
3. Klicken Sie auf **Speichern**, wenn Sie Ihre Änderungen vorgenommen haben. Klicken Sie auf **Abbrechen** oder auf die Schaltfläche mit dem durchgestrichenen Stift, um zur Ansicht **Details** der Familie zurückzukehren, ohne die Änderungen zu speichern.

## Einer Familie ein neues XML-Format hinzufügen

Nach dem Erstellen einer Dokumentfamilie können Sie der Familie neue XML-Formate hinzufügen. Dazu müssen Sie die folgenden Schritte ausführen:

**Anmerkung:** In diesem Abschnitt wird häufig der Begriff "XPath-Ausdruck" verwendet. Wenn ein XML-Format eine Option für große Dateien verwendet, ist damit ein Elementpfadausdruck gemeint; dies ist ein einfacher Pfad vom Stamm eines Dokuments zu einem Element, das einen Wert aufweist.

1. Klicken Sie ausgehend von der Anzeige **Details** der Dokumentfamilie auf **XML-Format erstellen**. Die Anzeige für die XML-Formatdefinition wird geöffnet. Diese Seite ist in vier Abschnitte mit den folgenden Überschriften unterteilt: **Dokumenttypdefinition**, **Kriterien für die Dokumenttypdefinition**, **Dokumentattribute** und **Benutzerdefinierte Attribute**.
2. Vervollständigen Sie den Abschnitt **Dokumenttypdefinition**.

   Im Abschnitt **Dokumenttypdefinition** befindet sich eine Auswahlliste mit den Dokumenttypen, die in dem Protokoll enthalten sind, das der Dokumentfamilie zugeordnet ist. Wählen Sie einen Dokumenttyp aus der Liste aus. Stimmt ein Dokument mit dem XML-Format überein, werden das der Dokumentfamilie zugeordnete Protokoll und der dem Format zugeordnete Dokumenttyp zum Weiterleiten des Dokuments verwendet.
3. Vervollständigen Sie den Abschnitt **Kriterien für die Dokumenttypdefinition**.

   Der Abschnitt **Kriterien für die Dokumenttypdefinition** und der Abschnitt **Dokumentattribute** enthalten Felder, in die Sie bei Verwendung einer Option

für große Dateien Werte und Elementpfade eingeben. Sollten Sie keine Option für große Dateien verwenden, geben Sie XPath-Ausdrücke, Präfix-Namespaces und Rückgabetypen ein.

**Wert** Geben Sie in dieses Feld einen Wert für die Formatkennung ein. Dies ist ein erforderliches Feld.

**Elementpfad**
Geben Sie in dieses Feld einen Elementpfad ein. Dies ist ein erforderliches Feld. Beachten Sie, dass der Elementpfad nur auf Formate angewendet wird, die eine Option für große Dateien verwenden.

**XPath-Ausdruck**
Geben Sie in dieses Feld entweder einen gültigen XPath-Ausdruck für das Dokument ein, das mit dem Format übereinstimmt, oder geben Sie einen Literalzeichenfolgewert ein, der als Konstante für jedes Dokument zurückgegeben wird. Dies ist ein erforderliches Feld. Beachten Sie, dass XPath-Ausdrücke nur in Formaten verwendet werden, die keine Option für große Dateien verwenden.

**Präfix-Namespace**
Geben Sie in diesem Feld gegebenenfalls die Definition des letzten Namespacepräfixes ein, das in Ihrem XPath-Ausdruck verwendet wird. Die Eingabe erfolgt im Format präfix=namespace-qualifikationsmerkmal. Wenn das letzte Namespacepräfix in Ihrem Ausdruck beispielsweise SOAPENV und das zugehörige Qualifikationsmerkmal http://schemas.xmlsoap.org/soap/envelope/ lautet, geben Sie für das Namespacepräfix SOAPENV=http://schemas.xmlsoap.org/soap/envelope/ ein. Beachten Sie, dass für Formate, die eine Option für große Dateien verwenden, definitionsgemäß keine Präfix-Namespace-Felder vorhanden sind.

**Rückgabetyp**
Wählen Sie in diesem Feld entweder **Konstante**, **Text** oder **Tagname des Elements** aus der Auswahlliste aus. Verwenden Sie **Konstante**, wenn das Feld für den XPath-Ausdruck als Zeichenfolgeliteral für alle Dokumente interpretiert werden soll. Verwenden Sie **Text**, wenn die XPath-Auswertungsfunktion zur Auswertung des Ausdrucks im Kontext des Dokuments verwendet werden soll. Verwenden Sie **Tagname des Elements**, wenn der Elementname für das erste Element ermittelt werden soll, das von der XPath-Auswertung des Ausdrucks zurückgegeben wird. Beachten Sie, dass Formate, die eine Option für große Dateien verwenden, den Tagnamen des Elements als Rückgabetyp nicht enthalten.

Im Abschnitt **Kriterien für die Dokumenttypdefinition** werden Werte und XPath-Ausdrücke angegeben. Die Werte und die Auswertungsergebnisse für den Ausdruck werden bei der Verarbeitung von Dokumenten verglichen, um festzustellen, ob ein XML-Format mit einem Dokument übereinstimmt. Wenn zwischen einem Dokument und einem Format eine Übereinstimmung vorliegt und die Geschäftskennungen für Quelle und Ziel mithilfe des Formats gefunden werden können, wird das Dokument unter Verwendung des Protokolls und des Dokumenttyps weitergeleitet, die im Abschnitt **Dokumenttypdefinition** enthalten sind. Detaillierte Informationen zu den Feldern in diesem Abschnitt finden Sie in Tabelle 24 auf Seite 164.

*Tabelle 24. Kriterien für die Dokumenttypdefinition - Felder*

| Feld | Erforderlich/ Optional | Aktion |
|---|---|---|
| Format-ung | Erforderlich | Geben Sie den XPath-Ausdruck oder den Elementpfad ein, der den Pfad zu dem Inhalt innerhalb eines XML-Dokuments definiert, der das Dokument eindeutig identifiziert. Wenn der Root-Tag für Bestellungen (Purchase Order) beispielsweise <PurchasingMessage type="Purchase Order"> und für Auftragsbestätigungen (Order Confirmation) <PurchasingMessage type="Order Confirmation"> lautet, gibt der XPath-Ausdruck /PurchasingMessage/@type für einige Nachrichten den Text "Purchase Order" und für andere Nachrichten den Text "Order Confirmation" zurück. Zwei XML-Formate, eines für Bestellungen und eines für Auftragsbestätigungen, werden geschrieben. Das Wertefeld für Bestellungen lautet "Purchase Order", und das Wertefeld für Auftragsbestätigung lautet "Order Confirmation". Während der Laufzeit kann das richtige Format vom System lokalisiert werden, da nach einem Format gesucht wird, für das die Auswertung des Ausdrucks ein Ergebnis zurückgibt, das mit dem Wert übereinstimmt. Im Falle einer Übereinstimmung wird vom System der Routing-Dokumenttyp verwendet, der dem Format zugeordnet ist. |
| Formatversion | Erforderlich | Geben Sie den XPath-Ausdruck oder den Elementpfad ein, der die Formatversion definiert. Die Formatversion wird auf ähnliche Weise ausgewertet wie die Formatkennung. Wenn der Ausdruck für die Version mit dem Versionswert in einem Format übereinstimmt, kann das Format verwendet werden, sofern die Kennung ebenfalls übereinstimmt. Wenn nur eine Version eines Dokuments vorhanden ist, können Sie "1" für den Ausdruck mit dem Rückgabetyp einer Konstante und "1" für den Wert eingeben. Dies bedeutet, dass die Version stets übereinstimmt und zur Ermittlung eines übereinstimmenden Formats nur die Kennung verwendet wird. |

4. Vervollständigen Sie den Abschnitt **Dokumentattribute**.

   Im Abschnitt **Dokumentattribute** geben Sie Werte und XPath-Ausdrücke an, wie Sie es bereits im Abschnitt **Dokumenttypdefinition** getan haben. Detaillierte Informationen zu den Feldern in diesem Abschnitt finden Sie in Tabelle 25.

*Tabelle 25. Dokumentattribute - Felder*

| Feld | Erforder-lich/ Optional | Aktion |
|---|---|---|
| Quellengeschäfts-kennung | Erforderlich | Geben Sie den XPath-Ausdruck oder den Elementpfad ein, der den Pfad der Quellengeschäftskennung innerhalb des XML-Dokuments definiert. Damit wird der Quellenpartner zu Routingzwecken identifiziert. Beachten Sie, dass diese Daten für das zu verwendende Format gesucht werden müssen. |

*Tabelle 25. Dokumentattribute - Felder (Forts.)*

| Feld | Erforderlich/ Optional | Aktion |
|---|---|---|
| Zielgeschäftskennung | Erforderlich | Geben Sie den XPath-Ausdruck oder den Elementpfad ein, der den Pfad der Zielgeschäftskennung innerhalb des XML-Dokuments definiert. Damit wird der Zielpartner zu Routingzwecken identifiziert. Beachten Sie, dass diese Daten für das zu verwendende Format gesucht werden müssen. |
| Dokumentkennung | Optional | Geben Sie den XPath-Ausdruck oder den Elementpfad ein, der den Pfad der Dokument-ID innerhalb des XML-Dokuments definiert. Dieser Wert wird in der Dokumentanzeige angezeigt. |
| Dokumentzeitmarke | Optional | Geben Sie den XPath-Ausdruck oder den Elementpfad ein, der den Pfad der Zeitmarke für die Dokumenterstellung innerhalb des XML-Dokuments definiert. Dieser Wert wird in der Dokumentanzeige angezeigt. |
| Duplikatprüfschlüssel 1 - 5 | Optional | Geben Sie die XPath-Ausdrücke oder Elementpfade ein, die die Pfade definieren, mit deren Hilfe festgestellt wird, ob ein Dokument einmal oder doppelt vorhanden ist. |
| Markierung für "Synchron" | Optional | Geben Sie einen XPath-Ausdruck oder Elementpfad ein, der als *Wahr* oder *Falsch* ausgewertet wird und damit angibt, ob für diesen Dokumenttyp eine synchrone Antwort erforderlich ist. Sie können entweder einen XPath-Ausdruck eingeben, der den Wert anhand des Dokumentinhalts definiert, oder Sie können das Zeichenfolgeliteral "Wahr" oder "Falsch" mit dem Rückgabetyp "Konstante" eingeben. Wenn dieses Feld auf "Wahr" gesetzt ist, wird das Attribut BCGDocumentConstants.BCG_GET_SYNC_RESPONSE während der Kanalparsing-Verarbeitung im Geschäftsdokumentobjekt definiert. |
| Validierungsstammelement | Optional | Geben Sie den XPath-Ausdruck ein, der den Rootknoten des Inhalts (Nutzdaten) einer mit einem Umschlag versehenen Nachricht innerhalb des XML-Dokuments definiert. WebSphere Partner Gateway validiert Dokumente, die mit diesem Element beginnen. Sie müssen eine Aktion angeben, die Validierungen durchführt, damit diese Funktion ausgeführt werden kann. Dieses Feld ist für Formate, die eine Option für große Dateien verwenden, nicht vorhanden. |
| Zugehörige Dokument-ID | Optional | Geben Sie den XPath-Ausdruck oder den Elementpfad ein, der die Dokumentkennung eines zuvor weitergeleiteten Dokuments bereitstellt, dem das aktuelle Dokument zugeordnet ist. Zum Beispiel bezieht sich eine Auftragsbestätigung normalerweise auf eine Bestellung. Der Wert der Dokumentkennung für eine Bestellung kann mithilfe eines XPath-Ausdrucks (siehe oben) ermittelt werden. Wenn die Auftragsbestätigung die Kennung der Bestellung enthält, kann sie mithilfe des zugehörigen Dokument-ID-Ausdrucks ermittelt werden. Dabei werden die Dokumente in der Dokumentanzeige miteinander verknüpft. |

*Tabelle 25. Dokumentattribute - Felder (Forts.)*

| Feld | Erforderlich/ Optional | Aktion |
|---|---|---|
| Suchfelder 1 - 10 | Optional | Geben Sie die XPath-Ausdrücke oder Elementpfade ein, die den Pfad zu dem Dokumentinhalt definieren, den Sie für benutzerdefinierte Suchen innerhalb des XML-Dokuments verwenden möchten. In der Dokumentanzeige können Sie basierend auf den Werten in diesen Feldern nach Dokumenten suchen. |

5. Vervollständigen Sie den Abschnitt **Benutzerdefinierte Attribute**.

   Im Abschnitt **Benutzerdefinierte Attribute** können benutzerdefinierte Attribute hinzugefügt werden. Sie können ein Attribut hinzufügen, indem Sie den entsprechenden Namen in das Eingabefeld eingeben und auf **Hinzufügen** klicken. Dann können Sie das neue Attribut wie die anderen Standardattribute definieren, indem Sie je nach Bedarf den XPath-Ausdruck, den Elementpfad und den Präfix-Namespace eingeben und einen Rückgabetyp für dieses Attribut auswählen.

   Nachdem Sie die Attribute hinzugefügt haben, werden diese wie Standardattribute verwendet. Wenn Sie ein benutzerdefiniertes Attribut aus einem Format entfernen möchten, klicken Sie auf das rote X, das neben dem entsprechenden Namen angezeigt wird. Benutzerdefinierte Attribute werden von Handlern verwendet, die vom Benutzer geschrieben werden und das Dokument verarbeiten. Die Attributnamen und die zugehörigen Werte werden dem Geschäftsdokument bei der Verarbeitung des Dokuments hinzugefügt. Der Handler-Code kann diese aufrufen, indem er sie unter Verwendung der definierten Namen aus dem Geschäftsdokument abruft. Weitere Informationen hierzu finden Sie im *WebSphere Partner Gateway Programmer Guide*.
6. Blättern Sie nach Eingabe der Werte in dieser Anzeige nach unten und klicken Sie auf **Speichern**, um die Änderungen zu speichern. Klicken Sie auf **Abbrechen** oder auf die Schaltfläche mit dem durchgestrichenen Stift, um die Änderungen zu widerrufen und zur Anzeige mit der Familienzusammenfassung zurückzukehren.

## XML-Nachrichten mit unterschiedlichen Namespacepräfixen weiterleiten

Beim Weiterleiten von XML-Nachrichten müssen Sie eine XML-Formatdefinition einrichten, die exakt den in der XML-Nachricht Namespace und das Präfix enthält. Wenn Sie abweichende Namespacepräfixe verwenden, müssen Sie die Weiterleitung von XML-Nachrichten in der Konsole von WebSphere Partner Gateway konfigurieren. Die folgenden drei Methoden zum Ausführen der Konfiguration werden bereitgestellt:

- Dokumentfamilie und XML-Format für jede Nachricht konfigurieren, die die abweichenden Namespacepräfixe verwendet.
- Eine Dokumentfamilie und ein XML-Format für "local-name" erstellen (Schema-Root-Tag).
- Eine Dokumentfamilie und ein XML-Format unter Verwendung einer Kombination von "local-name" und Namespace erstellen.

**Dokumentfamilie und XML-Format für jede Nachricht konfigurieren, die die abweichenden Namespacepräfixe verwendet:**

1. Navigieren Sie zu **Hubadmin** > **Hubkonfiguration** > **XML-Formate**.

2. Klicken Sie auf den Link **Dokumentfamilie erstellen**.
3. Erstellen Sie auf der Seite **Neue Dokumentfamilie** eine neue Dokumentfamilie mit dem Typ *Namespace*.
4. Klicken Sie auf **Speichern**.
5. Klicken Sie auf den Link **XML-Format erstellen**. Dieses XML-Format wird unter der neu erstellten Dokumentfamilie erstellt.
6. Definieren Sie auf der Seite **XML-Formatdefinition** das XML-Format für den Namespace und das von der Nachricht zu verwendende Präfix.
7. Wiederholen Sie die Schritte 2, 3, 4, 5 und 6 für jedes XML-Format, das für das Namespacepräfix definiert ist. Erstellen Sie jedoch für jedes XML-Format eine andere Dokumentfamilie.

**Eine Dokumentfamilie und ein XML-Format für "local-name" erstellen (Schema-Root-Tag):**

1. Erstellen Sie auf der Seite **Neue Dokumentfamilie** eine Dokumentfamilie des Typs *Root-Tag*.
2. Erstellen Sie das XML-Format unter unter der neu erstellten Dokumentfamilie. Wenn Sie den **XPath-Ausdruck** definieren, verwenden Sie "local-name" (Root-Tag) als Formatkennung (**Quellengeschäftskennung** und **Zielgeschäftskennung**).
3. Klicken Sie auf **Speichern**.
4. Senden Sie die XML-Nachricht, die die abweichenden XML-Namespacepräfixe enthält.

   **Anmerkung:** "local-name" für das XML-Schema kann auch verwendet werden, um andere Felder im XML-Format, wie beispielsweise Suchfelder, zu definieren. Suchfelder können auch mit Zuordnungsbefehlen unter Verwendung des DIS-Clients oder über angepasste Benutzerexits definiert werden.

**Eine Dokumentfamilie und ein XML-Format unter Verwendung einer Kombination von "local-name" und Namespace erstellen:**

1. Erstellen Sie auf der Seite **Neue Dokumentfamilie** eine Dokumentfamilie des Typs *Namespace*.
2. Klicken Sie auf **Speichern**, um die neu erstellte Dokumentfamilie zu speichern.
3. Erstellen Sie das XML-Format unter unter der neu erstellten Dokumentfamilie. Definieren Sie das XML-Format und verwenden Sie dabei eine Kombination aus "local-name" (Root-Tag) und Namespace. Beispiel: **XPath-Ausdruck für die Quellengeschäftskennung:** *//*[namespace-uri()='http://edi.mycompany.com/2007/types/transnet' and local-name()="purchaseOrder"]/* [namespace-uri()='http://edi.mycompany.com/2007/types/transnet' and local-name()="senderID"]* **XPath-Ausdruck für die Zielgeschäftskennung:** *//*[namespace-uri()='http://edi.mycompany.com/2007/types/transnet' and local-name()="purchaseOrder"]/* [namespace-uri()='http://edi.mycompany.com/2007/types/transnet' and local-name()="receiverID"]*
4. Senden Sie die XML-Nachricht, die die abweichenden XML-Namespacepräfixe enthält.

   **Anmerkung:** Die Kombination aus "local-name" und Namespace für das XML-Schema kann auch verwendet werden, um andere Felder im XML-Format, wie beispielsweise Suchfelder, zu definieren. Suchfelder können auch mit Zuordnungsbefehlen unter Verwendung des DIS-Clients oder über angepasste Benutzerexits definiert werden.

## Protokolldefinition erstellen

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

1. Klicken Sie auf **Hubadmin > Hubkonfiguration > Dokumentdefinition > Dokumentdefinition erstellen**.
2. Wählen Sie für **Typ der Dokumentdefinition** den Eintrag **Protokoll** aus.
3. Geben Sie für **Name** eine Kennung für die Dokumentdefinition ein. Sie könnten z. B. für ein angepasstes XML-Protokoll 'Custom XML' eingeben. Dieses Feld ist erforderlich.
4. Geben Sie für **Version** einen Wert für die Version des Protokolls ein. Es können numerische Werte oder Zeichenfolgewerte verwendet werden.
5. Geben Sie eine optionale Beschreibung des Protokolls ein.
6. Setzen Sie **Dokumentebene** auf **Nein**, da Sie ein Protokoll und keinen Dokumenttyp definieren (den Dokumenttyp werden Sie im nächsten Abschnitt definieren).
7. Setzen Sie **Status** auf **Aktiviert**.
8. Legen Sie für dieses Protokoll **Sichtbarkeit** fest. Sie wollen es möglicherweise für alle Partner sichtbar machen.
9. Wählen Sie die Pakete aus, in denen dieses neue Protokoll gepackt sein wird. Wenn Sie z. B. wollen, dass dieses Protokoll den Paketen **AS**, **None** und **Backend Integration** zugeordnet werden soll, wählen Sie **Paket: AS**, **Paket: None** und **Paket: Backend Integration** aus.
10. Klicken Sie auf **Speichern**.

## Dokumenttypdefinition erstellen

Verwenden Sie als Nächstes wieder die Seite **Dokumentdefinition erstellen**, um einen Dokumenttyp zu erstellen.

1. Klicken Sie auf **Hubadmin > Hubkonfiguration > Dokumentdefinition > Dokumentdefinition erstellen**.
2. Wählen Sie für **Typ der Dokumentdefinition** den Eintrag **Dokumenttyp** aus.
3. Geben Sie für **Name** eine Kennung für die Dokumentdefinition ein. Sie könnten z. B. `Purchase order` als Namen für den Dokumenttyp eingeben. Dieses Feld ist erforderlich.
4. Geben Sie für **Version** einen Wert für die Version des Dokumenttyps ein. Es können numerische Werte oder Zeichenfolgewerte verwendet werden.
5. Geben Sie eine optionale Beschreibung des Dokumenttyps ein.
6. Setzen Sie **Dokumentebene** auf **Ja**, weil Sie ein Routingobjekt definieren, das einem tatsächlichen Dokument entspricht.
7. Setzen Sie **Status** auf **Aktiviert**.
8. Legen Sie für diesen Fluss **Sichtbarkeit** fest. Sie wollen es möglicherweise für alle Partner sichtbar machen.
9. Klicken Sie auf das Symbol **Erweitern**, um jedes Paket zu erweitern, das Sie in Schritt 9 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 "Custom XML").
10. Klicken Sie auf **Speichern**.

Wenn Sie die Beispielwerte verwendet haben, enthält die Seite **Dokumentdefinitionen verwalten** nun den Dokumenttyp 'Purchase order' und das Protokoll 'Custom XML' unter den Paketen **AS**, **None** und **Backend Integration**.

## Konfiguration fertigstellen

Nach Festlegung der Protokolldefinition können Sie diese als Routing-Protokoll für eine XML-Dokumentfamilie auswählen. Nachdem Sie dem Protokoll Dokumenttypen hinzugefügt haben, können Sie diese den XML-Formatdefinitionen zuordnen, die sich in der Dokumentfamilie befinden. Nachrichten, die mit einem Format in der Familie übereinstimmen, werden unter Verwendung des Protokolls, das der Familie zugeordnet ist, und des Dokumenttyps, der dem übereinstimmenden Format zugeordnet ist, weitergeleitet.

Bevor Sie Kanäle definieren können, die diese neuen Definitionen verwenden, müssen Sie Interaktionen zwischen den neuen Protokollen und Dokumenttypen und anderen Protokollen und Dokumenttypen aktivieren. Ferner müssen Sie die B2B-Funktionalität der Partner aktivieren, um diesen das Senden und Empfangen von Dokumenten mithilfe der neuen Protokolle und Dokumenttypen zu ermöglichen.

## Angepasste XML-Datei anhand einer XSD-Datei überprüfen

Wenn die allgemeine Konfiguration der angepassten XML (Dokumenttypdefinition, Erstellen der XML-Familie oder des XML-Formats, der B2B-Funktionalität und der Verbindung) abgeschlossen ist und die XML für die Weiterleitung durch die einfache Aktion "Pass Through" bereit ist, müssen Sie die folgenden Schritte ausführen, um die Überprüfung der XML-Datei vor der Aktion "Pass Through" zu ermöglichen:

1. Wählen Sie auf der Seite **Verbindungen** die Aktion *Pass-Through von angepasster XML mit Validierung* als neue Aktion aus.
2. Navigieren Sie zu **Hubadmin** > **Hubkonfiguration** > **Dokumentdefinition**.
3. Klicken Sie auf das Symbol **Attributwerte bearbeiten** (den blauen Pfeil) für den angepassten XML-Dokumenttyp.
4. Wählen Sie **Zuordnung hochladen** aus.
5. Wählen Sie die zugehörige XSD-Datei aus und klicken Sie auf **Hochladen**.
6. Wiederholen Sie die Schritte 2 und 3.
7. Klicken Sie auf **Attribute hinzufügen**, um die Attribute für den Kontext der Dokumentdefinition hinzuzufügen.
8. Wählen Sie **Validierungszuordnung** aus und klicken Sie auf **Speichern**.
9. Suchen Sie in **Kontenadmin** > **Verbindungen** nach der Verbindung.
10. Klicken Sie auf der Seite **Quelle** der Verbindung auf **Attribute**.
11. Erweitern Sie das Symbol für einen ausgeblendeten Knoten (blauer Ordner) für den Dokumenttyp.
12. Wählen Sie in der Dropdown-Liste **Validierungszuordnung** die XSD-Validierungszuordnung und klicken Sie auf **Speichern**.

Wenn Sie eine neuere Version der XSD hochladen wollen, müssen Sie zunächst die alte XSD entfernen. Verwenden Sie hierzu die Seite **Hubadmin** > **Hubkonfiguration** > **Zuordnungen** > **Validierungszuordnungen**. Wiederholen Sie Schritt 12 nach dem Hochladen der neuen Zuordnung, da dieses Verbindungsattribut durch das Entfernen einer Zuordnung zurückgesetzt wird.

## Validierungszuordnungen verwenden

WebSphere Partner Gateway verwendet Validierungszuordnungen, um die Struktur von bestimmten Dokumenten zu validieren. Wenn Sie einem Dokument eine Validierungszuordnung zuordnen wollen, stellen Sie zuerst sicher, dass die Validierungszuordnung WebSphere Partner Gateway zur Verfügung steht, wie in „Validierungszuordnungen hinzufügen" beschrieben. Informationen zum Verwalten von Validierungszuordnungen finden Sie im Kapitel "Hubverwaltungstasks" des Handbuchs *IBM WebSphere Partner Gateway Verwaltung*.

### Validierungszuordnungen hinzufügen

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

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

Gehen Sie wie folgt vor, um dem Hub eine neue Validierungszuordnung hinzuzufügen:

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

### Zuordnungen zu Dokumentdefinitionen zuordnen

Gehen Sie wie folgt vor, um eine Validierungszuordnung einer Dokumentdefinition zuzuordnen:

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

## Transformationszuordnungen verwenden

Schritte zur Verwendung von Transformationszuordnungen, die zum Konvertieren eines Dokuments von einem Format in ein anderes Format verwendet werden.

WebSphere Partner Gateway verwendet Transformationszuordnungen, um Dokumente von einem Format in ein anderes Format (beispielsweise ein XML-Dokument in EDI) zu konvertieren.

Im Folgenden werden die Schritte für die Verwendung von Transformationszuordnungen beschrieben:

1. Melden Sie sich an der Administrationskonsole von WebSphere Partner Gateway an.
2. Klicken Sie auf **Assistenten**.
3. Klicken Sie im Assistenten für den EIF-Import auf **Durchsuchen**, und geben Sie die Position der .EIF-Datei an.
4. Klicken Sie auf **Importieren**.
5. Klicken Sie auf der Seite **Zusammenfassung der Importoperation** auf **Weiter**.
6. Wählen Sie in der Anzeige **Prüfen Sie die Transformationszuordnungen und ändern Sie die zu erstellenden Interaktionen** die Transformationszuordnung aus, fügen Sie eine Interaktion hinzu, und wählen Sie die Aktion für die erstellte Interaktion aus.
7. Klicken Sie auf **Fertigstellen**.

**Wichtig:** Wenn Sie eine Transformationszuordnung aus der Konsole von WebSphere Partner Gateway herunterladen, wird eine Datei mit der Größe 0 KB heruntergeladen. Dies ist ein bekanntes Problem. Als Fehlerumgehung können Sie den DIS-Client verwenden, um Transformationszuordnungen herunterzuladen oder zu extrahieren.

## Dokumente anzeigen

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

Gehen Sie wie folgt vor, um die Dokumentanzeige zu öffnen:

1. Klicken Sie auf **Anzeigen > Dokumentanzeige**.
2. Wählen Sie die entsprechenden Suchkriterien aus.
3. Klicken Sie auf **Suchen**.

Informationen zur Verwendung der Dokumentanzeige finden Sie im Handbuch *WebSphere Partner Gateway Verwaltung*.

## Protokollierung der Unbestreitbarkeit konfigurieren

Sie können die Protokollierung der Unbestreitbarkeit für Nachrichten mithilfe von Attributen für Pakete, Protokolle oder Dokumentenflüsse konfigurieren, die für das Routing von Dokumenten verwendet werden. Der Name des Attributs lautet "Unbestreitbarkeit erforderlich" und kann auf **Ja** oder **Nein** gesetzt sein. Die Attributdefinition erfolgt auf der Ebene des Routing-Objekts. Diese Definition kann auf der Ebene der B2B-Funktionalität oder auf Verbindungsebene überschrieben werden.

## Nachrichtenspeicher konfigurieren

Sie können den Nachrichtenspeicher mithilfe der für das Routing von Dokumenten verwendeten Attribute für das Paket, das Protokoll oder den Dokumentenfluss konfigurieren. Der Name des Attributs lautet "Nachrichtenspeicherung erforderlich", und das Attribut kann den Wert **Ja** oder **Nein** annehmen. Die Attributdefinition erfolgt auf der Ebene des Routing-Objekts. Diese Definition kann auf der Ebene der B2B-Funktionalität oder auf Verbindungsebene überschrieben werden.

# Kapitel 10. EDI-Dokumentenflüsse konfigurieren

In diesem Kapitel wird beschrieben, wie Sie die Dokumentdefinitionen und Interaktionen für Standard-EDI-Austauschvorgänge konfigurieren. Darüber wird in diesem Kapitel das Empfangen und Transformieren von XML- und ROD-Dokumenten (ROD - satzorientierte Daten) beschrieben. Dieses Kapitel behandelt die folgenden Themen.



Es besteht auch die Möglichkeit, einen EDI-Austausch ohne Entfernen des Umschlags oder Transformation weiterzuleiten. Die Schritte für das Erstellen von Interaktionen für diesen Austauschtyp werden in „EDI-Dokumente mit Pass-Through-Aktion" auf Seite 112 beschrieben.

**Anmerkung:** Verwenden Sie stets die Browserinstanz, mit der Sie sich an Community Console angemeldet haben, wenn Sie Konfigurationsänderungen an WebSphere Partner Gateway vornehmen. Die gleichzeitige Verwendung mehrerer Browserinstanzen kann dazu führen, dass die Konfigurationsänderungen aufgehoben werden.

## Übersicht über EDI

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

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

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

## EDI-Austauschstruktur

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

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

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

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

Ein Austausch verfügt immer über ein Austauschheadersegment und ein Austauschtrailersegment.

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

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

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

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

*Tabelle 26. Segmente für unterstützte EDI-Standards*

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

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

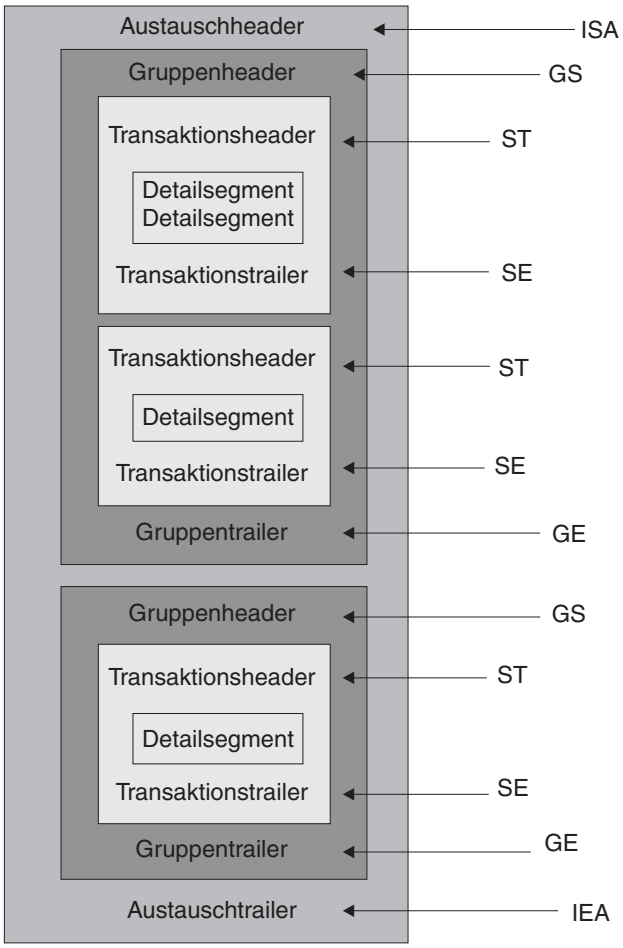



*Abbildung 22. Ein Austauschumschlag*

## Zuordnungen

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

Zuordnungen können mit DIS oder WTX Design Studio erstellt werden. DIS wird zur Erstellung von Zuordnungen für WDI-Transformationen und WTX Design Studio für WTX-Transformationen verwendet. Die mit DIS erstellten Zuordnungen können nicht für eine WTX-Transformation migriert werden, sondern müssen neu geschrieben werden. Je nach Aktion wird die entsprechende Transformationsengine ausgewählt, sofern sie betriebsbereit ist.

Zur Erstellung einer Zuordnung werden die Definitionen der Quellen- und Zieldokumente benötigt. Die Definitionen der Quellendokumente für EDI werden von WDI selbst bereitgestellt, für ROD und XML müssen sie mithilfe des DIS-Clients erstellt werden. Zur Verwendung dieses Standards durch den Laufzeitcode ist eine Kompilierung erforderlich. In älteren Versionen sind für den Standard Transformationszuordnungen erforderlich; in dieser Version kann die Kompilierung jedoch ohne die Transformationszuordnung erfolgen. Die Standard-EIF wird für EDI importiert, für ROD wird sie mithilfe des DIS-Clients erstellt. Im Falle von XML wird die DTD/XSD-Datei in die Entwicklungsdatenbank importiert. Im Falle von EDI rufen Sie in der Administrationskonsole die EDI-Assistenten auf. Daraufhin werden die in der EIF-Datei enthaltenen Datenformate/Standards angezeigt. Sie können entweder alle gleichzeitig importieren oder eine bestimmte Auswahl treffen. Ist die Auswahl erfolgreich, wird die Steuerzeichenfolge für den Standard in die Laufzeitdatenbank importiert.

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

Zusätzlich zu Transformationszuordnungen können Sie Zuordnungen der funktionalen Bestätigungen und Validierungszuordnungen verwenden. Zuordnungen der funktionalen Bestätigungen bieten Anweisungen dazu, wie eine funktionale Bestätigung hergestellt wird, die den Absender eines EDI-Dokuments darüber informiert, dass das Dokument angekommen ist. Mehrere EDI-Standardzuordnungen der funktionalen Bestätigungen werden bei der Installation von WebSphere Partner Gateway installiert. Eine Liste mit diesen Zuordnungen finden Sie in „Bestätigungen konfigurieren” auf Seite 223.

Wenn der sendende Hub eine funktionale Bestätigung erwartet und diese Bestätigung nicht innerhalb der Bestätigungszeit eintrifft, wird das Originaldokument erneut gesendet. Die Anzahl der Wiederholungen und das Wiederholungsintervall sind konfigurierbar. Diese Funktion ist standardmäßig nicht aktiviert. Der Wert muss in den EDI-Eigenschaften manuell festgelegt werden. Wenn der Wert für die Bestätigungszeit auf "Ja" gesetzt ist, müssen für Wiederholungszähler und Intervall Werte definiert werden. Die Wiederholungsereignisse werden zu Überwachungszwecken protokolliert. Wird das Wiederholungslimit ohne funktionale Bestätigung erreicht, wird das entsprechende Ereignis zu Überwachungszwecken protokolliert.

Zusätzliche Zuordnungen der funktionalen Bestätigungen können vom Zuordnungsexperten des Data Interchange Services-Clients erstellt werden. WebSphere Partner Gateway generiert eine funktionale Bestätigung, wenn eine EDI-Transaktion validiert wird, und der EDI-Transaktion eine Zuordnung der funktionalen Bestätigungen zugeordnet ist. Das Quellendokument muss ein EDI-Dokument sein.

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

## Überblick über XML- und ROD-Dokumente

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

### XML-Dokumente

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

### ROD-Dokumente

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

### Verteiler und mehrere Dokumente

XML- oder ROD-Dokumente können in den Hub als einzelne Dokumente oder als Gruppe von Dokumenten innerhalb derselben Datei gelangen.Mehrere Dokumente könnten in derselben Datei abgelegt werden, wenn z. B. ein terminierter Job beim Partner bzw. beim internen Partner regelmäßig zu sendende Dokumente hochlädt. Wenn mehrere XML- oder ROD-Dokumente in einer Datei ankommen, ruft der Empfänger den zugeordneten Verteilerhandler (XMLSplitterHander oder RODSplitterHandler) auf, um die Gruppe von Dokumenten aufzuteilen. (Die Verteilerhandler werden konfiguriert, wenn Sie ein Ziel erstellen. Weitere Informationen finden Sie in „ Vorverarbeitung” auf Seite 77.) Die Dokumente werden dann erneut in den Document Manager eingeführt, um individuell verarbeitet zu werden.

**Anmerkung:** Die Absender- und Empfänger-IDs müssen Teil der ROD-Dokumentdefinition sein, die der Transformationszuordnung zugeordnet ist. Die Informationen, die zum Ermitteln des Dokumenttyps und der Wörterbuchwerte nötig sind,

müssen ebenso in der Dokumentdefinition vorhanden sein. Stellen Sie sicher, dass der Zuordnungsexperte des Data Interchange Services-Clients diese Anforderungen kennt, wenn er die Transformationszuordnung erstellt.

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

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

## Übersicht - Dokumenttypen erstellen und Attribute festlegen

Eine Dokumentdefinition besteht aus mindestens einem Paket, einem Protokoll und einem Dokumenttyp. Die Dokumentdefinitionen geben die Dokumenttypen an, die von WebSphere Partner Gateway verarbeitet werden.

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

Die folgenden Abschnitte beschreiben kurz den Gesamtablauf für das Konfigurieren eines Dokumentenflusses zwischen dem internen Partner und einem externen Partner. Die Abschnitte beschreiben auch die Punkte, an denen Sie Attribute festlegen können.

### Schritt 1: Sicherstellen, dass die Dokumentdefinition verfügbar ist

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

Im Rahmen der Erstellung der Dokumentdefinition können Sie bestimmte Attribute ändern. Attribute werden verwendet, um verschiedene Dokumentverarbeitungs- und Routing-Funktionen auszuführen, wie z. B. Validierung, Verschlüsselungsüberprüfung und Wiederholungszähler. Die Attribute, die Sie auf der Dokumentdefinitionsebene festlegen, liefern eine globale Einstellung für das zugeordnete Paket und Protokoll sowie den zugeordneten Dokumenttyp. Die Attribute, die zur Verfügung stehen, variieren je nach Dokumentdefinition. Attribute für EDI-Dokumentdefinitionen unterscheiden sich von den Attributen für RosettaNet-Dokumentdefinitionen.

Wenn Sie z. B. einen Wert für **TA1-Anforderung zulassen** auf der Dokumenttypebene **ISA** angeben, wird diese Einstellung auf alle ISA-Dokumente angewendet. Wenn Sie später **TA1-Anforderung zulassen** auf B2B-Funktionalitätsebene für einen Partner oder den internen Partner festlegen, überschreibt diese Einstellung diejenige, die auf Dokumentdefinitionsebene festgelegt wurde.

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

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

## Schritt 2: Interaktionen erstellen

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

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

## Schritt 3: Partnerprofile, Ziele und B2B-Funktionalität erstellen

Erstellen Sie als Nächstes Partnerprofile für den internen Partner und für die externen Partner. Sie definieren Ziele, die bestimmen, wohin Dokumente gesendet werden, und B2B-Funktionalität, die die Dokumente angibt, welche der interne Partner oder ein Partner senden und empfangen kann. Die Seite **B2B-Funktionalität** listet alle Dokumenttypen auf, die definiert worden sind.

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

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

Sie müssen die Profile und die B2B-Funktionalität des internen Partners und der externen Partner definiert haben, bevor Sie Verbindungen zwischen ihnen erstellen können.

### Schritt 4: Verbindungen aktivieren

Schließlich aktivieren Sie Verbindungen zwischen dem internen Partner und den externen Partnern. Die verfügbaren Verbindungen basieren auf der B2B-Funktionalität der Partner und den von Ihnen erstellten Interaktionen. Die Interaktionen hängen von den Dokumentdefinitionen ab, die zur Verfügung stehen.

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

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

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

## Übersicht über mögliche Dokumentenflüsse

Dieser Abschnitt gibt Ihnen eine kurze Übersicht über die Transformationstypen, die WebSphere Partner Gateway ausführen kann. In „Dokumentaustauschvorgänge definieren" auf Seite 208 werden die Details dieser Transformationen beschrieben und wie Sie diese festlegen müssen.

### Dokumentenfluss: EDI zu EDI

WebSphere Partner Gateway kann einen EDI-Austausch von einem Partner oder vom internen Partner akzeptieren, ihn in einen anderen EDI-Austauschtyp (z. B. EDI-X12 zu EDIFACT) transformieren und das Dokument an den internen Partner oder den Partner senden. Die folgenden Schritte treten auf, wenn ein EDI-Austausch in einen anderen EDI-Austausch transformiert wird:

1. Vom EDI-Austausch, der auf dem Hub empfangen wird, wird der Umschlag entfernt.
2. Die einzelnen Transaktionen innerhalb des EDI-Austauschs werden zu dem EDI-Format des Empfängers transformiert.

3. Die transformierten EDI-Transaktionen werden mit einem Umschlag versehen und an den Empfänger gesendet.

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

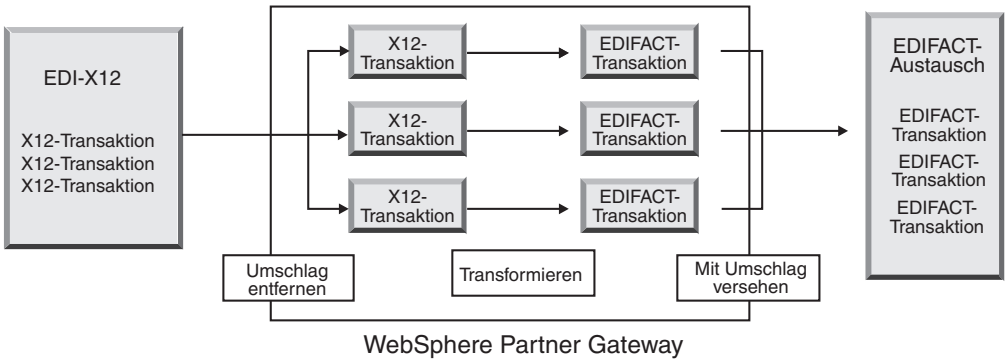



*Abbildung 23. Dokumentenfluss: EDI-Austausch zu EDI-Austausch*

Jeder Transaktion wurde eine Transformationszuordnung zugeordnet, die angibt, wie die Transaktion transformiert wird. Die Transaktion kann in eine einzelne Transaktion transformiert werden, oder, falls die Zuordnungsverkettung zur Erstellung der Zuordnung verwendet wurde, in mehrere Transaktionen transformiert werden. Wenn der Stapelbetrieb des Programms zur Umschlagsgenerierung aktiviert ist, verlassen Transaktionen, die auf dem Hub in einem Umschlag eintreffen, den Hub in einem Umschlag. Wenn jedoch Umschlagsunterbrechungspunkte, z. B. verschiedene Werte für EDI-Attribute oder ein unterschiedliches Umschlagsprofil, vorhanden sind oder wenn der Stapelbetrieb inaktiviert wurde, verlassen die Transaktionen den Hub in unterschiedlichen Umschlägen. Eine allgemeine Beschreibung des Programms zur Umschlagsgenerierung (die Komponente, die eine Gruppe von Transaktionen zusammenstellt, welche an einen Partner gesendet werden sollen, sie mit einem Umschlag versieht und sendet) finden Sie in „Programm zur Umschlagsgenerierung" auf Seite 195. Weitere Informationen zum Stapelbetrieb finden Sie in „Stapelbetrieb" auf Seite 196.

Der Transaktion könnte auch eine Validierungszuordnung zugeordnet sein.

## Dokumentenfluss: EDI zu XML oder ROD

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

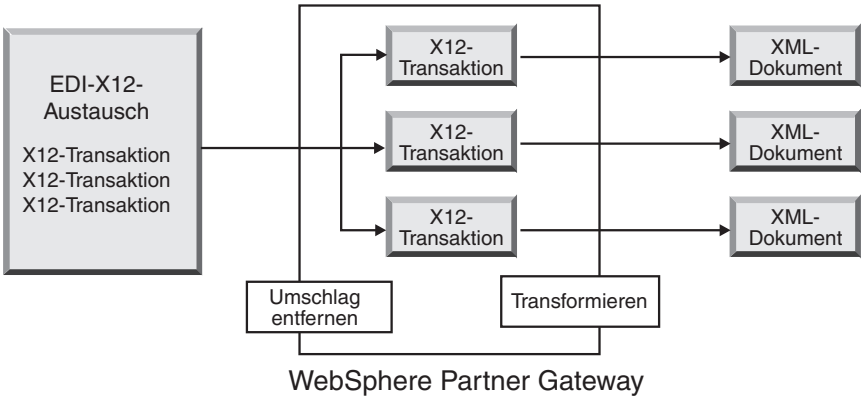



*Abbildung 24. Dokumentenfluss: EDI-Austausch zu XML-Dokumenten*

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

## Dokumentenfluss: XML oder ROD zu EDI

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

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

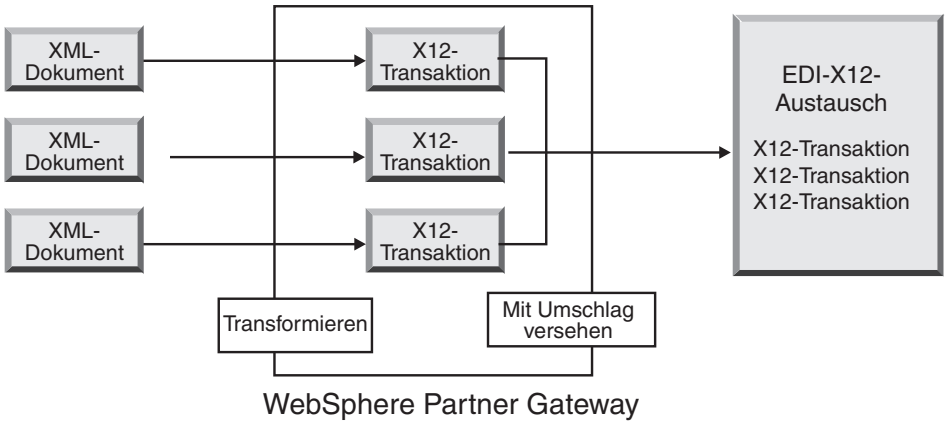



*Abbildung 25. Dokumentenfluss: XML-Dokument zu EDI-Austausch*

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

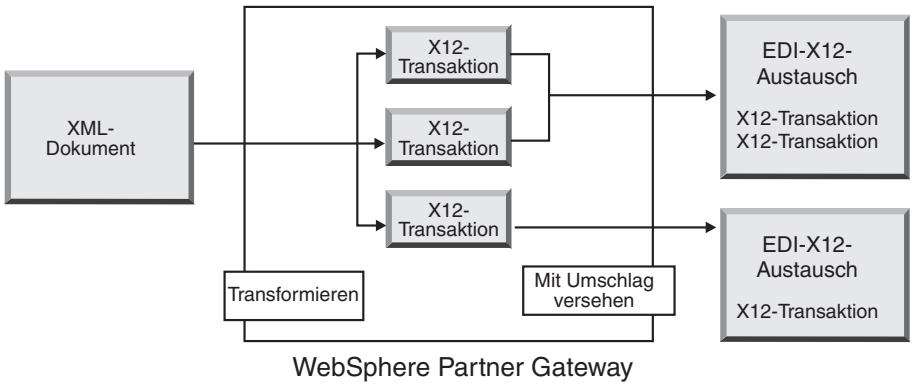



*Abbildung 26. Dokumentenfluss: XML-Dokument zu mehreren EDI-Transaktionen*

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

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

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

**Hinweise:**

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

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

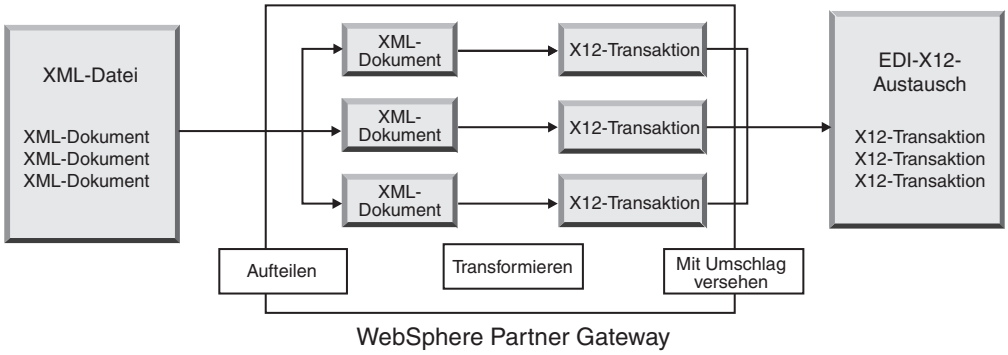



*Abbildung 27. Dokumentenfluss: Mehrere XML-Dokumente zu EDI-Austausch*

In Abb. 27 werden die Dokumente vom XML-Verteilerhandler aufgeteilt und die transformierten Transaktionen zusammen mit einem Umschlag versehen. Für den XML-Verteilerhandler muss die Option BCG_BATCHDOCS auf ON (der Standardwert) gesetzt sein, damit dieses Szenario auftritt. Wenn BCG_BATCHDOCS auf ON gesetzt ist und der Stapelbetrieb des Programms zur Umschlagsgenerierung aktiviert ist, können diese Transaktionen mit demselben EDI-Umschlag versehen werden. Das Attribut für den Stapelbetrieb des Programms zur Umschlagsgenerierung wird in „Stapelbetrieb" auf Seite 196 beschrieben.

## Dokumentenfluss: XML zu ROD oder ROD zu XML

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

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

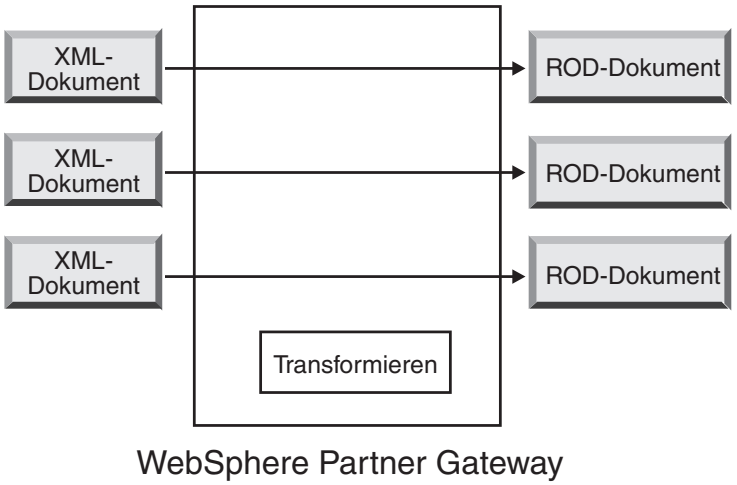



*Abbildung 28. Dokumentenfluss: XML-Dokument zu ROD-Dokument*

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

## Dokumentenfluss: XML zu XML oder ROD zu ROD

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

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

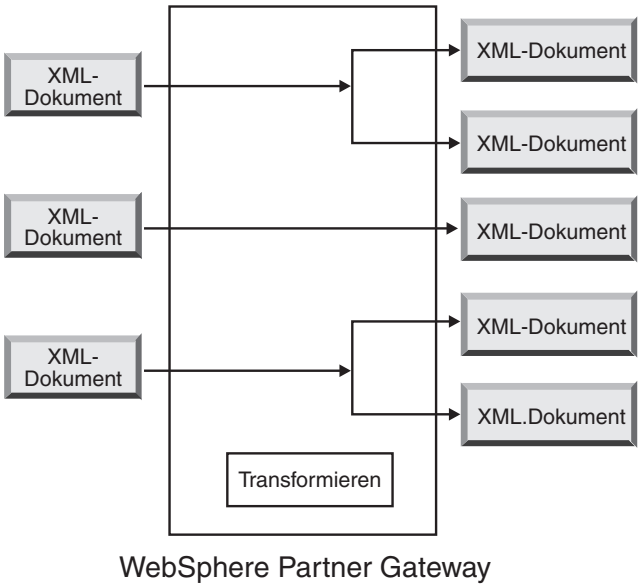


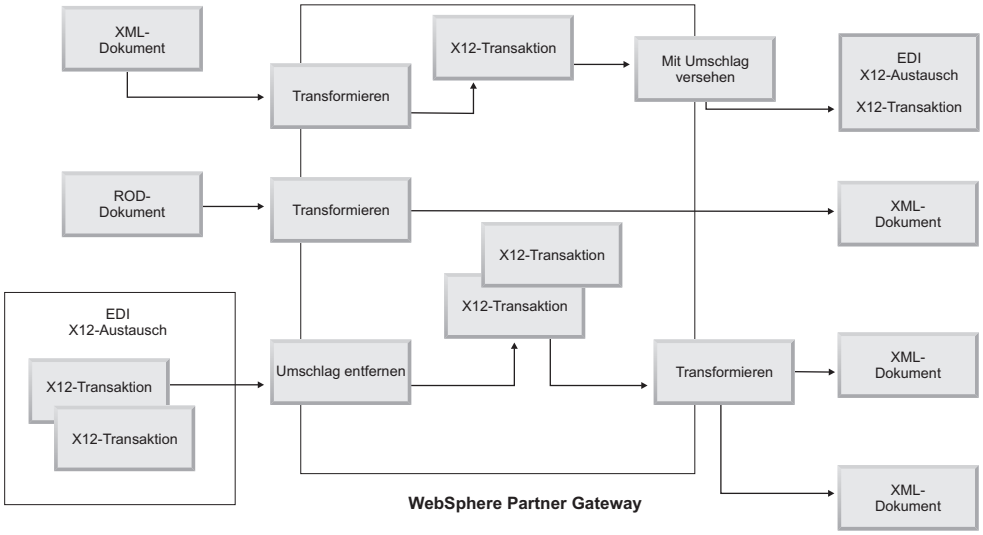

*Abbildung 29. Dokumentenfluss: XML-Dokument zu XML-Dokument*

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

## Dokumentenfluss: Any zu Any

Mit WTX kann das Any zu Any-Format (Umwandlung eines beliebigen Formats in ein anderes beliebiges Format) transformiert werden. WTX Design Studio wird zur Erstellung von Zuordnungen verwendet. Die verschiedenen Dokumentenflüsse sind ROD zu Any, XML zu Any und EDI zu Any. Gegebenenfalls müssen Sie den Verteiler so konfigurieren, dass die Dokumente aufgeteilt werden. Im Falle eines ROD-Quellendokuments müssen auch die Routing-Informationen konfiguriert werden. Im Falle eines XML-Quellendokuments werden die erforderlichen Routing-Informationen durch die XML-Formate bereitgestellt. Die Aktionen für die verschiedenen Dokumentenflüsse lauten wie folgt:

- ROD zu Any - WTX-Transformation
- XML zu Any - WTX-Transformation
- EDI zu Any - EDI - Umschlag entfernen, wenn Sie den Umschlag vom Austausch entfernen möchten, um so die einzelnen Transaktionen zu erhalten. Danach werden die Transaktionen mithilfe der Aktionen "EDI-ReEnveloper" und "WTX-Transformation" erneut mit einem Umschlag versehen und in das EDI zu Any-Format transformiert. EDI validieren, wenn die Transaktionen validiert werden müssen. Validierung des EDI-Austauschs, wenn der Austausch validiert werden soll, ohne den Umschlag zu entfernen.



## Übersicht über die Transformationsengines

WebSphere Partner Gateway unterstützt zwei unterschiedliche Transformationsengines: - natives WDI und WTX.

**Natives WDI** - Für natives WDI werden Transformationszuordnungen im DIS-Client erstellt. WebSphere Partner Gateway stellt die folgenden Aktionen für die Integration mit WDI bereit: EDI - Umschlag entfernen (EDI De-envelope), EDI konvertieren (EDI Translate), EDI validieren (EDI Validate), EDI-ReEnveloper, EDI - Mit Umschlag versehen (EDI Envelope), ROD konvertieren (ROD Translate) und XML konvertieren (XML Translate). Für die Integration ist keine separate Konfiguration erforderlich, da es sich um natives WDI handelt.

**WTX** - Transformationszuordnungen werden mit WTX Design Studio erstellt. WebSphere Partner Gateway stellt die folgenden Aktionen für die Integration mit WTX bereit: WTX-Transformation (WTX Transformation), Validierung des EDI-Austauschs (EDI Interchange Validation), EDI - Umschlag entfernen (EDI De-envelope), EDI validieren (EDI Validate), EDI-ReEnveloper und EDI - Mit Umschlag versehen (EDI Envelope). RMI und die native Methode stellen zwei unterschiedliche Ansätze für WTX dar. RMI wird empfohlen, wenn WTX nicht auf derselben Maschine wie WebSphere Partner Gateway installiert ist. Führen Sie zum Aufrufen von WTX über Fernzugriff die folgenden Schritte aus:

1. Öffnen Sie im Verzeichnis "DTXHome" die Datei "rmiserver.properties" und nehmen Sie Änderungen an den Eigenschaften vor. Sie können beispielsweise die Portnummer definieren.
2. Führen Sie im Verzeichnis "DTXHome" die Datei "startrmiserver.bat" aus.
3. Geben Sie in den gemeinsamen Eigenschaften der Konsole den Hostnamen (Host, auf dem der RMI-Server ausgeführt wird) und die Portnummer an. Setzen Sie die Option für den RMI-Server auf **Ja**.
4. Geben Sie die physische Position der Zuordnung an.

Bei der nativen Methode geben Sie für den Systempfad das WTX-Ausgangsverzeichnis an. Ferner müssen Sie für "rmiuseserver" die Eigenschaft auf **No** setzen.

## Transaktionen vom Back-End mit einem Umschlag versehen

Bei der Verwendung von WTX im asynchronen Modus werden die von WTX generierten EDI-Transaktionen von der Back-End-Anwendung verarbeitet und an WebSphere Partner Gateway gesendet, um sie gemäß des Back-End-Paketstandards mit einem Umschlag zu versehen. Die Transaktionsdetails werden mithilfe der Back-End-Standardheader (x-aux-senderid, x-aux-receiverid, x-aux-protocol, x-aux-protocol-version, x-aux-process-type, x-aux-process-version und x-aux-docSyntax) bereitgestellt. Die Back-End-Paketheader enthalten Informationen zum EDI-Wörterverzeichnis/-Protokoll (z. B. X12v4R1), zu "Docsyntax" (EDI_transaction) und zu den Prozesstransaktionsinformationen (z. B. 850) für die oben genannten Header. Weitere Informationen hierzu finden Sie im Abschnitt "WTX - Mit Umschlag versehen".

## Verarbeitung von EDI-Austauschvorgängen

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

1. Entfernt die Umschläge der Austauschvorgänge.

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

   - Auf der Austauschebene die Geschäfts-IDs der sendenden und empfangenden Partner, der Nutzungsanzeiger, der angibt, ob der Austausch für eine Produktions- oder Testumgebung bestimmt ist, sowie das Datum und die Uhrzeit, wann der Austausch vorbereitet worden ist
   - Auf der Gruppenebene die Anwendungs-IDs des Absenders und Empfängers sowie das Datum und die Uhrzeit, wann die Gruppe vorbereitet worden ist
   - Auf der Transaktionsebene der Transaktionstyp (wie z. B. X12 850 oder EDIFACT ORDERS)
   - Sollte für einzelne Transaktionen eine Validierung erforderlich sein, wird der Umschlag von der EDI-Transaktion entfernt. Nach Abschluss der Validierung werden die validierten Transaktionen mit einem Umschlag versehen und in Abhängigkeit von der Aktion entweder an die Transformationsengine (WDI oder WTX zur Verarbeitung) oder an das Ziel gesendet.
2. Transformiert die erste Transaktion entsprechend der ihr zugeordneten Zuordnung.
3. Transformiert die zweite Transaktion entsprechend der ihr zugeordneten Zuordnung.
4. Stellt der Back-End-Anwendung die transformierten Dokumente zu.

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

Die einzelnen Transaktionen, Gruppen und Austauschvorgänge werden durch Kontrollnummern angegeben. WebSphere Partner Gateway legt diese Nummern fest, wenn ein Austausch stattfindet. Sie können die Kontrollnummern jedoch anpassen, wie in „Kontrollnummern” auf Seite 205 beschrieben.

Die folgende Abbildung zeigt den Gesamtüberblick darüber, wie ein EDI-Austausch in einem AS-Paket von einem Partner mit dem letztendlichen Ziel gesendet wird, zwei transformierte XML-Dokumente an zwei unterschiedliche Ziele auf dem Back-End-System des internen Partners zuzustellen. In diesem Beispiel werden die 850-Transaktionen in Bestellungen transformiert, die eine Back-End-Anwendung verarbeiten kann. Die 890-Transaktionen werden in Versandaufträge des Warenlagers transformiert, die die Back-End-Anwendung verarbeiten kann.

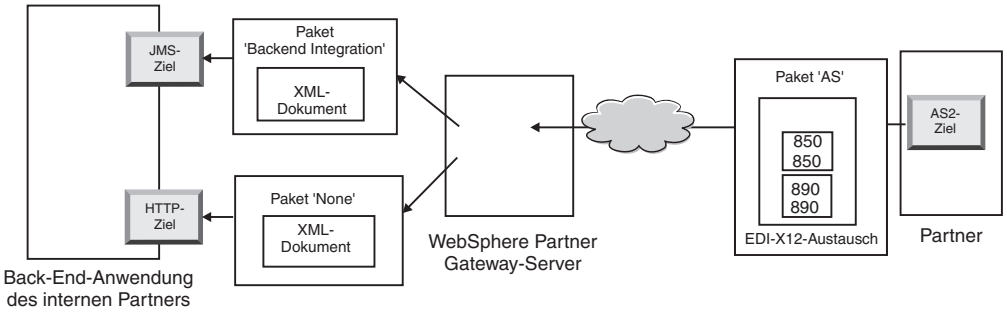



*Abbildung 30. Gesamtdokumentenfluss von einem Partner zum internen Partner*

Anstatt nur eine Verbindung vom Partner zum internen Partner zu erfordern, sind für diesen Austausch drei Verbindungen erforderlich:

- Eine Verbindung vom Partner zum Hub, um den Umschlag vom Austausch zu entfernen. Da dies ein Zwischenschritt ist (der Umschlag wird vom Austausch entfernt, dem Partner aber nicht zugestellt), gilt für die Zielseite der Partnerverbindung **N/A** (nicht vorhanden).

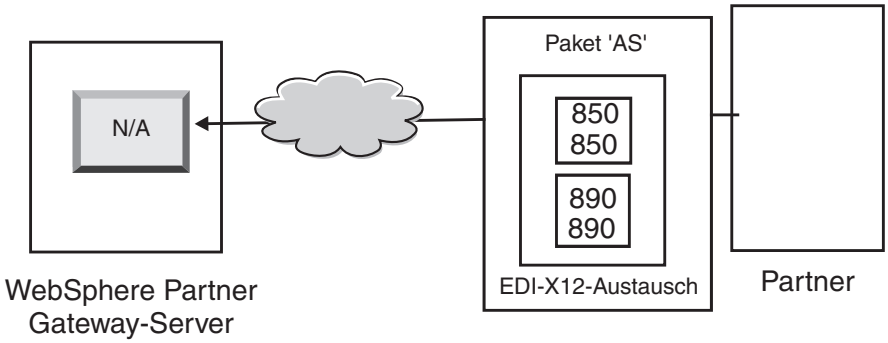



*Abbildung 31. Die Verbindung für die Umschlagsentfernung*

- Eine Verbindung für die erste Transaktion, die transformiert und dem JMS-Ziel des internen Partners zugestellt werden soll, und eine Verbindung für die zweite Transaktion, die transformiert und an das HTTP-Ziel des internen Partners gesendet werden soll. Für die Transaktionen ist das Quellenpaket nicht zutreffend, da die Transaktionen mit dem ursprünglichen Austausch gekommen sind, dessen Umschlag vom System entfernt worden ist.

Für die Quellenseite der Transaktionen sollte daher in der Partnerverbindung **Paket: N/A** angegeben sein.

Für die Transaktion, die in XML transformiert wird und über JMS zur Back-End-Anwendung fließt, sollte das Ziel in der Partnerverbindung dieser Transaktion als das JMS-Ziel des internen Partners angegeben werden. Für die Transaktion, die in XML transformiert wurde und die über HTTP zur Back-End-Anwendung fließt, sollte das Ziel in der Partnerverbindung dieser Transaktion als das HTTP-Ziel angegeben werden.

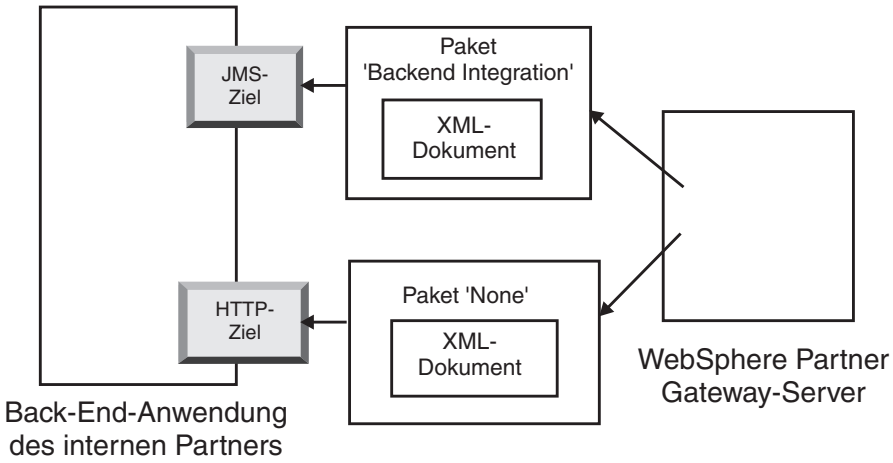



*Abbildung 32. Verbindungen für einzelne Transaktionen*

Sie können die Dokumentanzeige zum Anzeigen des Austauschs und der einzelnen Transaktionen verwenden, welche in der Dokumentanzeige als *untergeordnete Elemente* des Austauschs betrachtet werden. Sie können mit der Dokumentanzeige die untergeordneten Elemente anzeigen, die einem Quellen- oder Zielaustausch zugeordnet sind, und Sie können die ihnen zugeordneten Ereignisse anzeigen. Die Dokumentanzeige wird im Abschnitt über das Anzeigen von Ereignissen und Dokumenten des Handbuchs *WebSphere Partner Gateway Verwaltung* beschrieben.

Wenn der Absender Bestätigungen anfordert, benötigen Sie zusätzliche Verbindungen:

- Eine Verbindung für jede Bestätigung, die zurück an den Partner gesendet wird. Die funktionalen Bestätigungen werden vom System generiert, und daher sollte für die Quellenseite der Partnerverbindung **Paket: N/A** angegeben sein. Die funktionalen Bestätigungen werden vor ihrer Zustellung mit Umschlägen versehen, und daher sollte für die Zielseite der Partnerverbindung **Paket: N/A** angegeben sein. Das Programm zur Umschlagsgenerierung stellt diese Bestätigungen entsprechend einem von Ihnen festgelegten Zeitplan zusammen. Informationen zum Festlegen des Zeitplans finden Sie in „Programm zur Umschlagsgenerierung” auf Seite 195.
- Eine Verbindung, um die Bestätigungen mit einem Umschlag zu versehen, bevor Sie zurück an den Partner gesendet werden. Der Umschlag wird vom System generiert, und daher sollte für die Quellenseite der Partnerverbindung **Paket: N/A** angegeben sein. Für die Zielseite der Partnerverbindung sollte als Ziel das Ziel des Partners, in diesem Fall **Paket: AS**, angegeben sein. Sie können einen Standardumschlag für den EDI-Standard verwenden, oder Sie können Umschläge anpassen. Informationen zum Anpassen von Umschlägen finden Sie in „ Umschlagsprofile” auf Seite 197.

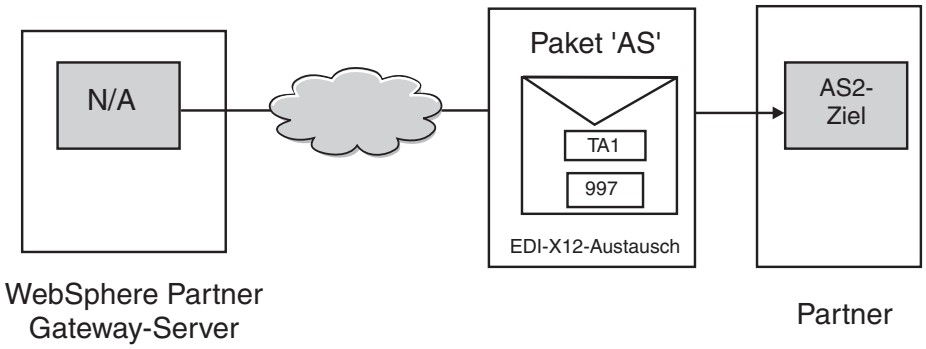



*Abbildung 33. Bestätigungen mit Umschlägen versehen und diese an den Absender senden*

## Synchrone Transformation

WTX ermöglicht eine Transformation des Any zu Any-Formats unter Verwendung einer einzelnen Zuordnung. Über eine Option sind direkte Aufrufe an die WTX-API für die Transformation möglich. Die mit einem Umschlag versehene Transaktion wird nach der Umschlagsentfernung und Validierung an WTX gesendet.

**Anmerkung:** Informationen zu den verschiedenen verfügbaren EDI-Formaten finden Sie im Abschnitt „Übersicht über EDI" auf Seite 173.

**Eine Ausgabe** - Das Weiterleitungsattribut legt fest, ob das Ausgabedokument erneut in den Arbeitsablauf eingeführt oder direkt zur Verarbeitung an den Ausgangsarbeitsablauf gesendet wird.

**Mehrere Ausgaben** - Basierend auf der Markierung für Weiterleitung (Reroute) wird das untergeordnete Element entweder direkt an den Ausgangsarbeitsablauf übergeben oder an den festen Eingangsarbeitsablauf weitergeleitet, um durch einen neuen Kanal zu fließen.

## Asynchrone Transformation

Wenn ein interner Partner eine asynchrone Nachricht an einen externen Partner sendet, kann der externe Partner WESB/WMB oder WTX zur Transformation verwenden. Eine Konfiguration ist nicht erforderlich, da WTX als JMS-Ziel betrachtet wird. WTX sendet das Dokument nach der Verarbeitung an das Back-End. Ein Informationsfluss zurück zu WebSphere Partner Gateway findet nicht statt. Das EDI-Dokument wird nach der erfolgreichen Zustellung an das JMS-Gateway als "Gesendet" markiert.

# Verarbeitung von XML- oder ROD-Dokumenten

Ein XML- oder ROD-Dokument wird auf dem Hub als einzelnes Dokument oder als Gruppe von Dokumenten in derselben Datei empfangen. Wenn eine Gruppe von Dokumenten auf dem Hub in derselben Datei empfangen wird, führt WebSphere Partner Gateway die folgenden Aktionen aus:

1. Teilt die Gruppe von Dokumenten in einzelne Dokumente auf.
2. Transformiert jedes Dokument entsprechend der ihm zugeordneten Zuordnung.
3. Wenn die Dokumente in EDI-Transaktionen transformiert werden, versieht es die Transaktionen mit Umschlägen und stellt diese der Back-End-Anwendung zu. Wenn die Dokumente in XML- oder ROD-Dokumente transformiert werden, stellt es die transformierten Dokumente der Back-End-Anwendung zu.

Wenn das XML- oder ROD-Dokument als einzelnes Dokument ankommt, führt WebSphere Partner Gateway die folgenden Aktionen aus:

1. Transformiert das Dokument entsprechend der ihm zugeordneten Zuordnung.
2. Wenn das Dokument in eine EDI-Transaktion transformiert wird, versieht es die Transaktion mit einem Umschlag und stellt es der Back-End-Anwendung zu. Wenn das Dokument in ein anderes XML- oder ROD-Dokument transformiert wird, wird das Dokument der Back-End-Anwendung zugestellt.

Ebenso, wenn der Hub ein bzw. mehrere Dokumente sendet, die von der Back-End-Anwendung des internen Partners stammen, werden die Dokumente in XML- oder ROD-Dokumente transformiert, oder sie werden in EDI-Transaktionen transformiert. Bei EDI-Transaktionen werden die Transaktionen mit einem Umschlag versehen, bevor sie an den Partner gesendet werden. Wie in dem Fall, wenn ein EDI-Austausch empfangen wird, sind mehrere Aktionen erforderlich, um das Dokument bzw. die Dokumente zu transformieren, die entstehenden Transaktionen mit einem Umschlag zu versehen und den EDI-Austausch zu senden.

## WTX-Integration und polymorphe Zuordnung mit einem Umschlag versehen

In WebSphere Partner Gateway ist eine Baumstruktur für Metadatentypen definiert. Sie können Informationen zu den Datentypen in den einzelnen Karten konfigurieren und weitergeben. Normalerweise werden die folgenden Eigenschaften konfiguriert. Bei der Angabe von Eigenschaftsnamen und -werten muss die Groß-/Kleinschreibung beachtet werden. Die Groß-/Kleinschreibung muss nur bei booleschen Werten nicht beachtet werden.

*Tabelle 27. Eigenschaften der Baumstruktur für Metadatentypen*

| Name der Eigenschaft | Eigenschaftswert | Beschreibung |
|---|---|---|
| BCG_DOCSYNTAX | EDI_INTERCHANGE<br>EDI_TRANSACTION<br>XML ROD | EDI_INTERCHANGE muss definiert werden, wenn die Ausgabe ein mit einem Umschlag versehener EDI-Austausch ist. EDI_TRANSACTION muss definiert werden, wenn die Ausgabe eine EDI-Transaktion ist, die nicht mit einem Umschlag versehen ist. XML und ROD müssen der XML- und ROD-Ausgabe entsprechend definiert werden. |
| BCG_REENVELOPE | true/false | Wenn der Wert "true" (wahr) lautet und für BCG_DOCSYNTAX der Wert EDI_INTERCHANGE definiert wurde, wird der EDI-Umschlag entfernt. Nach Entfernung des Umschlags wird jede generierte Transaktion für die nachfolgenden Schritte als einzelnes Dokument angesehen. |
| BCG_REROUTE | true/false | Wenn der Wert "true" (wahr) lautet, wird das Dokument weitergeleitet. Wenn der Wert "false" (falsch) lautet und eine einzelne Ausgabe vorhanden ist, wird das vorhandene BDO mit der neuen Datei aktualisiert und gesendet. |
| ProtocolName | Angepasst | Der Protokollname des Ausgabedokuments. Dieser Wert muss angegeben werden, wenn der ReRoute-Wert auf "true" (wahr) gesetzt ist. Dieser Wert wird zur Erfassung des Kanals für das weitergeleitete Dokument verwendet. |

*Tabelle 27. Eigenschaften der Baumstruktur für Metadatentypen (Forts.)*

| Name der Eigenschaft | Eigenschaftswert | Beschreibung |
|---|---|---|
| ProtocolVersion | Angepasst | Die Protokollversion für das Ausgabedokument. Dieser Wert muss angegeben werden, wenn der ReRoute-Wert auf "true" (wahr) gesetzt ist. Dieser Wert wird zur Erfassung des Kanals für das weitergeleitete Dokument verwendet. |
| ProcessCode | Angepasst | Der Prozesscode für das Ausgabedokument. Dieser Wert muss angegeben werden, wenn der ReRoute-Wert auf "true" (wahr) gesetzt ist. Dieser Wert wird zur Erfassung des Kanals für das weitergeleitete Dokument verwendet. |
| ProcessVersion | Angepasst | Die Prozessversion für das Ausgabedokument. Dieser Wert muss angegeben werden, wenn der ReRoute-Wert auf "true" (wahr) gesetzt ist. Dieser Wert wird zur Erfassung des Kanals für das weitergeleitete Dokument verwendet. |
| SegmentCountElementName | SE01/UNT01 | Wenn die Ausgabe EDI_TRANSACTION lautet, muss dieses Attribut angegeben werden. Dieses Attribut muss entsprechend dem gewünschten Umschlag definiert werden. |
| SegmentCount | Angepasst | Wenn die Ausgabe EDI_TRANSACTION lautet, muss dieses Attribut angegeben werden. Dieses Attribut enthält die Informationen zur Anzahl der Segmente in der Transaktion. |

Wenn das Ziel nach der Transformation EDI lautet, muss es mit einem Umschlag versehen werden, bevor es an die externen Partner gesendet wird. Das transformierte Ausgabedokument kann aus einer beliebigen Kombination von Formaten bestehen. Dies hängt davon ab, welche Informationen in der Kartennummer der Metadatenkarte codiert sind. Diese enthält die Eigenschaften anderer Kartendetails. Der Ersteller der Zuordnung codiert die Karte. Dabei werden die Attribute ReRoute, ReEnvelope und DocSyntax berücksichtigt. ReRoute und ReEnvelope können die Werte "true" (wahr) oder "false" (falsch) aufweisen; für DocSyntax kann der Benutzer einen beliebigen Wert eingeben. Nur wenn DocSyntax den Wert ediInchg aufweist, wird dieses Attribut beim Entfernen des Umschlags berücksichtigt. Im Folgenden werden die möglichen Ergebnisse für die verschiedenen Kombinationen von ReRoute und ReEnvelope beschrieben. Es wird davon ausgegangen, dass docSyntax auf EDI_INTERCHANGE gesetzt ist:

- ReRoute = True, ReEnvelope = False: Das Dokument wird auf ähnliche Weise verarbeitet wie andere Dokumente (XML oder ROD).
- ReRoute = False, ReEnvelope = False: Das Dokument wird auf ähnliche Weise verarbeitet wie andere Dokumente (XML oder ROD).
- Reroute = True, ReEnvelope = True: Zuerst wird der Umschlag vom Dokument entfernt. Für jede untergeordnete Transaktion wird ein untergeordnetes BDO erstellt. Das Wörterverzeichnis und das Dokument werden als Protokoll und Prozess definiert. Jedes dieser untergeordneten BDOs (Transaktion) wird mit dem Paket N/A weitergeleitet. Ein entsprechender Kanal muss vorhanden sein. Das Profil des Programms zur Umschlaggenerierung kann in den Zielattributen des Kanals konfiguriert werden. Für den Umschlag muss ein separater Kanal erstellt werden.

- Reroute = False, Reenvelope = True: Zuerst wird der Umschlag vom Dokument entfernt. Besteht die Ausgabe aus einer einzelnen Transaktion, wird das Geschäftsdokument mit der Transaktionsdatei als Position aktualisiert und gesendet. Besteht die Ausgabe aus vielen Transaktionen, werden untergeordnete BDOs so erstellt, dass sie nicht weitergeleitet werden, und gesendet. Das Zielattribut für diesen Kanal muss für das Profil des Programms zur Umschlaggenerierung entsprechend konfiguriert werden. Für das Programm zur Umschlaggenerierung muss ein Kanal vorhanden sein.

# EDI-Umgebung konfigurieren

Wie im vorherigen Abschnitt erwähnt, können Sie viele Attribute angeben, die zum Austausch der EDI-Austauschvorgänge gehören. Sie können z. B. die vom Produkt bereitgestellten Umschlagsprofile ändern, Sie können bestimmte Umschläge definieren, die für bestimmte Verbindungen verwendet werden sollen, Sie können Kontrollnummern festlegen, die den verschiedenen Teilen eines Austauschs zugeordnet sind, und Sie können Verbindungsprofile festlegen, sodass derselbe Austausch in unterschiedlicher Weise zugestellt werden kann. Diese Aufgaben werden in diesem Abschnitt beschrieben.

## Programm zur Umschlagsgenerierung

Das Programm zur Umschlagsgenerierung ist die Komponente, die eine Gruppe von Transaktionen zusammenstellt, die an einen Partner gesendet werden sollen, sie mit einem Umschlag versieht und sendet. Sie terminieren das Programm zur Umschlagsgenerierung oder akzeptieren den Standardzeitplan, um WebSphere Partner Gateway anzugeben, wann das Programm zur Umschlagsgenerierung nach zu sendenden Transaktionen suchen soll. Sie können auch die Standardwerte für die Sperrenzeit, das Höchstalter der Warteschlange und Stapelbetrieb aktualisieren.

**Anmerkung:** Das Konfigurieren des Programms zur Umschlagsgenerierung ist optional. Wenn Sie die Werte für das Programm zur Umschlagsgenerierung nicht ändern, werden die vom Produkt bereitgestellten Werte verwendet.

### Sperren

Jede Instanz von Document Manager hat ihr eigenes Programm zur Umschlagsgenerierung. Wenn auf Ihrem System zwei Document Manager installiert sind, verfügen Sie über zwei Programme zur Umschlagsgenerierung. Es ist daher möglich, dass zwei oder mehr Instanzen eines Programms zur Umschlagsgenerierung versuchen, eine Abfrage nach Transaktionen durchzuführen, die darauf warten, mit einem Umschlag versehen zu werden. Sperren werden verwendet, um sicherzustellen, dass eine gegebene Transaktion von genau einem Programm zur Umschlagsgenerierung abgefragt wird. Sperren stellen sicher, dass, wenn mehrere Programme zur Umschlagsgenerierung einbezogen werden, nur ein Programm zur Umschlagsgenerierung eine gegebene Transaktion abfragt und verarbeitet. Die Programme zur Umschlagsgenerierung führen Abfragen gleichzeitig durch, sie arbeiten aber an verschiedenen Transaktionen.

Für die Sperre ist ein Zeitlimit festgelegt worden. Der Standardwert für eine Instanz des Programms zur Umschlagsgenerierung, um die Sperre zu halten, beträgt 240 Sekunden.

Wenn das Programm zur Umschlagsgenerierung auf die Sperre warten muss, wird es in eine Warteschlange gestellt. Das Höchstalter der Warteschlange, d. h. die Dauer, die das Programm zur Umschlagsgenerierung warten sollte, beträgt 740 Sekunden.

In der Regel müssen Sie die Standardwerte für das Sperren nicht ändern.

### Stapelbetrieb

Mehrere Dokumente, die in einer Datei ankommen, werden entsprechend dem Verteilerhandler aufgeteilt, den Sie für diesen Dokumenttyp konfiguriert haben. (Das Konfigurieren von Verteilerhandlern, welches zum Definieren von Zielen gehört, wird in „ Konfigurationspunkte ändern" auf Seite 77 beschrieben.) Eines der Attribute des Verteilerhandlers ist BCG_BATCHDOCS. Wenn BCG_BATCHDOCS auf ON (den Standardwert) gesetzt ist, fügt der Verteiler den Dokumenten Stapel-IDs hinzu, nachdem die Dokumente aufgeteilt wurden.

Das Programm zur Umschlagsgenerierung verfügt über ein Attribut für den Stapelbetrieb, welches sich auf das Attribut BCG_BATCHDOCS bezieht. Wenn Stapel-IDs den einzelnen Dokumenten zugeordnet worden sind und Sie den Standardwert (ON) für Stapelbetrieb akzeptieren, stellt das Programm zur Umschlagsgenerierung sicher, dass alle Dokumente, die gemeinsam in derselben Datei ankommen, verarbeitet werden, bevor es diese mit einem Umschlag versieht und sie sendet, damit sichergestellt ist, dass die Transaktionen zusammen mit einem Umschlag versehen werden. Angenommen, es kommen z. B. fünf XML-Dokumente in derselben Datei an. Die XML-Dokumente sollen in EDI-Transaktionen transformiert und demselben Empfänger zugestellt werden. Nachdem nur drei der Dokumente transformiert wurden, beginnt das Programm zur Umschlagsgenerierung damit, seine terminierte Abfrage nach Transaktionen durchzuführen. Wenn der Stapelbetrieb ausgewählt ist, verarbeitet das Programm zur Umschlagsgenerierung die drei bereiten Transaktionen nicht, d. h. es versieht sie nicht mit einem Umschlag. Stattdessen wartet es so lange, bis die Verarbeitung aller fünf Transaktionen beendet wurde, bevor es sie mit einem Umschlag versieht und sie sendet. Die Transaktionen werden mit demselben Umschlag versehen, es sei denn, der gültige EDI-Standard verhindert das.

## Standardwerte ändern

Führen Sie die folgenden Schritte aus, um beliebige Standardwerte für das Programm zur Umschlagsgenerierung zu ändern:

1. Klicken Sie auf **Hubadmin > Hubkonfiguration > EDI > Programm zur Umschlagsgenerierung**.
2. Klicken Sie auf das Symbol **Bearbeiten**.
3. Geben Sie neue Werte für **Maximale Sperrenzeit (Sekunden)** und **Höchstalter der Warteschlange (Sekunden)** ein, wenn Sie diesen Attributen mehr oder weniger Zeit zuordnen wollen.

   **Anmerkung:** In der Regel müssen Sie die Standardwerte nicht ändern.
4. Wenn Sie den Stapelbetrieb inaktivieren wollen, entfernen Sie das Häkchen neben **Stapelbetrieb verwenden**.
5. Wenn Sie ändern wollen, wie oft das Programm zur Umschlagsgenerierung eine Überprüfung auf zu sendende Transaktionen durchführt, führen Sie eine der folgenden Aufgabengruppen aus:
   - Um die intervallbasierte Zeitplanung (dies ist die Standardeinstellung) mit Änderung des Zeitraums zu verwenden, geben Sie eine neue Zeit neben **Intervall** ein. Wenn Sie z. B. den Wert in 30 Sekunden ändern, führt das Programm zur Umschlagsgenerierung alle 30 Sekunden eine Überprüfung auf Dokumente durch, versieht diese Dokumente mit Umschlägen und sendet sie an den Empfänger.
   - Führen Sie die folgenden Aufgaben aus, um die kalenderbasierte Zeitplanung zu verwenden:

a. Klicken Sie auf **Kalenderbasierte Zeitplanung**.
b. Wählen Sie den Zeitplanungstyp **Täglicher Zeitplan**, **Wöchentlicher Zeitplan** oder **Angepasster Zeitplan** aus.
   – Wenn Sie **Täglicher Zeitplan** auswählen, dann wählen Sie die Uhrzeit (Stunde und Minute) aus, wann das Programm zur Umschlagsgenerierung eine Überprüfung auf Dokumente durchführen soll.
   – Wenn Sie **Wöchentlicher Zeitplan** auswählen, wählen Sie mindestens einen Tag in der Woche zusätzlich zur Uhrzeit aus.
   – Wenn Sie **Angepasster Zeitplan** auswählen, wählen Sie die Uhrzeit und schließlich noch **Bereich** oder **Ausgewählte Tage** für die Woche und den Monat aus. Mit **Bereich** geben Sie das Startdatum und das Enddatum an. (Sie können z. B. auf **Mo** und **Fr** klicken, wenn Sie wollen, dass das Programm zur Umschlagsgenerierung nur an Wochentagen zu einer bestimmten Uhrzeit eine Überprüfung auf Dokumente durchführt.) Mit der Option **Ausgewählte Tage** wählen Sie bestimmte Tage in der Woche und im Monat aus.
6. Klicken Sie auf **Speichern**.

## Umschlagsprofile

Ein Umschlagsprofil legt die Werte fest, die in bestimmte Elemente des Umschlags gestellt werden. Sie ordnen das Umschlagsprofil den EDI-Transaktionen im Dokumentdefinitionsattribut **Umschlagsprofil** zu. WebSphere Partner Gateway stellt ein vordefiniertes Umschlagsprofil für jeden unterstützten Standard (X12, EDIFACT oder UCS) bereit. Sie können diese vordefinierten Umschläge direkt verwenden, Sie können sie ändern, oder Sie können sie in neue Umschlagsprofile kopieren. Die Schritte zum Ändern oder Erstellen eines Umschlagsprofils sind in „Die Standardwerte ändern” auf Seite 198 beschrieben.

Die Umschlagsprofile haben für jedes Element im Umschlagsstandard ein Feld. Die Profile stellen konstante oder Literaldaten für das Erstellen von Header- und Trailersegmenten für Transaktionsgruppen, Nachrichten, funktionale Gruppen und Austauschvorgänge bereit. Sie geben nur die Werte an, die ausgefüllt werden müssen und für die keine andere Quelle einen Wert bereitstellt.

Die Feldnamen sind für das problemlose Arbeiten mit Querverweisen entworfen worden. Das Feld UNB03 ist z. B. das dritte Datenelement im UNB-Segment.

Wie in „ Umschlagsattribute” beschrieben, haben Attribute, die woanders festgelegt wurden, Vorrang vor den Werten, die Sie im Umschlagsprofil festlegen. Einige der Attribute können in Attributen oder Zuordnungen überschrieben werden, die sich auf die Dokumentdefinition beziehen.

### Umschlagsattribute

Umschlagsattribute können an mehreren unterschiedlichen Punkten während des Konfigurationsprozesses festgelegt werden, und sie können auch in der Transformationszuordnung festgelegt werden, die den Dokumenten zugeordnet ist. Der Zuordnungsexperte des Data Interchange Services-Clients kann z. B. das Merkmal **CtlNumFlag** angeben, wenn er eine Zuordnung definiert. Dieses Merkmal kann auch als Teil des Umschlagsprofils im Feld **Kontrollnummern nach Transaktions-IDs** festgelegt werden. Jedes Attribut, das in der Transformationszuordnung festgelegt ist, überschreibt die zugehörigen Werte, die in Community Console festgelegt wurden. Wenn z. B. für **CtlNumFlag** in der Transformationszuordnung **N** (nein) festgelegt wurde und Sie den Wert **Y** (ja) im Feld **Kontrollnummern nach Transaktions-IDs** eingeben, wird der Wert **N** verwendet.

Weitere Umschlagsprofile können auf Protokollebene über die Seite **Dokumentdefinitionenverwalten** bzw. über die einem Partner zugeordnete Seite **B2B-Funktionalität** festgelegt werden, oder sie können als Teil der Verbindung festgelegt werden. Die Rangfolge wird in der folgenden Liste aufgezeigt:

1. Merkmale, die in der Transformationszuordnung festgelegt sind, haben Vorrang vor den zugehörigen Attributen, die in Community Console festgelegt wurden.
2. Attribute, die auf der Verbindungsebene festgelegt sind, haben Vorrang vor denen, die auf der B2B-Funktionalitätsebene festgelegt wurden.
3. Attribute, die auf der B2B-Funktionalitätsebene festgelegt sind, haben Vorrang vor denen, die auf derEbene der Dokumentdefinition festgelegt wurden.
4. Attribute, die an einem beliebigen Ort (entweder in der Transformationszuordnung oder auf der Ebene der Dokumentdefinition, der B2B-Funktionalität oder der Verbindung) festgelegt sind, haben Vorrang vor den Werten, die im Umschlagsprofil festgelegt wurden.

Eine Liste der Transformationszuordnungsmerkmale und ihrer zugeordneten Community Console-Attribute finden Sie in „Data Interchange Services-Clientmerkmale" auf Seite 450.

## Die Standardwerte ändern

„ Attribute für Umschlagsprofil" auf Seite 437 stellt eine Tabelle bereit, die die Standardwerte für jedes EDI-Standardumschlagsattribut zeigt, wenn Sie keinen Wert in das Profil eingeben, oder wenn Sie kein Profil erstellen. Stellen Sie sicher, dass die von Ihnen verwendeten Umschlagsprofile jedes obligatorische Element bereitstellen, das nicht vom System zur Ausführungszeit bereitgestellt wird.

Führen Sie die folgenden Schritte aus, um ein Umschlagsprofil zu konfigurieren:

1. Klicken Sie auf **Hubadmin > Hubkonfiguration > EDI > Umschlagsprofil**.
2. Führen Sie eine der folgenden Schrittegruppen aus:
   - Umschlag erstellen
     a. Klicken Sie auf **Erstellen**.
     b. Geben Sie einen Namen für das Umschlagsprofil ein. Dies ist der Name, der in der Liste **Umschlagsprofile** angezeigt wird.
     c. Geben Sie optional eine Beschreibung des Profils ein.
     d. Klicken Sie auf den EDI-Standard, zu dem der Umschlag gehört. Wenn Sie z. B. Dokumente austauschen, die dem EDI-X12-Standard entsprechen, wählen Sie **X12** aus.
   - Umschlag ändern
     a. Wählen Sie eines der vorhandenen Umschlagsprofile aus, indem Sie auf das Symbol **Details anzeigen** neben dem Namen des Profils klicken.
     b. Klicken Sie auf das Symbol **Bearbeiten**.
3. Die Schaltfläche **Allgemein** ist standardmäßig ausgewählt. Sie können einen Wert für ein beliebiges Feld eingeben mit Ausnahme von ENVTYPE, welcher mit dem Standard vorab ausgefüllt wurde, den Sie in Schritt 2d ausgewählt haben.

Sie können für die folgenden Felder Werte hinzufügen:

- **Länge der Austauschkontrollnummer**. Gibt an, wie viele Zeichen verwendet werden sollten, wenn eine Kontrollnummer einem Austausch im Umschlag zugeordnet wird.
- **Länge der Gruppenkontrollnummer**. Gibt an, wie viele Zeichen verwendet werden sollten, wenn eine Kontrollnummer einer Gruppe im Umschlag zugeordnet wird.
- **Länge der Transaktionskontrollnummer**. Gibt an, wie viele Zeichen verwendet werden sollten, wenn eine Kontrollnummer einer Transaktion im Umschlag zugeordnet wird.
- **Max. Anzahl an Transaktionen**. Gibt die maximale Anzahl Transaktionen an, die in diesem Umschlag zulässig sind.
- **Kontrollnummern nach Transaktions-IDs**. Gibt an, ob Sie die Transaktions-ID als Teil des Schlüssels verwenden wollen, wenn die Gruppennummern in der Datenbank gesucht werden. Ist dies der Fall, werden verschiedene Gruppen von Kontrollnummern für jede Transaktions-ID verwendet.

Die Felder für das Umschlagsprofil **Allgemein** sind in allen drei Standards gleich, außer dass EDIFACT über ein zusätzliches Feld verfügt: **Gruppen für EDI erstellen**.

Wenn Sie Änderungen an der Seite **Allgemein** vorgenommen haben, klicken Sie auf **Speichern**.

4. Um Werte für den Austausch anzugeben, klicken Sie auf **Austausch**. Eine neue Gruppe von Feldern wird auf der Seite angezeigt. Die Felder variieren je nach EDI-Standard. Beachten Sie, dass einige von den Werten schon ausgefüllt sind bzw. während der Ausführung ausgefüllt werden.
   - Für den EDI-X12-Standard können Sie die folgenden Felder ändern:
     - **ISA01: Qualifikationsmerkmal für Autorisierungsinformationen**. Dies ist ein Code für den Informationstyp in ISA02.
     - **ISA02: Autorisierungsinformationen**. Das sind Informationen, die verwendet werden, um den Absender der Austauschdaten noch weiter anzugeben bzw. zu autorisieren.
     - **ISA03: Qualifikationsmerkmal für Sicherheitsinformationen**. Dies ist ein Code für den Informationstyp in ISA04. Gültige Werte:

       **00** ISA04 ist nicht aussagekräftig.

       **01** ISA04 enthält ein Kennwort.
     - **ISA04: Sicherheitsinformationen**. Das sind Sicherheitsinformationen zu dem Absender oder den Austauschdaten. Der Code in ISA03 definiert den Informationstyp.
     - **ISA11: ID der Austauschstandards**. Das ist ein Code für die Stelle, die den Austausch kontrolliert. Gültige Werte sind **U** (US EDI Community von ASC X12), **TDCC**, und **UCS**.

       **Anmerkung:** Dieses Attribut wird für X12-Versionen bis 4010 verwendet. In X12 4020 wird das ISA11-Element als Wiederholungstrennzeichen verwendet.
     - **ISA12: ID der Austauschversion**. Das ist die Versionsnummer der Syntax in den Austauschsegmenten und den Steuerungssegmenten der funktionalen Gruppe.
     - **ISA14: Bestätigung angefordert**. Das ist der Code des Absenders für das Anfordern einer Bestätigung. Gültige Werte:

**0** Keine Bestätigung anfordern.

**1** Bestätigung darüber anfordern, dass ISA- und IEA-Segmente empfangen und erkannt wurden.

– **ISA15: Testanzeiger**. Das ist eine Meldung darüber, dass der Austausch für Testzwecke oder die Produktion ist. Gültige Werte:

**T** Für Testdaten.

**P** Für Produktionsdaten.

- Für den UCS-Standard können Sie die folgenden Felder ändern:
  – **BG01: Kommunikations-ID**. Das ist die Kennung des übertragenden Unternehmens.
  – **BG02: Kommunikationskennwort**. Das ist ein vom Empfänger zugeordnetes Kennwort, das von den Partnern als vereinbart verwendet werden soll.
- Für den EDIFACT-Standard können Sie die folgenden Felder ändern:
  – **UNB0101: Syntax-ID**. Das ist die Kennung der Stelle, die die verwendete Syntax kontrolliert. Die kontrollierende Stelle lautet UNO. Die Ebene ist A oder B.
  – **UNB0102: Syntaxversion**. Das ist die Versionsnummer der Syntax, die von der Syntax-ID angegeben wird.
  – **UNB0601: Referenz/Kennwort des Empfängers**. Das ist ein vom Empfänger zugeordnetes Kennwort, das von den Partnern als vereinbart verwendet werden soll.
  – **UNB0602: Qualifikationsmerkmal für Referenz/Kennwort des Empfängers**. Das ist ein Qualifikationsmerkmal für das Kennwort des Empfängers, das von den Partner als vereinbart verwendet werden soll.
  – **UNB07: Anwendungsreferenz**. Das ist die Kennung des Funktionsbereichs vom Absender, auf die die Austauschnachrichten verweisen.
  – **UNB08: Priorität**. Das ist der Code des Absenders für die Verarbeitungspriorität, wie mit dem Partner vereinbart. Code A hat die höchste Priorität.
  – **UNB09: Bestätigungsanforderung**. Das ist der Code des Absenders für das Anfordern einer Bestätigung.
  – **UNB10: ID der Kommunikationsvereinbarung**. Das ist der Name oder Code für den Vereinbarungstyp, der für diesen Austausch verwendet wird, wie mit dem Partner vereinbart.
  – **UNB11: Testanzeiger (Nutzungsanzeiger)**. Das ist eine Meldung darüber, dass der Austausch für Testzwecke ist. 1 gibt einen Testaustausch an.

Wenn Sie Änderungen an der Seite **Austausch** vorgenommen haben, klicken Sie auf **Speichern**.

5. Um Werte für die Gruppen im Austausch anzugeben, klicken Sie auf **Gruppe**. Eine neue Gruppe von Feldern wird angezeigt. Die Felder variieren je nach EDI-Standard.

   Die Felder auf dieser Seite definieren in der Regel den Absender und den Empfänger der Gruppe.

   - Für die EDI-X12- und UCS-Standards können Sie in den folgenden Feldern Werte eingeben:
     – **GS01: ID der funktionalen Gruppe**. Das ist eine Kennung des Transaktionsgruppentyps in der Gruppe.
     – **GS02: Anwendungsabsender**. Das ist der Name oder Code für eine bestimmte Abteilung im Unternehmen des Absenders.

- **GS03: Anwendungsempfänger**. Das ist der Name oder Code für die bestimmte Abteilung im Unternehmen des Empfängers, die die Gruppe empfangen soll.
- **GS07: Gruppenstelle**. Das ist ein Code, der mit GS08 verwendet wird, um die Stelle anzugeben, die den Standard kontrolliert.
- **GS08: Gruppenversion**. Das ist ein Code für die Version, das Release und die Branche des Standards.

• Für den EDIFACT-Standard können Sie in den folgenden Feldern Werte eingeben:
- **UNG01: ID der funktionalen Gruppe**. Das ist eine Kennung des Nachrichtentyps in der Gruppe.
- **UNG0201: Anwendungsabsender-ID**. Das ist der Name oder Code für eine bestimmte Abteilung im Unternehmen des Absenders.
- **UNG0202: Qualifikationsmerkmal für Anwendungsabsender-ID**. Das ist das Qualifikationsmerkmal für den Absender-ID-Code. Eine Liste der Qualifikationsmerkmale für den Code finden Sie im Datenelementverzeichnis.
- **UNG0301: Anwendungsempfänger-ID**. Das ist der Name oder Code für die bestimmte Abteilung im Unternehmen des Empfängers, die die Gruppe empfangen soll.
- **UNG0302: Qualifikationsmerkmal für Anwendungsempfänger-ID**. Das ist das Qualifikationsmerkmal für den Empfänger-ID-Code. Eine Liste der Qualifikationsmerkmale für den Code finden Sie im Datenelementverzeichnis.
- **UNG06: Kontrollierende Stelle**. Der Code, der die Stelle angibt, welche die Kontrolle über den Nachrichtentyp in der funktionalen Gruppe hat.
- **UNG0701: Nachrichtenversion**. Das ist die Versionsnummer für den Nachrichtentyp.
- **UNG0702: Nachrichtenrelease**. Das ist die Releasenummer in der Versionsnummer für den Nachrichtentyp.
- **UNG0703: Zugeordnete Assoziation**. Das ist der Code, der von der verantwortlichen Assoziation zugeordnet wurde, der den Nachrichtentyp noch weiter angibt.
- **UNG08: Anwendungskennwort**. Das ist das Kennwort, das von der bestimmten Abteilung im Unternehmen des Empfängers zugeordnet wurde.

Wenn Sie Änderungen an der Seite **Gruppe** vorgenommen haben, klicken Sie auf **Speichern**.

6. Um Werte für Transaktionen in einer Gruppe anzugeben, klicken Sie auf **Transaktion**, oder bei EDIFACT klicken Sie auf **Nachricht**. Eine neue Gruppe von Feldern wird angezeigt. Die Felder variieren je nach EDI-Standard.
   • Für den EDI-X12- oder USC-Standard können Sie einen Wert für **ST03: ID-Zeichenfolge der Implementierungskonvention** eingeben.
   • Für den EDIFACT-Standard können Sie in den folgenden Feldern einen Wert eingeben:
   - **UNH0201: Nachrichtentyp**. Das ist ein Code, der von der kontrollierenden Stelle zugeordnet wurde, um den Nachrichtentyp anzugeben.
   - **UNH0202: Nachrichtenversion**. Das ist die Versionsnummer für den Nachrichtentyp.
   - **UNH0203: Nachrichtenrelease**. Das ist die Releasenummer in der Versionsnummer für den Nachrichtentyp.

- **UNH0204: Kontrollierende Stelle**. Das ist ein Code für die Stelle, die den Nachrichtentyp kontrolliert.
- **UNH0205: Von Assoziation zugeordneter Code**. Das ist der Code, der von der verantwortlichen Assoziation zugeordnet wurde, der den Nachrichtentyp noch weiter angibt.
- **UNH03: Referenz für allgemeinen Zugriff**. Das ist der Schlüssel, der auf alle nachfolgenden Datenübertragungen in eine gemeinsame Datei verweist. Partner können der Verwendung eines Schlüssels zustimmen, der aus Komponenten besteht, aber Unterelementseparatoren können nicht verwendet werden.

Wenn Sie Änderungen an der Seite **Transaktion** vorgenommen haben, klicken Sie auf **Speichern**.

7. Klicken Sie auf **Speichern**.
8. Wiederholen Sie die Schritte 2 auf Seite 198 bis 7 für jedes weitere Umschlagsprofil, das Sie definieren oder ändern wollen.

Nachdem ein Umschlagsprofil definiert ist, wird es in der Liste **Umschlagsprofile** aufgelistet. Sie können das Profil in der Liste auswählen, und klicken Sie dann auf das Symbol **Verwendet von**, um die Verbindungen zu ermitteln, die das Profil verwenden.

## Verbindungsprofile

Sie verwenden Verbindungsprofile mit Transaktionen, von denen der Umschlag entfernt wurde, und mit EDI-Austauschvorgängen, die vom Programm zur Umschlaggenerierung erstellt wurden. Bei Transaktionen bestimmt das Verbindungsprofil, wie die Transaktion verarbeitet wird, nachdem ihr Umschlag entfernt wurde. Bei Austauschvorgängen bestimmt das Verbindungsprofil, wie der Austausch zugestellt wird.

Über das Fenster **Verbindungsprofile** können Sie ein neues Profil erstellen oder die vorhandenen Profilinformationen bearbeiten. In der Liste der Verbindungsprofil finden Sie die Namen der derzeit definierten Profile und eine Beschreibung, falls vorhanden. Weitere Informationen zu Verbindungsprofilen finden Sie im Handbuch *WebSphere Partner Gateway Hubkonfiguration*.

### Transaktionen

Wenn ein EDI-Austausch bei WebSphere Partner Gateway eingeht, besteht die erste Aktion in der Regel darin, vom Austausch den Umschlag zu entfernen, um so die einzelnen Transaktionen zu erhalten. Wenn die Transaktionen erstellt sind, legt die Aktion zum Umschlag entfernen den **Nutzungsanzeiger für Austausch** und die Gruppeninformationen (**Kennung für Absender der Gruppenanwendung**, **Kennung für Empfänger der Gruppenanwendung** und **Kennwort für Gruppenanwendung**) in den Transaktionsmetadaten fest. Jede Transaktion wird dann erneut von WebSphere Partner Gateway in ihrem eigenen Arbeitsablauf verarbeitet.

Angenommen, Sie verfügen über zwei Transaktionen desselben Typs (z. B. 850), die abhängig von der Gruppe, in der sie sich befinden, oder von den Werten Ihrer Nutzungsanzeiger für Austausch unterschiedlich verarbeitet werden müssen. Wenn der **Nutzungsanzeiger** z. B. Produktion (**P**) lautet, wollen Sie unter Umständen eine Zuordnung (A) verwenden, und wenn der **Nutzungsanzeiger** Test (**T**) lautet, wollen Sie möglicherweise eine zweite Zuordnung (B) verwenden. Zwei ähnliche Verbindungen sind für diese 850-Transaktion erforderlich, der einzige Unterschied besteht darin, dass eine Verbindung Zuordnung A und die andere Verbindung Zuordnung B verwendet.

Da die Transaktionen sich sonst nicht unterscheiden (sie verfügen über Partner, Paket, Protokoll und Dokumenttyp derselben Quelle und desselben Ziels), benötigt Document Manager eine Möglichkeit, um zu ermitteln, welche Verbindung verwendet werden soll. Er tut dies, indem er das Verbindungsprofilattribut in Übereinstimmung bringt, das Sie in den Transaktionsmetadaten festgelegt haben. Wenn Sie in diesem Beispiel zwei Verbindungsprofile erstellt haben, ein Verbindungsprofil (CPProduction) mit **EDI-Verwendungstyp** auf **P** und das andere Verbindungsprofil (CPTest) mit **EDI-Verwendungstyp** auf **T** gesetzt, bringt Document Manager die Transaktion mit einem **Nutzungsanzeiger** von **P** mit dem CPProduction-Profil in Übereinstimmung. Er weiß dann, dass Zuordnung A zu verwenden ist, um die Transaktion zu konvertieren.

Das Beispiel in diesem Abschnitt hat das Attribut **Nutzungsanzeiger für Austausch** verwendet, aber Sie können auch die Attribute **Kennung für Absender der Gruppenanwendung**, **Kennung für Empfänger der Gruppenanwendung** und **Kennwort für Gruppenanwendung** als Unterscheidungsfaktor für eine Transaktion verwenden.

## Austauschvorgänge

Bei Austauschvorgängen verwenden Sie das Attribut **Qualifikationsmerkmal1 für Verbindungsprofil**.

Angenommen, Sie sind z. B. mitten bei der Migration Ihres Unternehmens von der Verwendung eines VAN (Paket **None**) oder des Internets (Paket **AS2**). Sie wollen, dass 840-Transaktionen (Request for Quote) das VAN und 850-Transaktionen (Purchase Order) das Internet verwenden. Sie konfigurieren zwei Partnerverbindungen, die beide denselben Quellenaustausch, aber unterschiedliche Ziele haben (eine Verbindung mit Paket **None** und die andere Verbindung mit Paket **AS2**). Die Verbindungsprofile sind bei der Unterscheidung der zwei Verbindungen hilfreich.

Das Konfigurieren des Verbindungsprofils für Austauschvorgänge schließt mehrere Schritte ein. Die folgenden Schritte würden Sie ausführen, um zwei Verbindungsprofile für das Beispiel zu erstellen:

1. Erstellen Sie zwei Verbindungen für die Transaktionen. Legen Sie das Attribut **Qualifikationsmerkmal1 für Verbindungsprofil** auf der Seite "An" von beiden Verbindungen fest. Der Wert sollte aussagekräftig sein, z. B. 'ConNone' und 'ConAS2'.
2. Definieren Sie zwei Verbindungsprofile, z. B. CPNone und CPAS2, legen Sie den Wert **Qualifikationsmerkmal1** für beide so fest, dass sie mit den Attributen **Qualifikationsmerkmal1 für Verbindungsprofil** übereinstimmen, die Sie in Schritt 1 (ConNone und ConAS2) festgelegt haben.
3. Erstellen Sie zwei Verbindungen für den Austausch. Jede Verbindung hat dasselbe Quellenpaket **N/A**, aber unterschiedliche Zielpakete (**None** und **AS2**). Für die Partnerverbindung mit dem Verbindungsprofil 'ConNone' ist als Ziel das FTP-Scripting-Ziel festgelegt, das eine Verbindung zum VAN herstellen kann. Für die Partnerverbindung mit dem Verbindungsprofil 'CPAS2' ist als Zielpaket **AS** festgelegt.
4. Ordnen Sie die entsprechenden Verbindungsprofile einander zu.

Das Programm zur Umschlagsgenerierung verwendet das Attribut **Qualifikationsmerkmal1 für Verbindungsprofil** auf der Seite "An" der Partnerverbindung als Umschlagsunterbrechungspunkt. Daher werden Transaktionen, die unterschiedliche Werte für das Attribut **Qualifikationsmerkmal1 für Verbindungsprofil** haben, mit unterschiedlichen Umschlägen versehen. Wenn Sie unterschiedliche Werte für die

Transaktionen festlegen, wird das Programm zur Umschlagsgenerierung die 840- und 850-Transaktionen nie mit einem Umschlag für denselben Austausch versehen.

Wenn Document Manager die Verbindung sucht, werden die zwei möglichen Verbindungen gefunden, aber die Verbindung mit dem übereinstimmenden Verbindungsprofil wird verwendet.

## Verbindungsprofile konfigurieren

Das Konfigurieren der Verbindungsprofile ist optional. Wenn Sie für jeden Dokumenttyp nur jeweils eine Verbindung benötigen, dann führen Sie den Austausch für einen Partner durch. Überspringen Sie diesen Abschnitt.

Gehen Sie wie folgt vor, um ein Verbindungsprofil zu konfigurieren:

1. Klicken Sie auf **Hubadmin > Hubkonfiguration > EDI > Verbindungsprofile**.
2. Klicken Sie auf **Verbindungsprofil erstellen**.
3. Geben Sie auf der Seite **Details des Verbindungsprofils** einen erforderlichen Namen für dieses Verbindungsprofil ein.
4. Geben Sie eine optionale Beschreibung des Profils ein.

   Der Name und die Beschreibung, falls Sie eine Beschreibung eingeben, werden auf der Seite **Liste der Verbindungsprofile** angezeigt.
5. Geben Sie optional einen Wert für **Qualifikationsmerkmal1** zur Angabe des Werts ein, der bestimmt, welche Verbindung für einen EDI-Austausch verwendet wird. Ein Beispiel zur Verwendung von **Qualifikationsmerkmal1** finden Sie im Abschnitt „ Austauschvorgänge" auf Seite 203.
6. Geben Sie optional einen Wert für **EDI-Verwendungstyp** ein, um anzugeben, ob dies ein Test-, Produktions- oder Informationsaustausch ist. Ein Beispiel zur Verwendung von **EDI-Verwendungstyp** finden Sie im Abschnitt „ Transaktionen" auf Seite 202.
7. Geben Sie optional einen Wert für **Anwendungsabsender-ID** ein, um die Anwendung oder den Unternehmensbereich anzugeben, die bzw. der dem Absender der Gruppe zugeordnet ist.
8. Geben Sie optional einen Wert für **Anwendungsempfänger-ID** ein, um die Anwendung oder den Unternehmensbereich anzugeben, die bzw. der dem Empfänger der Gruppe zugeordnet ist.
9. Geben Sie optional einen Wert für **Kennwort** ein, falls ein Kennwort zwischen dem Anwendungsabsender und dem Anwendungsempfänger erforderlich ist.
10. Klicken Sie auf **Speichern**.

Für die Transaktionen, die Sie in bestimmten Austauschumschläge ablegen wollen, können Sie den Attributwert **Qualifikationsmerkmal1 für Verbindungsprofil** angeben, der dem Verbindungsprofil mit demselben Wert für das Attribut **Qualifikationsmerkmal1** entspricht. Das Attribut **Qualifikationsmerkmal1 für Verbindungsprofil** kann auf der Protokollebene einer Dokumentdefinition festgelegt werden. Sie könnten z. B. die Attribute des X12V5R1-Protokolls in der Anzeige **Dokumentdefinitionen verwalten** bearbeiten, um das zu verwendende Verbindungsprofil anzugeben, indem Sie auf den entsprechenden Attributwert **Qualifikationsmerkmal1 für Verbindungsprofil** klicken. Dann, wenn Sie die Austauschverbindung aktiviert haben, ordnen Sie das Verbindungsprofil zu, indem Sie auf die Schaltfläche **Verbindungsprofil** klicken und ein Profil in der Liste auswählen.

## Kontrollnummern

Das Programm zur Umschlaggenerierung verwendet Kontrollnummern, um eine eindeutige Nummerierung für Austauschvorgänge, Gruppen und Transaktionen in einem Umschlag bereitzustellen. Kontrollnummern werden für den internen Partner und für externe Partner erstellt. Wenn der Austausch von Dokumenten stattfindet, werden Kontrollnummern auch für das *Paar* von Partnern generiert.

Für jeden Partner, der über die EDI-B2B-Funktionalität verfügt, gibt es eine Gruppe von Startinitialisierungswerten für Kontrollnummern. Diese Werte werden verwendet, wenn ein EDI-Austausch das erste Mal erstellt und zwischen einem Partnerpaar gesendet wird. Die Initialisierungswerte werden auf den Partner angewendet, an den der Austausch gesendet wird. Nachdem ein Dokument von einem Partner zum anderen gesendet wurde, können die zuletzt verwendeten Nummern auf der Seite **Aktuelle Kontrollnummern** angezeigt werden. Es kann mehrere Einträge für ein gegebenes Partnerpaar geben, wenn **Kontrollnummern nach Transaktions-IDs** auf **Y** gesetzt ist. Nachdem ein Eintrag vorhanden ist, werden mit ihm neue Kontrollnummern generiert.

Als Teil der Kontrollnummerninitialisierung können Sie Masken verwenden, um die normale Kontrollnummernerstellung durch das Programm zur Umschlaggenerierung zu ändern. Die Masken werden verwendet, damit die Kontrollnummer entweder auf dem Austausch oder auf der Gruppenkontrollnummer basiert. Die Maskenbeschreibungen folgen. Ersetzen Sie das *n* in der Bearbeitungsmaske mit der Anzahl Byte, die Sie für die Erstellung des Kontrollnummernwerts verwenden wollen. In Tabelle 28 sind die Beschreibungen der verfügbaren Codes enthalten:

*Tabelle 28. Kontrollnummernmasken*

| Code | Kontrollnummer | Beschreibung |
|---|---|---|
| G | Transaktion | Die Transaktionskontrollnummer entspricht der Gruppenkontrollnummer. Es ist nur eine Transaktion für jede Gruppe zulässig. |
| G*n* | Transaktion | *n* Byte werden von der Gruppenkontrollnummer genommen. Der Rest der Transaktionskontrollnummer wird bis zu ihrer Maximalgröße mit Nullen aufgefüllt. Es ist nur eine Transaktion für jede Gruppe zulässig. |
| C | Gruppe, Transaktion | Die übrigen Byte im Feld für die Gruppen- oder Transaktionskontrollnummer werden verwendet, um eine Kontrollnummer für diesen Partner zu verwalten. |
| V | Gruppe, Transaktion | Ein zunehmender Wert wird verwendet, sodass die erste Gruppe oder Transaktion einen Wert von 1 hat, die zweite einen Wert von 2 usw. |
| V*n* | Transaktion | Ein zunehmender Wert, der *n* Byte lang ist, wird verwendet, sodass die erste Transaktion einen Wert von 1 hat, die zweite einen Wert von 2 usw. |
| G*n*C | Transaktion | *n* Byte werden von der Gruppenkontrollnummer genommen und die übrigen Byte im Feld für die Transaktionskontrollnummer werden verwendet, um eine Kontrollnummer zu verwalten. Die Anzahl ausgelassener Stellen bestimmt den Höchstwert der Kontrollnummer. G5C lässt z. B. vier Stellen aus; daher beträgt der Höchstwert 9999. Die Kontrollnummer springt vom Höchstwert wieder auf 1 zurück. |

*Tabelle 28. Kontrollnummernmasken (Forts.)*

| Code | Kontrollnummer | Beschreibung |
|---|---|---|
| G*n*V | Transaktion | *n* Byte werden von der Gruppenkontrollnummer genommen. Für die übrigen Byte im Feld für die Transaktionskontrollnummer wird ein zunehmender Wert verwendet, sodass die erste Transaktion einen Wert von 1 hat, die zweite einen Wert von 2 usw. |
| G*n*V*m* | Transaktion | *n* Byte werden von der Gruppenkontrollnummer genommen. Für die übrigen Byte, bis zu *m* Byte, im Feld für die Transaktionskontrollnummer wird ein zunehmender Wert verwendet, sodass die erste Transaktion einen Wert von 1 hat, die zweite einen Wert von 2 usw. |
| I | Gruppe, Transaktion | Die Gruppen- oder Transaktionskontrollnummer sollte der Austauschkontrollnummer gleichen. Für den Austausch ist nur eine Gruppe zulässig und für die Gruppe oder den Austausch ist nur eine Transaktion zulässig. |
| I*n* | Gruppe, Transaktion | *n* Byte werden von der Austauschkontrollnummer genommen. Der Rest des Felds für die Gruppen- oder Transaktionskontrollnummer wird bis zur Maximalgröße mit Nullen aufgefüllt. Für jeden Austausch ist nur eine Gruppe zulässig und für jede Gruppe ist nur eine Transaktion zulässig. |
| I*n*C | Gruppe, Transaktion | *n* Byte werden von der Austauschkontrollnummer genommen. Die übrigen Byte im Feld für die Gruppen- oder Transaktionskontrollnummer werden verwendet, um eine Kontrollnummer zu verwalten. Die Anzahl ausgelassener Stellen bestimmt den Höchstwert der Kontrollnummer. I5C lässt z. B. vier Stellen aus; daher beträgt der Höchstwert 9999. Die Kontrollnummer springt vom Höchstwert wieder auf 1 zurück. |
| I*n*V | Gruppe, Transaktion | *n* Byte werden von der Austauschkontrollnummer genommen. Für die übrigen Byte im Feld für die Gruppen- oder Transaktionskontrollnummer wird ein zunehmender Wert verwendet, sodass die erste Gruppe oder Transaktion einen Wert von 1 hat, die zweite einen Wert von 2 usw. |
| I*n*V*m* | Transaktion | *n* Byte werden von der Austauschkontrollnummer genommen. Für die übrigen Byte, bis zu *m* Byte, im Feld für die Transaktionskontrollnummer wird ein zunehmender Wert verwendet, sodass die erste Transaktion einen Wert von 1 hat, die zweite einen Wert von 2 usw. |
| I*n*G*m* | Transaktion | *n* Byte werden von der Austauschkontrollnummer genommen und ein Maximum von *m* Byte werden von der Gruppenkontrollnummer genommen. Wenn *n* + *m* größer als 9 ist, werden nur 9 - *n* Byte von der Gruppenkontrollnummer genommen. Wenn Sie z. B. I4G6 verwenden, dann werden 4 Byte vom Austausch genommen. |

*Tabelle 28. Kontrollnummernmasken (Forts.)*

| Code | Kontrollnummer | Beschreibung |
|---|---|---|
| I*n*G*m*C | Transaktion | *n* Byte werden von der Austauschkontrollnummer genommen und *m* Byte werden von der Gruppenkontrollnummer genommen. Die übrigen Byte im Feld für die Transaktionskontrollnummer werden verwendet, um eine Kontrollnummer zu verwalten. Die Anzahl ausgelassener Stellen bestimmt den Höchstwert der Kontrollnummer. I2G4C lässt z. B. drei Stellen aus; daher beträgt der Höchstwert 999. Die Kontrollnummer springt vom Höchstwert wieder auf 1 zurück. |
| I*n*G*m*V | Transaktion | *n* Byte werden von der Austauschkontrollnummer genommen und *m* Byte werden von der Gruppenkontrollnummer genommen. Für die übrigen Byte im Feld für die Transaktionskontrollnummer wird ein zunehmender Wert verwendet, sodass die erste Transaktion einen Wert von 1 hat, die zweite einen Wert von 2 usw. |
| I*n*G*m*V*o* | Transaktion | *n* Byte werden von der Austauschkontrollnummer genommen und *m* Byte werden von der Gruppenkontrollnummer genommen. Für die übrigen Byte, bis zu *o* Byte, im Feld für die Transaktionskontrollnummer wird ein zunehmender Wert verwendet, sodass die erste Transaktion einen Wert von 1 hat, die zweite einen Wert von 2 usw. |

## Kontrollnummer initialisieren

Führen Sie die folgenden Schritte aus, um die Kontrollnummern zu konfigurieren, die das Programm zur Umschlaggenerierung verwenden wird:

1. Klicken Sie auf **Hubadmin > Hubkonfiguration > EDI > Initialisierung der Kontrollnummer**.
2. Geben Sie einen Partnernamen ein und klicken Sie auf **Suchen**, oder klicken Sie auf **Suchen**, ohne einen Namen einzugeben, um alle Partner anzuzeigen. Wenn Sie **EDI-fähige suchen** auswählen, begrenzen Sie die Suche auf die Partner, die über EDI-Dokument-B2B-Funktionalität verfügen. Wenn Sie das Häkchen entfernen, durchsuchen Sie alle Partner.
3. Klicken Sie auf das Symbol **Details anzeigen** neben dem Partner.
4. Die aktuellen Kontrollnummernzuordnungen des Partners (sofern vorhanden) werden auf der Seite **Konfigurationsdetails der Kontrollnummer** angezeigt. Klicken Sie auf das Symbol **Bearbeiten**, um die Werte hinzuzufügen oder zu ändern.
5. Geben Sie den Wert neben **Austausch** ein oder ändern Sie ihn, um die Nummer anzugeben, mit der Sie die Kontrollnummerngenerierung für Austauschvorgänge initialisieren wollen.
6. Geben Sie den Wert neben **Gruppen** ein oder ändern Sie ihn, um die Nummer anzugeben, mit der Sie die Kontrollnummerngenerierung für Gruppen initialisieren wollen. Alternativ hierzu können Sie auf **Maske** klicken und anstelle eines festen Werts eine zu verwendende Maske eingeben.

7. Geben Sie den Wert neben **Transaktion** ein oder ändern Sie ihn, um die Nummer anzugeben, mit der Sie die Kontrollnummerngenerierung für Transaktionen initialisieren wollen. Alternativ hierzu können Sie auf **Maske** klicken und anstelle eines festen Werts eine zu verwendende Maske eingeben.
8. Klicken Sie auf **Speichern**.

### Aktuelle Kontrollnummern

Für ein gegebenes Partnerpaar, das bereits über Daten in der Steuertabelle verfügt, können Sie die Kontrollnummerngenerierung ändern. Sie können Folgendes ausführen:

- Setzen Sie die Kontrollnummerngenerierung für das Paar auf einen Anfangsstatus zurück.
- Bearbeiten Sie die Austausch-, Gruppen- oder Transaktionsnummer (oder eine beliebige Kombination dieser Nummern), und speichern Sie diese mit einem neuen Wert.

**Anmerkung:** Das Zurücksetzen der Kontrollnummerngenerierung bzw. das Bearbeiten einer Gruppe oder Maske sollte mit Vorsicht durchgeführt werden, sodass Probleme mit Nummern in falscher Reihenfolge oder mit duplizierten Kontrollnummern nicht auftreten. Sie könnten eine von diesen Aktionen während der Testphase durchführen oder wenn ein Partner ausdrücklich verschiedene Kontrollnummern anfordert.

Sie verwenden die Funktion **Aktuelle Kontrollnummern**, um zu ermitteln, welchen Partnern Kontrollnummern zugeordnet sind, und um zu ermitteln, wie diese Nummern lauten.

1. Klicken Sie auf **Hubadmin > Hubkonfiguration > EDI > Aktuelle Kontrollnummern**.
2. Führen Sie eine der folgenden Schrittegruppen aus:
   - Wenn Sie den aktuellen Status aller Partner anzeigen wollen, behalten Sie die Auswahl von **Alle Partner** in den Partnerlisten bei, und klicken Sie auf **Aktuellen Status anzeigen**.
   - Wenn Sie den Status ausgewählter Partner anzeigen wollen, führen Sie die folgenden Schritte aus:
     a. Geben Sie den Namen der Quellen- und Zielpartner ein, und klicken Sie auf **Suchen**. Wenn Sie die Suchergebnisse auf nur die Partner beschränken wollen, die EDI-Dokumente austauschen, behalten Sie die Auswahl von **EDI-fähige suchen** bei.
     b. Wählen Sie in den Ergebnislisten mindestens einen Partner in jeder Liste aus, und klicken Sie auf **Aktuellen Status anzeigen**.

## Dokumentaustauschvorgänge definieren

Dokumentaustauschvorgänge können manuell oder mithilfe von Assistenten definiert werden. Wenn Sie Ihre Verbindungen mithilfe der Assistenten definieren möchten, lesen Sie die Informationen in „Dokumentaustauschvorgänge mithilfe von Assistenten definieren" auf Seite 209. Wenn Sie die Verbindungen manuell definieren oder ändern möchten, lesen Sie die Informationen in „Dokumentaustauschvorgänge manuell definieren" auf Seite 211.

## Dokumentaustauschvorgänge mithilfe von Assistenten definieren

WebSphere Partner Gateway enthält zwei Assistenten, die Sie beim Definieren von Dokumentaustauschvorgängen unterstützen. Dabei handelt es sich um den Assistenten für EIF-Import und den Assistenten für EDI-Verbindung.

Der Assistent für EIF-Import führt Sie durch die erforderlichen Schritte für den Import von Zuordnungen, die in EIF-Dateien enthalten sind. Darüber hinaus zeigt er Details zu den hochgeladenen Zuordnungen an, ordnet diese Zuordnungen den richtigen Routingobjekten zu und erstellt logische Interaktionen. Nach erfolgter Ausführung des Assistenten werden die neuen Zuordnungen hochgeladen und erforderliche Interaktionen im System erstellt. Verwenden Sie anschließend den Assistenten für EDI-Verbindung, um Verbindungen mithilfe der neu hochgeladenen Zuordnungen zu erstellen.

**Anmerkung:** Zur Vermeidung von Unklarheiten kann der Assistent für EIF-Import jeweils nur von einem Benutzer verwendet werden.

Der Assistent für EDI-Verbindung, der nach Ausführung des EIF-Assistenten verwendet wird, führt Sie durch die erforderlichen Schritte für die Konfiguration einer EDI-Interaktion (Senden oder Empfangen eines EDI-Dokuments). Nach erfolgter Ausführung des Assistenten sind die ausgewählten Partner vollständig für die EDI-Interaktion konfiguriert. Dies umfasst die Aktivierung der B2B-Funktionalität, die Erstellung von gültigen Interaktionen, die Erstellung von Partnerverbindungen und die Zuordnung der erforderlichen EDI-Attribute. Der Verbindungsassistent generiert empfohlene Partnerverbindungen auf der Basis Ihrer Eingaben. Die folgenden Verbindungen können generiert werden:

- Programm zum Entfernen des Umschlags für Basisnachricht
- Transformation
- Programm zum Generieren des Umschlags für Basisnachricht
- TA1-Generierung
- FA-Generierung
- Programm zum Generieren des Umschlags für TA1 und/oder FA
- Programm zum Entfernen des Umschlags für TA1 und/oder FA

Die beiden Assistenten können über die Registerkarte **Assistenten** in der Konsole aufgerufen werden.

### Zuordnungen mithilfe des Assistenten für EIF-Import importieren

Führen Sie die folgenden Schritte aus, um Zuordnungen mithilfe des Assistenten für EIF-Import zu importieren:

1. Starten Sie WebSphere Partner Gateway Console.
2. Klicken Sie auf **Assistenten**.
3. Klicken Sie auf **Assistent für EIF-Import**.
4. Geben Sie den Namen der gewünschten Datei ein, oder klicken Sie auf **Durchsuchen**.

   **Anmerkung:** Stellen Sie beim Import einer EIF-Datei mit mehreren Zuordnungen sicher, dass die Namen der Zuordnungen in der Datei eindeutig sind. Werden in einer EIF-Datei mehrere Zuordnungen mit demselben Namenhochgeladen werden, überschreibt die letzte übereinstimmende Zuordnung die vorherigen übereinstimmenden Zuordnungen in der Datenbank.

5. Klicken Sie auf **Importieren**.
6. Daraufhin wird eine Liste der Zuordnung angezeigt, die erfolgreich importiert wurden. Klicken Sie auf **Fertigstellen**, um die Standardwerte zu akzeptieren, oder klicken Sie auf **Weiter**, um die Werte anzuzeigen oder zu ändern.
7. Wenn Sie auf **Weiter** klicken, werden Sie aufgefordert, die Transformationszuordnungen zu überprüfen und eventuelle Interaktionen zu ändern. Wählen Sie eine Transformationszuordnung aus. Wenn eine Interaktion vorhanden ist, wird sie schreibgeschützt angezeigt. Klicken Sie zum Hinzufügen einer Interaktion auf **Interaktion hinzufügen**.
8. Wählen Sie im Fenster **Interaktion hinzufügen** eine Interaktion aus, und klicken Sie auf **Diese Interaktion hinzufügen**, um der Liste eine Interaktion hinzuzufügen.
9. Wenn die Überprüfung der Transformationszuordnungen abgeschlossen ist, klicken Sie auf **Weiter**, um die Validierungszuordnungen zu überprüfen.
10. Überprüfen Sie die importierten Validierungszuordnungen. Wenn alle Angaben korrekt sind, klicken Sie auf **Fertigstellen**. Wenn Sie die FA-Zuordnungen (FA - Functional Acknowledgement, funktionale Bestätigung) anzeigen wollen, klicken Sie auf **Weiter**.
11. Überprüfen Sie die importierten FA-Zuordnungen, und klicken Sie auf **Fertigstellen**. Daraufhin werden in einem letzten Fenster die erfolgreich importierten Zuordnungen sowie die erstellten Interaktionen angezeigt.

## Verbindungen mithilfe des Assistenten für EDI-Verbindung konfigurieren

Bevor Sie Verbindungen mit dem Assistenten für EDI-Verbindung konfigurieren können, müssen Sie Folgendes erstellen:

- Den internen Partner.
- Mindestens einen externen Partner.
- Eine EDI-Geschäfts-ID für jeden Partner. In diesem Assistenten wird die EDI-Geschäfts-ID als unformatierte Geschäftskennung im Format *qq-xxxxxxxxx* definiert, wobei *qq* das zweistellige Qualifikationsmerkmal für den EDI-Austausch und *xxxxxxxxx* die neunstellige Kennung für den EDI-Austausch angibt.
- Ziele und Standardziele.
- Umschlagsprofile

Möglicherweise sind mehrere zusätzliche Konfigurationsschritte erforderlich, bevor EDI-Flüsse erfolgreich ausgeführt werden können. Zum Beispiel:

- Konfigurieren von XML-Formaten (beim Senden oder Empfangen von XML)
- Konfigurieren von Empfängern mit ROD-Verteilern (beim Empfang von ROD)
- Konfigurieren von zusätzlichen Verbindungsattributen für AS oder AS2 (bei Verwendung von AS-Paketen)

Führen Sie die folgenden Schritte aus, um Verbindungen mithilfe des Assistenten für EDI-Verbindung zu erstellen:

1. Starten Sie WebSphere Partner Gateway Console.
2. Klicken Sie auf **Assistenten**.
3. Klicken Sie auf **Assistent für EDI-Verbindung**.
4. Klicken Sie auf den Aufgabentyp, der konfiguriert werden soll (entweder **EDI-Dokument an einen EDI-Partner senden** oder **EDI-Dokument von einem EDI-Partner empfangen**). Klicken Sie dann auf **Weiter**.

5. Geben Sie in Abhängigkeit davon, ob Sie **EDI-Dokument an einen EDI-Partner senden** oder **EDI-Dokument von einem EDI-Partner empfangen** ausgewählt haben, den Quellen- oder den Zielpartner ein. Klicken Sie dann auf **Suchen**.
6. Wählen Sie einen Quellen- oder einen Zielpartner aus der Dropdown-Liste aus, und klicken Sie auf **Weiter**.
7. Wählen Sie die allgemeinen Merkmale für den Quellen- oder den Zielpartner aus. Bei EDI-Syntax müssen Sie außerdem EDI-Merkmale angeben. Klicken Sie nach Auswahl aller gewünschten Merkmale auf **Weiter**.

   **Anmerkung:**

   a. Die TA1- und FA-Merkmale werden nur dann angezeigt, wenn die Quelle ein externer Partner ist. Die erforderliche FA-Zeit wird nur dann angezeigt, wenn das Ziel ein externer Partner ist.
   b. Der Assistent für EDI-Verbindung enthält eine Liste der allgemeinen Werte, die als EDI-Begrenzerwerte verwendet werden. Wenn Sie einen Wert verwenden möchten, der nicht in der Liste enthalten ist, müssen Sie das Verbindungsattribut nach Ausführung des Assistenten manuell bearbeiten. Klicken Sie auf **Kontenadmin > Verbindungen**, um die Verbindungsattribute zu bearbeiten.
   c. Sie müssen ein Ziel für jeden Betriebsmodus angeben. Dies bedeutet, dass Sie die leere Option ("Kein Ziel ausgewählt") nicht auswählen können. Das Erzwingen dieser zusätzlichen Verbindungskonfiguration wirkt sich auf die meisten Dokumentenversand- oder -empfangssituationen nicht negativ aus. Wenn Sie die Zielspezifikation aus der Verbindung entfernen müssen, klicken Sie nach Ausführung des Assistenten auf **Kontenadmin > Verbindungen**.
8. Wählen Sie **Validierungszuordnung**, **Aktion** und **Transformationszuordnung** für den Quellen- oder Zielpartner aus. Die Beschreibung einer Zuordnung wird nach deren Auswahl angezeigt. **Paket** kann nicht ausgewählt werden, um Unklarheiten in Fällen zu vermeiden, in denen zum Beispiel EDI das AS-Paket verwendet. Klicken Sie nach Auswahl dieser Optionen auf **Weiter**.
9. Überprüfen Sie die empfohlenen Verbindungen. Klicken Sie auf **Attribute**, **Aktionen** oder **Ziele**, um diese Einstellungen zu überprüfen.

   **Anmerkung:** Verbindungen, die bereits vorhanden sind und nicht erstellt werden, sind abgeblendet. Ferner wird neben diesen Verbindungen das Symbol **Vorhanden** angezeigt, und das Kontrollkästchen **Erstellen** ist nicht vorhanden. Vorhandene Verbindungen werden von diesem Assistenten nicht überschrieben. Stattdessen wird eine Warnung mit einer Beschreibung der Situation angezeigt. Wenn die Verbindungen geändert werden müssen, klicken Sie auf **Zurück**. Wenn Sie mit den aufgelisteten Verbindungen zufrieden sind, klicken Sie auf **Fertigstellen**. Wenn sie geändert werden müssen, klicken Sie auf **Zurück**. In einem letzten Fenster werden die Verbindungen angezeigt, die erfolgreich erstellt wurden.

## Dokumentaustauschvorgänge manuell definieren

Mithilfe des Assistenten für EIF-Import und des Assistenten für EDI-Verbindung können Dokumentaustauschvorgänge definiert werden. Weitere Informationen zu diesen Assistenten finden Sie in „Dokumentaustauschvorgänge mithilfe von Assistenten definieren" auf Seite 209. Dokumente können jedoch auch manuell definiert werden. Dieser Abschnitt bietet eine umfassende Übersicht über die Aufgaben, die Sie ausführen müssen, um den Austausch von Dokumenten für EDI-Austauschvorgänge, die auf dem Hub eingehen, Dokumente oder Transaktionen, die auf dem Hub transformiert werden, sowie für EDI-Austauschvorgänge, die vom Hub gesen-

det werden, zu erstellen. Die in den folgenden Abschnitten gezeigten Schritte sind allgemein und gelten nur für das Importieren von Zuordnungen und das Konfigurieren von Interaktionen. Die allgemeinen Schritte für das Aktivieren der B2B-Funktionalität für Partner für alle Dokumentaustauschtypen werden in „B2B-Funktionalität konfigurieren" auf Seite 28 beschrieben. Die allgemeinen Schritte für das Verwalten von Verbindungen für alle Dokumentaustauschtypen wird in Kapitel 12, „Verbindungen verwalten", auf Seite 251 beschrieben. Wenn Sie ein umfassendes Beispiel für einen EDI-Dokumentaustausch vom Importieren der Zuordnungen bis zum Verwalten der Verbindungen sehen wollen, lesen Sie Kapitel 20, „EDI-Beispiele", auf Seite 345. Der Anhang umfasst die folgenden spezifischen Beispiele:

- „ Beispiel: EDI zu ROD" auf Seite 345
- „ Beispiel: EDI zu XML" auf Seite 359
- „ Beispiel: ROD zu EDI" auf Seite 372
- „ Beispiel: XML zu EDI" auf Seite 364

## Zuordnungen manuell importieren

Transformationszuordnungen für EDI-, XML- oder ROD-Dokumente können mit dem Data Interchange Services-Clientprogramm erstellt werden. Der Data Interchange Services-Client ist ein Programm, mit dem XML-Schemadokumentdefinitionen, XML-DTD-Dokumentdefinitionen, EDI-Standards, ROD-Dokumentdefinitionen sowie Zuordnungen erstellt und verwaltet werden.

WTX-Zuordnungen werden unter Verwendung von WTX Design Studio erstellt und in WebSphere Partner Gateway importiert.

Der Data Interchange Services-Client ist ein separat installiertes Programm, das auf dem WebSphere Partner Gateway-Datenträger enthalten ist, sich aber in der Regel auf einem anderen Computer befindet. Der Zuordnungsexperte von Data Interchange Services erstellt eine Zuordnung, die angibt, wie die Elemente in einem Dokument in die Elemente eines anderen, unterschiedlichen Dokuments versetzt werden. Zusätzlich zu den Anweisungen, die erklären, wie ein Dokument von einem Format in ein anderes konvertiert wird, muss Data Interchange Services auch das Layout oder Format des Quellen- und des Zieldokuments kennen. In Data Interchange Services ist das Layout eines Dokuments eine *Dokumentdefinition*.

Wenn die Transformationszuordnung in WebSphere Partner Gateway importiert ist, werden die Dokumentdefinitionen, die in Data Interchange Services erstellt wurden, als Dokumentdefinitionen (Paket, Protokoll und Dokumenttyp) auf der Seite **Transformationszuordnung** und auf der Seite **Dokumentdefinitionen verwalten** angezeigt.

Wenn Sie z. B. ein XML-Dokument in eine X12-Transaktion konvertieren, importieren Sie die Zuordnung, die die XML- und X12-Transaktionsdokumentdefinitionen und die Transformation definiert, die durchgeführt werden soll.

Es gibt zwei Methoden für das Empfangen der Zuordnungsdateien von Data Interchange Services. Wenn der Data Interchange Services-Client über eine Direktverbindung zur WebSphere Partner Gateway-Datenbank verfügt, kann der Zuordnungsexperte von Data Interchange Services die Datei direkt in die Datenbank exportieren. Ein wahrscheinlicheres Szenario ist, dass Sie die Dateien per E-Mail oder als eine FTP-Übertragung empfangen. Wenn die Dateien über FTP zu Ihnen übertragen wurden, beachten Sie, dass sie im binären Format sein müssen.

Wenn ein Fehler während des Exports einer Zuordnung vom Data Interchange Services-Client auftritt, können Sie unter Umständen den Namen der Zuordnung in Community Console sehen. Die Zuordnung kann nicht zum Konvertieren von Dokumenten verwendet werden. Sie müssen den Zuordnungsexperten des Data Interchange Services-Clients über das Exportproblem informieren und den Zuordnungsexperten bitten, die Zuordnung erneut zu exportieren, bevor diese zum Konvertieren von Dokumenten verwendet werden kann.

Führen Sie die folgenden Schritte aus, um eine Zuordnung zu importieren:

1. Öffnen Sie ein Befehlsfenster.
2. Geben Sie den folgenden Befehl bzw. das folgende Script ein:
   - Auf einem UNIX-System:

     `<Produktverz>/bin/bcgDISImport.sh <steuerzeichenfolge_für_zuordnung>`
   - Auf einem Windows-System:

     `<Produktverz>\bin\bcgDISImport.bat <steuerzeichenfolge_für_zuordnung>`

     Dabei gilt Folgendes: *<datenbankbenutzer-ID>* und *<kennwort>* sind die Werte, die Sie verwendet haben, als Sie die Datenbank als Teil der WebSphere Partner Gateway-Installation installiert haben. Die *<steuerzeichenfolge_für_zuordnung>* ist der vollständige Pfad der Datei für die Steuerzeichenfolge für Zuordnung, die vom Data Interchange Services-Client exportiert wurde.
3. Prüfen Sie für Transformationszuordnungen, ob die Dokumentdefinition importiert wurde.
   a. Klicken Sie auf **Hubadmin > Hubkonfiguration > Zuordnungen > Transformationszuordnungen**.
   b. Klicken Sie über die Seite **Transformationszuordnungen** auf das Symbol **Details anzeigen** neben der Zuordnung von Data Interchange Services. Sie werden bemerken, dass die Dokumentdefinitionen für die Quelle und das Ziel angezeigt werden; diese geben das Format, in dem das Dokument auf dem Hub empfangen wird, sowie das Format an, in dem es vom Hub zugestellt wird.
   c. Klicken Sie auf **Hubadmin > Hubkonfiguration > Dokumentdefinition**.
   d. Erweitern Sie die Pakete und Protokolle, die den Dokumentdefinitionen zugeordnet sind, welche auf der Seite **Transformationszuordnungen** angezeigt wurden, um zu überprüfen, ob die Dokumenttypen auf der Seite **Dokumentdefinitionen verwalten** angezeigt werden.

Sie können Validierungszuordnungen zusammen mit Transformationszuordnungen verwenden, um zusätzliche EDI-Standardvalidierung einem beliebigen Konvertierungsprozess mit EDI-Standards hinzuzufügen. Validierungszuordnungen geben Ihnen die vollständige Steuerung über die Validierung eines EDI-Dokuments.

Beachten Sie, dass die Transformations- und Validierungszuordnungen, die vom Data Interchange Services-Client exportiert bzw. mit dem Dienstprogramm bcgDISImport importiert wurden, nicht von WebSphere Partner Gateway Community Console heruntergeladen werden können. Der Zuordnungsexperte des Data Interchange Services-Clients verwaltet diese Zuordnungen, indem er eine Verbindung zur WebSphere Partner Gateway-Datenbank über den Data Interchange Services-Client herstellt.

## WTX-Zuordnungen importieren

Die mit WTX Design Studio erstellten WTX-Zuordnungen müssen in WebSphere Partner Gateway importiert werden, damit sie einer bestimmten Partnerverbindung

zugeordnet werden können. Die DFDs müssen manuell erstellt werden. Die erstellten DFDs werden von WTX Design Studio in Form einer Zuordnung exportiert, die für das native Betriebssystem kompiliert wird. Für den Import in WebSphere Partner Gateway müssen Sie zu **Hubadmin > Zuordnungen > Transformationszuordnungen** navigieren und auf **Erstellen** klicken. Die importierte Zuordnung wird im gemeinsamen Dateisystem in einem für WTX-Zuordnungen vorgesehenen Ordner (common/maps) gespeichert.

## WDI - Standard-EIF importieren

Für die Validierung von EDI-Transaktionen in WebSphere Partner Gateway muss die kompilierte Form des EDI-Standards in WebSphere Partner Gateway zur Verfügung stehen. Gehen Sie wie folgt vor, um die Steuerzeichenfolge für den kompilierten Standard zu erstellen:

1. Laden Sie den EDI-Standard von der WDI-Unterstützungswebsite herunter.
2. Erstellen Sie eine Datentransformationszuordnung für die Transformation und wählen Sie die EDI-Transaktion aus, die in WebSphere Partner Gateway validiert werden soll. Wenn beispielsweise Transaktion 810 von X12V4R1 validiert werden soll, müssen Sie eine Datentransformationszuordnung von X12V4R1-810 bis X12V4R1-810 erstellen.
3. Ordnen Sie nur ein obligatorisches Segment zu und kompilieren Sie die Transformationszuordnung.
4. Exportieren Sie die Steuerzeichenfolge für die Datentransformationszuordnung in die Document Manager-Datenbank. Dadurch wird auch der kompilierte Standard in die Document Manager-Datenbank exportiert, der zur Validierung verwendet werden kann.

**Anmerkung:** Alternativ werden einige Beispiel-EIFs bereitgestellt, die nur die Steuerzeichenfolge für den kompilierten Standard enthalten.

## Dokumentenfluss konfigurieren: EDI zu EDI

Dieser Abschnitt beschreibt die nötigen Interaktionen, um einen EDI-Austausch zu empfangen, vom Austausch den Umschlag zu entfernen, eine Transaktion von einem EDI-Format in ein anderes zu transformieren, die Transaktion mit einem Umschlag zu versehen und diese zuzustellen.

1. Prüfen Sie, ob eine Dokumentdefinition für den EDI-Austausch vorhanden ist, der auf dem Hub empfangen wird. Denken Sie daran, dass, nachdem vom Austausch der Umschlag entfernt wurde, der ursprüngliche Umschlag nicht weiter verarbeitet wird. Anders gesagt, es gibt für ihn keinen Zustellpunkt. Daher verwenden Sie das Paket **N/A** für die Zielinteraktion.
   a. Klicken Sie auf **Hubadmin > Hubkonfiguration > Dokumentdefinition**.
   b. Überprüfen Sie, ob eine Dokumentdefinition bereits vorhanden ist. Wenn z. B. ein Partner einen EDI-Austausch in einem AS-Paket, EDI-X12-Protokoll und ISA-Dokumenttyp sendet, ist die Definition bereits verfügbar. Ebenso ist eine N/A/EDI-X12/ISA-Dokumentdefinition bereits vorhanden.
   c. Geben Sie für ein beliebiges Attribut einen Wert ein (oder wählen Sie einen in der Liste aus), das Sie dem Profil zuordnen wollen. Wenn Sie z. B. angeben wollen, dass der Umschlag gelöscht werden soll, falls Fehler bei einer der Transaktionen auftreten, klicken Sie auf das Symbol **Attributwerte bearbeiten** neben **Dokumentdefinitionen**. Wählen Sie in der Zeile **Umschlag bei Fehlern löschen** die Option **Ja** in der Liste aus.
   d. Wenn eine Dokumentdefinition nicht vorhanden ist, erstellen Sie eine, indem Sie das Paket, das Protokoll und den Dokumenttyp auswählen.

**Anmerkung:** Das Attribut "Umschlag bei Fehlern löschen" kann nicht verwendet werden, wenn die Aktion in der Verbindung "EDI-Austausch validieren" ist.

2. Erstellen Sie eine Interaktion für den Austausch.
   a. Klicken Sie auf **Hubadmin > Hubkonfiguration > Dokumentdefinition > Interaktionen verwalten**.
   b. Klicken Sie in der Anzeige **Interaktionen verwalten** auf den Link **Interaktion erstellen**.
   c. Wählen Sie die Quellen- und Ziel-Dokumentdefinitionen aus. Mit Ausnahme des Pakets, das für das Ziel **N/A** ist, werden die Dokumentdefinitionen identisch sein.
   d. Wählen Sie **EDI - Umschlag entfernen** in der Liste **Aktion** aus.
3. Importieren Sie die Transformationszuordnung, die die Dokumentdefinitionen der EDI-Transaktionen bereitstellt und die beschreibt, wie die Transaktion von einem EDI-Format in ein anderes transformiert wird. Siehe „ Zuordnungen manuell importieren” auf Seite 212.

   Wenn der Austausch mehr als eine Transaktion enthält, wiederholen Sie diesen Schritt für jede Transaktion.
4. Wenn Sie Attribute der Dokumentdefinitionen, die der Zuordnung zugeordnet sind, bearbeiten wollen, führen Sie die folgenden Schritte aus:
   a. Klicken Sie auf **Hubadmin > Hubkonfiguration > Dokumentdefinition**.
   b. Klicken Sie auf das Symbol **Attributwerte bearbeiten** neben dem Protokoll. Für EDI-Protokolle wird eine lange Liste mit Attributen angezeigt, die Sie festlegen können.
   c. Geben Sie für ein beliebiges Attribut einen Wert ein (oder wählen Sie einen in der Liste aus), das Sie dem Protokoll zuordnen wollen.
   d. Klicken Sie auf das Symbol **Attributwerte bearbeiten** neben der Dokumentdefinition. Es wird in der Regel eine kürzere Liste mit Attributen angezeigt als die, die dem Protokoll zugeordnet ist.
   e. Geben Sie für ein beliebiges Attribut einen Wert ein (oder wählen Sie einen in der Liste aus), das Sie dem Dokumenttyp zuordnen wollen. Sie können z. B. die Validierungszuordnung ändern, die dem Dokumenttyp zugeordnet ist.

      Stellen Sie sicher, dass Sie ein Umschlagsprofil für die Transaktion auswählen.
5. Erstellen Sie eine Interaktion für die Zuordnung, die Sie gerade importiert haben.
   a. Klicken Sie auf **Hubadmin > Hubkonfiguration > Dokumentdefinition > Interaktionen verwalten**.
   b. Klicken Sie in der Anzeige **Interaktionen verwalten** auf den Link **Interaktion erstellen**.
   c. Wählen Sie unter **Quelle** den Dokumenttyp aus, der der Transaktion zugeordnet ist. Erweitern Sie das Paket und das Protokoll und wählen Sie den Dokumenttyp aus. Dies wird normalerweise **N/A** (da die Transaktion selbst nicht von einem Partner stammt), das in der Zuordnung definierte Protokoll (z. B. **X12V4R1**) und das tatsächliche EDI-Dokument sein, das in der Zuordnung definiert ist (z. B. **850**).
   d. Wählen Sie unter **Ziel** die Dokumentdefinition für das transformierte Dokument aus. Erweitern Sie das Paket und das Protokoll und wählen Sie den Dokumenttyp aus. Da die Transaktion mit einem Umschlag versehen und daher nicht direkt einem Partner zugestellt wird, wird erneut das Paket **N/A** verwendet.

e. Wählen Sie in der Transformationszuordnungsliste die Zuordnung aus, die die Transformation dieses Dokuments definiert.
f. Wählen Sie in der Liste **Aktion** den Eintrag **EDI validieren und EDI konvertieren** für natives WDI aus. Im Falle von WTX wählen Sie **EDI validieren und WTX transformieren** aus.

6. Prüfen Sie, ob eine Dokumentdefinition für den EDI-Austausch vorhanden ist, der vom Hub gesendet wird, und legen Sie die Attribute fest, die Sie dem Austausch zuordnen wollen.
   a. Klicken Sie auf **Hubadmin > Hubkonfiguration > Dokumentdefinition**.
   b. Überprüfen Sie, ob eine Dokumentdefinition bereits vorhanden ist. Das Quellenpaket wird **N/A** sein, und das Protokoll und der Dokumenttyp stimmen mit dem Protokoll und dem Dokumenttyp überein, mit denen der Austausch zugestellt wird. Wenn der Austausch z. B. als AS/EDI-X12/ISA zugestellt wird, wird die Quelle N/A/EDI-X12/ISA lauten.
   c. Bearbeiten Sie alle Attribute, die auf den zugestellten Austausch angewendet werden.
   d. Wenn eine Dokumentdefinition nicht vorhanden ist, erstellen Sie eine, indem Sie das Paket, das Protokoll und den Dokumenttyp auswählen.
7. Erstellen Sie eine Interaktion für den EDI-Austausch, der vom Hub gesendet wird, nachdem die Transaktion transformiert wurde.
   a. Klicken Sie auf **Hubadmin > Hubkonfiguration > Dokumentdefinition > Interaktionen verwalten**.
   b. Klicken Sie in der Anzeige **Interaktionen verwalten** auf den Link **Interaktion erstellen**.
   c. Wählen Sie die Quellen- und Zieldokumente aus. Mit Ausnahme des Pakets, das für das Quellendokument **N/A** ist, werden die Dokumentdefinitionen identisch sein.
   d. Wählen Sie **Pass-Through** in der Liste **Aktion** aus.

Zum Hinzufügen einer Bestätigung zum Dokumentenfluss lesen Sie „Bestätigungen konfigurieren” auf Seite 223.

Nachdem Sie die Interaktionen konfiguriert haben, erstellen Sie die B2B-Funktionalität für die Partner.

- Aktivieren Sie für den Quellenpartner drei Dokumentdefinitionen unter **Quelle festlegen**: eine für den Quellendokumenttyp, eine für die EDI-Transaktion und eine für den Umschlag.
- Aktivieren Sie für den Zielpartner drei Dokumentdefinitionen unter **Ziel festlegen**: eine für den vom Umschlag entfernten Dokumenttyp, eine für die transformierte EDI-Transaktion und eine für den EDI-Umschlag.

Die detaillierten Schritte für das Erstellen der B2B-Funktionalität werden in „B2B-Funktionalität konfigurieren” auf Seite 28 beschrieben.

Nachdem Sie die B2B-Funktionalität für die Partner konfiguriert haben, erstellen Sie Verbindungen. Sie benötigen drei Verbindungen:

- Eine für den Umschlag vom Quellenpartner zum Hub.
- Eine für die EDI-Quellentransaktion zur EDI-Zieltransaktion.
- Eine für den Umschlag vom Hub zum Zielpartner.

Die detaillierten Schritte für das Erstellen von Verbindungen werden in Kapitel 12, „Verbindungen verwalten”, auf Seite 251 beschrieben.

## Dokumentenfluss konfigurieren: EDI zu XML oder ROD

Dieser Abschnitt beschreibt die nötigen Interaktionen, um einen EDI-Austausch zu empfangen, vom Austausch den Umschlag zu entfernen, eine Transaktion von einem EDI-Format in ein XML- oder ROD-Dokument zu transformieren und die Transaktion zuzustellen.

**Anmerkung:** Ein umfassendes Beispiel für den Dokumentenfluss von EDI zu XML finden Sie in „ Beispiel: EDI zu XML" auf Seite 359. Ein umfassendes Beispiel für den Dokumentenfluss von EDI zu ROD finden Sie in „ Beispiel: EDI zu ROD" auf Seite 345.

1. Prüfen Sie, ob eine Dokumentdefinition für den EDI-Austausch vorhanden ist, der auf dem Hub empfangen wird. Denken Sie daran, dass, nachdem vom Austausch der Umschlag entfernt wurde, der Umschlag nicht weiter verarbeitet wird. Anders gesagt, es gibt für ihn keinen Zustellpunkt. Daher verwenden Sie das Paket **N/A** für die Zielinteraktion.
   a. Klicken Sie auf **Hubadmin > Hubkonfiguration > Dokumentdefinition**.
   b. Überprüfen Sie, ob eine Dokumentdefinition bereits vorhanden ist. Wenn z. B. ein Partner einen EDI-Austausch in einem AS-Paket, EDI-X12-Protokoll und ISA-Dokumenttyp sendet, ist die Definition bereits verfügbar. Ebenso ist eine N/A/EDI-X12/ISA-Dokumentdefinition bereits vorhanden.
   c. Wenn eine Dokumentdefinition nicht vorhanden ist, erstellen Sie eine.
2. Erstellen Sie eine Interaktion für den EDI-Austausch, der auf dem Hub empfangen wird.
   a. Klicken Sie auf **Hubadmin > Hubkonfiguration > Dokumentdefinition > Interaktionen verwalten**.
   b. Klicken Sie in der Anzeige **Interaktionen verwalten** auf den Link **Interaktion erstellen**.
   c. Wählen Sie die Quellen- und Zieldokumente aus. Mit Ausnahme des Pakets, das für das Ziel **N/A** ist, werden die Dokumentdefinitionen identisch sein.
   d. Wählen Sie **EDI - Umschlag entfernen** in der Liste **Aktion** aus.
3. Importieren Sie die Transformationszuordnung, die die Dokumentdefinitionen der EDI-Transaktion und des XML- oder ROD-Dokuments bereitstellt und beschreibt, wie die Transaktion in das XML- oder ROD-Dokument transformiert wird. Siehe „ Zuordnungen manuell importieren" auf Seite 212.

   Wenn der Austausch mehr als eine Transaktion enthält, wiederholen Sie diesen Schritt für jede Transaktion.
4. Erstellen Sie eine Interaktion für die Zuordnung, die Sie gerade importiert haben.
   a. Klicken Sie auf **Hubadmin > Hubkonfiguration > Dokumentdefinition > Interaktionen verwalten**.
   b. Klicken Sie in der Anzeige **Interaktionen verwalten** auf den Link **Interaktion erstellen**.
   c. Wählen Sie unter **Quelle** den Dokumenttyp aus, der der Transaktion zugeordnet ist. Erweitern Sie das Paket und das Protokoll, und wählen Sie den Dokumenttyp aus. Dies wird normalerweise **N/A** (da die Transaktion selbst nicht von einem Partner stammt), das in der Zuordnung definierte Protokoll (z. B. **X12V4R1**) und das tatsächliche EDI-Dokument sein, das in der Zuordnung definiert ist (z. B. **850**).
   d. Wählen Sie unter **Ziel** die Dokumentdefinition für das transformierte Dokument (XML oder ROD) aus. Erweitern Sie das Paket und das Protokoll, und wählen Sie den Dokumenttyp aus.

e. Wählen Sie in der Transformationszuordnungsliste die Zuordnung aus, die die Transformation dieses Dokuments definiert.
f. Wählen Sie in der Liste **Aktion** die Option **EDI validieren und EDI konvertieren** für natives WDI aus. Im Falle von WTX wählen Sie **EDI validieren und WTX transformieren** aus.

Zum Hinzufügen einer Bestätigung zum Dokumentenfluss lesen Sie „Bestätigungen konfigurieren" auf Seite 223.

Nachdem Sie die Interaktionen konfiguriert haben, erstellen Sie die B2B-Funktionalität für die Partner.

- Aktivieren Sie für den Quellenpartner zwei Dokumentdefinitionen unter **Quelle festlegen**: eine für den Umschlag und eine für die EDI-Transaktion.
- Aktivieren Sie für den Zielpartner zwei Dokumentdefinitionen unter **Ziel festlegen**: eine für den EDI-Umschlag und eine für das XML- oder ROD-Dokument.

Die detaillierten Schritte für das Erstellen der B2B-Funktionalität werden in „B2B-Funktionalität konfigurieren" auf Seite 28 beschrieben.

Nachdem Sie die B2B-Funktionalität für die Partner konfiguriert haben, erstellen Sie Verbindungen. Sie benötigen zwei Verbindungen:

- Eine für den Umschlag vom Quellenpartner zum Hub.
- Eine für die EDI-Quellentransaktion zum XML- oder ROD-Dokument.

Die detaillierten Schritte für das Erstellen von Verbindungen werden in Kapitel 12, „Verbindungen verwalten", auf Seite 251 beschrieben.

## Dokumentenfluss konfigurieren: XML oder ROD zu EDI

Dieser Abschnitt beschreibt die nötigen Interaktionen, um ein XML- oder ROD-Dokument zu empfangen, es in eine EDI-Transaktion zu transformieren, die Transaktion mit einem Umschlag zu versehen und diese zuzustellen.

**Anmerkung:** Ein umfassendes Beispiel für den Dokumentenfluss von XML zu EDI finden Sie in „ Beispiel: XML zu EDI" auf Seite 364. Ein umfassendes Beispiel für den Dokumentenfluss von ROD zu EDI finden Sie in „ Beispiel: ROD zu EDI" auf Seite 372.

1. Importieren Sie die Transformationszuordnung, die die Dokumentdefinitionen des XML- oder ROD-Dokuments und der EDI-Transaktion bereitstellt und beschreibt, wie das Dokument in die EDI-Transaktion transformiert wird. Siehe „ Zuordnungen manuell importieren" auf Seite 212.
2. Erstellen Sie eine Interaktion für die Zuordnung, die Sie gerade importiert haben.
   a. Klicken Sie auf **Hubadmin > Hubkonfiguration > Dokumentdefinition > Interaktionen verwalten**.
   b. Klicken Sie in der Anzeige **Interaktionen verwalten** auf den Link **Interaktion erstellen**.
   c. Wählen Sie unter **Quelle** die Dokumentdefinition aus, die dem XML- oder ROD-Dokument zugeordnet ist. Erweitern Sie das Paket und das Protokoll, und wählen Sie den Dokumenttyp aus.
   d. Wählen Sie unter **Ziel** den Dokumenttyp aus, der der EDI-Transaktion zugeordnet ist. Erweitern Sie das Paket und das Protokoll, und wählen Sie den

Dokumenttyp aus. Da die Transaktion nicht direkt zugestellt wird, es wird vor der Zustellung mit einem Umschlag versehen, wird **N/A** als Paket aufgelistet.

e. Wählen Sie in der Transformationszuordnungsliste die Zuordnung aus, die die Transformation dieses Dokuments definiert.

f. Wählen Sie in der Liste **Aktion** die Option **XML konvertieren und EDI validieren** oder **ROD konvertieren und EDI validieren** für natives WDI aus. Im Falle von WTX wählen Sie **WTX-Transformation** aus.

3. Prüfen Sie, ob eine Dokumentdefinition für den EDI-Austausch vorhanden ist, der vom Hub gesendet wird, und legen Sie die Attribute fest, die Sie dem Austausch zuordnen wollen.
   a. Klicken Sie auf **Hubadmin > Hubkonfiguration > Dokumentdefinition**.
   b. Überprüfen Sie, ob eine Dokumentdefinition bereits vorhanden ist. **N/A** sollte als Paket für das Quellendokument verwendet werden (der Austausch wird vom Hub gesendet).
   c. Bearbeiten Sie alle Attribute, die auf den zugestellten Austausch angewendet werden.
   d. Wenn eine Dokumentdefinition nicht vorhanden ist, erstellen Sie eine, indem Sie das Paket, das Protokoll und den Dokumenttyp auswählen.
4. Erstellen Sie eine Interaktion für den EDI-Austausch, der vom Hub gesendet wird, nachdem das Dokument transformiert wurde.
   a. Klicken Sie auf **Hubadmin > Hubkonfiguration > Dokumentdefinition > Interaktionen verwalten**.
   b. Klicken Sie in der Anzeige **Interaktionen verwalten** auf den Link **Interaktion erstellen**.
   c. Wählen Sie die Quellen- und Zieldokumente aus. Die Quellen- und Zieldokumente sind in unterschiedlichen Paketen (das Quellendokument ist in einem Paket **N/A**), aber das Protokoll (z. B. EDI-X12) und der Dokumenttyp (z. B. ISA) sollten identisch sein.
   d. Wählen Sie **Pass-Through** in der Liste **Aktion** aus.

Nachdem Sie die Interaktionen konfiguriert haben, erstellen Sie die B2B-Funktionalität für die Partner.

- Die Anzahl der Dokumentdefinitionen, die Sie für den Quellenpartner unter **Quelle festlegen** festlegen müssen, variiert je nach Dokumenttyp.
  - Beispiel: Aktivieren Sie für ein XML-Dokument, in dem ICGPO der Dokumenttyp und MX12V3R1 die konvertierte EDI-Transaktion ist, drei Dokumentdefinitionen unter **Quelle festlegen**: eine für das XML-Dokument (ICGPO), eine für die EDI-Transaktion (MX12V3R1) und eine für den Umschlag, der vom Hub gesendet wird.
  - Aktivieren Sie für weitere XML-Dokumente und für ROD-Dokumente zwei Dokumentdefinitionen unter **Quelle festlegen**: eine für das XML- oder ROD-Dokument und eine für den Umschlag, der vom Hub gesendet wird.
- Aktivieren Sie für den Zielpartner zwei Dokumentdefinitionen unter **Ziel festlegen**: eine für die EDI-Transaktion und eine für den EDI-Umschlag, der empfangen wird. Klicken Sie für die EDI-Transaktion auf das Symbol **Attributwerte bearbeiten** neben dem Protokoll, und geben Sie ein Umschlagsprofil an. Sie können auch weitere Attribute angeben.

Die detaillierten Schritte für das Erstellen der B2B-Funktionalität werden in „B2B-Funktionalität konfigurieren" auf Seite 28 beschrieben.

Nachdem Sie die B2B-Funktionalität für die Partner konfiguriert haben, erstellen Sie Verbindungen. Sie benötigen zwei Verbindungen:

- Eine für das XML- oder ROD-Quellendokument zur EDI-Transaktion.
- Eine für den Umschlag vom Hub zum Partner.

Die detaillierten Schritte für das Erstellen von Verbindungen werden in Kapitel 12, „Verbindungen verwalten", auf Seite 251 beschrieben.

## Dokumentenfluss konfigurieren: Mehrere XML- oder ROD-Dokumente in einer Datei zu EDI

Dieser Abschnitt beschreibt die nötigen Interaktionen, um mehrere XML- oder ROD-Dokumente in einer Datei zu empfangen, die Dokumente in EDI-Transaktionen zu transformieren, die Transaktionen mit einem Umschlag zu versehen und den EDI-Austausch zuzustellen.

1. Importieren Sie die Transformationszuordnung, die die Dokumentdefinitionen der XML- oder ROD-Dokumente und der EDI-Transaktionen bereitstellt und die Transformation beschreibt. Siehe „ Zuordnungen manuell importieren" auf Seite 212.
2. Erstellen Sie eine Interaktion für die Quellen- und Zieldokumente.
   a. Klicken Sie auf **Hubadmin > Hubkonfiguration > Dokumentdefinition > Interaktionen verwalten**.
   b. Klicken Sie in der Anzeige **Interaktionen verwalten** auf den Link **Interaktion erstellen**.
   c. Wählen Sie für natives WDI die Quellen- und Zieldokumente aus. Wählen Sie dann **XML konvertieren und EDI validieren** oder **ROD konvertieren und EDI validieren** in der Liste **Aktion** aus. Wählen Sie für WTX **WTX-Transformation** und **Validierung des EDI-Austauschs** aus.
3. Wiederholen Sie Schritt 2 für das Quellendokument und jedes Zieldokument, das durch die Transformationszuordnung hergestellt wurde.
4. Prüfen Sie, ob eine Dokumentdefinition für den EDI-Austausch vorhanden ist, der vom Hub gesendet wird, und legen Sie die Attribute fest, die Sie dem Austausch zuordnen wollen.
   a. Klicken Sie auf **Hubadmin > Hubkonfiguration > Dokumentdefinition**.
   b. Überprüfen Sie, ob eine Dokumentdefinition bereits vorhanden ist. Die Quelle wird **N/A** sein, und das Protokoll und der Dokumenttyp stimmen mit dem Protokoll und dem Dokumenttyp überein, mit denen der Austausch zugestellt wird. Wenn der Austausch z. B. als AS/EDI-X12/ISA zugestellt wird, wird die Quelle N/A/EDI-X12/ISA lauten.
   c. Bearbeiten Sie alle Attribute, die auf den zugestellten Austausch angewendet werden.
   d. Wenn eine Dokumentdefinition nicht vorhanden ist, erstellen Sie eine, indem Sie das Paket, das Protokoll und den Dokumenttyp auswählen.
5. Erstellen Sie eine Interaktion für den EDI-Austausch, der vom Hub gesendet wird, nachdem die Transaktion transformiert wurde.
   a. Klicken Sie auf **Hubadmin > Hubkonfiguration > Dokumentdefinition > Interaktionen verwalten**.
   b. Klicken Sie in der Anzeige **Interaktionen verwalten** auf den Link **Interaktion erstellen**.

c. Wählen Sie die Quellen- und Zieldokumente aus. Die Quellen- und Zieldokumente sind in unterschiedlichen Paketen (das Quellendokument ist in einem Paket **N/A**), aber das Protokoll (z. B. EDI-X12) und der Dokumenttyp (z. B. ISA) sollten identisch sein.

d. Wählen Sie **Pass-Through** in der Liste **Aktion** aus.

Nachdem Sie die Interaktionen konfiguriert haben, erstellen Sie die B2B-Funktionalität für die Partner.

- Die Anzahl der Dokumentdefinitionen, die Sie für den Quellenpartner unter **Quelle festlegen** festlegen müssen, variiert je nach Dokumenttyp.
  - Beispiel: Aktivieren Sie für ein XML-Dokument, in dem ICGPO der Dokumenttyp und MX12V3R1 die konvertierte EDI-Transaktion ist, drei Dokumentdefinitionen unter **Quelle festlegen**: eine für das XML-Dokument (ICGPO), eine für die EDI-Transaktion (MX12V3R1) und eine für den Umschlag, der vom Hub gesendet wird.
  - Aktivieren Sie für weitere XML-Dokumente und für ROD-Dokumente zwei Dokumentdefinitionen unter **Quelle festlegen**: eine für das XML- oder ROD-Dokument und eine für den Umschlag, der vom Hub gesendet wird.

Die detaillierten Schritte für das Erstellen der B2B-Funktionalität werden in „B2B-Funktionalität konfigurieren" auf Seite 28 beschrieben.

Nachdem Sie die B2B-Funktionalität für die Partner konfiguriert haben, erstellen Sie Verbindungen. Sie benötigen mehrere Verbindungen:

- Eine für jedes XML- oder ROD-Dokument, das in eine EDI-Transaktion transformiert wird.
- Eine für den Umschlag vom Hub zum Partner.

Die detaillierten Schritte für das Erstellen von Verbindungen werden in Kapitel 12, „Verbindungen verwalten", auf Seite 251 beschrieben.

## Dokumentenfluss konfigurieren: XML zu ROD oder ROD zu XML

Dieser Abschnitt beschreibt die nötigen Interaktionen, um ein XML- oder ROD-Dokument zu empfangen, es in den anderen Dokumenttyp (XML zu ROD oder ROD zu XML) zu transformieren und es zuzustellen.

1. Importieren Sie die Transformationszuordnung, die die Dokumentdefinitionen der XML- und ROD-Dokumente bereitstellt und die Transformation der Dokumente beschreibt. Siehe „ Zuordnungen manuell importieren" auf Seite 212.
2. Klicken Sie auf **Hubadmin > Hubkonfiguration > Zuordnungen > Transformationszuordnungen**, und klicken Sie auf das Symbol **Details anzeigen** neben der Zuordnung, die Sie gerade importiert haben.
3. Erstellen Sie eine Interaktion für die Zuordnung, die Sie gerade importiert haben.
   a. Klicken Sie auf **Hubadmin > Hubkonfiguration > Dokumentdefinition > Interaktionen verwalten**.
   b. Klicken Sie in der Anzeige **Interaktionen verwalten** auf den Link **Interaktion erstellen**.
4. Wählen Sie die Quellen- und Zieldokumente aus. Wählen Sie dann **WTX-Transformation** für WTX oder **ROD konvertieren und EDI validieren** in der Liste **Aktion** aus.

Nachdem Sie die Interaktionen konfiguriert haben, erstellen Sie die B2B-Funktionalität für die Partner.

- Aktivieren Sie für den Quellenpartner Dokumentdefinitionen unter **Quelle festlegen** für das XML- oder ROD-Dokument.
- Aktivieren Sie für den Zielpartner Dokumentdefinitionen unter **Ziel festlegen** für das XML- oder ROD-Dokument.

Die detaillierten Schritte für das Erstellen der B2B-Funktionalität werden in „B2B-Funktionalität konfigurieren" auf Seite 28 beschrieben.

Nachdem Sie die B2B-Funktionalität für die Partner konfiguriert haben, erstellen Sie Verbindungen. Sie benötigen eine Verbindung für den Dokumentenfluss von XML zu ROD oder für den Dokumentenfluss von ROD zu XML. Die detaillierten Schritte für das Erstellen von Verbindungen werden in Kapitel 12, „Verbindungen verwalten", auf Seite 251 beschrieben.

## Dokumentenfluss konfigurieren: XML zu XML oder ROD zu ROD

Dieser Abschnitt beschreibt die nötigen Interaktionen, um ein XML- oder ROD-Dokument zu empfangen, es in ein Dokument desselben Typs (XML zu XML oder ROD zu ROD) zu transformieren und es zuzustellen.

1. Importieren Sie die Transformationszuordnung, die die Dokumentdefinitionen der XML- oder ROD-Dokumente bereitstellt und die Transformation der Dokumente beschreibt. Siehe „ Zuordnungen manuell importieren" auf Seite 212.
2. Klicken Sie auf **Hubadmin > Hubkonfiguration > Zuordnungen > Transformationszuordnungen**, und klicken Sie auf das Symbol **Details anzeigen** neben der Zuordnung, die Sie gerade importiert haben.
3. Erstellen Sie eine Interaktion für die Zuordnung, die Sie gerade importiert haben.
   a. Klicken Sie auf **Hubadmin > Hubkonfiguration > Dokumentdefinition > Interaktionen verwalten**.
   b. Klicken Sie in der Anzeige **Interaktionen verwalten** auf den Link **Interaktion erstellen**.
   c. Wählen Sie die Quellen- und Zieldokumente aus.
   d. Wählen Sie für natives WDI **XML konvertieren und EDI validieren** oder **ROD konvertieren und EDI validieren** in der Liste **Aktion** aus. Wählen Sie für WTX **WTX-Transformation** und **Validierung des EDI-Austauschs** aus.

Nachdem Sie die Interaktionen konfiguriert haben, erstellen Sie die B2B-Funktionalität für die Partner.

- Aktivieren Sie für den Quellenpartner eine Dokumentdefinition unter **Quelle festlegen** für das XML- oder ROD-Dokument.
- Aktivieren Sie für den Zielpartner eine Dokumentdefinition unter **Ziel festlegen** für das XML- oder ROD-Dokument.

Die detaillierten Schritte für das Erstellen der B2B-Funktionalität werden in „B2B-Funktionalität konfigurieren" auf Seite 28 beschrieben.

Nachdem Sie die B2B-Funktionalität für die Partner konfiguriert haben, erstellen Sie Verbindungen. Sie benötigen eine Verbindung für den Dokumentenfluss von XML zu XML oder für den Dokumentenfluss von ROD zu ROD. Die detaillierten Schritte für das Erstellen von Verbindungen werden in Kapitel 12, „Verbindungen verwalten", auf Seite 251 beschrieben.

## Bestätigungen konfigurieren

Dieser Abschnitt beschreibt, wie Sie Interaktionen installieren, um dem Absender des Dokuments Bestätigungen für den Austausch oder den Transaktionsempfang zu senden.

### Funktionale Bestätigungen

Zuordnungen der funktionalen Bestätigungen werden verwendet, um die Generierung von funktionalen Bestätigungen bereitzustellen, wenn auf EDI-Dokumente geantwortet wird, die von einem Partner wurden. WebSphere Partner Gateway stellt eine Gruppe von Zuordnungen der funktionalen Bestätigungen bereit, die die häufig verwendeten funktionalen EDI-Bestätigungen herstellen. Der Zuordnungsexperte kann auch FA- und Validierungszuordnungen erstellen, in diesem Fall würden die Zuordnungen in WebSphere Partner Gateway hochgeladen werden.

**Anmerkung:** Eine Zuordnung der funktionalen Bestätigungen sollte nur erstellt werden, wenn eine angepasste funktionale Bestätigung erforderlich ist.

Neben den Zuordnungen der funktionalen Bestätigungen, die mit WebSphere Partner Gateway bereitgestellt werden, wird das Protokoll &FUNC_ACK_METADATA_DICTIONARY und das zugehörige &FUNC_ACK_META zur Verfügung gestellt. Sie werden unter **Paket: None** auf der Seite **Dokumentdefinitionen** aufgelistet. &FUNC_ACK_META ist die Quellendokumentdefinition für alle Zuordnungen der funktionalen Bestätigungen. Diese Zuordnung stellt die Struktur der funktionalen Bestätigung bereit. Eine funktionale Bestätigung fließt zu Partnern, und die Zuordnung der funktionalen Bestätigungen teilt dem System mit, wie die Bestätigung generiert werden soll. Der Name der Quellendokumentdefinition kann nicht geändert werden. Der Zuordnungsexperte des Data Interchange Services-Clients kann eine Zuordnung der funktionalen Bestätigungen ohne diese Dokumentdefinition in Ihrer Datenbank nicht erstellen.

Die Zieldokumentdefinition in einer Zuordnung der funktionalen Bestätigungen beschreibt das Layout der funktionalen Bestätigung. Sie muss eine EDI-Dokumentdefinition mit einem der folgenden Namen sein: 997, 999 oder CONTRL.

Die folgenden Zuordnungen der funktionalen Bestätigungen werden mit WebSphere Partner Gateway installiert und auf der Seite **Dokumentdefinitionen verwalten** unter **Paket: N/A** angezeigt:

*Tabelle 29. Vom Produkt bereitgestellte Zuordnungen der funktionalen Bestätigungen*

| Protokoll | Dokumenttyp | Beschreibung |
|---|---|---|
| &DTCTL21 | CONTRL | Funktionale Bestätigung CONTRL – UN/EDIFACT Version 2 Release 1 (D94B) |
| &DTCTL | CONTRL | Funktionale Bestätigung CONTRL – UN/EDIFACT vor D94B |
| &DT99933 | 999 | Funktionale Bestätigung 999 – UCS Version 3 Release 3 |
| &DT99737 | 997 | Funktionale Bestätigung 997 – X12 Version 3 Release 7 |
| &DT99735 | 997 | Funktionale Bestätigung 997 – X12 Version 3 Release 5 |
| &DT99724 | 997 | Funktionale Bestätigung 997 – X12 Version 2 Release 4 |

Darüber hinaus werden das Protokoll &X44TA1 und ein zugeordneter TA1-Dokumenttyp unter **Paket: N/A** aufgelistet. Diese Zuordnung wird zur Generierung einer TA1 verwendet. TA1 ist eine funktionale Bestätigung, die für eingehende X12-Austauschvorgänge generiert wird.

Das Protokoll &WDIEVAL und ein zugeordnetes X12ENV wird auch unter **Paket: N/A** bereitgestellt.

Genau wie EDI-Transaktionen werden auch funktionale Bestätigungen vor ihrer Zustellung stets in einen EDI-Austausch gestellt.

### TA1-Bestätigungen

TA1 ist ein EDI-Segment, das eine X12-Austauschbestätigung bereitstellt. Es bestätigt den Empfang und die syntaktische Korrektheit eines X12-Austauschheader- und -trailerpaares (ISA und IEA). Der Absender kann TA1 vom Empfänger anfordern, indem er das Element 14 des ISA-Austauschkontrollheaders mit **1** festlegt. Die Austauschkontrollnummer von TA1 wird mit einem zuvor übertragenen X12-Austausch mit derselben Kontrollnummer in Übereinstimmung gebracht, um den Bestätigungsprozess abzuschließen.

Genau wie EDI-Transaktionen und funktionale Bestätigungen werden auch TA1s vor ihrer Zustellung stets in einen EDI-Austausch gestellt.

## Dem Dokumenttyp eine Bestätigung hinzufügen

Führen Sie die folgenden Schritte aus, um einem Dokumentenfluss eine Bestätigung hinzuzufügen:

1. Wenn die Zuordnung der funktionalen Bestätigungen nicht von WebSphere Partner Gateway bereitgestellt wird, importieren Sie die Zuordnung vom Data Interchange Services-Client. Siehe „ Zuordnungen manuell importieren" auf Seite 212.
2. Ordnen Sie die Zuordnung der funktionalen Bestätigungen einer Dokumentdefinition zu:
   a. Klicken Sie auf **Hubadmin > Hubkonfiguration > Zuordnungen > EDI FA-Zuordnungen**.
   b. Klicken Sie auf das Symbol **Details anzeigen** neben der Zuordnung.
   c. Klicken Sie auf das Symbol **Erweitern** neben einem Paket, um es einzeln auf die gewünschte Ebene zu erweitern, erweitern Sie z. B. die Ordner **Paket** und **Protokoll**, und wählen Sie die Transaktion aus.
   d. Klicken Sie auf **Speichern**.
3. Erstellen Sie eine Interaktion für die Zuordnung, die Sie gerade importiert haben.
   a. Klicken Sie auf **Hubadmin > Hubkonfiguration > Dokumentdefinition > Interaktionen verwalten**.
   b. Klicken Sie in der Anzeige **Interaktionen verwalten** auf den Link **Interaktion erstellen**.
   c. Wählen Sie unter **Quelle** den Dokumenttyp aus, der der funktionalen Bestätigung zugeordnet ist. Erweitern Sie das Paket und das Protokoll und wählen Sie den Dokumenttyp aus.
   d. Wählen Sie unter **Ziel** dieselben Werte aus.
   e. Wählen Sie in der Liste **Aktion** die Option **Pass-Through** aus.

4. Prüfen Sie, ob eine Dokumentdefinition für den EDI-Austausch vorhanden ist, der vom Hub gesendet wird, und legen Sie die Attribute fest, die Sie dem Austausch zuordnen wollen.
   a. Klicken Sie auf **Hubadmin > Hubkonfiguration > Dokumentdefinition**.
   b. Überprüfen Sie, ob eine Dokumentdefinition bereits vorhanden ist. Die Quelle wird **N/A** sein, und das Protokoll und der Dokumenttyp stimmen mit dem Protokoll und dem Dokumenttyp überein, mit denen der Austausch zugestellt wird. Wenn der Austausch z. B. als AS/EDI-X12/ISA zugestellt wird, wird die Quelle N/A/EDI-X12/ISA lauten.
   c. Bearbeiten Sie alle Attribute, die auf den zugestellten Austausch angewendet werden.
   d. Wenn eine Dokumentdefinition nicht vorhanden ist, erstellen Sie eine, indem Sie das Paket, das Protokoll und den Dokumenttyp auswählen.
5. Erstellen Sie eine Interaktion für den EDI-Austausch, der vom Hub gesendet wird, nachdem das Dokument transformiert wurde.
   a. Klicken Sie auf **Hubadmin > Hubkonfiguration > Dokumentdefinition > Interaktionen verwalten**.
   b. Klicken Sie in der Anzeige **Interaktionen verwalten** auf den Link **Interaktion erstellen**.
   c. Wählen Sie die Quellen- und Zieldokumente aus.
   d. Wählen Sie **Pass-Through** in der Liste **Aktion** aus.

Nachdem Sie die Interaktionen konfiguriert haben, erstellen Sie die B2B-Funktionalität für die Partner. Beachten Sie, dass der Zielpartner in einer Übertragung der funktionalen Bestätigung der Quellenpartner des ursprünglichen EDI-Dokuments ist.

- Aktivieren Sie für den Quellenpartner Dokumentdefinitionen unter **Quelle festlegen** für die funktionale Bestätigung. Aktivieren Sie außerdem eine Dokumentdefinition für den Umschlag, der vom Hub gesendet wird.
- Aktivieren Sie für den Zielpartner eine Dokumentdefinition unter **Ziel festlegen** für die funktionale Bestätigung. Aktivieren Sie außerdem eine Dokumentdefinition für den EDI-Umschlag, der empfangen wird.

  Klicken Sie für die funktionale Bestätigung auf das Symbol **Attributwerte bearbeiten** neben dem Protokoll und geben Sie ein Umschlagsprofil an.

Die detaillierten Schritte für das Erstellen der B2B-Funktionalität werden in „B2B-Funktionalität konfigurieren" auf Seite 28 beschrieben.

Nachdem Sie die B2B-Funktionalität für die Partner konfiguriert haben, erstellen Sie Verbindungen. Sie benötigen zwei Verbindungen:

- Eine für die funktionale Bestätigung.
- Eine für den Umschlag vom Hub zum Partner.

Die detaillierten Schritte für das Erstellen von Verbindungen werden in Kapitel 12, „Verbindungen verwalten", auf Seite 251 beschrieben.

## EDI-Austauschvorgänge und -Transaktionen anzeigen

Wie zuvor in diesem Kapitel erwähnt, verwenden Sie die Dokumentanzeige, um Informationen zu EDI-Austauschvorgängen und EDI-Transaktionen anzuzeigen, die einen Dokumentenfluss ausmachen. Sie können unformatierte Dokumente und zugeordnete Dokumentverarbeitungsdetails und Ereignisse mithilfe von bestimmten Suchkriterien anzeigen. Diese Informationen sind nützlich, wenn Sie zu ermitteln versuchen, ob ein EDI-Austausch erfolgreich zugestellt wurde bzw. worin die Ursache eines Fehlers besteht.

Gehen Sie wie folgt vor, um die Dokumentanzeige zu öffnen:

1. Klicken Sie auf **Anzeigen > Dokumentanzeige**.
2. Wählen Sie die entsprechenden Suchkriterien aus.
3. Klicken Sie auf **Suchen**.

Informationen zur Verwendung der Dokumentanzeige finden Sie im Handbuch *WebSphere Partner Gateway Verwaltung*.

## Einschränkungen von OpenPGP beim Empfangen und Senden von EDI-Dokumenten über verschiedene Transportprotokolle

Beim Empfangen von EDI-Dokumenten werden die Geschäfts-IDs anhand des Inhalts ermittelt. Diese IDs müssen mit den Geschäfts-IDs übereinstimmen, die anhand des Pakets oder der Ordnerstruktur ermittelt wurden. Im Folgenden werden die Einschränkungen beim Empfangen von EDI-Daten über verschiedene Transportprotokolle aufgelistet:

1. Beim Empfangen eines Dokuments über HTTP ermittelt die Basisauthentifizierung den sendenden Partner. Wird der Parameter 'Empfänger' verwendet, ermittelt sie die Geschäfts-ID des empfangenden Partners. Der Transportheader 'X-receiver' kann ebenfalls verwendet werden, um den empfangenden Partner zu ermitteln. Der Header muss die Geschäfts-ID des empfangenden Partners enthalten. Ist der empfangende Partner nicht angegeben, wird der standardmäßige interne Partner als Empfänger betrachtet. Die Basisauthentifizierung enthält die Benutzer-ID und das Kennwort. Es wird empfohlen, HTTP(S) mit der Serverauthentifizierung und der Basisauthentifizierung zu verwenden.
2. Wird ein Dokument über FTP(S) empfangen, wird der absendende Partner anhand der für WebSphere Partner Gateway spezifischen Ordnerstruktur ermittelt, die für FTP(S)-Empfänger konfiguriert ist.
3. Werden binäre Dokumente über SFTP empfangen, wird der absendende Partner auf der Basis der Konfigurationswerte ermittelt, die im der angehängten generischen Vorverarbeitungshandler des SFTP-Empfängers angegeben werden.

# Kapitel 11. Ziele erstellen

Nachdem Sie die Partner erstellt haben, definieren Sie Ziele für die Partner. Ziele definieren Einstiegspunkte in das System des Partners.

Dieses Kapitel behandelt die folgenden Themen:



**Anmerkung:** Verwenden Sie stets die Browserinstanz, mit der Sie sich an Community Console angemeldet haben, wenn Sie Konfigurationsänderungen an WebSphere Partner Gateway vornehmen. Die gleichzeitige Verwendung mehrerer Browserinstanzen kann dazu führen, dass die Konfigurationsänderungen aufgehoben werden.

## Übersicht über Ziele

WebSphere Partner Gateway verwendet Ziele, um Dokumente an ihren ordnungsgemäßen Bestimmungsort weiterzuleiten. Der Empfänger kann ein externer Partner oder der interne Partner sein. Das Ausgangstransportprotokoll bestimmt, welche Informationen während der Konfiguration des Ziels verwendet werden.

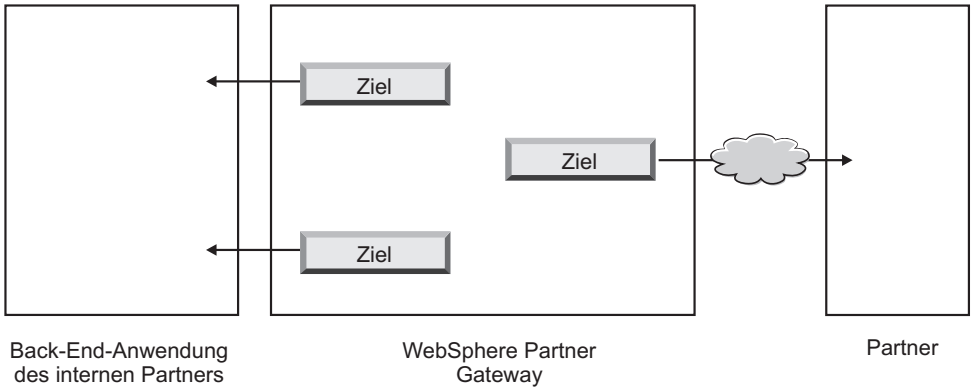



*Abbildung 34. Ziele zum internen Partner und zu externen Partnern*

Die folgenden Transporte werden standardmäßig für Partnerziele unterstützt:

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

  **Anmerkung:** Ein SMTP-Ziel kann nur für externe Partner und nicht für den internen Partner definiert werden.
- SFTP
- Dateiverzeichnis
- FTP-Scripting

Sie können auch einen benutzerdefinierten Transport angeben, den Sie während der Erstellung des Ziels hochladen.

Als Hubadministrator können Sie das Ziel Ihrer Partner konfigurieren bzw. die Partner können diese Aufgabe selbst ausführen. In diesem Kapitel erfahren Sie, wie Sie diese Aufgabe für die Partner ausführen. Informationen zum Verwalten von Zielen finden Sie im Kapitel "Hubverwaltungstasks" des Handbuchs *IBM WebSphere Partner Gateway Verwaltung*.

## Globale Transportwerte konfigurieren

Sie legen globale Transportattribute fest, die auf alle FTP-Scripting-Ziele angewendet werden. Wenn Sie keine FTP-Scripting-Ziele definieren, können Sie diesen Abschnitt überspringen.

Der FTP-Scripting-Transport verwendet einen Sperrmechanismus, der verhindert, dass mehr als eine FTP-Scripting-Instanz gleichzeitig auf dassselbe Ziel zugreift. Standardwerte werden für Folgendes bereitgestellt: wie lange eine Gatewayinstanz wartet, um die Sperre zu erhalten, und wie oft es versucht, die Sperre abzurufen, falls diese verwendet wird. Sie können diese Standardwerte verwenden bzw. diese ändern.

1. Klicken Sie auf **Kontenadmin > Profile**.
2. Klicken Sie auf **Ziele**.
3. Wählen Sie **Globale Transportattribute** aus den Zieldetails aus.

   Wenn Sie entweder **Maximale Sperrenzeit (Sekunden)** oder **Höchstalter der Warteschlange (Sekunden)** aktualisiert haben, als Sie die globalen Transportwerte während der Erstellung der Ziele angegeben haben, werden diese aktualisierten Werte hier wiedergegeben.
4. Wenn die Standardwerte für Ihre Konfiguration geeignet sind, klicken Sie auf **Abbrechen**. Andernfalls fahren Sie mit den übrigen Schritten in diesem Abschnitt fort.
5. Klicken Sie auf das Symbol **Bearbeiten** neben **FTP-Scripting-Transport**.
6. Um mindestens einen Wert zu ändern, geben Sie den neuen Wert ein. Sie können Folgendes ändern:
   - **Wiederholungszähler für Sperren**. Gibt an, wie oft das Ziel versucht, eine Sperre zu erhalten, wenn die Sperre gerade verwendet wird. Der Standardwert ist 3.
   - **Wiederholungsintervall für Sperren (Sekunden)**. Gibt an, wie viel Zeit zwischen den Versuchen, eine Sperre zu erhalten, verstreichen wird. Der Standardwert ist 260 Sekunden.
   - **Maximale Sperrenzeit (Sekunden)**. Gibt an, wie lange das Ziel die Sperre beibehalten kann. Der Standardwert ist 240 Sekunden, es sei denn, Sie haben ihn geändert, als Sie die Ziele erstellt haben.
   - **Höchstalter der Warteschlange (Sekunden)**. Gibt an, wie lange das Ziel in einer Warteschlange wartet, um die Sperre zu erhalten. Der Standardwert ist 740 Sekunden, es sei denn, Sie haben ihn geändert, als Sie die Ziele erstellt haben.
7. Klicken Sie auf **Speichern**.

## Forward Proxy konfigurieren

Für den HTTP-Transport können Sie eine Forward Proxy-Unterstützung konfigurieren, sodass Dokumente über einen konfigurierten Proxy-Server gesendet werden. Sie können mit WebSphere Partner Gateway die folgenden Unterstützungstypen konfigurieren:

- Proxy-Unterstützung über HTTP
- Proxy-Unterstützung über HTTP mit Authentifizierung
- Proxy-Unterstützung über SOCKS

**Anmerkung:** WebSphere Partner Gateway stellt die Verbindung zum Proxy-Server nur über den HTTP-Port her.

Nachdem Sie einen Forward Proxy konfiguriert haben, können Sie ihn global für den Transport einrichten, indem Sie ihn als Standardziel definieren (sodass beispielsweise alle HTTP-Ziele den Forward Proxy verwenden).

Führen Sie die folgenden Schritte aus, um einen Forward Proxy zu konfigurieren:

1. Klicken Sie auf **Kontenadmin > Profile > Partner**.
2. Klicken Sie auf **Ziele**.
3. Klicken Sie auf **Forward Proxy-Unterstützung**.
4. Klicken Sie auf der Seite **Forward Proxy-Liste** auf **Erstellen**.
5. Geben Sie einen Namen für den Proxy-Server ein.
6. Geben Sie optional eine Beschreibung des Proxy-Servers ein.
7. Wählen Sie den Transporttyp in der Liste aus.

   **Anmerkung:** Die verfügbaren Transporte sind HTTP und HTTPS.
8. Geben Sie die folgenden Informationen ein. Geben Sie entweder Proxy-Host und Proxy-Port *oder* Socks-Proxy-Host und Socks-Proxy-Port ein.
   - Geben Sie für **Proxy-Host** den zu verwendenden Proxy-Server ein, z. B. http://proxy.abc.com.
   - Geben Sie für **Proxy-Port** die Portnummer ein.
   - Wenn der Proxy-Server einen Benutzername und ein Kennwort erfordert, geben Sie diese in die Felder **Benutzername** und **Kennwort** ein.
   - Geben Sie für **Socks-Proxy-Host** den zu verwendenden Socks-Proxy-Server ein.
   - Geben Sie für **Socks-Proxy-Port** die Portnummer ein.
9. Wählen Sie das Kontrollkästchen aus, wenn Sie diesen Proxy-Server als Standard-Proxy-Server verwenden wollen, der von jedem Partner mit Proxy-Unterstützung verwendet werden kann.
10. Klicken Sie auf **Speichern**.

**Anmerkung:** Beim Forward Proxy wird das HTTP-Tunnelungsverfahren verwendet, Secure Forward Proxy wird allerdings nicht unterstützt. Der HTTP-Tunnel wird mit dem Proxy-Server erstellt. Die Konnektivität muss geprüft werden, bevor Sie einen Datentyp (HTTP oder HTTPS) an den Endpartner weiterleiten. Die Daten werden mit SSL verschlüsselt. Für den Forward Proxy muss HTTP-Port 80 verwendet werden. Dabei handelt es sich im Wesentlichen um einen Durchgang für den SSL-Handshake zwischen WebSphere Partner Gateway und dem Partner.

# HTTP-Ziel einrichten

Sie können ein HTTP-Ziel so einrichten, dass Dokumente vom Hub an die IP-Adresse Ihres Partners gesendet werden. Beim Einrichten eines HTTP-Ziels können Sie außerdem angeben, dass die zu verarbeitenden Dokumente über einen konfigurierten Proxy-Server gesendet werden sollen.

Gehen Sie wie folgt vor, um mit dem Erstellungsprozess für ein HTTP-Ziel zu beginnen:

1. Klicken Sie auf **Kontenadmin > Profile**.
2. Geben Sie Suchkriterien ein, und klicken Sie auf **Suchen**. Sie können auch auf **Suchen** klicken, ohne Suchkriterien einzugeben, um eine Liste aller Partner anzuzeigen.
3. Klicken Sie auf das Symbol **Details anzeigen**, um das Profil des Partners anzuzeigen.
4. Klicken Sie auf **Ziele**.
5. Klicken Sie auf **Erstellen**.

## Zieldetails

Führen Sie auf der Seite **Liste der Ziele** die folgenden Schritte aus:

1. Geben Sie einen Namen ein, um das Ziel zu identifizieren. Dies ist ein erforderliches Feld. Dies ist der Name, der in der Liste der Ziele angezeigt wird.
2. Geben Sie optional den Status des Ziels an. **Aktiviert** ist die Standardeinstellung. Ein aktiviertes Ziel steht für das Senden von Dokumenten zur Verfügung. Ein inaktiviertes Ziel kann keine Dokumente senden.
3. Geben Sie optional an, ob das Ziel online oder offline ist. Die Standardeinstellung ist **Online**.
4. Geben Sie optional eine Beschreibung für das Ziel ein.

## Konfiguration des Ziels

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

1. Wählen Sie optional einen zu verwendenden Proxy-Server aus. Die **Forward Proxy-Liste** schließt alle Proxy-Server ein, die Sie erstellt haben, einschließlich dem Standard-Proxy-Server. Der Standardwert für dieses Feld ist **Standardmäßigen Forward Proxy verwenden**. Wenn Sie wollen, dass der ausgewählte Partner einen anderen Proxy-Server verwendet, wählen Sie diesen Server aus der Liste aus. Wenn Sie diese Funktion nicht mit dem ausgewählten Partner verwenden wollen, wählen Sie **Keinen Forward Proxy verwenden** aus.

2. Geben Sie im Feld **Adresse** die URI ein, an die das Dokument zugestellt werden soll. Dieses Feld ist erforderlich.

   Das Format lautet wie folgt: http://*<servername>*:*<optionaler_port>*/*<pfad>*

   Beispiel für dieses Format:

   ```
   http://weitererserver.ibm.com:57080/bcgreceiver/Receiver
   ```

   **Anmerkung:** Handelt es sich um eine IPv6-Adresse, müssen Sie das numerische Format und nicht den Maschinen-/Hostnamen angeben.

   Beispiele für IPv6-Adressen:

   ```
   http://[FEDC:BA98:7654:3210:FEDC:BA98:7654:3210]:80/index.html
   http://[1080:0:0:0:8:800:200C:417A]/index.html
   http://[3ffe:2a00:100:7031::1]
   http://[1080::8:800:200C:417A]/foo
   http://[::192.9.5.5]/ipng
   http://[::FFFF:129.144.52.38]:80/index.html
   http://[2010:836B:4179::836B:4179]
   ```

   Wenn Sie ein Ziel für die Verwendung durch einen Web-Service konfigurieren, geben Sie die private URL an, die vom Web-Service-Provider bereitgestellt wird. Dort wird WebSphere Partner Gateway den Web-Service aufrufen, wenn er als Proxy-Server für den Web-Service-Provider agiert.
3. Geben Sie optional einen Benutzernamen und ein Kennwort ein, wenn ein Benutzername und ein Kennwort für den Zugriff auf den HTTP-Server erforderlich sind.
4. Geben Sie im Feld **Wiederholungszähler** ein, wie oft das Ziel versuchen soll, ein Dokument zu senden, bevor der Vorgang fehlschlägt. Der Standardwert ist 3.
5. Geben Sie im Feld **Wiederholungsintervall** die Zeitdauer ein, die das Ziel zwischen den einzelnen Wiederholungsversuchen warten soll. Der Standardwert ist 300 Sekunden.
6. Geben Sie im Feld **Anzahl Threads** die Anzahl der Dokumente ein, die gleichzeitig verarbeitet werden können. Der Standardwert ist 3.
7. Wählen Sie im Feld **Client-IP prüfen** die Option **Ja** aus, wenn Sie wollen, dass die IP-Adresse des Absenders geprüft wird, bevor das Dokument verarbeitet wird. Wählen Sie andernfalls **Nein** aus. Die Standardeinstellung ist **Nein**.
8. Wählen Sie im Feld **Autom. Warteschlange** die Option **Ja** aus, wenn Sie wollen, dass das Ziel (automatisch) offline gehen soll, wenn ein Zustellungsfehler auftritt, weil die Anzahl der Wiederholungen aufgebraucht ist. Wählen Sie andernfalls **Nein** aus. Die Standardeinstellung ist **Nein**.

   Wird die Option **Autom. Warteschlange** ausgewählt, verbleiben alle Dokumente in der Warteschlange, bis das Ziel manuell wieder in den Onlinemodus versetzt wird.
9. Geben Sie im Feld **Verbindungszeitlimit** die Zeitdauer in Sekunden ein, die ein Socket ohne Datenverkehr geöffnet bleiben soll. Der Standardwert ist 120 Sekunden.
10. Wenn Sie den Vorverarbeitungs- oder den Nachverarbeitungsschritt für das Ziel konfigurieren wollen, fahren Sie mit „Handler konfigurieren" auf Seite 248 fort. Ansonsten klicken Sie auf **Speichern**.

# HTTP-Ziel einrichten

Sie können ein HTTPS-Ziel so einrichten, dass Dokumente vom Hub an die IP-Adresse Ihres Partners gesendet werden. Beim Einrichten eines HTTPS-Ziels können Sie außerdem angeben, dass die zu verarbeitenden Dokumente über einen konfigurierten Proxy-Server gesendet werden sollen.

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

1. Klicken Sie auf **Kontenadmin > Profile > Partner**.
2. Geben Sie Suchkriterien ein, und klicken Sie auf **Suchen**. Sie können auch auf **Suchen** klicken, ohne Suchkriterien einzugeben, um eine Liste aller Partner anzuzeigen.
3. Klicken Sie auf das Symbol **Details anzeigen**, um das Profil des Partners anzuzeigen.
4. Klicken Sie auf **Ziele**.
5. Klicken Sie auf **Erstellen**.

## Zieldetails

Führen Sie auf der Seite **Zieldetails** die folgenden Schritte aus:

1. Geben Sie einen Namen ein, um das Ziel zu identifizieren. Dies ist ein erforderliches Feld.
2. Geben Sie optional den Status des Ziels an. **Aktiviert** ist die Standardeinstellung. Ein aktiviertes Ziel steht für das Senden von Dokumenten zur Verfügung. Ein inaktiviertes Ziel kann keine Dokumente senden.
3. Geben Sie optional an, ob das Ziel online oder offline ist. Die Standardeinstellung ist **Online**.
4. Geben Sie optional eine Beschreibung für das Ziel ein.
5. Wählen Sie in der Liste **Transport** den Eintrag **HTTPS/1.0** oder **HTTPS/1.1** aus.

## Konfiguration des Ziels

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

1. Wählen Sie optional einen zu verwendenden Proxy-Server aus. Die **Forward Proxy-Liste** schließt alle Proxy-Server ein, die Sie erstellt haben, einschließlich dem Standard-Proxy-Server. Der Standardwert für dieses Feld ist **Standardmäßigen Forward Proxy verwenden**. Wenn Sie wollen, dass der ausgewählte Partner einen anderen Proxy-Server verwendet, wählen Sie diesen Server aus der Liste aus. Wenn Sie diese Funktion nicht mit dem ausgewählten Partner verwenden wollen, wählen Sie **Keinen Forward Proxy verwenden** aus.
2. Geben Sie im Feld **Adresse** die URI ein, an die das Dokument zugestellt werden soll. Dieses Feld ist erforderlich.

   Das Format lautet wie folgt: https://*<servername>:<optionaler_port>/<pfad>*

   Beispiel:

   ```
   https://weitererserver.ibm.com:57443/bcgreceiver/Receiver
   ```

   **Anmerkung:** Handelt es sich um eine IPv6-Adresse, müssen Sie das numerische Format und nicht den Maschinen-/Hostnamen angeben.

Beispiele für IPv6-Adressen:

```
https://[FEDC:BA98:7654:3210:FEDC:BA98:7654:3210]:80/index.html
https://[1080:0:0:0:8:800:200C:417A]/index.html
https://[3ffe:2a00:100:7031::1]
https://[1080::8:800:200C:417A]/foo
https://[::192.9.5.5]/ipng
https://[::FFFF:129.144.52.38]:80/index.html
https://[2010:836B:4179::836B:4179]
```

3. Geben Sie optional einen Benutzernamen und ein Kennwort ein, wenn ein Benutzername und ein Kennwort für den Zugriff auf den HTTPS-Server erforderlich sind.
4. Geben Sie im Feld **Wiederholungszähler** ein, wie oft das Ziel versuchen soll, ein Dokument zu senden, bevor der Vorgang fehlschlägt. Der Standardwert ist 3.
5. Geben Sie im Feld **Wiederholungsintervall** die Zeitdauer ein, die das Ziel zwischen den einzelnen Wiederholungsversuchen warten soll. Der Standardwert ist 300 Sekunden.
6. Geben Sie im Feld **Anzahl Threads** die Anzahl der Dokumente ein, die gleichzeitig verarbeitet werden können. Der Standardwert ist 3.
7. Wählen Sie im Feld **Client-IP prüfen** die Option **Ja** aus, wenn Sie wollen, dass die IP-Adresse des Absenders geprüft wird, bevor das Dokument verarbeitet wird. Wählen Sie andernfalls **Nein** aus. Die Standardeinstellung ist **Nein**.
8. Wählen Sie im Feld **Client-SSL-Zertifikat prüfen** die Option **Ja** aus, wenn Sie wollen, dass das digitale Zertifikat des sendenden Partners mit der dem Dokument zugeordneten Geschäfts-ID geprüft wird. Die Standardeinstellung ist **Nein**.
9. Wählen Sie im Feld **Autom. Warteschlange** die Option **Ja** aus, wenn Sie wollen, dass das Ziel (automatisch) offline gehen soll, wenn ein Zustellungsfehler auftritt, weil die Anzahl der Wiederholungen aufgebraucht ist. Wählen Sie andernfalls **Nein** aus. Die Standardeinstellung ist **Nein**.

   Wird die Option **Autom. Warteschlange** ausgewählt, verbleiben alle Dokumente in der Warteschlange, bis das Ziel manuell wieder in den Onlinemodus versetzt wird.
10. Geben Sie im Feld **Verbindungszeitlimit** die Zeitdauer in Sekunden ein, die ein Socket ohne Datenverkehr geöffnet bleiben soll. Der Standardwert ist 120 Sekunden.
11. Wenn Sie den Vorverarbeitungs- oder den Nachverarbeitungsschritt für das Ziel konfigurieren wollen, fahren Sie mit „Handler konfigurieren" auf Seite 248 fort. Ansonsten klicken Sie auf **Speichern**.

## FTP-Ziel einrichten

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

1. Klicken Sie auf **Kontenadmin > Profile > Partner**.
2. Geben Sie Suchkriterien ein, und klicken Sie auf **Suchen**. Sie können auch auf **Suchen** klicken, ohne Suchkriterien einzugeben, um eine Liste aller Partner anzuzeigen.
3. Klicken Sie auf das Symbol **Details anzeigen**, um das Profil des Partners anzuzeigen.
4. Klicken Sie auf **Ziele**.
5. Klicken Sie auf **Erstellen**.

**Anmerkung:** FTP im passiven Modus wird nicht unterstützt. Informationen zur Unterstützung im passiven Modus finden Sie in „FTP-Scripting-Ziel einrichten" auf Seite 244.

## Zieldetails

Führen Sie auf der Seite **Zieldetails** die folgenden Schritte aus:

1. Geben Sie einen Namen ein, um das Ziel zu identifizieren. Dies ist ein erforderliches Feld.
2. Geben Sie optional den Status des Ziels an. **Aktiviert** ist die Standardeinstellung. Ein aktiviertes Ziel steht für das Senden von Dokumenten zur Verfügung. Ein inaktiviertes Ziel kann keine Dokumente senden.
3. Geben Sie optional an, ob das Ziel online oder offline ist. Die Standardeinstellung ist **Online**.
4. Geben Sie optional eine Beschreibung für das Ziel ein.

## Konfiguration des Ziels

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

1. Geben Sie im Feld **Adresse** die URI ein, an die das Dokument zugestellt werden soll. Dieses Feld ist erforderlich.

   Das Format lautet wie folgt: ftp://<*ftp-servername*>:<*portnr*>

   Beispiel:

   ```
   ftp://ftpserver1.ibm.com:2115
   ```

   Wenn Sie keine Portnummer eingeben, wird der Standard-FTP-Port verwendet.

   **Anmerkung:** Handelt es sich um eine IPv6-Adresse, müssen Sie das numerische Format und nicht den Maschinen-/Hostnamen angeben.

   Beispiele für IPv6-Adressen:

   ```
   ftp://[FEDC:BA98:7654:3210:FEDC:BA98:7654:3210]:21
   ftp://[1080:0:0:0:8:800:200C:417A]:21
   ftp://[3ffe:2a00:100:7031::1]:21
   ftp://[1080::8:800:200C:417A]:21
   ftp://[::192.9.5.5]:21
   ftp://[::FFFF:129.144.52.38]:21
   ftp://[2010:836B:4179::836B:4179]:21
   ```
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 im Feld **Wiederholungszähler** ein, wie oft das Ziel versuchen soll, ein Dokument zu senden, bevor der Vorgang fehlschlägt. Der Standardwert ist 3.
4. Geben Sie im Feld **Wiederholungsintervall** die Zeitdauer ein, die das Ziel zwischen den einzelnen Wiederholungsversuchen warten soll. Der Standardwert ist 300 Sekunden.
5. Geben Sie im Feld **Anzahl Threads** die Anzahl der Dokumente ein, die gleichzeitig verarbeitet werden können. 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 Ziel (automatisch) offline gehen soll, wenn ein Zustellungsfehler auftritt, weil die Anzahl der Wiederholungen aufgebraucht ist. Wählen Sie andernfalls **Nein** aus. Die Standardeinstellung ist **Nein**.

   Wird die Option **Autom. Warteschlange** ausgewählt, verbleiben alle Dokumente in der Warteschlange, bis das Ziel manuell wieder in den Onlinemodus versetzt wird.
8. Geben Sie im Feld **Verbindungszeitlimit** die Zeitdauer in Sekunden ein, die ein Socket ohne Datenverkehr geöffnet bleiben soll. Der Standardwert ist 120 Sekunden.
9. Wenn Sie wollen, dass das Dokument seinen ursprünglichen Namen beibehält, wenn es an sein Ziel gesendet wird, dürfen Sie die Option **Eindeutigen Dateinamen verwenden** nicht auswählen. Wählen Sie diese Option aus, wenn WebSphere Partner Gateway der Datei einen Namen zuordnen soll.
10. Wenn Sie den Vorverarbeitungs- oder den Nachverarbeitungsschritt für das Ziel konfigurieren wollen, fahren Sie mit „Handler konfigurieren" auf Seite 248 fort. Ansonsten klicken Sie auf **Speichern**.

## SMTP-Ziel einrichten

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

1. Klicken Sie auf **Kontenadmin > Profile > Partner**.
2. Geben Sie Suchkriterien ein, und klicken Sie auf **Suchen**. Sie können auch auf **Suchen** klicken, ohne Suchkriterien einzugeben, um eine Liste aller Partner anzuzeigen.
3. Klicken Sie auf das Symbol **Details anzeigen**, um das Profil des Partners anzuzeigen.
4. Klicken Sie auf **Ziele**.
5. Klicken Sie auf **Erstellen**.

### Zieldetails

Führen Sie auf der Seite **Liste der Ziele** die folgenden Schritte aus:

1. Geben Sie einen Namen ein, um das Ziel zu identifizieren. Dies ist ein erforderliches Feld.
2. Geben Sie optional den Status des Ziels an. **Aktiviert** ist die Standardeinstellung. Ein aktiviertes Ziel steht für das Senden von Dokumenten zur Verfügung. Ein inaktiviertes Ziel kann keine Dokumente senden.
3. Geben Sie optional an, ob das Ziel online oder offline ist. Die Standardeinstellung ist **Online**.
4. Geben Sie optional eine Beschreibung für das Ziel ein.

### Konfiguration des Ziels

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

1. Geben Sie im Feld **Adresse** die URI ein, an die das Dokument zugestellt werden soll. Dieses Feld ist erforderlich.

   Das Format lautet wie folgt: mailto:<*benutzer@servername*>

   Beispiel:

   ```
   mailto:admin@weitererserver.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 im Feld **Wiederholungszähler** ein, wie oft das Ziel versuchen soll, ein Dokument zu senden, bevor der Vorgang fehlschlägt. Der Standardwert ist 3.
4. Geben Sie im Feld **Wiederholungsintervall** die Zeitdauer ein, die das Ziel zwischen den einzelnen Wiederholungsversuchen warten soll. Der Standardwert ist 300 Sekunden.
5. Geben Sie im Feld **Anzahl Threads** die Anzahl der Dokumente ein, die gleichzeitig verarbeitet werden können. 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 Ziel (automatisch) offline gehen soll, wenn ein Zustellungsfehler auftritt, weil die Anzahl der Wiederholungen aufgebraucht ist. Wählen Sie andernfalls **Nein** aus. Die Standardeinstellung ist **Nein**.

   Wird die Option **Autom. Warteschlange** ausgewählt, verbleiben alle Dokumente in der Warteschlange, bis das Ziel manuell wieder in den Onlinemodus versetzt 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. Wenn Sie den Vorverarbeitungs- oder den Nachverarbeitungsschritt für das Ziel konfigurieren wollen, fahren Sie mit „Handler konfigurieren" auf Seite 248 fort. Ansonsten klicken Sie auf **Speichern**.

## JMS-Ziel einrichten

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

1. Klicken Sie auf **Kontenadmin > Profile > Partner**.
2. Geben Sie Suchkriterien ein, und klicken Sie auf **Suchen**. Sie können auch auf **Suchen** klicken, ohne Suchkriterien einzugeben, um eine Liste aller Partner anzuzeigen.
3. Klicken Sie auf das Symbol **Details anzeigen**, um das Profil des Partners anzuzeigen.
4. Klicken Sie auf **Ziele**.
5. Klicken Sie auf **Erstellen**.

**Anmerkung:** Informationen zum Konfigurieren der Laufzeitbibliotheken, um die erforderlichen WebSphere MQ-JAR-Dateien für WebSphere Partner Gateway sichtbar zu machen, finden Sie in „Laufzeitbibliotheken konfigurieren" auf Seite 42.

### Zieldetails

Führen Sie auf der Seite **Liste der Ziele** die folgenden Schritte aus:

1. Geben Sie einen Namen ein, um das Ziel zu identifizieren. Dies ist ein erforderliches Feld.

2. Geben Sie optional den Status des Ziels an. **Aktiviert** ist die Standardeinstellung. Ein aktiviertes Ziel steht für das Senden von Dokumenten zur Verfügung. Ein inaktiviertes Ziel kann keine Dokumente senden.
3. Geben Sie optional an, ob das Ziel online oder offline ist. Die Standardeinstellung ist **Online**.
4. Geben Sie optional eine Beschreibung für das Ziel ein.

## Konfiguration des Ziels

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

1. Geben Sie im Feld **Adresse** die URL ein, an die das Dokument zugestellt werden soll. Dieses Feld ist erforderlich.

   Für WebSphere MQ-JMS lautet das Format der Ziel-URL wie folgt:

   `file:///<benutzerdefinierter_MQ_JNDI_bindings_pfad>`

   Beispiel:

   ```
   file:///opt/JNDI-Directory unter UNIX und
   file://c:/temp/ (unter Windows)
   ```

   Das Verzeichnis enthält die Bindungsdatei (".bindings") für die dateibasierte JNDI. Diese Datei gibt für WebSphere Partner Gateway an, wie das Dokument an das angegebene Ziel weitergeleitet werden soll.

   - Für ein internes JMS-Ziel (d. h., das Ziel für Ihr Back-End-System) sollte dies mit dem Wert übereinstimmen, den Sie eingegeben haben (der Dateisystempfad zur Bindungsdatei), als Sie WebSphere Partner Gateway für JMS konfiguriert haben (Schritt 5 auf Seite 40). Sie können den Unterordner für den JMS-Kontext auch als Teil der JMS-Provider-URL angeben.

     Geben Sie ohne den JMS-Kontext beispielsweise `c:/temp/JMS` ein. Geben Sie mit dem JMS-Kontext beispielsweise `c:/temp/JMS/JMS` ein.
   - Für Partnerziele stellt der Partner wahrscheinlich die Bindungsdatei (".bindings") bereit.

   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 im Feld **Wiederholungszähler** ein, wie oft das Ziel versuchen soll, ein Dokument zu senden, bevor der Vorgang fehlschlägt. Der Standardwert ist 3.
4. Geben Sie im Feld **Wiederholungsintervall** die Zeitdauer ein, die das Ziel zwischen den einzelnen Wiederholungsversuchen warten soll. Der Standardwert ist 300 Sekunden.
5. Geben Sie im Feld **Anzahl Threads** die Anzahl der Dokumente ein, die gleichzeitig verarbeitet werden können. 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 Ziel (automatisch) offline gehen soll, wenn ein Zustellungsfehler auftritt, weil die Anzahl der Wiederholungen aufgebraucht ist. Wählen Sie andernfalls **Nein** aus. Die Standardeinstellung ist **Nein**.

   Wird die Option **Autom. Warteschlange** ausgewählt, verbleiben alle Dokumente in der Warteschlange, bis das Ziel manuell wieder in den Onlinemodus versetzt 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.

   Für interne JMS-Ziele sollte dieser Name mit dem Namen übereinstimmen, den Sie mit dem Befehl `define qcf` angegeben haben, als Sie die Bindungsdatei erstellt haben (Schritt 4 auf Seite 41).

   Wenn Sie den Unterordner für den JMS-Kontext in Schritt 1 auf Seite 238 eingegeben haben, geben Sie hier nur den Factory-Namen ein (z. B. `Hub`). Wenn Sie den Unterordner für den JMS-Kontext nicht im Feld **Adresse** eingegeben haben, geben Sie den Unterordner vor dem Factory-Namen ein, z. B. `JMS/Hub`.
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 im Feld **JMS-Nachrichtentyp** den Nachrichtentyp ein. Da die Zuordnung des JMS-Nachrichtentyps durch die Empfängerkomponente festgelegt wird, ist der Wert für den JMS-Nachrichtentyp optional.
12. Geben Sie im Feld **Provider-URL-Pakete** den Namen der Klassen (oder der JAR-Datei) ein, mit denen Java die JMS-Kontext-URL versteht. Dieses Feld ist optional. Wenn Sie keinen Wert angeben, wird der Dateisystempfad zur Bindungsdatei verwendet.
13. Geben Sie im Feld **JMS-Warteschlangenname** den Namen der JMS-Warteschlange ein, an die Dokumente gesendet werden. Dieses Feld ist erforderlich.

    Für interne JMS-Ziele sollte dieser Name mit dem Namen übereinstimmen, den Sie mit dem Befehl `define q` angegeben haben, als Sie die Bindungsdatei erstellt haben (Schritt 4 auf Seite 41).

    Wenn Sie den Unterordner für den JMS-Kontext in Schritt 1 auf Seite 238 eingegeben haben, geben Sie hier nur den Namen der Warteschlange ein, z. B. `outQ`. Wenn Sie den Unterordner für den JMS-Kontext nicht in der JMS-Provider-URL eingegeben haben, geben Sie den Unterordner vor dem Factory-Namen ein (z. B. `JMS/outQ`).
14. Geben Sie im 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 „Hub für das JMS-Transportprotokoll konfigurieren" auf Seite 39 beschrieben, für WebSphere MQ einrichten.
15. Wenn Sie den Vorverarbeitungs- oder den Nachverarbeitungsschritt für das Ziel konfigurieren wollen, fahren Sie mit „Handler konfigurieren" auf Seite 248 fort. Ansonsten klicken Sie auf **Speichern**.

## Dateiverzeichnisziel einrichten

Gehen Sie wie folgt vor, um Dateiverzeichnisziele zu erstellen:

1. Klicken Sie auf **Kontenadmin > Profile > Partner**.
2. Geben Sie Suchkriterien ein, und klicken Sie auf **Suchen**. Sie können auch auf **Suchen** klicken, ohne Suchkriterien einzugeben, um eine Liste aller Partner anzuzeigen.
3. Klicken Sie auf das Symbol **Details anzeigen**, um das Profil des Partners anzuzeigen.

4. Klicken Sie auf **Ziele**.
5. Klicken Sie auf **Erstellen**.

## Zieldetails

Führen Sie auf der Seite **Liste der Ziele** die folgenden Schritte aus:

1. Geben Sie einen Namen ein, um das Ziel zu identifizieren. Dies ist ein erforderliches Feld.
2. Geben Sie optional den Status des Ziels an. **Aktiviert** ist die Standardeinstellung. Ein aktiviertes Ziel steht für das Senden von Dokumenten zur Verfügung. Ein inaktiviertes Ziel kann keine Dokumente senden.
3. Geben Sie optional an, ob das Ziel online oder offline ist. Die Standardeinstellung ist **Online**.
4. Geben Sie optional eine Beschreibung für das Ziel ein.

## Konfiguration des Ziels

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

1. Geben Sie im Feld **Adresse** die URI ein, an die das Dokument zugestellt werden soll. Dieses Feld ist erforderlich.

   Das Format für UNIX- und Windows-Systeme, bei denen sich das Dateiverzeichnis auf demselben Laufwerk befindet wie die WebSphere Partner Gateway-Installation, lautet wie folgt: file://*<pfad_zu_zielverzeichnis>*.

   Beispiel:

   ```
   file://lokalesdateiverz
   ```

   Dabei steht *lokalesdateiverz* für ein Verzeichnis im Stammverzeichnis.

   Wenn das Dateiverzeichnisziel unter Windows auf einem anderen Laufwerk erstellt werden muss, als dem Laufwerk, auf dem WebSphere Partner Gateway installiert ist, lautet der Pfad wie folgt: file:///*<laufwerkbuchstabe>*:/*<pfad>*.
2. Geben Sie im Feld **Wiederholungszähler** ein, wie oft das Ziel versuchen soll, ein Dokument zu senden, bevor der Vorgang fehlschlägt. Der Standardwert ist 3.
3. Geben Sie im Feld **Wiederholungsintervall** die Zeitdauer ein, die das Ziel zwischen den einzelnen Wiederholungsversuchen warten soll. Der Standardwert ist 300 Sekunden.
4. Geben Sie im Feld **Anzahl Threads** die Anzahl der 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 Ziel (automatisch) offline gehen soll, wenn ein Zustellungsfehler auftritt, weil die Anzahl der Wiederholungen aufgebraucht ist. Wählen Sie andernfalls **Nein** aus. Die Standardeinstellung ist **Nein**.

   Wird die Option **Autom. Warteschlange** ausgewählt, verbleiben alle Dokumente in der Warteschlange, bis das Ziel manuell wieder in den Onlinemodus versetzt wird.
7. Wenn Sie wollen, dass das Dokument seinen ursprünglichen Namen beibehält, wenn es an sein Ziel gesendet wird, dürfen Sie die Option **Eindeutigen Dateinamen verwenden** nicht auswählen. Wählen Sie diese Option aus, wenn WebSphere Partner Gateway der Datei einen Namen zuordnen soll.

8. Wenn Sie den Vorverarbeitungs- oder den Nachverarbeitungsschritt für das Ziel konfigurieren wollen, fahren Sie mit „Handler konfigurieren" auf Seite 248 fort. Ansonsten klicken Sie auf **Speichern**.

## FTPS-Ziel einrichten

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

1. Klicken Sie auf **Kontenadmin > Profile > Partner**.
2. Geben Sie Suchkriterien ein, und klicken Sie auf **Suchen**. Sie können auch auf **Suchen** klicken, ohne Suchkriterien einzugeben, um eine Liste aller Partner anzuzeigen.
3. Klicken Sie auf das Symbol **Details anzeigen**, um das Profil des Partners anzuzeigen.
4. Klicken Sie auf **Ziele**.
5. Klicken Sie auf **Erstellen**.

**Anmerkung:** FTPS im passiven Modus wird nicht unterstützt. Informationen zur Unterstützung im passiven Modus finden Sie in „FTP-Scripting-Ziel einrichten" auf Seite 244.

### Zieldetails

Führen Sie auf der Seite **Liste der Ziele** die folgenden Schritte aus:

1. Geben Sie einen Namen ein, um das Ziel zu identifizieren. Dies ist ein erforderliches Feld.
2. Geben Sie optional den Status des Ziels an. **Aktiviert** ist die Standardeinstellung. Ein aktiviertes Ziel steht für das Senden von Dokumenten zur Verfügung. Ein inaktiviertes Ziel kann keine Dokumente senden.
3. Geben Sie optional an, ob das Ziel online oder offline ist. Die Standardeinstellung ist **Online**.
4. Geben Sie optional eine Beschreibung für das Ziel ein.

### Konfiguration des Ziels

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

1. Geben Sie im Feld **Adresse** die URI ein, an die das Dokument zugestellt werden soll. Dieses Feld ist erforderlich.

   Das Format lautet wie folgt: 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 im Feld **Wiederholungszähler** ein, wie oft das Ziel versuchen soll, ein Dokument zu senden, bevor der Vorgang fehlschlägt. Der Standardwert ist 3.

4. Geben Sie im Feld **Wiederholungsintervall** die Zeitdauer ein, die das Ziel zwischen den einzelnen Wiederholungsversuchen warten soll. Der Standardwert ist 300 Sekunden.
5. Geben Sie im Feld **Anzahl Threads** die Anzahl der 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 Ziel (automatisch) offline gehen soll, wenn ein Zustellungsfehler auftritt, weil die Anzahl der Wiederholungen aufgebraucht ist. Wählen Sie andernfalls **Nein** aus. Die Standardeinstellung ist **Nein**.

   Wird die Option **Autom. Warteschlange** ausgewählt, verbleiben alle Dokumente in der Warteschlange, bis das Ziel manuell wieder in den Onlinemodus versetzt wird.
8. Geben Sie im Feld **Verbindungszeitlimit** die Zeitdauer in Sekunden ein, die ein Socket ohne Datenverkehr geöffnet bleiben soll. Der Standardwert ist 120 Sekunden.
9. Wenn Sie wollen, dass das Dokument seinen ursprünglichen Namen beibehält, wenn es an sein Ziel gesendet wird, dürfen Sie die Option **Eindeutigen Dateinamen verwenden** nicht auswählen. Wählen Sie diese Option aus, wenn WebSphere Partner Gateway der Datei einen Namen zuordnen soll.
10. Wenn Sie den Vorverarbeitungs- oder den Nachverarbeitungsschritt für das Ziel konfigurieren wollen, fahren Sie mit „Handler konfigurieren" auf Seite 248 fort. Klicken Sie ansonsten auf **Speichern**.

## SFTP-Ziel einrichten

Sie können ein SFTP-Ziel so einrichten, dass Dokumente vom Hub an die IP-Adresse Ihres Partners gesendet werden. Ein Adapter stellt eine Verbindung zum SFTP-Server her und sendet das Dokument an den SFTP-Server. Die Dokumentdaten erhält der Adapter in Form eines Datenstroms.

Gehen Sie wie folgt vor, um SFTP-Ziele zu erstellen:

1. Klicken Sie auf **Kontenadmin > Profile > Partner**.
2. Geben Sie Suchkriterien ein, und klicken Sie auf **Suchen**. Sie können auch auf **Suchen** klicken, ohne Suchkriterien einzugeben, um eine Liste aller Partner anzuzeigen.
3. Klicken Sie auf das Symbol **Details anzeigen**, um das Profil des Partners anzuzeigen.
4. Klicken Sie auf **Ziele**.
5. Klicken Sie auf **Erstellen**.

### Zieldetails

Führen Sie auf der Seite **Zieldetails** die folgenden Schritte aus:

1. Geben Sie einen Namen ein, um das Ziel zu identifizieren. Dies ist ein erforderliches Feld.
2. Geben Sie optional den Status des Ziels an. **Aktiviert** ist die Standardeinstellung. Ein aktiviertes Ziel steht für das Senden von Dokumenten zur Verfügung. Ein inaktiviertes Ziel kann keine Dokumente senden.

3. Geben Sie optional an, ob das Ziel online oder offline ist. Die Standardeinstellung ist **Online**.
4. Geben Sie optional eine Beschreibung für das Ziel ein.
5. Wählen Sie in der Liste **Transport** den Eintrag **SFTP** aus.

## Konfiguration des Ziels

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

1. Geben Sie den Wert für **SFTP-Host-IP/-Hostname** ein. Es sind maximal 100 Zeichen zulässig. Ferner können Sie IP-Adressen, IPv4- und IPv6-Adressen eingeben.
2. Geben Sie einen Wert für die **Portnummer** ein. Der Mindestwert ist 1 und der Maximalwert ist 65535. Der Standardwert ist 22.
3. Geben Sie das **Ausgabeverzeichnis** ein. Es sind maximal 100 Zeichen zulässig. Die Eingabe von auf einer Locale basierenden Zeichen ist möglich.
4. Wählen Sie im Feld **Authentifizierungstyp** die Option **Benutzername/ Kennwort** oder **Authentifizierung über privaten Schlüssel** aus.
5. Wählen Sie im Feld **Autom. Warteschlange** die Option **Ja** aus, wenn Sie wollen, dass das Ziel (automatisch) offline gehen soll, wenn ein Zustellungsfehler auftritt. Wählen Sie andernfalls **Nein** aus. Die Standardeinstellung ist **Nein**.
6. Geben Sie für Benutzername/Kennwort einen Wert für **Benutzername** und **Kennwort** ein. Ist als Authentifizierungstyp die Authentifizierung über einen privaten Schlüssel ausgewählt, müssen Sie die Felder **Benutzername**, **Datei mit privatem Schlüssel** und **Verschlüsselungstext** ausfüllen. **Datei mit privatem Schlüssel** gibt den Pfad der Datei mit dem privatem Schlüssel im OpenSSH-Format an.
7. Geben Sie einen Wert für **Wiederholungszähler** ein. Hiermit wird angegeben, wie oft der Empfänger das Herstellen der Verbindung zum SFTP-Server wiederholt, wenn die Verbindung nicht hergestellt werden konnte.
8. Geben Sie einen Wert für **Wiederholungsintervall** ein. Dies ist die Wartezeit des Empfängers zwischen den einzelnen Versuchen zum Herstellen der Verbindung.
9. Geben Sie die **Anzahl Threads** ein.
10. Die **EIS-Codierung** ist die Codierung des FTP-Servers. Mit diesem Wert können Sie die Codierung für die Steuerverbindung des FTP-Servers festlegen.
11. Die Option **Serverauthentifizierung aktivieren** kann ausgewählt werden, um den Server, zu dem eine Verbindung hergestellt wird, zu authentifizieren. Ist die Serverauthentifizierung aktiviert, müssen Sie den Pfad für die Hostschlüsseldatei angeben. Die Hostschlüsseldatei muss im Format OpenSSH vorliegen.
12. Klicken Sie auf **Speichern**, um die Konfiguration zu speichern.
13. Geben Sie die Handlerkonfiguration an und klicken Sie auf **Speichern**, um die Konfigurationsdetails zu speichern.

**Anmerkung:** Starten Sie den jeweiligen Server neu, nachdem Sie die Konfiguration gespeichert haben:

- Starten Sie im einfachen Modus den Server "bcgserver" neu.
- Starten Sie im einfachen verteilten Modus den Cluster "bcgserver" neu.
- Starten Sie im vollständig verteilten Modus den Cluster "BCGDocMgr" neu.

## FTP-Scripting-Ziel einrichten

Ein FTP-Scripting-Ziel wird nach einem von Ihnen definierten Zeitplan ausgeführt. Die Funktionsweise eines FTP-Scripting-Ziels wird über ein FTP-Befehlsscript gesteuert.

**Anmerkung:** Wenn die Datenbank inaktiv und **Benutzer sperren** auf "Ja" gesetzt ist, arbeitet das FTP-Scripting-Ziel möglicherweise nicht korrekt, weil es die Sperre nicht aus der Datenbank abrufen kann.

**Anmerkung:** Verwenden Sie auf der Plattform AIX den passiven Modus, um Dokumente mit hohen Transaktionsumfängen zuzustellen. Geben Sie bei der Dateiübertragungsoperation den passiven Modus in dem vom FTP-Scripting-Ziel verwendeten Script an. Die Befehle 'passive' und 'pasv' können im Script synonym verwendet werden. Bei Verwendung des aktiven Modus wird ein Fehler generiert.

## FTP-Script erstellen

Zur Verwendung eines FTP-Scripting-Ziels müssen Sie eine Datei erstellen, die alle erforderlichen FTP-Befehle enthält, die vom FTP-Server akzeptiert werden.

1. Erstellen Sie ein Script für die Ziele, in dem die auszuführenden Aktionen aufgeführt sind. Das folgende Script ist ein Beispiel für das Herstellen einer Verbindung zu dem angegebenen FTP-Server (mit dem angegebenen Namen und Kennwort), für das Wechseln zum angegebenen Verzeichnis auf dem FTP-Server und für das Senden aller Dateien zu dem angegebenen Verzeichnis auf dem Server:

   ```
   open %BCGSERVERIP% %BCGUSERID% %BCGPASSWORD% %BCGOPTIONx%
   cd %BCGOPTIONx%
             mput *
   quit
   ```

   Beim Aktivieren der Ziele werden die Platzhalterzeichen (z. B. %BCGSERVERIP%) durch die Werte ersetzt, die Sie beim Erstellen einer bestimmten Instanz eines FTP-Scripting-Ziels eingeben. Die entsprechenden Angaben sind in der folgenden Tabelle aufgeführt:

   *Tabelle 30. Zuordnung von Scriptparametern zu Feldeinträgen des FTP-Scripting-Ziels*

| Scriptparameter | Feldeintrag des FTP-Scripting-Ziels |
|---|---|
| %BCGSERVERIP% | Server-IP |
| %BCGUSERID% | Benutzer-ID |
| %BCGPASSWORD% | Kennwort |
| %BCGOPTIONx% | Option*x* unter **Benutzerdefinierte Attribute** |

   Sie können über bis zu 10 benutzerdefinierte Optionen verfügen.
2. Speichern Sie die Datei.

## FTP-Scriptbefehle

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

- ascii, binary, passive, epsv

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

Dieser Befehl wechselt zum angegebenen Verzeichnis.

- delete

  Dieser Befehl entfernt eine Datei vom FTP-Server.

- mkdir

  Dieser Befehl erstellt ein Verzeichnis auf dem FTP-Server.

- mput

  Dieser Befehl verfügt über ein einzelnes Argument, das mindestens eine Datei angibt, die auf das ferne System übertragen werden soll. Dieses Argument kann die Standardplatzhalterzeichen ('*' und '?') enthalten, um mehrere Dateien anzugeben.

- mputren

  Dieser Befehl verwendet drei Argumente <quellendatei>, <temporäre_datei> und <zieldatei>, wobei ein Stern (*) den Namen der aktuellen Datei angibt, die verarbeitet wird.

  **quellendatei**
  Der Name der Datei, die auf den FTP-Server gestellt wird. Der erwartete Wert ist ein Stern (*).

  **temporäre_datei**
  Der Name der temporären Datei, die verwendet wird, wenn <quellendatei> auf den FTP-Server gestellt wird.

  **Ziel** Der Name, in den die temporäre Datei <temporäre_datei> umbenannt wird. Nach der Umbenennung ist die temporäre Datei nicht länger vorhanden.

  **Beispiele:**

  **`mputren * *.tmp *`**
  In diesem Beispiel wird die aktuelle Datei mit der Erweiterung .tmp auf den FTP-Server gestellt. Danach wird die Datei wieder in den ursprünglichen Namen umbenannt.

  **`mputren * *.tmp *.ready`**
  In diesem Beispiel wird die aktuelle Datei mit der Erweiterung .tmp auf den FTP-Server gestellt. Danach wird die Datei wieder in den ursprünglichen Namen mit der Erweiterung .ready umbenannt.

  **`mputren * *.tmp /complete/*`**
  In diesem Beispiel wird die aktuelle Datei mit der Erweiterung .tmp auf den FTP-Server gestellt. Danach wird die Datei wieder in den ursprünglichen Namen umbenannt und in das Verzeichnis /complete gestellt. Die temporäre Datei *.tmp ist nicht länger vorhanden.

  **`mputren * *.tmp /complete/*.final`**
  In diesem Beispiel wird die aktuelle Datei mit der Erweiterung .tmp auf den FTP-Server gestellt. Danach wird die Datei wieder in den ursprünglichen Namen umbenannt und mit der Erweiterung .final in das Verzeichnis /complete gestellt. Die temporäre Datei *.tmp ist nicht länger vorhanden.

- open

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

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

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

- quit

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

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

  Dieser Befehl entfernt ein Verzeichnis vom FTP-Server.
- site

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

## FTP-Scripting-Ziele

Wenn Sie mit FTP-Scripting-Zielen arbeiten, müssen Sie die folgenden Arbeitsschritte ausführen:

Gehen Sie wie folgt vor, um FTP-Scripting-Ziele zu erstellen:

1. Klicken Sie auf **Kontenadmin > Profile > Partner**.
2. Geben Sie Suchkriterien ein, und klicken Sie auf **Suchen**. Sie können auch auf **Suchen** klicken, ohne Suchkriterien einzugeben, um eine Liste aller Partner anzuzeigen.
3. Klicken Sie auf das Symbol **Details anzeigen**, um das Profil des Partners anzuzeigen.
4. Klicken Sie auf **Ziele**.
5. Klicken Sie auf **Erstellen**.

## Zieldetails

Führen Sie auf der Seite **Liste der Ziele** die folgenden Schritte aus:

1. Geben Sie einen Namen ein, um das Ziel zu identifizieren. Dies ist ein erforderliches Feld.
2. Geben Sie optional den Status des Ziels an. **Aktiviert** ist die Standardeinstellung. Ein aktiviertes Ziel steht für das Senden von Dokumenten zur Verfügung. Ein inaktiviertes Ziel kann keine Dokumente senden.
3. Geben Sie optional an, ob das Ziel online oder offline ist. Die Standardeinstellung ist **Online**.
4. Geben Sie optional eine Beschreibung für das Ziel ein.

## Konfiguration des Ziels

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

1. Geben Sie die IP-Adresse des FTP-Servers ein, zu dem Sie Dokumente senden. Der Wert, den Sie hier eingeben, wird %BCGSERVERIP% ersetzen, wenn das FTP-Script ausgeführt wird.

   **Anmerkung:** Handelt es sich um eine IPv6-Adresse, müssen Sie das numerische Format und nicht den Maschinen-/Hostnamen angeben.

Beispiele für IPv6-Adressen:

```
FEDC:BA98:7654:3210:FEDC:BA98:7654:3210
1080:0:0:0:8:800:200C:417A
3ffe:2a00:100:7031::1
1080::8:800:200C:417A
::192.9.5.5
::FFFF:129.144.52.38
2010:836B:4179::836B:4179
```

2. Geben Sie die Benutzer-ID und das Kennwort ein, die für den Zugriff auf den FTP-Server erforderlich sind. Die Werte, die Sie hier eingeben, werden %BCGUSERID% und %BCGPASSWORD% ersetzen, wenn das FTP-Script ausgeführt wird.
3. Wenn sich das Ziel im gesicherten Modus befindet, klicken Sie für **FTPS-Modus** auf **Ja**. Andernfalls verwenden Sie die Standardeinstellung **Nein**.
4. Laden Sie die Scriptdatei hoch, indem Sie die folgenden Schritte befolgen:
   a. Klicken Sie auf **Scriptdatei hochladen**.
   b. Geben Sie den Namen der Datei ein, die das Script für die Verarbeitung von Dokumenten enthält, oder navigieren Sie mit **Durchsuchen** zu der Datei.
   c. Wählen Sie den Codierungstyp für die Scriptdatei aus.
   d. Klicken Sie auf **Datei laden**, um die Scriptdatei in das Textfeld **Momentan geladene Scriptdatei** zu laden.
   e. Wenn es sich um die gewünschte Scriptdatei handelt, klicken Sie auf **Speichern**.
   f. Klicken Sie auf **Fenster schließen**.
5. Geben Sie im Feld **Wiederholungszähler** ein, wie oft das Ziel versuchen soll, ein Dokument zu senden, bevor der Vorgang fehlschlägt. Der Standardwert ist 3.
6. Geben Sie im Feld **Wiederholungsintervall** die Zeitdauer ein, die das Ziel zwischen den einzelnen Wiederholungsversuchen warten soll. Der Standardwert ist 300 Sekunden.
7. Geben Sie für **Verbindungszeitlimit** die Anzahl Sekunden ein, die ein Socket ohne Datenverkehr geöffnet bleibt. Der Standardwert ist 120 Sekunden.
8. Geben Sie im Feld **Benutzer sperren** an, ob das Ziel eine Sperre anfordern soll, sodass keine andere Instanz eines FTP-Scripting-Ziels gleichzeitig auf das gewünschte Verzeichnis des FTP-Servers zugreifen kann.

**Anmerkung:** Die Werte für **Attribute des globalen FTP-Scripting** sind bereits ausgefüllt und Sie können diese über diese Seite nicht bearbeiten. Verwenden Sie die Seite **Globale Transportattribute**, um diese Werte zu ändern, wie in „Globale Transportwerte konfigurieren” auf Seite 229 beschrieben.

## Benutzerdefinierte Attribute

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

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

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

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

%BCGOPTION% wäre in diesem Fall ein Verzeichnisname.

### Zeitplan

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

1. Geben Sie an, ob Sie intervallbasierte Zeitplanung oder kalenderbasierte Zeitplanung verwenden wollen.
   - Wenn Sie **Intervallbasierte Zeitplanung** auswählen, müssen Sie die Anzahl der Sekunden bis zum Sendeaufruf des Ziels angeben (oder den Standardwert übernehmen).
   - Wenn Sie **Kalenderbasierte Zeitplanung** auswählen, dann wählen Sie den Zeitplanungstyp (**Täglicher Zeitplan**, **Wöchentlicher Zeitplan** oder **Angepasster Zeitplan**) aus.
     – Wenn Sie **Täglicher Zeitplan** auswählen, müssen Sie die Uhrzeit eingeben, zu der der Sendeaufruf an das Ziel erfolgen soll.
     – Wenn Sie **Wöchentlicher Zeitplan** auswählen, wählen Sie mindestens einen Tag in der Woche zusätzlich zur Uhrzeit aus.
     – Wenn Sie **Angepasster Zeitplan** auswählen, wählen Sie die Uhrzeit und schließlich noch **Bereich** oder **Ausgewählte Tage** für die Woche und den Monat aus. Mit **Bereich** geben Sie das Startdatum und das Enddatum an. (Klicken Sie z. B. auf **Mo** und **Fr**, wenn Sie wollen, dass der Server nur an Wochentagen zu einer bestimmten Uhrzeit abgefragt wird.) Mit der Option **Ausgewählte Tage** wählen Sie bestimmte Tage in der Woche und im Monat aus.
2. Wenn Sie den Vorverarbeitungs- oder den Nachverarbeitungsschritt für das Ziel konfigurieren wollen, fahren Sie mit „Handler konfigurieren" fort. Ansonsten klicken Sie auf **Speichern**.

## Handler konfigurieren

Sie können zwei Verarbeitungspunkte für ein Ziel ändern: die Vorverarbeitung und die Nachverarbeitung.

Für den Vorverarbeitungs- oder Nachverarbeitungsschritt werden standardmäßig keine Handler bereitgestellt; daher sind auch standardmäßig keine Handler in der **Verfügbarkeitsliste** aufgelistet. Wenn Sie einen Handler hochgeladen haben, können Sie ihn auswählen und in die **Konfigurationsliste** versetzen.

Um einen benutzerdefinierten Handler auf diese Konfigurationspunkte anzuwenden, müssen Sie zuerst den Handler hochladen. Informationen zu den erforderlichen Schritten zum Hochladen des Handlers finden Sie im Handbuch *Hubkonfiguration*. Führen Sie dann die folgenden Schritte aus:

1. Wählen Sie **Vorverarbeitung** oder **Nachverarbeitung** in der Liste **Konfigurationspunkt-Handler** aus.
2. Wählen Sie den Handler in der **Verfügbarkeitsliste** aus und klicken Sie auf **Hinzufügen**.

3. Wenn Sie die Attribute des Handlers ändern wollen, wählen Sie ihn in der **Konfigurationsliste** aus und klicken Sie auf **Konfigurieren**. Eine Liste mit Attributen, die geändert werden können, wird angezeigt. Nehmen Sie die notwendigen Änderungen vor und klicken Sie auf **Festlegen**.
4. Klicken Sie auf **Speichern**.

Sie können die **Konfigurationsliste** wie folgt noch weiter ändern:

- Entfernen Sie einen Handler, indem Sie den Handler in der **Konfigurationsliste** auswählen, und klicken Sie auf **Entfernen**. Der Handler wird in die **Verfügbarkeitsliste** versetzt.
- Ändern Sie die Reihenfolge, in der der Handler verarbeitet wird, indem Sie den Handler auswählen und auf **Nach oben** oder **Nach unten** klicken.

## Ziel für benutzerdefinierten Transport einrichten

Wenn Sie einen benutzerdefinierten Transport hochladen wollen, führen Sie die folgenden Schritte aus:

1. Klicken Sie auf **Kontenadmin > Profile > Partner**.
2. Klicken Sie auf **Ziele**.
3. Klicken Sie auf **Transporttypen verwalten**.
4. Geben Sie den Namen einer XML-Datei ein, die den Transport definiert oder verwenden Sie **Durchsuchen**, um zur Datei zu navigieren.
5. Verwenden Sie die Standardeinstellung **Ja** für **In Datenbank festschreiben**. Wählen Sie **Nein** aus, wenn Sie diesen Transport testen, bevor Sie ihn in Produktion nehmen.
6. Geben Sie an, ob diese Datei eine Datei mit demselben Namen ersetzen soll, die sich schon in der Datenbank befindet.
7. Klicken Sie auf **Hochladen**.

   **Anmerkung:** Sie können über die Seite **Transporttypen verwalten** auch einen benutzerdefinierten Transporttyp löschen. Sie können keinen Transport löschen, der von WebSphere Partner Gateway bereitgestellt wurde. Darüber hinaus können Sie keinen benutzerdefinierten Transport löschen, nachdem er zum Erstellen eines Ziels verwendet wurde.
8. Klicken Sie auf **Erstellen**.
9. Geben Sie einen Namen ein, um das Ziel zu identifizieren. Dies ist ein erforderliches Feld.
10. Geben Sie optional den Status des Ziels an. **Aktiviert** ist die Standardeinstellung. Ein aktiviertes Ziel steht für das Senden von Dokumenten zur Verfügung. Ein inaktiviertes Ziel kann keine Dokumente senden.
11. Geben Sie optional an, ob das Ziel online oder offline ist. Die Standardeinstellung ist **Online**.
12. Geben Sie optional eine Beschreibung für das Ziel ein.
13. Füllen Sie die Felder aus, die für jeden benutzerdefinierten Transport eindeutig sind, und klicken Sie auf **Speichern**.

## Standardziel angeben

Nachdem Sie Ziele für den internen Partner bzw. den Partner erstellt haben, wählen Sie eines dieser Ziele als Standardziel aus.

1. Klicken Sie auf **Kontenadmin > Profile > Partner**.
2. Geben Sie Suchkriterien ein, und klicken Sie auf **Suchen**. Sie können auch auf **Suchen** klicken, ohne Suchkriterien einzugeben, um eine Liste aller Partner anzuzeigen.
3. Klicken Sie auf das Symbol **Details anzeigen**, um das Profil des Partners anzuzeigen.
4. Klicken Sie auf **Ziele**.
5. Klicken Sie auf **Standardziele anzeigen**.

   Daraufhin wird eine Liste mit den für den Partner definierten Ziele angezeigt.
6. Wählen Sie in der Liste **Produktion** das Ziel aus, das als Standardziel für den aktuellen Partner definiert werden soll. Sie können auch Standardziele für andere Zieltypen (z. B. **Test**) festlegen.
7. Klicken Sie auf **Speichern**.

# Kapitel 12. Verbindungen verwalten

Nachdem Sie die B2B-Funktionalität von Partnern sowie die Interaktionen erstellt haben, erstellen Sie Verbindungen zwischen den internen Partnern und den externen Partnern. Dieses Kapitel behandelt die folgenden Themen:

- „Übersicht über Verbindungen"
- „Partnerverbindungen aktivieren"
- „Attribute angeben oder ändern" auf Seite 253

**Anmerkung:** Verwenden Sie stets die Browserinstanz, mit der Sie sich an Community Console angemeldet haben, wenn Sie Konfigurationsänderungen an WebSphere Partner Gateway vornehmen. Die gleichzeitige Verwendung mehrerer Browserinstanzen kann dazu führen, dass die Konfigurationsänderungen aufgehoben werden.

## Übersicht über Verbindungen

Sie konfigurieren eine Verbindung zwischen Partnern für jeden Dokumenttyp, der ausgetauscht wird. Sie könnten beispielsweise über mehrere Verbindungen vom internen Partner zum selben Partner verfügen, da das Paket, das Protokoll, der Dokumenttyp, die Aktion oder die Zuordnung möglicherweise verschieden sind.

Wenn Sie Verbindungen aktivieren, können Sie Attribute für den Quellen- oder Zielpartner angeben. Jedes Attribut, das Sie auf der Verbindungsebene festgelegt haben, hat Vorrang vor Attributen, die Sie auf der B2B-Funktionalitätsebene für einen bestimmten Partner oder auf der Dokumentdefinitionsebene festgelegt haben.

Sie verfügen bei EDI-, XML- und ROD-Dokumenten über mehrere Verbindungen für jeden Austausch, wenn der Austausch das Versehen mit einem Umschlag oder eine Transformation miteinbezieht. Sie können für diese Dokumenttypen noch weitere Verbindungen definieren, indem Sie von einer Gruppe mit Profilen auswählen, die der Verbindung zugeordnet sind. Weitere Details finden Sie in „Verbindungsprofile" auf Seite 202.

## Mehrere interne Partner konfigurieren

In WebSphere Partner Gateway besteht keine Beschränkung für die Anzahl der internen Partner. Um die Abwärtskompatibilität für Web-Service-Dokumente und binäre Dokumente bereitzustellen, die über die FTPScript-Unterstützungsfunktionen weitergeleitet werden, muss ein standardmäßiger interner Partner konfiguriert werden. Weitere Informationen zum Konfigurieren von Web-Service-Dokumenten und binären Dokumenten für mehrere interne Partner finden Sie im Kapitel "Dokumenttypen konfigurieren".

## Partnerverbindungen aktivieren

Partnerverbindungen enthalten die Informationen, die für den ordnungsgemäßen Austausch jedes Dokumenttyps nötig sind. Ein Dokument kann nicht weitergeleitet werden, es sei denn, es ist eine Verbindung zwischen dem internen Partner und einem seiner externen Partner vorhanden.

Das System erstellt automatisch Verbindungen zwischen den internen Partnen und den externen Partnern auf der Basis ihrer B2B-Funktionalität und ihrer Interaktionen.

Suchen Sie nach diesen Verbindungen und aktivieren Sie diese dann.

Wenn Sie eine Quelle und ein Ziel auswählen, stellen Sie sicher, dass die Quelle eindeutig ist.

Verwenden Sie die folgende Prozedur, um eine grundlegende Suche nach Verbindungen auszuführen und dann die Verbindungen zu aktivieren.

1. Klicken Sie auf **Kontenadmin > Verbindungen**. Die Seite **Verbindungen verwalten** wird angezeigt.
2. Wählen Sie unter **Quelle** eine Quelle aus. Wenn Sie beispielsweise einen Austausch konfigurieren, der vom internen Partner stammt, wählen Sie den internen Partner aus.
3. Wählen Sie unter **Ziel** ein Ziel aus. Wenn Sie beispielsweise einen Austausch konfigurieren, der von einem Partner empfangen wird, wählen Sie diesen Partner aus.

   **Anmerkung:** Wenn Sie eine neue Verbindung erstellen, müssen die Quelle und das Ziel eindeutig sein.
4. Klicken Sie auf **Suchen**, um die Verbindungen zu suchen, die mit Ihren Kriterien übereinstimmen.

   **Anmerkung:** Sie können auch die Seite **Erweiterte Suche** verwenden, wenn Sie detailliertere Suchkriterien eingeben wollen.
5. Klicken Sie auf **Aktivieren**, um eine Verbindung zu aktivieren. Die Seite **Verbindungen verwalten** wird erneut angezeigt, diesmal ist die Verbindung grün hervorgehoben. Diese Seite zeigt das Paket, das Protokoll und den Dokumenttyp für die Quelle und das Ziel an. Sie stellt auch Schaltflächen bereit, auf die Sie klicken können, um den Status und die Parameter der Partnerverbindung anzuzeigen und zu ändern.
6. Informationen dazu, wie Sie Attribute für die Quelle oder das Ziel angeben, oder wie Sie ein Verbindungsprofil auswählen, finden Sie in „Attribute angeben oder ändern” auf Seite 253.

Aktivieren Sie bei einer Doppelaktions-PIP die Verbindung in beide Richtungen, um die zweite Aktion des PIP zu unterstützen. Um dies durchzuführen, definieren Sie die Quelle und das Ziel der zweiten Aktion als das Gegenüber der Quelle und des Ziels von der ersten Aktion.

Stellen Sie bei EDI-, XML- oder ROD-Dokumenten, für die Sie mehr als eine Interaktion definiert haben, sicher, dass Sie alle Verbindungen aktivieren, die den Interaktionen zugeordnet sind.

## Attribute angeben oder ändern

Wenn Sie die Verbindung aktivieren, können Sie Attribute festlegen oder zuvor definierte Attribute ändern. Gehen Sie wie folgt vor, um die Attribute für diese Verbindung anzugeben oder zu ändern:

1. Klicken Sie auf **Attribute**, um die Attributwerte anzuzeigen oder zu ändern.

   Angenommen, der interne Partner sendet ein Dokument im Paket **None** an einen Partner. Der Partner empfängt das Dokument dann in einem AS-Paket. Es ist möglich, dass dem internen Partner mehr als eine Geschäfts-ID zugeordnet ist. Gehen Sie wie folgt vor, um WebSphere Partner Gateway mitzuteilen, welche ID verwendet werden soll:

   a. Klicken Sie auf **Attribute** auf der Seite **Quelle** der Verbindung.
   b. Wenn die Seite **Verbindungsattribute** angezeigt wird, erweitern Sie den Ordner **None**.
   c. Wählen Sie in der Liste **Aktualisieren** die AS-ID aus, die Sie dem Partner senden wollen.
   d. Klicken Sie auf **Speichern**.

   **Anmerkung:** Wenn Sie vorher eine AS-ID angegeben haben (z. B. auf der Seite **B2B-Funktionalität**), wird der hier eingegebene Wert den früheren Wert überschreiben.

   Ein weiteres Beispiel für das Konfigurieren von Attributen ist, einen Wert für die MDN-Adresse einzugeben, wenn Sie von einem Partner Dokumente in AS-Paketen empfangen. Die Adresse gibt an, wohin die MDN zugestellt wird.
2. Klicken Sie auf **Aktionen**, wenn Sie eine Aktion oder eine Transformationszuordnung, die dieser Verbindung zugeordnet ist, anzeigen oder ändern wollen. Jeder Wert, den Sie hier ändern, überschreibt alle anderen Werte, die Sie für die Aktion oder Zuordnung festgelegt haben.
3. Klicken Sie auf **Ziele**, wenn Sie das Quellen- oder das Empfängerziel anzeigen oder ändern wollen.
4. Wenn die Schaltfläche **Verbindungsprofil hinzufügen** und die Liste **Aktive Profile** angezeigt werden, können Sie diese Verbindung einem bestimmten Profil zuordnen, das Sie vorher definiert haben.

Die Attribute, die Sie auf der Verbindungsebene festgelegt haben, haben Vorrang vor allen Attributen, die Sie auf der Protokoll- oder auf der Dokumenttypebene festgelegt haben. Ist das Attribut den Typen "Paket", "Protokoll" und "Dokument" zugeordnet, überschreibt der für den Typ "Dokument" festgelegte Wert die Werte für die Typen "Paket" und "Protokoll".

# Kapitel 13. Sicherheit für Dokumentenaustauschvorgänge aktivieren

Sie können mit WebSphere Partner Gateway mehrere Zertifikatstypen für sichere Eingangs- und Ausgangstransaktionen installieren und verwenden. Dieses Kapitel behandelt die folgenden Themen:



Zertifikate und Sicherheitsprotokolle verbessern die Sicherheit in WebSphere Partner Gateway wie folgt:

- Es wird überprüft, welcher Benutzer das Dokument sendet.
- Es wird überprüft, ob das Dokument während der Übertragung geändert wurde.
- Es wird verhindert, dass andere Benutzer den Dokumentinhalt anzeigen können.
- Es wird überprüft, ob der Absender des Dokuments zum Senden des Dokuments berechtigt ist.

**Anmerkung:** Verwenden Sie stets die Browserinstanz, mit der Sie sich an Community Console angemeldet haben, wenn Sie Konfigurationsänderungen an WebSphere Partner Gateway vornehmen. Die gleichzeitige Verwendung mehrerer Browserinstanzen kann dazu führen, dass die Konfigurationsänderungen aufgehoben werden.

# Übersicht über die Sicherheit

## In WebSphere Partner Gateway verwendete Sicherheitsmechanismen und Protokolle

Je nach Geschäftsprotokoll verwendet WebSphere Partner Gateway Zertifikate, um die folgenden Mechanismen für einen sicheren Dokumentenaustausch zu aktivieren:

**Verschlüsselung und Entschlüsselung**

Verschlüsselung bietet die Möglichkeit, Daten so zu ändern, dass sie bis zur Entschlüsselung unlesbar sind. WebSphere Partner Gateway verwendet ein verschlüsseltes System, die so genannte Verschlüsselung mit öffentlichem Schlüssel, um die Kommunikation zwischen den Partnern und dem Hub zu schützen. Verschiedene Geschäftsprotokolle wie AS2 oder RosettaNet stellen Anforderungen an die Verschlüsselung. SSL verwendet ebenfalls Verschlüsselung. Sofern nicht anders angegeben, bezieht sich der Begriff *Verschlüsselung* in diesem Kapitel auf Geschäftsprotokolle.

Bei der Entschlüsselung werden verschlüsselte Daten entschlüsselt, um sie lesbar zu machen. Die Entschlüsselung wird für eingehende Dokumente durchgeführt.

WebSphere Partner Gateway kann Daten versenden, die mit OpenPGP verschlüsselt wurden. Das empfangene Datenpaket wird mithilfe des privaten Schlüssels entschlüsselt. Wenn erwartet wird, dass das gesendete Dokument immer verschlüsselt ist, sollten Sie das Attribut **Verschlüsselung erforderlich** auf der Zielseite der Verbindung auf `Ja` setzen. Wenn erwartet wird, dass das verschlüsselte Dokument ein Paket mit Code zur Änderungserkennung (Modification Detection Code) enthält, sollten Sie das Attribut **Änderungserkennung** auf der Zielseite der Verbindung auf `Wahr` setzen. Falls Sie verschlüsselte Daten mit Integritätsschutz empfangen, wird die Integrität der Daten nach dem Entschlüsseln mithilfe des Pakets mit Code zur Änderungserkennung verifiziert. Das zuletzt entschlüsselte Paket in den Daten muss ein Paket mit Code zur Änderungserkennung sein. In einem solchen Szenario bestehen die verschlüsselten Daten aus einem symmetrisch verschlüsselten, integritätsgeschützten Datenpaket, sodass die Nachrichtenintegrität verifiziert werden kann. Legen Sie die Attribute für die Verschlüsselung auf der Zielseite der Verbindung fest. Für ein OpenPGP-Paket wird RFC 4880 unterstützt. Wenn Sie verschlüsselte Daten mit Integritätsschutz versenden wollen, müssen Sie das Attribut **Änderungserkennung** auf `Wahr` setzen und die Vorgaben für den symmetrischen Algorithmus auswählen. Diese Funktionalität wird ausschließlich in RFC 4880 definiert.

**Komprimierung**

Beim Senden eines Dokuments müssen die Daten im Schritt für das Packen komprimiert werden. Die Komprimierung folgt dabei den den Vorgaben für den Komprimierungsalgorithmus, die in der Verbindung auf dem Ziel festgelegt werden. Wenn Sie eine komprimierte Nachricht empfangen, wird sie dekomprimiert. Wenn erwartet wird, dass das gesendete Dokument immer komprimiert ist, sollten Sie das Attribut **Komprimierung erforderlich** auf der Zielseite der Verbindung auf `Ja` setzen. Für ein OpenPGP-Paket wird RFC 4880 unterstützt.

**Verschlüsselung und Komprimierung**

Wenn ein Dokument verschlüsselt und komprimiert werden soll, müssen Sie alle Attribute von Routing-Objekten für die Verschlüsselung und Kom-

primierung auf der Zielseite der Verbindung festlegen. Die Verschlüsselung folgt RFC 4880. Wenn Sie eine verschlüsselte und komprimierte Nachricht empfangen, wird zunächst die Entschlüsselung ausgeführt. Durch die Entschlüsselung wird ein komprimiertes Datenpaket erzeugt, für das die Dekomprimierung ausgeführt wird. Wenn Sie verschlüsselte Daten mit Integritätsschutz versenden, müssen Sie das Attribut **Änderungserkennung** auf der Zielseite der Verbindung festlegen.

**Digitale Signatur und Prüfung der digitalen Signatur**
Digitale Signatur ist der Mechanismus, der den Absender des Dokuments feststellt und überprüft, ob das Dokument während der Übertragung geändert wurde. Außerdem trägt dieser Mechanismus dazu bei, die Unbestreitbarkeit sicherzustellen. Unbestreitbarkeit bedeutet, dass ein Partner nicht bestreiten kann, eine Nachricht verfasst und gesendet zu haben. Es wird ferner sichergestellt, dass der Partner den Empfang einer Nachricht nicht bestreiten kann.

**Anmerkung:** Die Unbestreitbarkeitsinformationen werden aus den Parametern der Partnerverbindung abgerufen. Die Parameter der Partnerverbindung werden nach einer erfolgreichen Suche der Partnerverbindung ermittelt. Die Unbestreitbarkeit ist standardmäßig auf **Ja** gesetzt. Dies bedeutet, dass das Dokument im Unbestreitbarkeitsspeicher abgelegt wird, wenn die Informationen aus irgendwelchen Gründen nicht aus der Partnerverbindung abgerufen werden können.

**SSL** 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 Vertrauenswürdigkeit der jeweils anderen zu prüfen, und indem die Daten zur Sicherstellung der Vertraulichkeit verschlüsselt werden. Die Verschlüsselung ist unabhängig vom Datentyp. SSL wird über Transporte wie HTTP und FTP verwendet.

**Basisauthentifizierung**
Wird eine eingehende Nachricht über HTTP oder HTTPS gesendet, kann der Empfänger den sendenden Partner mithilfe des Berechtigungsnachweises für die Basisauthentifizierung identifizieren. Die Benutzer-ID und das Kennwort werden im HTTP-Header übergeben. Da das Kennwort ebenfalls gesendet wird, sollte die Basisauthentifizierung mit SSL/TLS verwendet werden, damit sichergestellt ist, dass die Header verschlüsselt werden. Die Authentifizierung wird über die Angabe "Geschäfts-ID/benutzername:kennwort" oder "Benutzername:Kennwort" in Base64-codiertem Format bereitgestellt. Der Wert im HTTP-Header wird nur verwendet, wenn die Option **Basisauthentifizierung aktivieren** auf "true" festgelegt ist. Wählen Sie auf der Seite **Empfängerdetails** der Konsole den Eintrag **Basisauthentifizierung** aus, um diesen Wert auf "true" zu setzen.

Schlägt die Authentifizierung fehl, wird die Antwort "Authentifizierung fehlgeschlagen" an den Absender zurückgegeben. Andernfalls wird das Dokument gesendet, damit es weiter verarbeitet werden kann. Wird die SSL-Clientauthentifizierung verwendet, werden die Geschäfts-IDs des sendenden Partners identifiziert. Wenn das Dokument empfangen wird, prüft der Empfänger, ob das Zertifikat einem Partner zugeordnet ist. Wird keine Übereinstimmung festgestellt, schlägt das Dokument fehl. Aus Gründen der Abwärtskompatibilität sollten Sie beim Senden einer SOAP-Nachricht mit Basisauthentifizierung die Option **Basisauthentifizierung aktivieren** beim Empfänger auf "Nein" festlegen. Sofern die Authentifizierung des Do-

kuments nicht beim Empfänger fehlschlägt, kann das Dokument in der Dokumentanzeige angezeigt werden. Die Basisauthentifizierung wird für die folgenden Dokumente unterstützt:

- EDI/XML-Dokumente
- AS2-Dokumente mit binären/EDI-/XML-Nutzdaten
- Web-Service-Anforderungen
- RosettaNet-Nachrichten
- ebMS-Nachrichten

Die Sicherheit kann entweder über den Transport oder das Geschäftsprotokoll sichergestellt werden. Die Authentifizierung von Benutzern beim Empfänger unterstützt binäre Dokumente von externen Partnern über HTTP. Der sendende Partner wird über die Berechtigungsnachweise der Basisauthentifizierung oder über die Berechtigungsnachweise der SSL-Clientauthentifizierung identifiziert.

## Zertifikate und Sicherheitsmechanismen

Zertifikate bilden die Basis für alle drei Sicherheitskonzepte: Verschlüsselung, digitale Signaturen und SSL. Durch Zertifikate werden diese Konzepte in WebSphere Partner Gateway aktiviert. Mithilfe von Zertifikaten wird die Sicherheit von Dokumenten während der Übertragung gewährleistet.

Jeder Partner verfügt zum Senden oder Empfangen von Dokumenten mit WebSphere Partner Gateway über mindestens ein Zertifikat. WebSphere Partner Gateway (vertreten durch den Hubbetreiber) verfügt ebenfalls über mindestens ein Zertifikat zum Senden und Empfangen von Dokumenten mit dem Partner.

**Anmerkung:** Die für einen Partner oder den Hubbetreiber verwendeten Zertifikate gelten für alle Dokumente. Zertifikat variieren nicht nach Dokumenttyp.

### Zertifikate und Verschlüsselung

Ein Zertifikat enthält den öffentlichen Teil des Schlüssel eines mathematisch miteinander in Beziehung stehenden Paars aus öffentlichem und privatem Schlüssel. Der öffentliche Schlüssel “sperrt” bzw. verschlüsselt ein Dokument vor dessen Versand so, dass es nach dem Versand nur vom privaten Schlüssel “entsperrt” bzw. entschlüsselt werden kann. Ein öffentlicher Schlüssel wird als öffentlicher Schlüssel bezeichnet, weil Sie ihn mit den Partnern, die Ihnen verschlüsselte Dokumente senden, gemeinsam nutzen. Der private Schlüssel hingegen wird nur von Ihnen zur Entschlüsselung der Dokumente verwendet. Ein Zertifikat enthält den öffentlichen Schlüssel und bindet diesen an den Namen der zertifizierten Person oder Personengruppe (Subject Name). Dieser Name ist der Name der End-Entität, die Eigner des Zertifikats ist.

Zertifikate werden vom Partner generiert und entweder vom Partner selbst signiert oder von der Zertifizierungsstelle (CA - Certificate Authority) ausgegeben. Ein von einer Zertifizierungsstelle ausgegebenes Zertifikat ist ein Zertifikat, das der Partner unter Verwendung einer Zertifikatsunterzeichungsanforderung (CSR - Certificate Signing Request) anfordert und von einer Zertifizierungsstelle erhält. Ein von einer Zertifizierungsstelle ausgegebenes Zertifikat wird von der Zertifizierungsstelle und nicht vom Partner signiert. Jeder Partner verfügt über mindestens ein Zertifikat, das beim Senden oder Empfangen von Dokumenten verwendet wird.

Die Verschlüsselung von Geschäftsdokumenten kommt nur dann zur Anwendung, wenn der Geschäftsstandard Verschlüsselung unterstützt. Nicht alle Standards unterstützen Verschlüsselung. Die Art und Weise, wie die Verschlüsselung zur An-

wendung kommt, ist bei allen Standards, die Verschlüsselung unterstützen, unterschiedlich. WebSphere Partner Gateway versteht die Unterschiede zwischen den Standards und weiß, wie die Verschlüsselung angewendet werden muss.

Wenn WebSphere Partner Gateway ein Dokument an einen Partner sendet, wird zur Verschlüsselung des Dokuments das Zertifikat dieses Partners verwendet. Auf diese Weise kann nur der Partner, der das Dokument mit einem eigenen privaten Schlüssel entschlüsselt, den Inhalt lesen. Das verwendete Zertifikat ist das Verschlüsselungszertifikat, das für diesen Partner in WebSphere Partner Gateway geladen wurde.

Wenn ein Partner ein Dokument an WebSphere Partner Gateway sendet, verwendet dieser Partner zur Verschlüsselung des Dokuments das Hubbetreiberzertifikat. Auf diese Weise kann nur der Hubbetreiber, der über den privaten Schlüssel verfügt, das Dokument entschlüsseln und seinen Inhalt lesen. Es wird der private Schlüssel verwendet, der für den Hubbetreiber unter der Option **PKCS12 laden** geladen wurde. Beachten Sie, dass der Administrator das Hubbetreiberzertifikat an den Partner übergeben muss.

**Hinweise:**

1. WebSphere Partner Gateway unterstützt die RC2- und TripleDES-Algorithmen. Der RC5-Algorithmus wird aber nicht unterstützt. Wenn Sie den RC5-Algorithmus in früheren Versionen verwendet haben, wechseln Sie zu einem der unterstützten Algorithmen.
2. WebSphere Partner Gateway unterstützt auch die folgenden Algorithmen:
   - AES, TripleDES und RC2: Für gesendete und empfangene ebMS-Dokumente.
   - TripleDES und RC2: Für RNIF-Dokumente.
   - DES: Für ebMS; es wird jedoch empfohlen, einen stärkeren Algorithmus, wie beispielsweise RC2, TripleDES oder AES zu verwenden.

   Sie können diese Algorithmen in der Anzeige Systemverwaltung > DocMgr-Verwaltung > Sicherheit von WebSphere Partner Gateway Console oder mit der SecurityService-API in Benutzerexits festlegen. Informationen zu den Sicherheitsmerkmalen finden Sie im Handbuch *WebSphere Partner Gateway Administrator Guide*. Informationen zu SecurityService finden Sie im *WebSphere Partner Gateway Programmer Guide*.

## Grundlegende Prozedur

Für den Empfang eines verschlüsselten Dokuments müssen Sie die folgenden grundlegenden Schritte ausführen. Informationen zur vollständigen Prozedur finden Sie in „Zertifikate zum Aktivieren der Verschlüsselung und der Entschlüsselung verwenden" auf Seite 268.

1. Beschaffen Sie sich ein öffentliches/privates Schlüsselpaar, das Sie entweder selbst generieren oder bei einer Zertifizierungsstelle anfordern.
2. Laden Sie den privaten Schlüssel auf den WebSphere Partner Gateway-Server unter dem Hubbetreiber (Schlüssel kann von allen internen Partnern verwendet werden) oder dem internen Partner (Schlüssel kann nur von diesem internen Partner verwendet werden) hoch, damit der Server eingehende Dokumente entschlüsseln kann.
3. Stellen Sie Ihrem Handelspartner das öffentliche Zertifikat zur Verfügung, damit dieser Partner das Zertifikat auf seinen Server hochladen und Dokumente verschlüsseln kann, bevor diese an Sie gesendet werden.

Nach Abschluss dieser Prozedur kann der Partner unter Verwendung Ihres Zertifikats Dokumente an Sie senden, die so verschlüsselt sind, dass sie nur von Ihnen entschlüsselt werden können. Zum Senden von Dokumenten an Partner müssen Sie diese Prozedur umkehren, indem Sie deren Zertifikate hochladen und mithilfe dieser Zertifikate die Dokumente verschlüsseln, die Sie an die Partner senden.

## Zertifikate und digitale Signaturen

WebSphere Partner Gateway unterstützt digitale Signaturen, wie dies für die B2B-Protokolle erforderlich ist. Zertifikate werden zum Signieren auf ähnliche Weise verwendet wie Verschlüsselungszertifikate; der Vorgang ist jedoch umgekehrt. Sie müssen das Zertifikat erstellen, um ein Dokument mit einer digitalen Signatur an die Partner zu senden, nicht umgekehrt.

Digitale Signaturen werden verwendet, um den tatsächlichen Absender des Dokuments zu überprüfen und sicherzustellen, dass das Dokument während der Übertragung nicht geändert wurde. Sie können nur dann angewendet werden, wenn der Geschäftsstandard digitale Signaturen unterstützt. Nicht alle Standards unterstützen digitale Signaturen. Die Art und Weise, wie digitalen Signaturen zur Anwendung kommen, ist bei allen Standards, die digitale Signaturen unterstützen, unterschiedlich. WebSphere Partner Gateway versteht die Unterschiede zwischen den Standards und weiß, wie die digitalen Signaturen angewendet werden müssen.

Wenn WebSphere Partner Gateway ein Dokument an einen Partner sendet, wird zum Signieren des Dokuments der private Schlüssel des Hubbetreibers verwendet, der unter der Option **PKCS12 laden** geladen wurde. Der Partner prüft mit dem Hubbetreiberzertifikat, ob WebSphere Partner Gateway das Dokument signiert hat. Wurde der private Schlüssel des Hubbetreibers nicht zum Signieren des Dokuments verwendet, können die Signaturen mithilfe des Hubbetreiberzertifikats, das dem Partner vorliegt, nicht überprüft werden. Beachten Sie, dass der Administrator das Hubbetreiberzertifikat an den Partner übergeben muss.

Wenn ein Partner ein Dokument an WebSphere Partner Gateway sendet, verwendet WebSphere Partner Gateway das Zertifikat für digitale Signatur des Partners, um zu prüfen, ob der Partner das Dokument signiert hat. Wurde das Dokument nicht mit dem privaten Schlüssel des Partners signiert, kann die Signatur mithilfe des Zertifikats, das WebSphere Partner Gateway für diesen Partner vorliegt, nicht überprüft werden.

### Grundlegende Prozedur:

Zum Senden eines digital signierten Dokuments müssen Sie die folgenden grundlegenden Schritte ausführen. Informationen zur vollständigen Prozedur finden Sie im Abschnitt „Zertifikate zum Aktivieren von digitalen Signaturen verwenden" auf Seite 273.

1. Beschaffen Sie sich ein öffentliches/privates Schlüsselpaar, das Sie entweder selbst generieren oder bei einer Zertifizierungsstelle anfordern.
2. Laden Sie den privaten Schlüssel auf den WebSphere Partner Gateway-Server unter dem Hubbetreiber hoch, damit der Server die Dokumente vor dem Versand signieren kann.
3. Stellen Sie Ihrem Handelspartner das öffentliche Zertifikat zur Verfügung, damit dieser Partner das Zertifikat auf seinen Server hochladen und die Dokumente überprüfen kann, die er von Ihnen empfängt.

Nach Beendigung dieser Prozedur können Sie mit Ihrem privaten Schlüssel digital signierte Dokumente senden, damit der Partner weiß, dass diese Dokumente von

von Ihnen stammen können. Für den Empfang gleichermaßen signierter Dokumente von Partnern müssen Sie diese Prozedur umkehren, indem Sie deren Zertifikate hochladen und mithilfe dieser Zertifikate ihren Ursprung ermitteln.

## Zertifikate und SSL/TLS

Beim Senden von Dokumenten können Sie zur Verschlüsselung von Dokumenten SSL verwenden, sodass nur der Empfänger die Dokumente lesen kann. Auf diese Weise wird die Vertraulichkeit der Daten gewährleistet.

Bei SSL spielen die Begriffe *Client* und *Server* eine Rolle. Der Client stellt eine Verbindung zu einem Server her, um ein Dokument an diesen Server zu senden. Wenn der Client die Verbindung mit dem Server herstellt, sendet der Server dem Client ein Zertifikat, das bei der Verschlüsselung des Dokuments verwendet wird. Dieses Serverzertifikat ist auch an der Serverauthentifizierung beteiligt, da der Server das Zertifikat verwendet, um sich bei den Clients zu authentifizieren. In manchen Fällen fordert der Server auch ein Zertifikat vom Client an. Dieser Vorgang wird als Clientauthentifizierung bezeichnet. Mithilfe der Clientauthentifizierung stellt der Server fest, ob der Client dem Server bekannt ist.

Wenn WebSphere Partner Gateway ein Dokument an einen Partner sendet, ist WebSphere Partner Gateway der Client, und der Partner ist der Server (das Dokument wird also an den Server des Partners gesendet).

**Anmerkung:** Der Server des Partners ist das Ziel, das in WebSphere Partner Gateway für diesen Partner definiert wurde.

Wenn ein Partner ein Dokument an WebSphere Partner Gateway sendet, dann ist der Partner der Client und WebSphere Partner Gateway der Server.

**Anmerkung:** Dies ist der Empfänger, der in WebSphere Partner Gateway definiert wurde.

Wenn der Partner ein Dokument mit SSL an WebSphere Partner Gateway sendet, ist die tatsächliche Identität des Partners nicht bekannt. Auch bei Verwendung der Clientauthentifizierung ist die Identität des Partners nicht bekannt. Bekannt ist jedoch, dass dieser Partner so vertrauenswürdig ist, dass er Dokumente an WebSphere Partner Gateway senden kann. WebSphere Partner Gateway verfügt darüber hinaus über eine zusätzliche Funktion, um den Partner anhand des vom Partner bereitgestellten Zertifikats für die Clientauthentifizierung zu identifizieren.

Wenn WebSphere Partner Gateway ein Dokument an einen Partner sendet, wird zur Verschlüsselung des Dokuments das Zertifikat dieses Partners verwendet. Da das Dokument mit dem eigenen privaten Schlüssel des Partners entschlüsselt wird, kann nur dieser Partner den Inhalt lesen. Im Rahmen von SSL wird das zur Verschlüsselung verwendete Zertifikat während der Laufzeit vom Partner dynamisch an WebSphere Partner Gateway gesendet. WebSphere Partner Gateway überprüft die Gültigkeit des Zertifikats durch Erstellung und Validierung des Zertifizierungspfads. Dazu werden die Zertifikate verwendet, die als Root-/Intermediate-Zertifikate unter dem Hubbetreiber geladen wurden.

Ein zweiter optionaler Bestandteil von SSL ist die Clientauthentifizierung zur Überprüfung des Absenders, wobei der Partner ein Zertifikat bei WebSphere Partner Gateway anfordert. WebSphere Partner Gateway sendet das Zertifikat für die Clientauthentifizierung, das unter dem Hubbetreiber geladen wurde. Beachten Sie, dass das Hubbetreiberzertifikat für die Clientauthentifizierung vom Administrator an den Partner übergeben werden muss. Wenn das Clientauthentifizierungszerti-

fikat selbst signiert ist, muss das selbst signierte Zertifikat an den Partner übergeben werden. Wenn das Clientauthentifizierungszertifikat von einer Zertifizierungsstelle (CA) ausgegeben wurde, muss das CA-Zertifikat gegebenenfalls an den Partner übergeben werden.

Wenn ein *Partner* ein Dokument mit SSL an WebSphere Partner Gateway sendet, wird zur Verschlüsselung des Dokuments das WebSphere Partner Gateway-Zertifikat verwendet. Der Inhalt kann nur von WebSphere Partner Gateway gelesen werden, da das Dokument mit dem eigenen privaten Schlüssel des Programms entschlüsselt wird. Im Rahmen von SSL wird das zur Verschlüsselung verwendete Zertifikat während der Laufzeit von WebSphere Partner Gateway dynamisch an den Partner gesendet. Der Partner überprüft die Gültigkeit des Zertifikats durch einen Vergleich mit den Zertifikaten, die dem Partner zuvor vom Administrator übergeben wurden. Ein zweiter optionaler Bestandteil von SSL ist die Clientauthentifizierung zur Überprüfung des Absenders, wobei WebSphere Partner Gateway ein Zertifikat beim Partner anfordert. Der Partner sendet das Zertifikat für die Clientauthentifizierung an WebSphere Partner Gateway; dieses Zertifikat wird anhand des Zertifikats überprüft, das dem Administrator zuvor vom Partner übergeben wurde.

**Anmerkung:** Für den Empfang von Dokumenten von Partnern mit SSL verwendet WebSphere Partner Gateway die zugrunde liegenden WebSphere Application Server-Funktionen. Deshalb werden die während der Laufzeit verwendeten Zertifikate nicht mithilfe von WebSphere Partner Gateway Console hochgeladen, sondern in den Keystore und in den Truststore von WebSphere Application Server geladen.

Die Clientauthentifizierung stellt eine zusätzliche Möglichkeit zur Identifizierung des Partners dar, die WebSphere Partner Gateway außerhalb des SSL-Transport durchführt. Das vom Partner bereitgestellte Zertifikat für die Clientauthentifizierung wird an WebSphere Partner Gateway übergeben. WebSphere Partner Gateway vergleicht dieses Zertifikat mit dem Zertifikat, das für den SSL-Client dieses Partners geladen wurde, damit der Partner identifiziert werden kann.

Eine HTTP-basierte SSL-Verbindung wird immer vom Client initiiert, der eine URL mit https:// am Anfang, an Stelle von http:// am Anfang, verwendet. Eine SSL-Verbindung beginnt mit einem Handshake. Während dieses Stadiums tauschen die Anwendungen Zertifikate aus, verständigen sich über die zu verwendenden Verschlüsselungsalgorithmen und generieren Verschlüsselungsschlüssel, die für den verbleibenden Teil der Sitzung verwendet werden.

### Grundlegende Vorgehensweisen

Zum *Senden* eines Dokuments mit SSL müssen Sie die folgenden grundlegenden Schritte ausführen. Informationen zur vollständigen Prozedur finden Sie im Abschnitt „Zertifikate zum Aktivieren von SSL verwenden" auf Seite 278.

1. Beschaffen Sie sich ein Zertifikat von Ihrem Partner und laden Sie dieses Zertifikat in den Truststore von WebSphere Application Server.
2. Beschaffen Sie sich für die Clientauthentifizierung beim Partner ein öffentliches/privates Schlüsselpaar, das Sie entweder selbst generieren oder bei einer Zertifizierungsstelle anfordern.
3. Laden Sie den privaten Schlüssel und das öffentliche Zertifikat in den Keystore von WebSphere Application Server hoch.

4. Stellen Sie Ihrem Handelspartner das öffentliche Zertifikat zur Verfügung, damit er das Zertifikat auf seinen Server hochladen und das Zertifikat für die Clientauthentifizierung überprüfen kann, das er während der SSL-Laufzeitkommunikation von Ihnen erhält.

Für den *Empfang* eines Dokuments mit SSL müssen Sie die folgenden grundlegenden Schritte ausführen. Informationen zur vollständigen Prozedur finden Sie im Abschnitt „Zertifikate zum Aktivieren von SSL verwenden" auf Seite 278.

1. Beschaffen Sie sich ein öffentliches/privates Schlüsselpaar, das Sie entweder selbst generieren oder bei einer Zertifizierungsstelle anfordern.
2. Laden Sie den privaten Schlüssel und das öffentliche Zertifikat in den Keystore von WebSphere Application Server hoch.
3. Stellen Sie Ihrem Handelspartner das öffentliche Zertifikat zur Verfügung, damit er das Zertifikat auf seinen Server hochladen und das Serverzertifikat überprüfen kann, das er während der SSL-Laufzeitkommunikation von Ihnen erhält.
4. Beschaffen Sie sich für die Clientauthentifizierung ein Zertifikat von Ihrem Partner und laden Sie es in den Truststore von WebSphere Application Server. Dieses Zertifikat wird während der SSL-Laufzeitkommunikation verwendet.
5. Laden Sie das Zertifikat des Partners unter der Clientauthentifizierung des Partners hoch, um den Partner über das Zertifikat für die Clientauthentifizierung in WebSphere Partner Gateway Console zu identifizieren.

## Zertifikate in Keystores und Truststores speichern

WebSphere Partner Gateway bietet zwei Möglichkeiten zum Speichern von Zertifikaten. Für Dokumente, die von einem Partner mit SSL an WebSphere Partner Gateway gesendet werden, werden Zertifikate im Keystore und im Truststore von WebSphere Application Server gespeichert. Truststores werden zur Speicherung von vertrauenswürdigen Zertifikaten verwendet, mit deren Hilfe wiederum überprüft wird, ob ein von einem Partner empfangenes Zertifikat gültig ist. Keystores werden zur Speicherung des öffentlichen und privaten Schlüssels des WebSphere Partner Gateway-Hubbetreibers verwendet. Zertifikate für die Sicherheit von Geschäftsdokumenten werden über WebSphere Partner Gateway Console geladen und gespeichert. In diesem Abschnitt werden der Keystore und der Truststore beschrieben, die mit WebSphere Application Server verwendet werden. Wenn Sie WebSphere Partner Gateway installieren, werden ein Keystore und ein Truststore für die WebSphere Application Server-Instanz erstellt, auf dem der Empfänger und die Konsole installiert sind.

- 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 Partner enthält. Der öffentliche Schlüssel wird als ein Unterzeichnerzertifikat gespeichert. Bei kommerziellen Zertifizierungsstellen wird das CA-Rootzertifikat hinzugefügt. Da die Truststore-Datei Ihren privaten Schlüssel nicht enthält, kann sie allgemein zugänglicher sein als die Keystore-Datei.
- Zur Verwaltung von Keystore und Truststore wird iKeyman verwendet. Dieses Dienstprogramm wird in den Abschnitten beschrieben, in denen seine Verwendung erforderlich ist.

  **Anmerkung:** Die Administrationskonsole von WebSphere Application Server kann ferner zur Verwaltung von Zertifikaten, Keystores und Truststores für Empfänger und Konsole verwendet werden. Detaillierte Informationen zur Verwaltung von Zertifikaten und Keystores mit der Administrationskonsole von

WebSphere Application Server finden Sie in der Dokumentation *Anwendungen und ihre Umgebung sichern* im Information Center für WebSphere Application Server.

Der Keystore und der Truststore werden standardmäßig im Verzeichnis `<Produktverz>/common/security/keystore` erstellt. Sie heißen wie folgt:

- bcgSecurity.jks
- bcgSecurityTrust.jks

### Standardkennwort ändern

Das Standardkennwort für den Zugriff auf die Speicher ist WebAS. WebSphere Application Server wird für die Verwendung dieser Speicher konfiguriert. Sie können das Kennwort mit dem Dienstprogramm iKeyman ändern. Alternativ hierzu können Sie auch den Befehl keytool verwenden, um das Kennwort für die Keystore-Datei zu ändern. Unter UNIX lautet der Befehl wie folgt:

```
/<WAS-Installationsverz>/java/bin/keytool
 -storepasswd -new $NEW_PASSWORD$ -keystore $KEYSTORE_LOCATION$
  -storepass $CURRENT_PASSWORD$ -storetype JKS
```

Dieser Befehl kann auch unter Windows ausgeführt werden. Sie müssen stattdessen allerdings Backslashes und Laufwerknamen verwenden.

Wenn die Keystore-Kennwörter geändert werden, muss jede WebSphere Application Server-Instanzkonfiguration ebenfalls geändert werden. Dies kann mithilfe des Scripts `bcgChgPassword.jacl` geschehen. Navigieren Sie für die Konsolinstanz zum folgenden Verzeichnis:

```
/<Produktverz>/bin
```

Setzen Sie den folgenden Befehl ab:

```
./bcgwsadmin.sh -f /<Produktverz>/scripts/
bcgChgPassword.jacl -conntype NONE
```

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

**Anmerkung:** Verwenden Sie für Windows-Installationen `bcgwsadmin.bat` an Stelle von `./bcgwsadmin.sh`.

Sie werden aufgefordert, das neue Kennwort einzugeben.

### Abgelaufenes Zertifikat ersetzen

Wenn ein Zertifikat in einem Truststore abgelaufen ist, müssen Sie es ersetzen, indem Sie ein neues Zertifikat hinzufügen. Gehen Sie hierzu wie folgt vor:

1. Starten Sie iKeyman, falls es nicht bereits ausgeführt wird.
2. Öffnen Sie die Truststore-Datei.
3. Geben Sie das Kennwort ein, und klicken Sie auf **OK**.
4. Wählen Sie **Signer Certificates** aus dem Menü aus.
5. Klicken Sie auf **Add**.
6. Klicken Sie auf **Data type**, und wählen Sie einen Datentyp, wie z. B. Base64-verschlüsselte ASCII-Daten, aus.

   Dieser Datentyp muss mit dem Datentyp des importierenden Zertifikats übereinstimmen.

7. Geben Sie einen Zertifikatsdateinamen und seine Position für das digitale CA-Rootzertifikat ein, oder klicken Sie auf **Browse**, um den Namen und die Position auszuwählen.
8. Klicken Sie auf **OK**.
9. Geben Sie eine Bezeichnung für das importierende Zertifikat ein.
10. Klicken Sie auf **OK**.

## Zertifikatsketten verwenden

Eine Zertifikatskette besteht aus einem Zertifikat eines Partners und beliebigen Zertifikaten, die zur Authentifizierung des Zertifikats eines Partners verwendet werden. Wenn beispielsweise eine Zertifizierungsstelle (CA) verwendet wurde, um das Zertifikat eines Partners zu erstellen, könnte die Zertifizierungsstelle selbst von einer anderen Zertifizierungsstelle zertifiziert worden sein. Die Anerkennungskette beginnt bei der *Stammzertifizierungsstelle*, dem Trust-Anchor. Das digitale Zertifikat der Stammzertifizierungsstelle ist selbst unterzeichnet, d. h. die Zertifizierungsstelle verwendet ihren eigenen privaten Schlüssel, um das digitale Zertifikat zu unterzeichnen. Alle Zertifikate zwischen dem Trust-Anchor und dem Zertifikat des Partners (dem Zielzertifikat) sind *Intermediate*-Zertifikate.

Bei jedem von einer Zertifizierungsstelle ausgegebenem Zertifikat müssen alle Zertifikate in der Kette hinzugefügt werden. Es müssen z. B. in einer Zertifikatskette, in der A (der Trust-Anchor) der Ausgeber von B ist und B der Ausgeber von C (dem Zielzertifikat) ist, die Zertifikate A und B als Zertifikate der Zertifizierungsstelle hochgeladen werden.

WebSphere Partner Gateway behandelt alle selbst unterzeichneten Zertifikate als Trust-Anchors. Das selbst signierte Zertifikat kann ein von einer Zertifizierungsstelle ausgegebenes Zertifikat sein, oder es kann ein selbst signiertes Zertifikat sein, das vom Partner generiert wurde.

Bei Eingangs-SSL werden alle Rootzertifikate (Trust-Anchor) und Intermediate-Zertifikate wie oben beschrieben im Truststore von WebSphere Application Server gespeichert. Für alle Partnerzertifikate werden die zugehörigen Rootzertifikate (Trust-Anchor) und Intermediate-Zertifikate unter dem Hubbetreiber hochgeladen.

## Primäre und sekundäre Zertifikate verwenden

Sie können mehr als ein Zertifikat eines bestimmten Typs erstellen und eines zum primären Zertifikat und eines zum sekundären Zertifikat bestimmen. Wenn das primäre Zertifikat abgelaufen ist oder andernfalls nicht verwendet werden kann, wechselt WebSphere Partner Gateway zum sekundären Zertifikat.

**Anmerkung:** Diese Funktion können Sie verwenden, um ohne Stoppen des Servers von einem alten zu einem neuen Zertifikat zu wechseln.
Sie geben in Community Console an, welches Zertifikat das primäre und welches das sekundäre ist.

Die Möglichkeit primäre und sekundäre Zertifikate bereitzustellen, ist für die folgenden Zertifikate verfügbar:

- Verschlüsselungszertifikat eines Partners
- Signaturzertifikat des Hubbetreibers
- SSL-Clientzertifikat des Hubbetreibers

## Verschlüsselungsstärke ändern

Java Runtime Environment (JRE), die mit WebSphere Partner Gateway geliefert wird, erzwingt Einschränkungen bezüglich der Verschlüsselungsalgorithmen und

maximalen Verschlüsselungsstärken, die zur Verwendung verfügbar sind. Eine eingeschränkte Richtlinie gibt z. B. Begrenzungen für die zulässige Länge und damit die Stärke der Verschlüsselungsschlüssel an. Diese Einschränkungen werden in Dateien angegeben, die als *JRE-Standortrichtliniendateien* (Jurisdiction Policy Files) bezeichnet werden. Die maximal zulässige Länge ist 2048 Byte.

Wenn Zertifikate mit einer Schlüsselgröße von mehr als 2048 Byte unterstützt werden sollen, müssen Sie die Version der Standortrichtliniendateien mit uneingeschränkter bzw. nicht begrenzter Stärke verwenden. Sie können angeben, dass eine stärkere, uneingeschränkte Richtlinie verwendet werden soll, indem Sie neue Richtliniendateien in einem Unterverzeichnis der installierten JRE installieren.

Darüber hinaus sind Verschlüsselungseinschränkungen für symmetrische Schlüsselalgorithmen, wie z. B. 3DES, vorhanden. Wenn Sie einen stärkeren symmetrischen Schlüsselalgorithmus benötigen, werden durch das Ersetzen der Standortrichtliniendateien auch die Einschränkungen für die symmetrischen Schlüssel entfernt. Wenn Sie beispielsweise den AES-Algorithmus verwenden, sind uneingeschränkte Verschlüsselungsrichtliniendateien erforderlich. Einzelheiten hierzu finden Sie unter der folgenden Adresse: http://www.ibm.com/developerworks/java/jdk/security/50.

Aufgrund von Einfuhrbeschränkungen lassen die im Lieferumfang von IBM SDK for Java 5 Development Kit enthaltenen Standortrichtliniendateien zwar **starke** aber nur eingeschränkte Verschlüsselung zu. In der folgenden Tabelle werden die maximalen Schlüsselgrößen aufgelistet, die für diese **starke** Version der Standortrichtliniendateien zulässig sind.

*Tabelle 31. Maximale Größe der in starken Standortrichtliniendateien verwendeten Algorithmen*

| **Algorithmus** | **Maximale Schlüsselgröße** |
|---|---|
| DES | 64 |
| DESede | 112 (effektiv) oder 168 (effektiv) |
| RC2 | 128 |
| RSA | 2048 |
| * (alle anderen) | 128 |

**Anmerkung:** Beim Verschlüsseln einer weitergeleiteten ebMS-Nachricht mit den folgenden Parametern tritt die Ausnahmebedingung 'Encryption failure XMLEncryptionException' auf:

- Verschlüsselungsalgorithmus: aes-192-cbc or aes-256-cbc
- Verschlüsselungsprotokoll: XML-Verschlüsselung

Um dieses Problem zu beheben, müssen Sie die Dateien für die uneingeschränkte Verschlüsselungsrichtlinie installieren, sofern dies rechtlich zulässig ist.

## Installationsanweisungen für die Betriebssysteme Windows, Linux und AIX

Führen Sie die folgenden Schritte aus, um uneingeschränkte Standortrichtliniendateien in WebSphere Partner Gateway zu installieren:

1. Laden Sie die Standortrichtliniendateien mit uneingeschränkter Stärke über den Link **IBM SDK Policy files** von der folgenden Website herunter: http://www.ibm.com/developerworks/java/jdk/security/50/.

2. Dekomprimieren Sie die heruntergeladene Datei in einen temporären Ordner.
3. Kopieren Sie 'local_policy.jar' und 'US_export_policy.jar' aus dem temporären Ordner.
4. Stoppen Sie alle Server in der WebSphere Application Server-Instanz, die konfiguriert wird.
5. Wechseln Sie in den Ordner <*WAS-Installationsverz*>\java\jre\lib\security.
6. Benennen Sie die vorhandenen Dateien 'local_policy.jar' und 'US_export_policy.jar' in 'local_policy.jar.bak' und 'US_export_policy.jar.bak' um.
7. Fügen Sie die in Schritt 3 kopierten JAR-Dateien in den Ordner <*WAS-Installationsverz*>\was\java\jre\lib\security ein.
8. Führen Sie einen Neustart für alle Server in der WebSphere Application Server-Instanz aus, die Sie gerade neu konfiguriert haben.

Diese Schritte gelten für alle WebSphere Application Server-Installationen, in denen WebSphere Partner Gateway-Anwendungen installiert sind.

### Installationsanweisungen für die Betriebssysteme HP-UX und Solaris

Für HP-UX- und Solaris-Plattformen gelten die folgenden Anweisungen:

1. Laden Sie die Standortrichtliniendateien mit uneingeschränkter Stärke über den Link **IBM SDK Policy files** von der folgenden Website herunter: http://www.ibm.com/developerworks/java/jdk/security/50/.
2. Dekomprimieren Sie die heruntergeladene Datei in einen temporären Ordner.
3. Stoppen Sie alle Server in der WebSphere Application Server-Instanz, die konfiguriert wird.
4. Wechseln Sie in den Ordner <*WAS-Installationsverz*>\java\jre\lib\security.
5. Benennen Sie die vorhandenen Dateien 'local_policy.jar' und 'US_export_policy.jar' in 'local_policy.jar.bak' und 'US_export_policy.jar.bak' um.
6. Kopieren Sie 'local_policy.jar' und 'US_export_policy.jar' aus dem temporären Ordner in den Ordner <*WAS-Installationsverz*>\java\jre\lib\security.
7. Führen Sie einen Neustart für alle Server in der WebSphere Application Server-Instanz aus, die Sie gerade neu konfiguriert haben.

Diese Schritte gelten für alle WebSphere Application Server-Installationen, in denen WebSphere Partner Gateway-Anwendungen installiert sind.

## SSL mit konfigurierter Clientauthentifizierung

Wenn Sie für den Dokumentenversand ein Transportprotokoll mit SSL mit Clientauthentifizierung verwenden, muss für den verwendeten JSSE-Provider eine zusätzliche Änderung vorgenommen werden. Weitere Informationen hierzu finden Sie in Kapitel 14, "Fehlerbehebung" im Abschnitt "SSL-Handshake schlägt fehl, weil kein Zertifikat empfangen wurde" im Handbuch *WebSphere Partner Gateway Verwaltung*.

## Ablauf von Zertifikaten

Nur die für Verschlüsselung, digitale Signaturen und SSL verwendeten Zertifikate werden inaktiviert, wenn sie abgelaufen sind. Bei diesen Zertifikaten sollte es sich um Zertifikate einer End-Entität und nicht um CA-Zertifikate handeln. CA-Zertifikate werden nicht inaktiviert, wenn sie abgelaufen sind.

Wenn die Root- oder Intermediate-Zertifikate zwischen Serverneustarts ablaufen, werden sie nicht in die Liste der vertrauenswürdigen Zertifikate eingefügt. Wenn also die Erstellung des Zertifizierungspfads fehlschlägt, weil das CA-Zertifikat

nicht gefunden wurde, ist dieses Zertifikat möglicherweise abgelaufen. Wenn ein Root- oder Intermediate-Zertifikat während der Laufzeit abläuft, schlägt die Erstellung des Zertifizierungspfads fehl, und das entsprechende Zertifikat der End-Entität wird in der Geschäftstransaktion nicht verwendet. In der Anzeige **Zertifikatliste** von WebSphere Partner Gateway Console können Sie den Gültigkeitszeitraum und den Status des Zertifikats überprüfen. Das Gültigkeitsdatum des abgelaufenen Zertifikats wird in dieser Anzeige rot angezeigt.

Wenn ein CA-Zertifikat abgelaufen ist, können Sie bei der betreffenden Zertifizierungsstelle ein neues Zertifikat anfordern. Laden Sie das neue CA-Zertifikat über WebSphere Partner Gateway Console hoch. Informationen zum Hochladen von Zertifikaten finden Sie in den Abschnitten „Zertifikate zum Aktivieren der Verschlüsselung und der Entschlüsselung verwenden", „Zertifikate zum Aktivieren von digitalen Signaturen verwenden" auf Seite 273 und „Zertifikate zum Aktivieren von SSL verwenden" auf Seite 278.

# Zertifikate zum Aktivieren der Verschlüsselung und der Entschlüsselung verwenden

Dieser Abschnitt beschreibt die Verschlüsselung und die Entschlüsselung von Zertifikaten.

## Eingehende Entschlüsselungszertifikate erstellen und installieren

Dieses Zertifikat wird vom Hub verwendet, um verschlüsselte Dateien zu entschlüsseln, die von Partnern empfangen wurden. Der Hub verwendet Ihren privaten Schlüssel, um die Dokumente zu entschlüsseln. Die Verschlüsselung wird verwendet, um zu verhindern, dass Dritte neben dem Absender und dem beabsichtigten Empfänger Transitdokumente anzeigen können.

Beachten Sie die folgende wichtige Einschränkung beim Empfangen von verschlüsselten AS2-Nachrichten von Partnern. Wenn ein Partner eine verschlüsselte AS2-Nachricht sendet, aber das falsche Zertifikat verwendet, schlägt die Entschlüsselung fehl. Es wird jedoch keine MDN an den Partner zurückgegeben, um auf den Fehler hinzuweisen. Damit Ihr Partner in dieser Situation MDNs empfängt, erstellen Sie eine Verbindung zu diesem Partner mit der folgenden Dokumentdefinition:

- Paket: **AS** zu Paket: **None**
- Protokoll: **Binary** zu Protokoll: **Binary**
- Dokumenttyp: **Binary** zu Dokumenttyp: **Binary**

Bei der erstellten Verbindung muss es sich um eine Verbindung des Typs "AS zu None" handeln. Eine solche Verbindung wird erstellt, indem die B2B-Funktionalität "AS auf einem Partner und die B2B-Funktionalität "None" auf dem anderen Partner aktiviert wird. Stellen Sie sicher, dass das Quellengateway auf der AS-Seite ein SMTP-Gateway (für AS1), ein HTTP-Gateway (für AS2) oder ein FTP-Gateway (für AS3) ist. Dies wird in der MDN-Adresse konfiguriert. Auf diese Weise wird die MDN bei einem Fehlschlag der Entschlüsselung über diese binäre Verbindung "AS zu None" zurückgesendet.

### Schritt 1: Zertifikat beschaffen

**Selbst signiertes Zertifikat generieren:** Wenn Sie die Entschlüsselung verwenden möchten, gehen Sie wie folgt vor:

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 Partner. 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 den internen Partner senden wollen. Wenn Ihr Zertifikat CA-unterzeichnet ist, stellen Sie das CA-Zertifikat ebenfalls zur Verfügung.
5. Verwenden Sie iKeyman, um das selbst signierte Zertifikat und das private Schlüsselpaar in Form einer PKCS12-Datei zu speichern.
6. Navigieren Sie zu **Profil** > **{Hubbetreiber/Interner Partner}** > **Zertifikate** > **Zertifikat laden**.
7. Wählen Sie in der Dropdown-Liste **Partner für das Zertifikat** den Partner aus, der dem neu hochgeladenen Zertifikat zugeordnet werden soll.
8. Klicken Sie auf **Suchen**, um einen bestimmten Partner oder Untergruppen von Partnern zu suchen.
9. Klicken Sie auf **Durchsuchen** neben **Zertifikatsposition**, um das Zertifikat hochzuladen.
10. Klicken Sie auf **Weiter**.
11. Geben Sie in das Feld **Zertifikatsdetails angeben** die folgenden Informationen zum Zertifikat ein: **Nicht hierarchisches Zertifikat**, **Root CA-Zertifikat** oder **Intermediate CA-Zertifikat**.
12. Ordnen Sie dieses Zertifikat einer **Entschlüsselung** zu.
13. Wählen Sie im Feld **Zertifikatverwendung** die Option **Primär** oder **Sekundär** aus.
14. Wählen Sie im Feld **Status** die Option **Aktiviert** oder **Inaktiviert** aus, abhängig davon, ob das Zertifikat nach dem Hochladen aktiviert oder inaktiviert werden soll.
15. Wählen Sie den **Betriebsmodus** aus.
16. Klicken Sie auf **Fertigstellen**, um die Änderungen zu speichern und den Assistenten zu schließen.

**Von Zertifizierungsstelle signiertes Zertifikat verwenden:** Wenn Sie ein von einer Zertifizierungsstelle signiertes Zertifikat verwenden, gehen Sie wie folgt vor:

1. Starten Sie das Dienstprogramm iKeyman.
2. Generieren Sie mit iKeyman eine Zertifikatsanforderung und ein Schlüsselpaar für den Empfänger.
3. Übergeben Sie eine Zertifikatsunterzeichungsanforderung (CSR - Certificate Signing Request) an eine Zertifizierungsstelle.
4. Wenn Sie das unterzeichnete Zertifikat von der Zertifizierungsstelle empfangen, stellen Sie das unterzeichnete Zertifikat mit iKeyman in den Keystore.

### Schritt 2: Zertifikat verteilen

Verteilen Sie das signierte CA-Zertifikat an alle Partner.

## Ausgehende Verschlüsselungszertifikate installieren

Das ausgehende Verschlüsselungszertifikat wird verwendet, wenn der Hub verschlüsselte Dokumente an die Partner sendet. WebSphere Partner Gateway ver-

schlüsselt Dokumente mit den öffentlichen Schlüsseln der Partner, und die Partner entschlüsseln die Dokumente mit ihren privaten Schlüsseln.

Der Partner kann mehr als ein Verschlüsselungszertifikat haben. Eines ist das primäre Zertifikat, welches standardmäßig verwendet wird. Das andere Zertifikat ist das sekundäre Zertifikat, welches verwendet wird, wenn das primäre Zertifikat abgelaufen ist.

## Schritt 1: Zertifikat des Partners abrufen

Rufen Sie das Verschlüsselungszertifikat des Partners ab. Das Zertifikat muss im Format 'X.509-DER' vorliegen. Beachten Sie, dass WebSphere Partner Gateway nur X5.09-Zertifikate unterstützt.

## Schritt 2: Zertifikat des Partners installieren

Gehen Sie wie folgt vor, um das Zertifikat über Community Console im Profil des Partners zu installieren:

1. Navigieren Sie zu **Profil** > **Externer Partner**> **Zertifikate** > **Zertifikat laden**.
2. Geben Sie auf der Seite zum Auswählen des Partners, der Dateiposition und des Kennworts die folgenden Werte ein:
   - **Partner für das Zertifikat:** Wählen Sie den Partner aus, der dem neu hochgeladenen Zertifikat zugeordnet werden soll. Klicken Sie auf **Suchen**, um einen bestimmten Partner oder eine Untergruppe von Partnern zu suchen. Ist der Partner der Hubbetreiber oder der interne Partner, müssen Sie die Position des Zertifikats, die Position des privaten Schlüssels und das Kennwort angeben *oder* den Truststore (Zertifikatsspeicher für vertrauenswürdige Zertifikate) oder Keystore (Schlüsselspeicher) mit dem entsprechenden Kennwort angeben. Für externe Partner müssen Sie die Position des Zertifikats *oder* die Position des Truststore, der die Zertifikatskette enthält, angeben.
   - **Position des Zertifikats:** Klicken Sie auf **Durchsuchen**, um die Position des öffentlichen Zertifikats auszuwählen.
3. Klicken Sie auf **Weiter**, um mit der Seite **Zertifikatsdetails** des Assistenten fortzufahren.
4. Geben Sie auf der Seite **Zertifikatsdetails** des Assistenten die folgenden Details des Zertifikats ein:
   - **Name des Leaf-Zertifikats** - Der Name des Leaf-Zertifikats (nicht hierarchisches Zertifikat). Der Name des Felds ist davon abhängig, ob es sich bei dem Zertifikat um ein Leaf-Zertifikat ein Root CA-Zertifikat (Zertifikat der Stammzertifizierungsstelle) oder ein Intermediate CA-Zertifikat (Zertifikat einer Zwischenzertifizierungsstelle) handelt.
   - **Beschreibung** - Die Beschreibung des Leaf-Zertifikats.
   - **Zertifikatstyp** - Ordnen Sie dieses Zertifikat der Verschlüsselung zu.
   - **Zertifikatverwendung** - Ordnen Sie eine Verwendung für das Zertifikat zu. Die zulässigen Werte sind **Primär** und **Sekundär**.
   - **Betriebsmodus** - Geben Sie den Betriebsmodus ein.
   - **Status** - Wählen Sie **Aktiviert** oder **Inaktiviert** aus, abhängig davon, ob das Zertifikat nach dem Hochladen aktiviert oder inaktiviert werden soll. Die Schaltfläche **Weiter** ist nur aktiviert, wenn das Zertifikat aktiviert ist.
   - **Gruppenverwaltung** - Sie können das Zertifikat einer vorhandenen Gruppe zuordnen oder eine neue Gruppe erstellen. Ist das Zertifikat ein sekundäres Zertifikat, kann es nur einer vorhandenen Gruppe zugeordnet werden. Für

einen internen Partner mit dem Typ "encrypt" oder für einen externen Partner mit dem Typ "SSL" (Incoming client auth) oder "Signing" (Verify) können Sie das Zertifikat einer beliebigen Gruppe zuordnen.

5. Klicken Sie auf **Weiter**, um mit der Seite **Gruppe** des Assistenten fortzufahren. Wenn es sich um ein primäres Zertifikat handelt, müssen Sie keine Gruppen erstellen und das Zertifikat einer Gruppe und einer Partnerverbindung zuordnen. Wenn Sie das Kontrollkästchen **Neue Gruppe erstellen** ausgewählt haben, wird die Seite **Neue Gruppe erstellen** des Assistenten geöffnet. Andernfalls wird die Seite **Zu vorhandener Gruppe hinzufügen** des Assistenten geöffnet. Wenn die Datei einen privaten Schlüssel des internen Partners oder das für SSL bzw. die digitale Signatur verwendete öffentliche Zertifikat des externen Partners enthält, können Sie auf **Fertigstellen** klicken.
6. Geben Sie auf der Seite **Neue Gruppe erstellen** des Assistenten die Details für die neue Gruppe ein. Für primäre Zertifikate müssen Sie keine Gruppen erstellen und ihnen ein Zertifikat zuordnen. Geben Sie die folgenden Werte ein:
   - **Gruppenname** - Der Name der Gruppe.
   - **Beschreibung** - Die Beschreibung der Gruppe.
   - **Status** - Wählen Sie "Aktiviert" oder "Inaktiviert" aus. Ist die Gruppe inaktiviert, ist die Schaltfläche **Weiter** nicht aktiviert.
   - **Als Standardeinstellung** - Wählen Sie dieses Kontrollkästchen aus, wenn Sie diese Gruppe als Standardgruppe festlegen wollen.
7. Wählen Sie auf der Seite **Zu vorhandener Gruppe hinzufügen** des Assistenten die Gruppe oder Gruppen aus, zu der bzw. denen das Zertifikat hinzugefügt werden soll. Geben Sie die folgenden Werte ein:
   - **Wählen Sie die Gruppe für den ausgewählten Zertifikatstyp aus** - Wählen Sie die Gruppe oder Gruppen aus, zu der bzw. denen das Zertifikat hinzugefügt werden soll.
   - **Als Standardeinstellung** - Wählen Sie dieses Kontrollkästchen aus, wenn Sie diese Gruppe als Standardgruppe festlegen wollen.
8. Klicken Sie auf der Seite **Neue Gruppe erstellen** oder **Zu vorhandener Gruppe hinzufügen** auf **Weiter**, um mit der Seite **Standardeinstellungen** des Assistenten fortzufahren. Die Schaltfläche **Weiter** ist nur aktiviert, wenn der Status der Gruppe **aktiviert** ist.
9. Wählen Sie im Feld **Status** die Option **aktiviert** oder **inaktiviert** aus, abhängig davon, ob das Zertifikat nach dem Hochladen aktiviert oder inaktiviert werden soll.

   **Anmerkung:** Wenn Sie auf der vorherigen Seite (**Neue Gruppe erstellen** oder **Zu vorhandener Gruppe hinzufügen**) das Kontrollkästchen **Als Standardeinstellung** ausgewählt haben, müssen Sie die Gruppe einem Betriebsmodus zuordnen. In diesem Fall werden Zertifikatverwendungen für Betriebsmodi angezeigt. Für interne Partner wird die Verschlüsselung inaktiviert. Für externe Partner werden SSL (Clientauthentifizierung) und die digitale Signatur inaktiviert.
10. Klicken Sie auf **Weiter**, um mit der Seite **Konfiguration** des Assistenten fortzufahren. Wenn Sie auf **Fertigstellen** klicken und weiterhin Root CA- oder Intermediate CA-Zertifikate fehlen, werden Sie aufgefordert, diese hochzuladen. Wenn Sie im Fenster mit der Eingabeaufforderung auf **Ja** klicken, wird die erste Seite des Assistenten geöffnet. Klicken Sie auf **Abbrechen**, wenn Sie die Zertifikate später hochladen wollen.
11. Geben Sie auf der Seite **Konfiguration** des Assistenten die folgenden Werte ein:

**Anmerkung:** Auf der Seite **Konfiguration** wird eine Liste mit Zertifikaten bzw. Zertifikatsgruppen für Betriebsmodi angezeigt. Der Name der aktuellen Gruppe ist für alle Gruppen im Voraus ausgefüllt; er kann jedoch geändert werden.

- **Absenderpartner** - Dieses Feld wird mit dem Wert des internen Partners im Voraus ausgefüllt.
- **Empfängerpartner** - Diese Dropdown-Liste ist mit der Liste aller externen Partner im Voraus ausgefüllt. Sie können auch den Wert **Alle** auswählen, um alle externen Partner einzuschließen.
- **Absenderpaket** - Wählen Sie in der Dropdown-Liste die Paketobjekte der Dokumentenflussdefinition des internen Partners aus.
- **Empfängerpaket** - Wählen Sie in der Liste die Paketobjekte der Dokumentenflussdefinition des externen Partners aus.

12. Klicken Sie auf **Weitere Verbindungen hinzufügen**, wenn Sie die Gruppe anderen Partnerverbindungen zuordnen wollen.
13. Klicken Sie auf **Sekundäres Zertifikat hinzufügen**, um ein sekundäres Zertifikat zur aktuellen Gruppe hinzuzufügen.
14. Klicken Sie auf **Fertigstellen**, um das Zertifikat hochzuladen. Wenn weiterhin Root CA- oder Intermediate CA-Zertifikate fehlen, werden Sie aufgefordert, diese hochzuladen. Wenn Sie im Fenster mit der Eingabeaufforderung auf **Ja** klicken, wird die erste Seite des Assistenten geöffnet. Klicken Sie in der Eingabeaufforderung auf **Abbrechen**, wenn Sie die Zertifikate später hochladen wollen.

Wiederholen Sie diesen Schritt, wenn der Partner über ein zweites Verschlüsselungszertifikat verfügt.

## Schritt 3: Von Zertifizierungsstelle ausgestellte Zertifikate installieren

Wenn das Zertifikat von einer Zertifizierungsstelle signiert wurde und das Rootzertifikat der Zertifizierungsstelle und alle weiteren Zertifikate, die Teil der Zertifikatskette sind, noch nicht im Profil des Hubbetreibers installiert sind, installieren Sie die Zertifikate. Gehen Sie dazu wie folgt vor:

**Anmerkung:** Sie müssen diesen Schritt nicht ausführen, wenn das von der Zertifizierungsstelle ausgestellte Zertifikat bereits installiert ist.

1. Navigieren Sie zu **Profil** > **Hubbetreiber** > **Benutzer** > **Zertifikate** > **Zertifikat laden**.
2. Wählen Sie in der Dropdown-Liste **Partner für das Zertifikat** den Partner aus, der dem neu hochgeladenen Zertifikat zugeordnet werden soll.
3. Klicken Sie auf **Suchen** um einen bestimmten Partner oder Untergruppen von Partnern zu suchen.
4. Klicken Sie auf **Durchsuchen** neben **Position des Truststore oder Keystore**.
5. Geben Sie für das Zertifikat und den Truststore das **Kennwort** ein.
6. Handelt es sich um einen Truststore, geben Sie den **Typ des Keystore** ein und klicken Sie auf **Weiter**.
7. Wählen Sie auf der Seite **Hochzuladendes Endentitätszertifikat auswählen** des Assistenten ein zu ladendes Zertifikat aus.

   **Anmerkung:** Wenn Sie Zertifikate mithilfe eines Truststore laden, in dem sich mehrere Zertifikate befinden, wird die Anzeige **Wählen Sie die Liste der hoch-**

**zuladenden Root-CA und Intermediate-CA-Zertifikate aus** mit allen Zertifikaten gefüllt. Sie können auch mehrere Zertifikate hochladen.

8. Klicken Sie auf **Fertigstellen**.

### Schritt 4: Verschlüsselung aktivieren

Aktivieren Sie die Verschlüsselung auf der Ebene für Pakete (höchste Ebene), Partner oder Verbindungen (unterste Ebene). Ihre Einstellung kann andere Einstellungen auf der Verbindungsebene überschreiben. Die Verbindungszusammenfassung informiert Sie darüber, ob ein erforderliches Attribut fehlt.

Klicken Sie zum Ändern der Attribute einer Partnerverbindung zum Beispiel auf **Kontenadmin > Verbindungen > Partnerverbindungen** und wählen Sie dann die Partner aus. Klicken Sie auf **Attribute** und bearbeiten Sie dann das Attribut. Beispiel: **AS verschlüsselt**.

Wenn die Fehlernachricht `Kein gültiges Verschlüsselungszertifikat gefunden` angezeigt wird, ist weder das primäre noch das sekundäre Zertifikat gültig. Die Zertifikate sind unter Umständen abgelaufen oder sie wurden widerrufen. Wenn die Zertifikate abgelaufen sind oder widerrufen wurden, kann das entsprechende Ereignis (`Certificate revoked or expired`) auch in der Ereignisanzeige angezeigt werden. Beachten Sie, dass diese zwei Ereignisse möglicherweise durch andere Ereignisse getrennt wurden.

Gehen Sie wie folgt vor, um die Ereignisanzeige zu öffnen:

1. Klicken Sie auf **Anzeigen > Ereignisanzeige**.
2. Wählen Sie die entsprechenden Suchkriterien aus.
3. Klicken Sie auf **Suchen**.

Informationen zur Verwendung der Ereignisanzeige finden Sie im Handbuch *WebSphere Partner Gateway Verwaltung*.

## Zertifikate zum Aktivieren von digitalen Signaturen verwenden

### Ausgehendes Signaturzertifikat erstellen

Document Manager verwendet dieses Zertifikat, wenn er ausgehende, signierte Dokumente an die Partner sendet. Dasselbe Zertifikat und derselbe Schlüssel werden für alle Ports und Protokolle verwendet.

Sie können über mehr als ein Zertifikat für digitale Signatur verfügen. Eines ist das primäre Zertifikat, welches standardmäßig verwendet wird. Das andere Zertifikat ist das sekundäre Zertifikat, welches verwendet wird, wenn das primäre Zertifikat abgelaufen ist.

#### Selbst signiertes Zertifikat generieren

Wenn Sie ein selbst signiertes Zertifikat verwenden möchten, gehen Sie wie folgt vor:

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 Partner. Die bevorzugte Verteilungsmethode ist das Senden des Zertifikats in einer kennwortgeschützten komprimierten Datei per E-Mail. Ihre Partner müssen sich an Sie wenden und das Kennwort für die komprimierte Datei anfordern.
5. Verwenden Sie iKeyman, um das selbst signierte Zertifikat und das private Schlüsselpaar in Form einer PKCS12-Datei zu exportieren.

## Ausgehendes selbst signiertes Zertifikat installieren

1. Navigieren Sie zu **Profil** > {**Hubbetreiber/Interner Partner**} > **Zertifikat** > **Zertifikat laden**.
2. Geben Sie auf der Seite zum Auswählen des Partners, der Dateiposition und des Kennworts die folgenden Werte ein:
   - **Partner für das Zertifikat:** Wählen Sie den Partner aus, der dem neu hochgeladenen Zertifikat zugeordnet werden soll. Klicken Sie auf **Suchen**, um einen bestimmten Partner oder eine Untergruppe von Partnern zu suchen. Ist der Partner der Hubbetreiber oder der interne Partner, müssen Sie die Position des Zertifikats, die Position des privaten Schlüssels und das Kennwort angeben *oder* den Truststore (Zertifikatsspeicher für vertrauenswürdige Zertifikate) oder Keystore (Schlüsselspeicher) mit dem entsprechenden Kennwort angeben. Für externe Partner müssen Sie die Position des Zertifikats *oder* die Position des Truststore, der die Zertifikatskette enthält, angeben.
   - **Privater Schlüssel:** Klicken Sie auf **Durchsuchen**, um den privaten Schlüssel des Zertifikats auszuwählen.
   - **Kennwort:** Geben Sie das Kennwort ein, wenn das Zertifikat über ein Kennwort verfügt.
   - **Position des Truststore oder Keystore:** Klicken Sie auf **Durchsuchen**, um die Position des Truststore bzw. Keystore auszuwählen. Ein Keystore ist eine Sammlung von privaten Schlüsseln und den ihnen zugeordneten Trusted-Root-und CA-Zertifikaten.
   - **Kennwort:** Geben Sie das Kennwort für die Position des Keystore ein.
   - **Typ:** Wählen Sie den Typ für den Truststore oder Keystore aus. Die folgenden Werte sind in der Dropdown-Liste verfügbar: JKS, JCEKS und PKCS12.

   **Anmerkung:** Beim Erstellen einer Schlüsseldatenbank des Typs CMS (Keystore) in WebSphere Partner Gateway mithilfe von iKeyman, wird der folgende Fehler angezeigt:

   ```
   "The CMS java native library was not found. Please make sure the
    SSL component required by your product is installed and library path is defined
   properly.
   ```

   . Da WebSphere Application Server und WebSphere Partner Gateway keine CMS-Keystores verwenden, müssen Sie die unterstützten Keystore-Typen JKS (der Standardtyp), PKCS12 oder JCEKS verwenden.
3. Klicken Sie auf **Weiter**, um mit der Seite **Zertifikatsdetails** des Assistenten fortzufahren. Die Seite **Endentitäts- und CA-Zertifikat auswählen** des Assistenten wird geöffnet, wenn Sie Zertifikate über einen Truststore laden, der mehrere Zertifikate enthält. Die Liste der im Truststore verfügbaren Zertifikate wird angezeigt.
4. Geben Sie auf der Seite **Endentitäts- und CA-Zertifikat auswählen** des Assistenten die folgenden Werte ein:
   - **Der Keystore enthält mehrere Endentitätszertifikate. Wählen Sie das hochzuladende Zertifikat aus.** - Die Dropdown-Liste enthält alle Endentitätszertifikate. Wählen Sie das hochzuladende Zertifikat aus.

- **Kennwort** - Verfügt der Keystore über ein Kennwort, wählen Sie dieses Kontrollkästchen aus und geben Sie das Kennwort im Textfeld ein.
- **Wählen Sie die Liste der hochzuladenden Root-CA und Intermediate-CA-Zertifikate aus** - Wählen Sie im Listenfenster die hochzuladenden Root CA- und Intermediate CA-Zertifikate aus.

5. Klicken Sie auf **Weiter**, um mit der Seite **Zertifikatsdetails** des Assistenten fortzufahren.
6. Geben Sie auf der Seite **Zertifikatsdetails** des Assistenten die folgenden Details des Zertifikats ein:
   - **Name des Leaf-Zertifikats** - Der Name des Leaf-Zertifikats (nicht hierarchisches Zertifikat). Der Name des Felds ist davon abhängig, ob es sich bei dem Zertifikat um ein Leaf-Zertifikat ein Root CA-Zertifikat (Zertifikat der Stammzertifizierungsstelle) oder ein Intermediate CA-Zertifikat (Zertifikat einer Zwischenzertifizierungsstelle) handelt.
   - **Beschreibung** - Die Beschreibung des Leaf-Zertifikats.
   - **Zertifikatstyp** - Ordnen Sie dieses Zertifikat der Verschlüsselung zu.
   - **Zertifikatverwendung** - Ordnen Sie eine Verwendung für das Zertifikat zu. Die zulässigen Werte sind **Primär** und **Sekundär**.
   - **Betriebsmodus** - Geben Sie den Betriebsmodus ein.
   - **Status** - Wählen Sie **Aktiviert** oder **Inaktiviert** aus, abhängig davon, ob das Zertifikat nach dem Hochladen aktiviert oder inaktiviert werden soll. Die Schaltfläche **Weiter** ist nur aktiviert, wenn das Zertifikat aktiviert ist.
   - **Gruppenverwaltung** - Sie können das Zertifikat einer vorhandenen Gruppe zuordnen oder eine neue Gruppe erstellen. Ist das Zertifikat ein sekundäres Zertifikat, kann es nur einer vorhandenen Gruppe zugeordnet werden. Für einen internen Partner mit dem Typ "encrypt" oder für einen externen Partner mit dem Typ "SSL" (Incoming client auth) oder "Signing" (Verify) können Sie das Zertifikat einer beliebigen Gruppe zuordnen.

     **Anmerkung:** Für den Hubbetreiber ist keine Gruppenverwaltung verfügbar. Die Zertifikate werden der erstellten Standardgruppe zugeordnet.
7. Klicken Sie auf **Weiter**, um mit der Seite **Gruppe** des Assistenten fortzufahren. Wenn es sich um ein primäres Zertifikat handelt, müssen Sie keine Gruppen erstellen und das Zertifikat einer Gruppe und einer Partnerverbindung zuordnen. Wenn Sie das Kontrollkästchen **Neue Gruppe erstellen** ausgewählt haben, wird die Seite **Neue Gruppe erstellen** des Assistenten geöffnet. Andernfalls wird die Seite **Zu vorhandener Gruppe hinzufügen** des Assistenten geöffnet. Wenn die Datei einen privaten Schlüssel des internen Partners oder das für SSL bzw. die digitale Signatur verwendete öffentliche Zertifikat des externen Partners enthält, können Sie auf **Fertigstellen** klicken.
8. Geben Sie auf der Seite **Neue Gruppe erstellen** des Assistenten die Details für die neue Gruppe ein. Für primäre Zertifikate müssen Sie keine Gruppen erstellen und ihnen ein Zertifikat zuordnen. Geben Sie die folgenden Werte ein:
   - **Gruppenname** - Der Name der Gruppe.
   - **Beschreibung** - Die Beschreibung der Gruppe.
   - **Status** - Wählen Sie "Aktiviert" oder "Inaktiviert" aus. Ist die Gruppe inaktiviert, ist die Schaltfläche **Weiter** nicht aktiviert.
   - **Als Standardeinstellung** - Wählen Sie dieses Kontrollkästchen aus, wenn Sie diese Gruppe als Standardgruppe festlegen wollen.
9. Wählen Sie auf der Seite **Zu vorhandener Gruppe hinzufügen** des Assistenten die Gruppe oder Gruppen aus, zu der bzw. denen das Zertifikat hinzugefügt werden soll. Geben Sie die folgenden Werte ein:

- **Wählen Sie die Gruppe für den ausgewählten Zertifikatstyp aus** - Wählen Sie die Gruppe oder Gruppen aus, zu der bzw. denen das Zertifikat hinzugefügt werden soll.
- **Als Standardeinstellung** - Wählen Sie dieses Kontrollkästchen aus, wenn Sie diese Gruppe als Standardgruppe festlegen wollen.

10. Klicken Sie auf der Seite **Neue Gruppe erstellen** oder **Zu vorhandener Gruppe hinzufügen** auf **Weiter**, um mit der Seite **Standardeinstellungen** des Assistenten fortzufahren. Die Schaltfläche **Weiter** ist nur aktiviert, wenn der Status der Gruppe **aktiviert** ist.
11. Wählen Sie im Feld **Status** die Option **aktiviert** oder **inaktiviert** aus, abhängig davon, ob das Zertifikat nach dem Hochladen aktiviert oder inaktiviert werden soll.

    **Anmerkung:** Wenn Sie auf der vorherigen Seite (**Neue Gruppe erstellen** oder **Zu vorhandener Gruppe hinzufügen**) das Kontrollkästchen **Als Standardeinstellung** ausgewählt haben, müssen Sie die Gruppe einem Betriebsmodus zuordnen. In diesem Fall werden Zertifikatverwendungen für Betriebsmodi angezeigt. Für interne Partner wird die Verschlüsselung inaktiviert. Für externe Partner werden SSL (Clientauthentifizierung) und die digitale Signatur inaktiviert.
12. Klicken Sie auf **Weiter**, um mit der Seite **Konfiguration** des Assistenten fortzufahren. Wenn Sie auf **Fertigstellen** klicken und weiterhin Root CA- oder Intermediate CA-Zertifikate fehlen, werden Sie aufgefordert, diese hochzuladen. Wenn Sie im Fenster mit der Eingabeaufforderung auf **Ja** klicken, wird die erste Seite des Assistenten geöffnet. Klicken Sie auf **Abbrechen**, wenn Sie die Zertifikate später hochladen wollen.
13. Geben Sie auf der Seite **Konfiguration** des Assistenten die folgenden Werte ein:

    **Anmerkung:** Auf der Seite **Konfiguration** wird eine Liste mit Zertifikaten bzw. Zertifikatsgruppen für Betriebsmodi angezeigt. Der Name der aktuellen Gruppe ist für alle Gruppen im Voraus ausgefüllt; er kann jedoch geändert werden.
    - **Absenderpartner** - Dieses Feld wird mit dem Wert des internen Partners im Voraus ausgefüllt.
    - **Empfängerpartner** - Diese Dropdown-Liste ist mit der Liste aller externen Partner im Voraus ausgefüllt. Sie können auch den Wert **Alle** auswählen, um alle externen Partner einzuschließen.
    - **Absenderpaket** - Wählen Sie in der Dropdown-Liste die Paketobjekte der Dokumentenflussdefinition des internen Partners aus.
    - **Empfängerpaket** - Wählen Sie in der Liste die Paketobjekte der Dokumentenflussdefinition des externen Partners aus.
14. Klicken Sie auf **Weitere Verbindungen hinzufügen**, wenn Sie die Gruppe anderen Partnerverbindungen zuordnen wollen.
15. Klicken Sie auf **Sekundäres Zertifikat hinzufügen**, um ein sekundäres Zertifikat zur aktuellen Gruppe hinzuzufügen.
16. Klicken Sie auf **Fertigstellen**, um das Zertifikat hochzuladen. Wenn weiterhin Root CA- oder Intermediate CA-Zertifikate fehlen, werden Sie aufgefordert, diese hochzuladen. Wenn Sie im Fenster mit der Eingabeaufforderung auf **Ja** klicken, wird die erste Seite des Assistenten geöffnet. Klicken Sie in der Eingabeaufforderung auf **Abbrechen**, wenn Sie die Zertifikate später hochladen wollen.

Wenn Sie primäre und sekundäre Zertifikate für die SSL-Clientauthentifizierung und die digitale Signatur hochladen und Sie die primären Zertifikate als zwei separate Einträge hochladen, stellen Sie sicher, dass die entsprechenden sekundären Zertifikate als zwei unterschiedliche Einträge hochgeladen werden.

### Von Zertifizierungsstelle signiertes Zertifikat abrufen

Wenn Sie ein von einer Zertifizierungsstelle signiertes Zertifikat verwenden, gehen Sie wie folgt vor:

1. Starten Sie das Dienstprogramm iKeyman.
2. Generieren Sie mit iKeyman eine Zertifikatsanforderung und ein Schlüsselpaar für den Empfänger.
3. Übergeben Sie eine Zertifikatsunterzeichungsanforderung (CSR - Certificate Signing Request) an eine Zertifizierungsstelle.
4. Wenn Sie das unterzeichnete Zertifikat von der Zertifizierungsstelle empfangen, stellen Sie das unterzeichnete Zertifikat mit iKeyman in den Keystore.
5. Verteilen Sie das signierte CA-Zertifikat an alle Partner.

## Zertifikat zur Prüfung der eingehenden digitalen Signatur installieren

Document Manager verwendet das signierte Zertifikat des Partners, um die Signatur des Absenders zu prüfen, wenn Sie Dokumente empfangen. Die Partner senden ihre selbst signierten Signaturzertifikate in X.509-DER-Format an Sie. Sie installieren Ihrerseits die Zertifikate der Partner über Community Console im Profil des jeweiligen Partners.

Gehen Sie wie folgt vor, um das Zertifikat zu installieren:

1. Empfangen Sie das X.509-Signaturzertifikat des Partners im DER-Format.
2. Navigieren Sie zu **Profil** > **Externer Partner** > **Zertifikate** > **Zertifikat laden**.
3. Klicken Sie auf **Suchen**, um einen bestimmten Partner oder Untergruppen von Partnern zu suchen.
4. Klicken Sie auf **Durchsuchen** neben **Zertifikatsposition**, um das Zertifikat hochzuladen.
5. Klicken Sie auf **Weiter**, um mit der Seite **Zertifikatsdetails** des Assistenten fortzufahren.
6. Ordnen Sie dieses Zertifikat dem Eintrag **Prüfung der digitalen Signatur** zu.
7. Wählen Sie im Feld **Status** die Option **Aktiviert** oder **Inaktiviert** aus, abhängig davon, ob das Zertifikat nach dem Hochladen aktiviert oder inaktiviert werden soll.
8. Wählen Sie den **Betriebsmodus** aus. Wenn Sie ein Hubbetreiber sind, haben Sie nicht die Option, den **Betriebsmodus** auszuwählen.
9. Klicken Sie auf **Fertigstellen**, um die Änderungen zu speichern und den Assistenten zu schließen.
10. Wenn das Zertifikat von einer Zertifizierungsstelle signiert wurde und das Rootzertifikat der Zertifizierungsstelle und alle anderen Zertifikate, die Teil der Zertifikatskette sind, noch nicht im Profil des Hubbetreibers installiert sind, installieren Sie die Zertifikate jetzt. Dies gilt nur für Truststore/Keystore.
    a. Klicken Sie auf **Hubadmin > Hub-Partnerprofil > Zertifikate**, um die Seite mit der Zertifikatliste aufzurufen.

Stellen Sie sicher, dass Sie an Community Console als Hubbetreiber angemeldet sind, und installieren Sie das Zertifikat in Ihrem eigenen Profil.

b. Klicken Sie auf **Zertifikat laden**.

c. Wählen Sie **Root und Intermediate** aus.

d. Geben Sie eine Beschreibung des Zertifikats ein, welches erforderlich ist.

e. Ändern Sie den Status in **Aktiviert**.

f. Klicken Sie auf **Durchsuchen**, und navigieren Sie zum Verzeichnis, in dem Sie das Zertifikat gespeichert haben.

g. Wählen Sie das Zertifikat aus, und klicken Sie auf **Öffnen**.

h. Klicken Sie auf **Hochladen** und dann auf **Speichern**.

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

11. Aktivieren Sie das Signieren auf der Ebene für Pakete (höchste Ebene), Partner oder Verbindungen (unterste Ebene). Ihre Einstellung kann andere Einstellungen auf der Verbindungsebene überschreiben. Die Verbindungszusammenfassung informiert Sie darüber, ob ein erforderliches Attribut fehlt.

    Klicken Sie zum Ändern der Attribute einer Partnerverbindung zum Beispiel auf **Kontenadmin > Verbindungen**, und wählen Sie dann die Partner aus. Klicken Sie auf **Attribute**, und bearbeiten Sie dann das Attribut. Beispiel: **AS unterzeichnet**.

# Zertifikate zum Aktivieren von SSL verwenden

In den folgenden Abschnitten wird beschrieben, wie Sie SSL-Zertifikate zur Verwendung mit WebSphere Partner Gateway erstellen und installieren. Außerdem ist eine Übersicht des SSL-Handshake-Prozesses enthalten. Wenn Ihre Community SSL nicht verwendet, benötigen weder Sie noch Ihre Partner ein eingehendes oder ausgehendes SSL-Zertifikat.

## SSL-Handshake

Jede SSL-Sitzung beginnt mit einem Handshake.

Wenn ein Client (der Partner oder der interne Partner) einen Nachrichtenaustausch initiiert, werden die folgenden Schritte ausgeführt:

1. Der Client sendet eine Clientnachricht "hello", die die verschlüsselten Funktionen des Clients (sortiert in der vom Client bevorzugten Reihenfolge) auflistet, wie z. B. die Version von SSL, die vom Client unterstützten Cipher Suites und die vom Client unterstützten Datenkomprimierungsmethoden. Die Nachricht enthält außerdem eine 28-Byte-Zufallszahl.
2. Der Server antwortet mit einer Servernachricht "hello done" (erledigt), die die verschlüsselte Methode (Cipher Suite) und die vom Server ausgewählte Datenkomprimierungsmethode, die Sitzungs-ID und eine weitere Zufallszahl enthält.

   **Anmerkung:** Der Client und der Server müssen mindestens eine gemeinsame Cipher Suite unterstützen, ansonsten schlägt der Handshake fehl. Der Server wählt im Allgemeinen die stärkste gemeinsame Cipher Suite aus.
3. Der Server sendet sein digitales Zertifikat.

   Serverauthentifizierung geschieht in diesem Schritt.

4. Der Server sendet eine Nachricht "digital certificate request" (Anforderung für digitales Zertifikat). In der Nachricht "digital certificate request" sendet der Server eine Liste mit den unterstützten digitalen Zertifikattypen und die definierten Namen von akzeptablen Zertifizierungsstellen.
5. Der Server sendet eine Servernachricht "hello done" und wartet auf die Clientantwort.
6. Nach Empfang der Servernachricht "hello done" prüft der Client die Gültigkeit des digitalen Zertifikats vom Server und überprüft, ob die Serverparameter für "hello" akzeptabel sind.
7. Wenn der Server ein digitales Zertifikat vom Client angefordert hat, sendet der Client ein digitales Zertifikat oder falls kein passendes digitales Zertifikat verfügbar ist, sendet der Client einen Alert "no digital certificate" (kein digitales Zertifikat). Dieser Alert ist nur eine Warnung, aber die Serveranwendung kann in der Sitzung fehlschlagen, wenn die Clientauthentifizierung obligatorisch ist.
8. Der Client sendet eine Nachricht "client key exchange" (Clientschlüsselaustausch). Diese Nachricht enthält einen geheimen Pre-Master-Secret-Wert (Pre-Master Secret), eine 46-Byte-Zufallszahl, die bei der Generierung der symmetrischen Verschlüsselungsschlüssel und der MAC-Schlüssel (MAC - Message Authentication Code - Nachrichtenauthentifizierungscode) verwendet wird, welche mit dem öffentlichen Schlüssel des Servers verschlüsselt sind.
9. Wenn der Client ein digitales Zertifikat an den Server sendet, sendet der Client eine Nachricht "digital certificate verify" (digitales Zertifikat prüfen), die mit dem privaten Schlüssel des Clients unterzeichnet ist. Indem der Server die Signatur dieser Nachricht prüft, kann er explizit das Eigentumsrecht des digitalen Zertifikats vom Client prüfen.

   **Anmerkung:** Ein zusätzlicher Prozess, um das digitale Zertifikat vom Server zu prüfen, ist nicht notwendig. Wenn der Server nicht über den privaten Schlüssel verfügt, der zum digitalen Zertifikat gehört, kann er den Pre-Master Secret nicht entschlüsseln und die richtigen Schlüssel für den symmetrischen Verschlüsselungsalgorithmus nicht erstellen und der Handshake schlägt fehl.
10. Der Client verwendet eine Reihe von verschlüsselten Operationen, um den geheimen Pre-Master-Secret-Wert in einen geheimen Master-Secret-Wert zu konvertieren, von dem alles Schlüsselmaterial abgeleitet wird, das zur Verschlüsselung und Nachrichtenauthentifizierung erforderlich ist. Der Client sendet dann eine Nachricht "change cipher spec" (Verschlüsselungsspezifikation ändern), damit der Server zur neu festgelegten Cipher Suite wechselt. Die nächste vom Client gesendete Nachricht "finished" (fertig) ist die erste Nachricht, die mit dieser Verschlüsselungsmethode und den Verschlüsselungsschlüsseln verschlüsselt ist.
11. Der Server antwortet mit einer Nachricht "change cipher spec" und einer eigenen Nachricht "finished".

Die Clientauthentifizierung erfordert die Schritte 4, 7 und 9.

Der SSL-Handshake wird beendet und die verschlüsselten Anwendungsdaten können gesendet werden.

## Eingehende SSL-Zertifikate konfigurieren

Dieser Abschnitt beschreibt, wie Sie die Server- und die Clientauthentifizierung für eingehende Verbindungsanforderungen von Partnern konfigurieren.

Wenn der Partner ein Dokument an WebSphere Partner Gateway sendet, ist dies eine eingehende Anforderung. Wenn Ihre Community SSL nicht verwendet, benötigen Sie kein eingehendes oder ausgehendes SSL-Zertifikat.

**Anmerkung:** Für eingehendes FTPS verwendet WebSphere Partner Gateway einen vom Kunden bereitgestellten FTP-Server, damit eingehende SSL-Konfigurationen über dieses vom Kunden verwendete FTP-Serverprodukt erfolgen.

## Schritt 1: SSL-Zertifikat abrufen

WebSphere Application Server verwendet das SSL-Zertifikat, wenn er Verbindungsanforderungen von Partnern über SSL empfängt. Es ist das Zertifikat, das der Empfänger präsentiert, um den Hub für den Partner zu identifizieren. Dieses Serverzertifikat kann selbst unterzeichnet oder von einer Zertifizierungsstelle (CA) unterzeichnet sein. In den meisten Fällen verwenden Sie ein CA-Zertifikat, um die Sicherheit zu erhöhen. Sie könnten ein selbst unterzeichnetes Zertifikat in einer Testumgebung verwenden. Verwenden Sie iKeyman oder die Administrationskonsole von WebSphere Application Server, um ein Zertifikat und ein Schlüsselpaar zu generieren. Weitere Informationen finden Sie in der von IBM bereitgestellten Dokumentation zur Verwendung von iKeyman oder der Administrationskonsole von WebSphere Application Server.

Nachdem Sie das Zertifikat und das Schlüsselpaar generiert haben, verwenden Sie das Zertifikat für den eingehenden SSL-Datenverkehr aller Partner. Wenn Sie über mehrere Empfänger oder Konsolen verfügen, kopieren Sie den generierten Keystore auf jede Instanz. Wenn das Zertifikat mit der Administrationskonsole von WebSphere Application Server generiert wird, können Schlüssel und Zertifikat mit der Administrationskonsole von WebSphere Application Server in einen anderen Keystore auf einem anderen Server importiert werden. Wenn das Zertifikat selbst signiert ist, stellen Sie dieses Zertifikat den Partnern zur Verfügung. Um dieses Zertifikat zu erhalten, extrahieren Sie mit iKeyman das öffentliche Zertifikat in eine Datei.

**Selbst signiertes Zertifikat generieren:** Wenn Sie selbst signierte Serverzertifikate verwenden, gehen Sie wie folgt vor:

1. Starten Sie das Dienstprogramm iKeyman, welches sich in */<WAS-Installationsverz>*/bin befindet. Wenn Sie iKeyman zum ersten Mal verwenden, löschen Sie das Zertifikat "dummy", das sich im Keystore befindet.
2. Öffnen Sie den Keystore des Empfängers bzw. der Konsole mit iKeyman, und generieren Sie mit iKeyman ein selbst signiertes Zertifikat und ein Schlüsselpaar für den Keystore des Empfängers bzw. der Konsole.
3. Extrahieren Sie mit iKeyman das Zertifikat in eine Datei, das Ihren öffentlichen Schlüssel enthalten wird.

   Speichern Sie den Keystore in einer JKS-, PKCS12- oder JCEKS-Datei.
4. Verteilen Sie das Zertifikat an Ihre Partner. Die bevorzugte Verteilungsmethode ist das Senden des Zertifikats in einer kennwortgeschützten komprimierten Datei per E-Mail. Ihre Partner müssen sich an Sie wenden und das Kennwort für die komprimierte Datei anfordern.
5. Definieren Sie unter Verwendung der Administrationskonsole von WebSphere Application Server das neue Zertifikat in der SSL-Konfiguration und in den Einstellungen für Empfänger und Konsole. Sie können dazu den Aliasnamen des neuen Zertifikats im Keystore in der Konfiguration für den jeweiligen Knoten oder Server auswählen.

**Von einer Zertifizierungsstelle generiertes Zertifikat abrufen:** Wenn Sie ein von einer Zertifizierungsstelle (CA) signiertes Zertifikat verwenden, gehen Sie wie folgt vor:

1. Starten Sie das Dienstprogramm iKeyman, welches sich im Verzeichnis /<*WAS-Installationsverz*>/bin befindet.
2. Generieren Sie mit iKeyman eine Zertifikatsanforderung und ein Schlüsselpaar für den Empfänger.
3. Übergeben Sie eine Zertifikatsunterzeichungsanforderung (CSR - Certificate Signing Request) an eine Zertifizierungsstelle.
4. Wenn Sie das unterzeichnete Zertifikat von der Zertifizierungsstelle empfangen, stellen Sie das unterzeichnete Zertifikat mit iKeyman in den Keystore.
5. Verteilen Sie das CA-Zertifikat gegebenenfalls an alle Partner.
6. Definieren Sie unter Verwendung der Administrationskonsole von WebSphere Application Server das neue Zertifikat in der SSL-Konfiguration und in den Einstellungen für Empfänger und Konsole. Sie können dazu den Aliasnamen des neuen Zertifikats im Keystore in der Konfiguration für den jeweiligen Knoten oder Server auswählen.

   **Anmerkung:** Zur Ausführung der obigen Schritte kann auch die Administrationskonsole von WebSphere Application Server verwendet werden.

## Schritt 2: Clients authentifizieren

Wenn Sie Partner authentifizieren wollen, die Dokumente senden, führen Sie die Schritte in diesem Abschnitt aus.

**Clientzertifikat installieren:**

Gehen Sie für die Clientauthentifizierung wie folgt vor:

1. Rufen Sie das Zertifikat Ihres Partners ab.
2. Wenn das Zertifikat selbst signiert ist, installieren Sie das Zertifikat mit iKeyman oder der Administrationskonsole von WebSphere Application Server im Truststore.
3. Wenn das Zertifikat von einer Zertifizierungsstelle ausgegeben wurde, fügen Sie die zugehörigen CA-Zertifikate mit iKeyman oder der Administrationskonsole von WebSphere Application Server in den entsprechenden Truststore ein.

**Anmerkung:** Wenn Sie Ihrer Hub-Community weitere Partner hinzufügen, können Sie deren Zertifikate mit iKeyman oder der Administrationskonsole von WebSphere Application Server dem Truststore hinzufügen. Wenn ein Partner die Community verlässt, können Sie die Zertifikate des Partners mit iKeyman oder der Administrationskonsole von WebSphere Application Server aus dem Truststore entfernen.

**Clientauthentifizierung konfigurieren:**

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

1. Navigieren Sie zum folgenden Verzeichnis: /<*Produktverz*>/bin
2. Zum Aktivieren der Clientauthentifizierung rufen Sie das Script wie folgt auf:

```
./bcgwsadmin.sh -f /<Produktverz>/scripts/bcgClientAuth.jacl
      -conntype NONE set
```

**Anmerkung:** Zum Inaktivieren der Clientauthentifizierung rufen Sie das Script wie folgt auf:

```
./bcgwsadmin.sh -f /<Produktverz>/receiver/scripts/bcgClientAuth.jacl
    -conntype NONE clear
```

Sie müssen den Server 'bcgreceiver' erneut starten, damit diese Änderungen wirksam werden. Sie können die Clientauthentifizierung auch über die Administrationskonsole von WebSphere Application Server aktivieren. Der Wert "Unterstützt" bedeutet, dass der Server das Clientzertifikat anfordert. Wenn das Clientzertifikat nicht verfügbar ist, kann aber dennoch ein SSL-Handshake hergestellt werden. Der Wert "Erforderlich" bedeutet, dass das Clientzertifikat gesendet werden muss. Ansonsten schlägt der SSL-Handshake fehl.

**Zertifikat des Clients validieren:**

Es gibt eine Zusatzfunktion, die mit der SSL-Clientauthentifizierung verwendet werden kann. Diese Funktion wird über Community Console aktiviert. Für HTTPS überprüft WebSphere Partner Gateway Zertifikate anhand der Geschäfts-IDs in den eingehenden Dokumenten. Zur Verwendung dieser Funktion erstellen Sie das Partnerprofil, importieren das Clientzertifikat und markieren es als SSL.

1. Importieren Sie das Clientzertifikat.
   a. Klicken Sie auf **Kontenadmin > Profile > Partner** und suchen Sie nach dem Profil des Partners.
   b. Klicken Sie auf **Zertifikate**.
   c. Klicken Sie auf **Zertifikat laden**.
   d. Klicken Sie auf **Durchsuchen** und navigieren Sie zu dem Verzeichnis, in dem Sie das Zertifikat gespeichert haben.
   e. Wählen Sie **SSL-Client** als Zertifikattyp aus.
   f. Geben Sie eine Beschreibung des Zertifikats ein (dies ist erforderlich).
   g. Ändern Sie den Status in **Aktiviert**.
   h. Wenn Sie einen anderen Betriebsmodus als **Produktion** (Standardeinstellung) auswählen wollen, wählen Sie ihn in der Liste aus.
   i. Klicken Sie auf **Fertigstellen**.
2. Aktualisieren Sie das Clientziel.
   a. Klicken Sie auf **Kontenadmin > Profile > Partner** und suchen Sie nach dem Profil des Partners.
   b. Klicken Sie auf **Ziele**.
   c. Wählen Sie das HTTPS-Ziel aus, das Sie zuvor erstellt haben. Wenn Sie das HTTPS-Ziel noch nicht erstellt haben, lesen Sie die Informationen in „HTTP-Ziel einrichten" auf Seite 233.
   d. Klicken Sie auf das Symbol **Bearbeiten**, um das Ziel zu bearbeiten.
   e. Wählen Sie **Ja** für **Client-SSL-Zertifikat prüfen** aus.
   f. Klicken Sie auf **Speichern**.

## Separate Keystores und Truststores für Empfänger und Konsole konfigurieren

Standardmäßig verwendet WebSphere Partner Gateway einen gemeinsamen Keystore und Truststore für den Empfänger und die Konsole. In einer Installation im verteilten Modus können Sie jedoch separate Keystores und Truststores für den Empfänger und die Konsole konfigurieren.

Um den Keystore und Truststore zu konfigurieren, müssen Sie einen separaten Keystore und Truststore für den Empfänger und die Konsole erstellen und definieren. Darüber hinaus müssen Sie separate SSL-Konfigurationen erstellen. Die SSL-Konfigurationen können auf der Clusterebene oder auf der Serverebene definiert werden. Das Definieren der SSL-Konfiguration auf der Clusterebene ist einfacher, da die Konfiguration dann für alle Server in diesem Cluster gilt und nicht jeder Server separat konfiguriert werden muss.

**SSL-Konfiguration auf der Clusterebene definieren:** Wird die SSL-Konfiguration mit einem neuen Keystore und Truststore auf der Clusterebene definiert, darf keine SSL-Konfiguration auf der Serverebene definiert sein. Ist eine SSL-Konfiguration auf der Serverebene definiert, wird die SSL-Konfiguration auf der Clusterebene nicht verwendet; statt dessen wird die für den Server definierte Konfiguration verwendet.

Führen Sie die folgenden Schritte aus, um die SSL-Konfiguration für "bcgconsoleCluster" zu definieren:

1. Erstellen Sie einen Keystore für den Konsolencluster. Der Keystore muss im Bereich des Clusters "bcgconsole" erstellt werden. Rufen Sie hierzu die Option **Sicherheit > Verwaltung von SSL-Zertifikaten und Schlüsseln > Keystores und Zertifikate** auf.
2. Erstellen Sie einen Truststore für den Konsolencluster. Der Truststore muss im Bereich des Clusters "bcgconsole" erstellt werden. Rufen Sie hierzu die Option **Sicherheit > Verwaltung von SSL-Zertifikaten und Schlüsseln > Keystores und Zertifikate** auf.
3. Erstellen Sie eine SSL-Konfiguration im Bereich des Konsolenclusters, indem Sie **Sicherheit > Verwaltung von SSL-Zertifikaten und Schlüsseln > SSL-Konfigurationen** aufrufen. Definieren Sie den Keystore und den Truststore, die in den vorherigen Schritten erstellt wurden. Aktualisieren Sie die Aliasnamen des Zertifikats, indem Sie auf **Zertifikataliasnamen abrufen** klicken und den für die Serverauthentifizierung zu verwendenden gewünschten Aliasnamen auswählen. Legen Sie den Trust Manager auf **IbmPKIX** fest.
4. Legen Sie diese SSL-Konfiguration im Cluster "bcgconsoleCluster" fest, indem Sie die übernommene SSL-Konfiguration überschreiben. Aktualisieren Sie die Aliasnamen des Zertifikats, indem Sie auf **Zertifikataliasnamen aktualisieren** klicken und den für die Serverauthentifizierung zu verwendenden Aliasnamen festlegen.
5. Starten Sie "bcgconsoleCluster" neu.

Führen Sie die folgenden Schritte aus, um die SSL-Konfiguration für "bcgreceiverCluster" zu definieren:

1. Erstellen Sie einen Keystore für den Empfängercluster. Der Keystore muss im Bereich des Clusters "bcgreceiver" erstellt werden. Rufen Sie hierzu die Option **Sicherheit > Verwaltung von SSL-Zertifikaten und Schlüsseln > Keystores und Zertifikate** auf.
2. Erstellen Sie einen Truststore für den Empfängercluster. Der Truststore muss im Bereich des Clusters "bcgconsole" erstellt werden. Rufen Sie hierzu die Option **Sicherheit > Verwaltung von SSL-Zertifikaten und Schlüsseln > Keystores und Zertifikate** auf.
3. Erstellen Sie eine SSL-Konfiguration für den Empfängercluster im Bereich des Empfängerclusters, indem Sie **Sicherheit > Verwaltung von SSL-Zertifikaten und Schlüsseln > SSL-Konfigurationen** aufrufen und den Keystore und Truststore, die in den vorherigen Schritten erstellt wurden, definieren. Rufen Sie die Aliasnamen des Zertifikats ab, indem Sie auf **Zertifikataliasnamen abrufen** kli-

cken und den für die Serverauthentifizierung zu verwendenden gewünschten Aliasnamen auswählen. Legen Sie den Trust Manager auf **IbmPKIX** fest.

4. Legen Sie diese SSL-Konfiguration im Cluster "bcgreceiverCluster" fest, indem Sie die übernommene SSL-Konfiguration überschreiben. Aktualisieren Sie die Aliasnamen des Zertifikats, indem Sie auf **Zertifikataliasnamen aktualisieren** klicken und den für die Serverauthentifizierung zu verwendenden Aliasnamen festlegen.
5. Starten Sie den Cluster "bcgreceiverCluster" neu.

Weitere Informationen zur Arbeit mit Keystores, Truststores, der SSL-Konfiguration und Endpunktkonfigurationen finden Sie im Abschnitt *"Anwendungen und ihre Umgebung sichern" in der Dokumentation für WebSphere Application Server.*

**NodeDefaultTrustStore in NodeDefaultSSLSetting im verteilten Modus definieren:** Diese Definition muss für den einfachen verteilten Modus vorgenommen werden. Sollen im vollständig verteilten Modus gemeinsame Keystores und Truststores für den Empfänge und die Konsole verwendet werden, gilt dieses Verfahren auch für den vollständig verteilten Modus. Ist ein Knoten in eine Zelle eingebunden, werden die Unterzeichnerzertifikate dieses Knotens zum Truststore "CellDefaultTrustStore" hinzugefügt. Standardmäßig verweist "NodeDefaultSSLSetting" auf "CellDefaultTrustStore" als Truststore. Für den Empfänger und die Konsole in WebSphere Partner Gateway ist es möglicherweise nicht empfehlenswert, Unterzeichnerzertifikate anderer Knoten zu verwenden. Um einen dedizierten Truststore für die Knoten, in denen WebSphere Partner Gateway installiert ist, zu verwenden, kann "NodeDefaultTrustStore" in der Einstellung "NodeDefaultSSLSettings" als Truststore definiert werden.

Führen Sie die folgenden Schritte aus, um diese Änderung vorzunehmen:

1. Rufen Sie in der Administrationskonsole von WebSphere Application Server den Eintrag **Sicherheit > Verwaltung von SSL-Zertifikaten und Schlüsseln > Sicherheitskonfigurationen für Endpoints verwalten > <knotenname> > SSL-Konfigurationen > NodeDefaultSSLSettings** auf.
2. Wählen Sie im Feld **Name des Truststore** die Option **NodeDefaultTrustStore** aus.

   **Anmerkung:** Stellen Sie sicher, dass NodeDefaultTrustStore für den gewünschten Truststore (z. B. bcgSecurityTrust.jks) konfiguriert ist.
3. Klicken Sie auf **Anwenden**.
4. Klicken Sie auf der nächsten Seite der Konsole auf **Speichern**, um die Masterkonfiguration mit den Änderungen zu aktualisieren.
5. Starten Sie die Server in diesem Knoten neu.

**Anmerkung:** Im vollständig verteilten Modus müssen diese Änderungen für alle Knoten gemacht werden, die den Server "bcgreceiver" und "bcgconsole" enthalten. Im einfachen verteilten Modus müssen diese Änderungen für alle Knoten gemacht werden, die "bcgserver" enthalten.

**Unterzeichnerzertifikate zu trust.p12 hinzufügen, wenn "NodeDefaultTrustStore" für den Knoten mit WebSphere Partner Gateway-Servern definiert ist:** Momentan bezieht sich "NodeDefaultTrustStore" auf "trust.p12". Ist "NodeDefaultTrustStore" für den Knoten definiert, der die WebSphere Partner Gateway-Server enthält, wird "bcgSecurityTrust.jks" nicht verwendet. Falls erforderlich, müssen Unterzeichnerzertifikate von "bcgSecurityTrust.jks" zu "trust.p12" hinzugefügt werden.

## Ausgehende SSL-Zertifikate konfigurieren

Wenn WebSphere Partner Gateway ein Dokument an einen Partner sendet, ist dies eine ausgehende Anforderung. Wenn Ihre Community SSL nicht verwendet, benötigen Sie kein eingehendes oder ausgehendes SSL-Zertifikat.

### Schritt 1: Server authentifizieren

Wenn SSL zum Senden der ausgehenden Dokumente an Ihre Partner verwendet wird, fordert WebSphere Partner Gateway ein serverseitiges Zertifikat von den Partnern an. Dasselbe CA-Zertifikat kann für mehrere Partner verwendet werden. Das Zertifikat muss im Format 'X.509-DER' vorliegen.

**Anmerkung:** Sie können das Format mit dem Dienstprogramm iKeyman konvertieren. Befolgen Sie diese Schritte, um das Format zu konvertieren:

1. Starten Sie das Dienstprogramm iKeyman.
2. Erstellen Sie einen neuen leeren Keystore, oder öffnen Sie einen vorhandenen Keystore.
3. Wählen Sie in **Key Database Content** die Option **Signer Certificates** aus.
4. Fügen Sie das ARM-Zertifikat mit der Option **Add** hinzu.
5. Extrahieren Sie dasselbe Zertifikat als Binary-DER-Daten mit der Option **Extract**.
6. Schließen Sie das Dienstprogramm iKeyman.

Installieren Sie das selbst signierte Zertifikat des Partners im Profil des Hubbetreibers. Wenn das Zertifikat von einer Zertifizierungsstelle unterzeichnet wurde und das Rootzertifikat der Zertifizierungsstelle und alle anderen Zertifikate, die Teil der Zertifikatskette sind, noch nicht im Profil des Hubbetreibers installiert sind, installieren Sie die Zertifikate jetzt im Profil des Hubbetreibers.

1. Klicken Sie auf **Kontenadmin > Profile > Zertifikate**, um die Seite **Zertifikatliste** anzuzeigen.

   Stellen Sie sicher, dass Sie an Community Console als Hubbetreiber oder interner Partner angemeldet sind.
2. Klicken Sie auf **PKCS12 laden**.

   **Anmerkung:** Die PKCS12-Datei, die hochgeladen wird, sollte nur einen privaten Schlüssel und das zugeordnete Zertifikat enthalten. Sie können das Zertifikat und den PKCS#8-formatierten privaten Schlüssel auch separat hochladen.
3. Wählen Sie **SSL-Client** als Zertifikattyp aus.
4. Geben Sie eine Beschreibung des Zertifikats ein, welches erforderlich ist.
5. Ändern Sie den Status in **Aktiviert**.
6. Klicken Sie auf **Durchsuchen** und navigieren Sie zum Verzeichnis, in dem Sie das Zertifikat gespeichert haben.
7. Wählen Sie das Zertifikat aus und klicken Sie auf **Öffnen**.
8. Geben Sie das Kennwort ein.
9. Wenn Sie einen anderen Betriebsmodus als **Produktion** (Standardeinstellung) auswählen wollen, wählen Sie ihn in der Liste aus.
10. Wenn Sie über zwei SSL-Zertifikate verfügen, geben Sie an, welches von ihnen das primäre bzw. das sekundäre Zertifikat ist, indem Sie **Primär** oder **Sekundär** in der Liste **Zertifikatverwendung** auswählen.
11. Klicken Sie auf **Hochladen** und dann auf **Speichern**.

**Anmerkung:** Sie müssen die vorherigen Schritte nicht ausführen, wenn das Zertifikat der Zertifizierungsstelle bereits installiert ist.

## Schritt 2: Clients authentifizieren

Wenn SSL-Clientauthentifizierung erforderlich ist, wird der Partner seinerseits ein Zertifikat vom Hub anfordern. Importieren Sie mit Community Console Ihr Zertifikat in WebSphere Partner Gateway. Sie können das Zertifikat mit iKeyman generieren. Wenn das Zertifikat ein selbst signiertes Zertifikat ist, muss es dem Partner zur Verfügung gestellt werden. Wenn es ein von einer Zertifizierungsstelle signiertes Zertifikat ist, muss das CA-Rootzertifikat an die Partner übergegeben werden, sodass diese es ihren vertrauenswürdigen Zertifikaten hinzufügen können.

Sie können über mehr als ein SSL-Zertifikat verfügen. Eines ist das primäre Zertifikat, welches standardmäßig verwendet wird. Das andere Zertifikat ist das sekundäre Zertifikat, welches verwendet wird, wenn das primäre Zertifikat abgelaufen ist.

**Selbst signiertes Zertifikat verwenden:**

Wenn Sie ein selbst signiertes Zertifikat verwenden möchten, gehen Sie wie folgt vor:

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 Partner. Die bevorzugte Verteilungsmethode ist das Senden des Zertifikats in einer kennwortgeschützten komprimierten Datei per E-Mail. Ihre Partner müssen sich an Sie wenden und das Kennwort für die komprimierte Datei anfordern.
5. Verwenden Sie iKeyman, um das selbst signierte Zertifikat und das private Schlüsselpaar in Form einer PKCS12-Datei zu exportieren.
6. Installieren Sie das selbst unterzeichnete Zertifikat und den Schlüssel über Community Console.
   a. Klicken Sie auf **Kontenadmin > Profile > Zertifikate**, um die Seite **Zertifikatliste** anzuzeigen.

      Stellen Sie sicher, dass Sie an Community Console als Hubbetreiber angemeldet sind.
   b. Klicken Sie auf **PKCS12 laden**.

      **Anmerkung:** Die PKCS12-Datei, die hochgeladen wird, sollte nur einen privaten Schlüssel und das zugeordnete Zertifikat enthalten. Sie können das Zertifikat und den PKCS#8-formatierten privaten Schlüssel auch separat hochladen.
   c. Wählen Sie **SSL-Client** als Zertifikattyp aus.
   d. Geben Sie eine Beschreibung des Zertifikats ein, welches erforderlich ist.
   e. Ändern Sie den Status in **Aktiviert**.
   f. Klicken Sie auf **Durchsuchen** und navigieren Sie zum Verzeichnis, in dem Sie das Zertifikat gespeichert haben.
   g. Wählen Sie das Zertifikat aus und klicken Sie auf **Öffnen**.
   h. Geben Sie das Kennwort ein.

i. Wenn Sie einen anderen Betriebsmodus als **Produktion** (Standardeinstellung) auswählen wollen, wählen Sie ihn in der Liste aus.
j. Wenn Sie über zwei SSL-Zertifikate verfügen, geben Sie an, welches von ihnen das primäre bzw. das sekundäre Zertifikat ist, indem Sie **Primär** oder **Sekundär** in der Liste **Zertifikatverwendung** auswählen.
k. Klicken Sie auf **Hochladen** und dann auf **Speichern**.

Wenn Sie primäre und sekundäre Zertifikate für die SSL-Clientauthentifizierung und die digitale Signatur hochladen und Sie die primären Zertifikate als zwei separate Einträge hochladen, stellen Sie sicher, dass die entsprechenden sekundären Zertifikate als zwei unterschiedliche Einträge hochgeladen werden.

**Von Zertifizierungsstelle signiertes Zertifikat verwenden:**

Wenn Sie ein von einer Zertifizierungsstelle signiertes Zertifikat verwenden, gehen Sie wie folgt vor:

1. Generieren Sie mit iKeyman eine Zertifikatsanforderung und ein Schlüsselpaar für den Empfänger.
2. Übergeben Sie eine Zertifikatsunterzeichungsanforderung (CSR - Certificate Signing Request) an eine Zertifizierungsstelle.
3. Wenn Sie das unterzeichnete Zertifikat von der Zertifizierungsstelle empfangen, stellen Sie das unterzeichnete Zertifikat mit iKeyman in den Keystore.
4. Verteilen Sie das signierte CA-Zertifikat an alle Partner.

## Zertifikatswiderrufsliste hinzufügen

WebSphere Partner Gateway enthält eine CRL-Funktion (CRL - Certificate Revocation List - Zertifikatswiderrufsliste). Die CRL, die von einer Zertifizierungsstelle ausgestellt wird, gibt Partner an, die Zertifikate vor ihrem terminierten Ablaufdatum widerrufen haben. Partnern mit widerrufenen Zertifikaten wird der Zugriff auf WebSphere Partner Gateway verweigert.

Jedes widerrufene Zertifikat wird in einer CRL durch seine fortlaufende Zertifikatsnummer angegeben. Document Manager durchsucht die CRL alle 60 Sekunden und lehnt ein Zertifikat ab, wenn es in der CRL-Liste enthalten ist. Sie können das Zeitintervall, in dem das CRL-Verzeichnis durchsucht wird, konfigurieren. Das Zeitintervall wird in der Konfigurationseigenschaft bcg.rosettanet.encrypt.CertDbRefreshInterval angegeben.

CRLs werden standardmäßig an der folgenden Position gespeichert: /<*gemeinsames_datenverzeichnis*>/security/crl. WebSphere Partner Gateway verwendet die Einstellung bcg.CRLDir in **Konsole > Systemverwaltung > DocMgr-Verwaltung > Sicherheit**, um die Position des CRL-Verzeichnisses anzugeben.

Speichern Sie die Zertifikatswiderrufslisten im CRL-Verzeichnis.

## CRL-DP konfigurieren

Zum Konfigurieren des CRL-DP (Certificate Revocation List Distribution Point - Verteilungspunkt der Zertifikatswiderrufsliste) müssen die Java Virtual Machine-Einstellungen geändert werden, d. h. der Wert von "-Dcom.ibm.security.enableCRLDP" muss auf "true" (wahr) gesetzt werden.

Im vollständig verteilten Modus muss diese Einstellung für "bcgdocmgr", "bcgreceiver" und "bcgconsole" vorgenommen werden. Im einfachen verteilten Modus und im einfachen Modus muss diese Einstellung für "bcgserver" vorgenommen werden.

Führen Sie die folgenden Schritte aus:

1. Melden Sie sich an der Administrationskonsole von WebSphere Application Server an.
2. Navigieren Sie zu **Server > Anwendungsserver** und wählen Sie **Server** aus.
3. Legen Sie die Eigenschaft wie folgt fest:
   a. Wählen Sie den Server aus (bcgdocmgr, bcgreceiver oder bcgconsole).
   b. Erweitern Sie auf der Konfigurationsseite im Bereich für die Serverinfrastruktur die Option **Java- und Prozessverwaltung** und wählen Sie **Prozessdefinition** aus.
   c. Wählen Sie auf der Seite für die Konfiguration der Prozessdefinition im Abschnitt mit den weiteren Eigenschaften die Option **Java Virtual Machine** aus.
   d. Fügen Sie dem (gegebenenfalls) vorhandenen Wert im Feld für generische JVM-Argumente Folgendes hinzu: -Dcom.ibm.security.enableCRLDP=true.
4. Klicken Sie auf **Anwenden** und danach auf **Speichern**, um die Konfiguration abzuschließen.
5. Starten Sie den Server neu.
6. Legen Sie diese Eigenschaft für alle Server im Cluster fest.

## Eingangs-SSL für Community Console und Empfängerkomponente konfigurieren

Die WebSphere Partner Gateway-Keystores sind in WebSphere Application Server vorkonfiguriert. Dieser Abschnitt gilt nur, wenn Sie verschiedene Keystores verwenden.

Verwenden Sie die folgende Prozedur, um SSL für Community Console und die Empfängerkomponente in WebSphere Partner Gateway zu konfigurieren.

1. Rufen Sie die folgenden Informationen ab:
   - Die vollständigen Pfadnamen der Schlüsseldatei und der Anerkennungsdatei für z. B. den Empfänger: <*Produktverz*>/common/security/keystore/bcgSecurity.jks und <*Produktverz*>/common/security/keystore/bcgSecurityTrust.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, JCEKS oder PKCS12. Geben Sie diesen Wert in Großbuchstaben genau wie angezeigt ein.
   - Der Pfad zur Scriptdatei namens 'bcgssl.jacl'.
2. Öffnen Sie ein Community Console-Fenster und wechseln Sie in das Verzeichnis /<*Produktverz*>/bin. Der Server muss zum Ändern der Kennwörter nicht aktiv sein.
3. Geben Sie den folgenden Befehl ein und ersetzen Sie die Werte, die in <> eingeschlossen sind. Alle Werte müssen eingegeben werden.

```
./bcgwsadmin.sh -f /<Produktverz>/
scripts/bcgssl.jacl -conntype NONE install
<schlüsseldatei_pfadname>
<schlüsseldatei_kennwort> <schlüsseldatei_format> <trust-datei_pfadname>
<trust-dateikennwort> <trust-dateiformat>
```

4. Starten Sie den Server. Wenn der Start des Servers fehlschlägt, könnte es an einem Fehler bei der Ausführung von 'bcgssl.jacl' liegen. Wenn Sie einen Fehler machen, können Sie das Script erneut ausführen, um ihn zu beheben.
5. Wenn Sie 'bcgClientAuth.jacl' verwendet haben, um das SSL-Merkmal **clientAuthentication** zu konfigurieren, setzen Sie es nach Verwendung von 'bcgssl.jacl' zurück. Dies liegt daran, dass 'bcgssl.jacl' jeden Wert, der für **clientAuthentication** gesetzt worden ist, mit dem Wert **false** überschreibt.

**Anmerkung:**

1. Wiederholen Sie diese Schritte für die Konsole und ersetzen Sie dabei den Eintrag **receiver** im Pfadnamen durch **console**.
2. Die Konfiguration für SSL, Keystore und Truststore kann auch über die Administrationskonsole von WebSphere Application Server erfolgen.

Standardmäßig unterstützt WebSphere Partner Gateway einen Keystore und Truststore für den Empfänger und die Konsole. Im vollständig verteilten Modus können Sie jedoch separate Keystores und Truststores für den Empfänger und die Konsole verwenden. Führen Sie die folgenden Konfigurationsschritte über die Administrationskonsole von WebSphere Application Server für den Empfänger aus, um separate Keystores und Truststores für den Empfänger und die Konsole zu verwenden:

1. Erstellen Sie einen Keystore für den Empfänger-Keystore. Weitere Informationen hierzu finden Sie im Abschnitt "Eine Keystore-Konfiguration erstellen" in der Dokumentation zu WebSphere Application Server.
2. Erstellen Sie einen Truststore für den Empfänger-Truststore. Weitere Informationen finden Sie im Abschnitt <*Eine Keystore-Konfiguration erstellen* im Dokument <*Anwendungen und ihre Umgebung sichern* für WebSphere Application Server.
3. Erstellen Sie eine SSL-Konfiguration für den Empfänger und definieren Sie den oben erstellten Keystore und Truststore in dieser Konfiguration. Wählen Sie den erforderlichen Aliasnamen aus, der für die Serverauthentifizierung im Keystore verwendet werden soll. Legen Sie den Trust Manager auf **IbmPKIX** fest. Weitere Informationen finden Sie im Abschnitt "SSL-Konfiguration erstellen" im Dokument *Anwendungen und ihre Umgebung sichern* für WebSphere Application Server.
4. Legen Sie diese SSL-Konfiguration in jedem Server "bcgreceiver" fest, indem Sie die übernommene SSL-Konfiguration überschreiben. Legen Sie den für die Serverauthentifizierung zu verwendenden Aliasnamen fest.
5. Starten Sie jeden Server "bcgreceiver" neu.

Die Schritte für die Konfiguration der Konsole sind ähnlich. Weitere Informationen finden Sie in den entsprechenden Abschnitten im Dokument *Anwendungen und ihre Umgebung sichern* für WebSphere Application Server.

1. Erstellen Sie einen Keystore für den Konsolen-Keystore.
2. Erstellen Sie einen Truststore für den Konsolen-Truststore.
3. Erstellen Sie eine SSL-Konfiguration für die Konsole und definieren Sie den oben erstellten Keystore und Truststore in dieser Konfiguration. Wählen Sie den erforderlichen Aliasnamen aus, der für die Serverauthentifizierung im Keystore verwendet werden soll. Legen Sie den Trust Manager auf **IbmPKIX** fest.

4. Legen Sie diese SSL-Konfiguration in jedem Server "bcgconsole" fest, indem Sie die übernommene SSL-Konfiguration überschreiben. Legen Sie den für die Serverauthentifizierung zu verwendenden Aliasnamen fest.
5. Starten Sie jeden Server "bcgconsole" neu.

Weitere Informationen zur Arbeit mit Keystores, Truststores, der SSL-Konfiguration und Endpunktkonfigurationen finden Sie im Dokument *Anwendungen und ihre Umgebung sichern* für WebSphere Application Server.

**Anmerkung:** Momentan bezieht sich "NodeDefaultTrustStore" auf "trust.p12". Ist "NodeDefaultTrustStore" für den Knoten "bcg" definiert, wird "bcgSecurityTrust.jks" nicht verwendet. Falls erforderlich, müssen Sie Unterzeichnerzertifikate von "bcgSecurityTrust.jks" zu "trust.p12" hinzufügen.

## Zertifikate mit dem Assistenten hochladen

Als Hubbetreiber können Sie Zertifikate für interne oder externe Partner hochladen. Gehen Sie dazu wie folgt vor:

- Laden Sie den privaten Schlüssel und die Zertifikate für die internen Partner hoch.
- Laden Sie die öffentlichen Zertifikate für die externen Partner hoch.
- Laden Sie das Root CA- und das Intermediate CA-Zertifikat hoch.

  **Wichtig:** Diese Funktionalität ist nur für X.509-Zertifikate verfügbar.
- Laden Sie eine Zertifikatskette von einem Truststore hoch.

  **Wichtig:** Diese Funktionalität ist nur für X.509-Zertifikate verfügbar.

Es wird ein Assistent zum Hochladen von Zertifikaten bereitgestellt, der Sie beim Hochladen der Zertifikate unterstützt. Wenn Sie den Assistenten verwenden, können Sie die Verwendung des Zertifikats festlegen (Signatur, Prüfung, Verschlüsselung, Entschlüsselung, SSL-Client, FTPS-Server oder SFTP-Server), das Zertifikat einem oder mehreren Betriebsmodi zuordnen, das Zertifikat zu einer (vorhandenen oder neu erstellten) Gruppe hinzufügen, das Zertifikat als Standard für alle Partnerverbindungen auswählen oder eine bestimmte Verbindung auswählen, für die diese Zertifikatsgruppe verwendet werden soll. Die Option zum Zuordnen des Zertifikats zu einer Verbindung wird nicht angezeigt, wenn das Zertifikat keiner Gruppe zugeordnet ist. Wenn Sie das Zertifikat hochladen, müssen Sie sicherstellen, dass das Zertifikat nicht abgelaufen ist.

Für OpenPGP kann auch eine Paketdatei mit einem öffentlichen Schlüssel verwendet werden, um den öffentlichen Schlüssel und das Zertifikat an einen externen Partner hochzuladen. Der externe Partner kann den Schlüssel aus dem Schlüsselring exportieren, ihn in einer Datei speichern und ihn an den Hubbetreiber senden. Der Hubbetreiber kann das vom externen Partner empfangene Zertifikat hochladen. Die Datei für den öffentlichen Schlüssel kann im Binärformat oder im ASCII-Armor-Format vorliegen.

Führen Sie die folgenden Schritte aus, um Zertifikate für interne oder externe Partner mithilfe des Assistenten hochzuladen:

1. Wählen Sie den Partner aus und klicken Sie auf **Kontenadmin** > **Profile** > **Zertifikate**.
2. Klicken Sie auf **Zertifikat laden**.

3. Geben Sie auf der Seite zum Auswählen des Partners, der Dateiposition und des Kennworts die folgenden Werte ein:
   - **Partner für das Zertifikat:** Wählen Sie den Partner aus, der dem neu hochgeladenen Zertifikat zugeordnet werden soll. Klicken Sie auf **Suchen**, um einen bestimmten Partner oder eine Untergruppe von Partnern zu suchen. Ist der Partner der Hubbetreiber oder der interne Partner, müssen Sie die Position des Zertifikats, die Position des privaten Schlüssels und das Kennwort angeben *oder* den Truststore (Zertifikatsspeicher für vertrauenswürdige Zertifikate) oder Keystore (Schlüsselspeicher) mit dem entsprechenden Kennwort angeben. Für externe Partner müssen Sie die Position des Zertifikats *oder* die Position des Truststore, der die Zertifikatskette enthält, angeben.

     **Anmerkung:** Wenn Sie auf **Zertifikat laden** klicken, ohne ein Partnerprofil auszuwählen, wird das Feld **Partner für das Zertifikat** nicht angezeigt. Das Zertifikat wird automatisch für das ausgewählte Partnerprofil hochgeladen.
   - **Root- und Intermediate-Zertifikat:** Wählen Sie dieses Kontrollkästchen aus, wenn das Zertifikat ein Root- und Intermediate-Zertifikat ist.

     **Anmerkung:** Der Zertifikatstyp **Root und Intermediate** ist nur für das Hubadministratorprofil anwendbar. Daher wird das Kontrollkästchen **Root und Intermediate** nur angezeigt, wenn der ausgewählte Partner der Hubadministrator ist. Darüber hinaus wird das Kontrollkästchen **Root und Intermediate** nur angezeigt, wenn Sie **Zertifikat laden** ausgewählt haben.
   - **Position des Zertifikats:** Klicken Sie auf **Durchsuchen**, um die Position des Zertifikats (öffentlich/privat) auszuwählen.
   - **Privater Schlüssel:** Klicken Sie auf **Durchsuchen**, um den privaten Schlüssel des Zertifikats auszuwählen.

     **Anmerkung:** Dies gilt nur für einen internen Partner.
   - **Kennwort:** Geben Sie das Kennwort ein, wenn das Zertifikat über ein Kennwort verfügt.
   - **Position des Truststore, Keystore oder Schlüsselrings:** Klicken Sie auf **Durchsuchen**, um die Position des Truststore, des Keystore oder des Schlüsselrings auszuwählen. Ein Truststore ist eine Datei, die eine Sammlung vertrauenswürdiger CA- und Stammzertifikate enthält. Ein Keystore ist eine Sammlung von privaten Schlüsseln und den ihnen zugeordneten Trusted-Root-und CA-Zertifikaten. Ein Schlüsselring ist eine Sammlung von Zertifikaten im OpenPGP-Format. Klicken Sie auf **Durchsuchen**, um die Datei im Pfad des Dialogs für die Datei des Schlüsselrings oder des Keystore oder des Truststore auszuwählen, oder geben Sie den Pfad im Textfeld ein. Wenn Sie ein Zertifikat des Typs 'OpenPGP-Schlüsselring' für einen internen Partner hochladen, müssen Sie den Pfad der geheimen Schlüsselringdatei angeben. Geben Sie für den externen Partner den Pfad der öffentlichen Schlüsselringdatei an.
   - **Kennwort:** Geben Sie das Kennwort ein, wenn die Position des Truststore oder des Keystore über ein Kennwort verfügt. Für einen Schlüsselring ist kein Kennwort erforderlich.
   - **Typ:** Wählen Sie den Typ für den Truststore, den Keystore oder den Schlüsselring aus. Die folgenden Werte sind in der Liste verfügbar: JKS, JCEKS, PKCS12 und OpenPGP.
4. Klicken Sie auf **Weiter**.

5. Die Seite **Endentitäts- und CA-Zertifikat** des Assistenten wird geöffnet, wenn Sie Zertifikate über einen Truststore laden, der mehrere Zertifikate enthält. Die Liste der im Truststore verfügbaren Zertifikate wird angezeigt. Die Seite **Wählen Sie die hochzuladenden OpenPGP-Schlüssel bzw. Zertifizierungen aus** wird angezeigt, wenn Sie auf der Seite zum Auswählen des Partners, der Dateiposition und des Kennworts im Assistenten einen Schlüsselring des Typs OpenPGP auswählen.
   - Wählen Sie auf der Seite **Hochzuladendes Endentitätszertifikat** des Assistenten ein Zertifikat aus. Wenn der Keystore mehrere private Schlüssel enthält, müssen Sie zusätzlich zu dem privaten Schlüssel ein Kennwort für den Schlüssel eingeben, wenn sich das Kennwort vom Schlüssel unterscheidet. Geben Sie auf der Seite **Endentitäts- und CA-Zertifikat** die folgenden Werte ein:
     – **Der Keystore enthält mehrere Endentitätszertifikate. Wählen Sie das hochzuladende Zertifikat aus.** - Dieses Feld enthält eine Liste aller Endentitätszertifikate. Wählen Sie das hochzuladende Zertifikat aus.
     – **Kennwort** - Verfügt der Keystore über ein Kennwort, wählen Sie dieses Kontrollkästchen aus und geben Sie das Kennwort im Textfeld ein.
     – **Wählen Sie die Liste der hochzuladenden Root-CA und Intermediate-CA-Zertifikate aus** - Wählen Sie im Listenfenster die hochzuladenden Root CA- und Intermediate CA-Zertifikate aus.
   - Auf der Seite **Wählen Sie die hochzuladenden OpenPGP-Schlüssel bzw. Zertifizierungen aus** des Assistenten werden die Zertifikate, die dem ausgewählten Schlüsselring zugeordnet sind, in der Liste angezeigt.

     **Anmerkung:** Sie können auf **Details anzeigen** klicken, um die Details des ausgewählten Zertifikats anzuzeigen. Ist bei einem Zertifikat die Schlüssel-ID und die Aussteller-ID identisch, handelt es sich bei dem Zertifikat um ein Eigenzertifikat.
     – Wählen Sie in der Liste einen Schlüssel der höchsten Ebene aus.
     – Geben Sie das Kennwort für den Schlüssel der höchsten Ebene ein, wenn Sie diesen Schlüssel hochladen wollen.

       **Anmerkung:** Wenn der Schlüssel der höchsten Ebene Unterschlüssel enthält, werden alle Unterschlüssel in der Liste **Wählen Sie den hochzuladenden Unterschlüssel aus** angezeigt.

       **Wichtig:** Dies gilt nicht, wenn Sie öffentliche Zertifikate zur Verschlüsselung laden.
     – Wählen Sie gegebenenfalls den Unterschlüssel aus.
     – Geben Sie das Kennwort des Unterschlüssels ein.

     **Wichtig:** Dies gilt nicht, wenn Sie öffentliche Zertifikate zur Verschlüsselung laden.

     **Hinweis:** Wenn Sie das Zertifikat für einen externen Partner hochladen, ist kein Kennwort für den Schlüssel der höchsten Ebene und den Unterschlüssel erforderlich.
6. Klicken Sie auf **Weiter**, um mit der Seite **Zertifikatsdetails** des Assistenten fortzufahren.
7. Geben Sie auf der Seite **Zertifikatsdetails** des Assistenten die folgenden Details des Zertifikats ein:

- **Name des Leaf-Zertifikats** - Der Name des Leaf-Zertifikats (nicht hierarchisches Zertifikat). Der Name des Felds ist davon abhängig, ob es sich bei dem Zertifikat um ein Leaf-Zertifikat ein Root CA-Zertifikat (Zertifikat der Stammzertifizierungsstelle) oder ein Intermediate CA-Zertifikat (Zertifikat einer Zwischenzertifizierungsstelle) handelt.
- **Beschreibung** - Die Beschreibung des Leaf-Zertifikats.
- **Zertifikat für FTP-Server-Authentifizierung** - Wählen Sie dieses Kontrollkästchen aus, wenn das hochgeladene Zertifikat zur Authentifizierung des FTP-Servers verwendet wird.
- **Zertifikat für SFTP-Server-Authentifizierung** - Wählen Sie dieses Kontrollkästchen aus, wenn das hochgeladene Zertifikat zur Authentifizierung des SFTP-Servers verwendet wird.

  **Wichtig:** Die FTP- und SFTP-Serverauthentifizierung gilt nicht für OpenPGP-Zertifikate.
- **Zertifikatstyp** - Ordnen Sie dieses Zertifikat einem Zertifikatstyp zu. Die folgenden Typen werden unterstützt: Digitale Signatur, Prüfung der digitalen Signatur, Verschlüsselung, Entschlüsselung, SSL-Server und SSL-Client.

  **Hinweis:**
  - Der Typ "Verschlüsselung" gilt für einen externen Partner; der Typ "Entschlüsselung" gilt für einen internen Partner.
  - Der Typ "SSL-Client" wird für OpenPGP-Zertifikate nicht unterstützt.
- **Zertifikatverwendung** - Ordnen Sie dem Zertifikat eine Verwendung zu. Die zulässigen Werte sind **Primär** und **Sekundär**.

  **Wichtig:** Dieses Attribut gilt nicht für Zertifikate des Typs "Entschlüsselung", "Prüfung der digitalen Signatur" und "SSL-Server".
- **Betriebsmodus** - Wählen Sie einen Betriebsmodus für Zertifikate des Typs "Verschlüsselung", "Digitale Signatur" und "SSL-Client" aus.

  **Wichtig:** Der Betriebsmodus gilt nicht für Zertifikate des Typs "Verschlüsselung" und "Prüfung der digitalen Signatur".
- **Status** - Wählen Sie **Aktiviert** oder **Inaktiviert** aus, abhängig davon, ob das Zertifikat nach dem Hochladen aktiviert oder inaktiviert werden soll. Die Schaltfläche **Weiter** ist nur aktiviert, wenn das Zertifikat aktiviert ist.
- **Gruppenverwaltung** - Sie können das Zertifikat einer vorhandenen Gruppe zuordnen oder eine neue Gruppe erstellen. Ist das Zertifikat ein sekundäres Zertifikat, kann es nur einer vorhandenen Gruppe zugeordnet werden. Für einen internen Partner mit dem Typ "encrypt" oder für einen externen Partner mit dem Typ "SSL" (Incoming client auth) oder "Signing" (Verify) können Sie das Zertifikat einer beliebigen Gruppe zuordnen.

  **Anmerkung:** Wird ein OpenPGP-Zertifikat für einen internen Partner hochgeladen, ist die Gruppenverwaltung nicht anwendbar. Beim Typ "Verschlüsselung" für einen externen Partner oder beim Typ "Digitale Signatur" oder "SSL-Client" für einen internen Partner können Sie die Option **Neue Gruppe hinzufügen** oder **Vorhandene Gruppe aktualisieren** auswählen. Dies ist nur anwendbar, wenn Sie Gruppen verwenden. Klicken Sie ansonsten auf **Fertigstellen**.

8. Klicken Sie auf **Weiter**, um mit der Seite **Gruppe** des Assistenten fortzufahren. Wenn es sich um ein primäres Zertifikat handelt, müssen Sie keine Gruppen erstellen und das Zertifikat einer Gruppe und einer Partnerverbindung zuord-

nen. Wenn Sie das Kontrollkästchen **Neue Gruppe erstellen** ausgewählt haben, wird die Seite **Neue Gruppe erstellen** des Assistenten geöffnet. Andernfalls wird die Seite **Zu vorhandener Gruppe hinzufügen** des Assistenten geöffnet. Wenn die Datei einen privaten Schlüssel des internen Partners oder das für SSL bzw. die digitale Signatur verwendete öffentliche Zertifikat des externen Partners enthält, können Sie auf **Fertigstellen** klicken.

**Wichtig:** Der Übergang von einem sekundären zu einem primären Zertifikat wird bei OpenPGP-Zertifikaten nicht unterstützt.

9. Geben Sie auf der Seite **Neue Gruppe erstellen** des Assistenten die Details für die neue Gruppe ein. Für primäre Zertifikate müssen Sie keine Gruppen erstellen und ihnen ein Zertifikat zuordnen. Geben Sie die folgenden Werte ein:
   - **Gruppenname** - Der Name der Gruppe.
   - **Beschreibung** - Die Beschreibung der Gruppe.
   - **Status** - Wählen Sie "Aktiviert" oder "Inaktiviert" aus. Ist die Gruppe inaktiviert, ist die Schaltfläche **Weiter** nicht aktiviert.
   - **Als Standardeinstellung** - Wählen Sie dieses Kontrollkästchen aus, wenn Sie diese Gruppe als Standardgruppe festlegen wollen.
10. Wählen Sie auf der Seite **Zu vorhandener Gruppe hinzufügen** des Assistenten die Gruppe oder Gruppen aus, zu der bzw. denen das Zertifikat hinzugefügt werden soll. Geben Sie die folgenden Werte ein:
    - **Wählen Sie die Gruppe für den ausgewählten Zertifikatstyp aus** - Wählen Sie die Gruppe oder Gruppen aus, zu der bzw. denen das Zertifikat hinzugefügt werden soll.
    - **Als Standardeinstellung** - Wählen Sie dieses Kontrollkästchen aus, wenn Sie diese Gruppe als Standardgruppe festlegen wollen.
11. Klicken Sie auf der Seite **Neue Gruppe erstellen** oder **Zu vorhandener Gruppe hinzufügen** auf **Weiter**, um mit der Seite **Standardeinstellungen** des Assistenten fortzufahren. Die Schaltfläche **Weiter** ist nur aktiviert, wenn der Status der Gruppe **aktiviert** ist.
12. Wählen Sie im Feld **Status** die Option **aktiviert** oder **inaktiviert** aus, abhängig davon, ob das Zertifikat nach dem Hochladen aktiviert oder inaktiviert werden soll.

    **Anmerkung:** Wenn Sie auf der vorherigen Seite (**Neue Gruppe erstellen** oder **Zu vorhandener Gruppe hinzufügen**) das Kontrollkästchen **Als Standardeinstellung** ausgewählt haben, müssen Sie die Gruppe einem Betriebsmodus zuordnen. In diesem Fall werden Zertifikatverwendungen für Betriebsmodi angezeigt. Für interne Partner wird die Verschlüsselung inaktiviert. Für externe Partner werden SSL (Clientauthentifizierung) und die digitale Signatur inaktiviert.
13. Klicken Sie auf **Weiter**, um mit der Seite **Konfiguration** des Assistenten fortzufahren. Wenn Sie auf **Fertigstellen** klicken und weiterhin Root CA- oder Intermediate CA-Zertifikate fehlen, werden Sie aufgefordert, diese hochzuladen. Wenn Sie im Fenster mit der Eingabeaufforderung auf **Ja** klicken, wird die erste Seite des Assistenten geöffnet. Klicken Sie auf **Abbrechen**, wenn Sie die Zertifikate später hochladen wollen.
14. Geben Sie auf der Seite **Konfiguration** des Assistenten die folgenden Werte ein:

**Anmerkung:** Auf der Seite **Konfiguration** wird eine Liste mit Zertifikaten bzw. Zertifikatsgruppen für Betriebsmodi angezeigt. Der Name der aktuellen Gruppe ist für alle Gruppen im Voraus ausgefüllt; er kann jedoch geändert werden.

- **Absenderpartner** - Dieses Feld wird mit dem Wert des internen Partners im Voraus ausgefüllt.
- **Empfängerpartner** - Diese Liste ist mit der Liste aller externen Partner im Voraus ausgefüllt. Sie können auch den Wert **Alle** auswählen, um alle externen Partner einzuschließen.
- **Absenderpaket** - Wählen Sie in der Liste die Paketobjekte der Dokumentenflussdefinition des internen Partners aus.
- **Empfängerpaket** - Wählen Sie in der Liste die Paketobjekte der Dokumentenflussdefinition des externen Partners aus.

15. Klicken Sie auf **Weitere Verbindungen hinzufügen**, wenn Sie die Gruppe anderen Partnerverbindungen zuordnen wollen.
16. Klicken Sie auf **Sekundäres Zertifikat hinzufügen**, um ein sekundäres Zertifikat zur aktuellen Gruppe hinzuzufügen.
17. Klicken Sie auf **Fertigstellen**, um das Zertifikat hochzuladen. Wenn weiterhin Root CA- oder Intermediate CA-Zertifikate fehlen, werden Sie aufgefordert, diese hochzuladen. Wenn Sie im Fenster mit der Eingabeaufforderung auf **Ja** klicken, wird die erste Seite des Assistenten geöffnet. Klicken Sie in der Eingabeaufforderung auf **Abbrechen**, wenn Sie die Zertifikate später hochladen wollen.

**Anmerkung:** Schlägt bei OpenPGP das Hochladen eines Zertifikats fehl, obwohl das korrekte Zertifikat geladen wurde, müssen Sie den Server neu starten.

## Zertifikatsgruppen erstellen

Für die folgenden Sicherheitsfunktionen wurden Zertifikatsgruppen eingeführt:

- SSL-Clientauthentifizierung für ausgehende (outbound) Nachrichten von einem internen Partner zu einem externen Partner.
- Hinzufügen einer digitalen Signatur zu ausgehenden Nachrichten von einem internen Partner zu einem externen Partner.
- Verschlüsseln ausgehender Nachrichten von einem internen Partner zu einem externen Partner.
- Gruppen werden für eingehende (inbound) Szenarios nicht verwendet. Solche Szenarios sind beispielsweise das Überprüfen des Zertifikats für die SSL-Clientauthentifizierung des externen Partners im WebSphere Partner Gateway-Truststore, das Überprüfen der digitalen Signatur des externen Partners oder das Entschlüsseln verschlüsselter Nachrichten an den internen Partner.

Gehen Sie wie folgt vor, um eine neue Zertifikatsgruppe zu erstellen:

1. Navigieren Sie in der Konsole zu **Profil** > **Partner** > **Zertifikatliste** > **Liste der Zertifikatsgruppen** > **Gruppe erstellen**.
2. Klicken Sie auf **Zertifikat > Zertifikatsgruppen > Gruppe erstellen**.
3. Geben Sie den **Gruppennamen** und die **Beschreibung** für die neue Zertifikatsgruppe ein.
4. Legen Sie den **Zertifikatstyp** fest.
5. Wählen Sie das Kotrollkästchen **Aktiviert** oder **Inaktiviert** aus, um die Zertifikatsgruppe zu aktivieren oder zu inaktivieren.
6. Klicken Sie auf **Zertifikat laden**.

**Anmerkung:** Die Dropdown-Listen **Primäres Zertifikat** und **Sekundäres Zertifikat** werden auf der Basis des ausgewählten Zertifikatstyps gefüllt. Sind bereits erstellte Zertifikate vorhanden, die noch keiner Gruppe zugeordnet wurden, können Sie diese Zertifikate zur momentan erstellten Gruppe hinzufügen. Wenn die Zertifikatliste leer ist, ist die Dropdown-Liste ebenfalls leer.

7. Wählen Sie in den Dropdown-Listen das **primäre Zertifikat** und das **sekundäre Zertifikat** aus.
8. Klicken Sie auf **Speichern**.

## Zertifikatgruppe löschen

1. Navigieren Sie in der Konsole zur Option **Profil** > **Partner** > **Liste der Zertifikatsgruppen**. In dieser Liste werden alle für den Partner erstellten Zertifikate angezeigt.
2. Klicken Sie auf das Symbol **Löschen**. Stellen Sie vor dem Löschen sicher, dass Sie alle Referenzen auf diese Gruppe in der Verbindung modifiziert haben.
3. Wird die Gruppe von einer oder mehreren Verbindungen verwendet, wird eine Warnung angezeigt. Sie können prüfen, wo ein bestimmtes Zertifikat verwendet wird, indem Sie die Schritte im Abschnitt „Zertifikate - Verwendet von" ausführen.
4. Klicken Sie im Fenster mit der Warnung auf **OK**, um die Gruppe zu löschen, oder klicken Sie auf **Abbrechen**, um das Löschen der Zertifikatsgruppe abzubrechen.

## Zertifikate - Verwendet von

Navigieren Sie in der Konsole zur Option **Profil** > **{Partner}** > **Zertifikatliste** > **Liste der Zertifikatsgruppen** > **Verwendet von**. In der daraufhin angezeigten Sicht werden die folgenden Details dargestellt:

- Absenderpartner
- Empfängerpartner
- Absenderpaket
- Empfängerpaket
- SSL-Client
- Digitale Signatur
- Prüfung der digitalen Signatur
- Verschlüsseln
- Entschlüsseln
- Gültigkeit

**Anmerkung:** Das Zertifikat ist möglicherweise aus einem der folgenden Gründe ungültig: Es ist kein primäres Zertifikat vorhanden, das primäre Zertifikat ist inaktiviert, die Gruppe ist inaktiviert, das primäre Zertifikat ist abgelaufen und kein sekundäres Zertifikat ist vorhanden oder sowohl das primäre als auch das sekundäre Zertifikat sind abgelaufen.

## SSL für den FTP-Scripting-Empfänger oder das FTP-Scripting-Ziel konfigurieren

Für den FTP-Scripting-Empfänger wird das Zertifikat für die SSL-Clientauthentifizierung in das Profil des Hubbetreibers hochgeladen. Auch wenn die Zertifikate für den internen Partner geladen werden, überschreibt dieser die globalen Einstellungen nicht.

## Standardzertifikatgruppe für alle internen Partner bereitstellen

Da WebSphere Partner Gateway mehrere interne Partner unterstützt, muss jeder interne Partner private Schlüssel hochladen. Wenn ein Unternehmen ein Zertifikat mit seinen Unterorganisationen gemeinsam nutzen will, muss das Zertifikat für jeden internen Partner hochgeladen werden. Um diesen Prozess zu vereinfachen, können Sie eine Standardoption angeben, sodass ein bestimmtes Zertifikat für alle internen Partner verwendet wird.

Navigieren Sie in der Konsole zur Option **Zertifikate** > **Zertifikate hochladen**. Laden Sie die Zertifikate hoch, und geben Sie Details zum Zertifikatstyp, zur Verwendung und zum Betriebsmodus an. Wenn Sie die angegebenen Informationen speichern, werden das Zertifikat und die Schlüssel auf der Ebene des Hubbetreibers gespeichert. Zur Laufzeit wird das Standardzertifikat auf der Ebene des Hubbetreibers verwendet, wenn kein anderes Zertifikat vorhanden ist.

## Zertifikate - Zusammenfassung

Tabelle 32 fasst die Art und Weise zusammen, wie Zertifikate in WebSphere Partner Gateway verwendet werden. Zertifikatspositionen werden in runden Klammern "( )" angezeigt.

*Tabelle 32. Übersichtsdaten zu Zertifikaten*

| Nachrichtenübermittlungsmethode (siehe Hinweis 1) | Hubbetreiberzertifikat | Zertifikat und Zertifizierungsstelle vom Partner abrufen | Zertifizierungsstelle (siehe Hinweis 2) | Partner ein Zertifikat übergeben (siehe Hinweis 3) | Kommentare |
|---|---|---|---|---|---|
| Eingangs-SSL | Auf WebSphere Application Server-seitigem SSL installieren. (In den WebSphere Application Server-Keystore stellen.) | Selbst signiertes Zertifikat des Partners. | Wird nur benötigt, wenn die Clientauthentifizierung verwendet wird. (Zertifizierungsstelle oder selbst unterzeichnetes Zertifikat in den WebSphere Application Server-Truststore stellen.) | Hub-Operatorzertifikat (falls selbst signiert) oder gegebenenfalls das CA-Rootzertifikat (falls von der Zertifizierungsstelle authentifiziert). | |
| Ausgangs-SSL | Wenn die Clientauthentifizierung verwendet wird. (WebSphere Partner Gateway) | Partnerserverseitiges Zertifikat oder CA-Rootzertifikat, falls es von der Zertifizierungsstelle authentifiziert ist. | WebSphere Partner Gateway | Hub-Operatorzertifikat (falls selbst signiert) oder CA-Zertifikat (falls von einem Dritthersteller signiert). | |

*Tabelle 32. Übersichtsdaten zu Zertifikaten (Forts.)*

| Nachrichtenübermittlungsmethode (siehe Hinweis 1) | Hubbetreiberzertifikat | Zertifikat und Zertifizierungsstelle vom Partner abrufen | Zertifizierungsstelle (siehe Hinweis 2) | Partner ein Zertifikat übergeben (siehe Hinweis 3) | Kommentare |
|---|---|---|---|---|---|
| Eingangsverschlüsselung | Privater Schlüssel (WebSphere Partner Gateway) | N/A | Falls das Zertifikat von einer Zertifizierungsstelle signiert wurde: CA-Zertifikate müssen als Root-/Intermediate-Zertifikate hochgeladen werden. | Hubbetreiberzertifikat | Für Entschlüsselung der Nachricht |
| Prüfung der eingehenden digitalen Signatur | N/A | Zertifikat zum Prüfen des Zertifikats, das für die digitale Signatur verwendet wird. (WebSphere Partner Gateway) | WebSphere Partner Gateway | N/A | Für Prüfung und Unbestreitbarkeit |
| Ausgangsverschlüsselung | N/A | Das Zertifikat verwenden, das vom Partner abgerufen wurde. (Zertifikat ist im Profil des Partners installiert.) | Zertifikatkette der Zertifizierungsstelle für Clientzertifikat, falls nicht selbst signiert. | N/A | Für Verschlüsselung von ausgehenden Nachrichten |
| Ausgangssignatur | Privater Schlüssel und Zertifikat (WebSphere Partner Gateway) | N/A | Zertifikatkette der Zertifizierungsstelle | Optional, hängt vom Partner ab; WebSphere Partner Gateway Zertifikat geben. | |
| Zertifikat für Geschäfts-ID-Validierung | N/A | In Partnerprofil laden. | | | Prüft, ob dieses Zertifikat für diese Geschäfts-ID vorgesehen ist, wenn die SSL-Clientüberprüfung abgeschlossen ist. |

**Hinweise:**

1. Eine eingehende Nachricht ist eine Nachricht, die in WebSphere Partner Gateway von einem Partner eingeht. Eine ausgehende Nachricht ist eine Nachricht, die von WebSphere Partner Gateway zu einem Partner ausgeht.
2. Wenn das Zertifikat von einer Zertifizierungsstelle ausgegeben ist, muss die ausgebende Zertifizierungsstelle abgerufen und gespeichert werden. Dies gilt für das Zertifikat des Hubbetreibers oder das Zertifikat des Partners.
3. Wenn ein privater Schlüssel mit einbezogen wird, entspricht dieses Zertifikat dem privaten Schlüssel.

# Mit PEM formatierte Zertifikate und Schlüssel mit WebSphere Partner verwenden

Dieser Abschnitt enthält Informationen zur Verwendung von Schlüsseln und Zertifikaten, die mit PEM (Privacy Enhanced Mail) verschlüsselt wurden.

## Mit PEM formatierte private Schlüssel verwenden

Wenn Sie einen privaten Schlüssel im PEM-Format verwenden und ihn ih WebSphere Partner Gateway hochladen wollen, ist diese Operation erst möglich, nachdem der private Schlüssel in das PKCS#8-Format konvertiert wurde.

Verwenden Sie zum Konvertieren das Tool OpenSSL.

Verwenden Sie den folgenden Befehl, um einen für PEM formatierten Schlüssel in das PKCS#8-Format zu konvertieren:

```
openssl pkcs8 -topk8 -in usr.key -out usr.p8 -outform DER
```

Dieser Befehl kann für Schlüssel verwendet werden, die mit OpenSSL erstellt wurden.

OpenSSL wird mit Linux-Distributionen bereitgestellt und kann darüber hinaus auch von der folgenden Website heruntergeladen werden: http://www.openssl.org.

## Mit PEM formatierte Zertifikate verwenden

Das Zertifikat kann in WebSphere Partner Gateway im PEM-Format (PEM - Privacy Enhanced Mail) hochgeladen werden. Dieses Verfahren kann für ein mit OpenSSL generiertes Zertifikat verwendet werden, das für PEM formatiert ist.

## Mit PKCS#7 codierte Zertifikate mit WebSphere Partner Gateway verwenden

Wenn Sie unter Windows Zertifikate verwenden, die im PKCS#7-Format codiert sind (Dateien mit der Erweiterung .p7b), müssen Sie die folgenden Schritte ausführen, um die Zertifikate aus der .p7b-Datei zu extrahieren:

1. Klicken Sie doppelt auf die .p7b-Datei.
2. Erweitern Sie die Verzeichnisstruktur im Navigationsfenster und klicken Sie auf **Zertifikate**. Auf der rechten Seite wird die Liste der in der Datei enthaltenen Zertifikate angezeigt.
3. Klicken Sie doppelt auf ein Zertifikat, um es in das Dateisystem zu kopieren. Die Details des Zertifikats werden angezeigt.
4. Klicken Sie in den Zertifikatsdetails auf die Registerkarte **Details**.
5. Klicken Sie auf **In Datei kopieren**, um die Datei in das Dateisystem zu kopieren.
6. Exportieren Sie das Zertifikat als mit DER (Distinguished Encoding Rules) verschlüsselte Datei.

## SFTP-Schlüssel laden

Schritte zum Laden von SFTP-Schlüsseln.

Führen Sie die folgenden Schritte aus, um SFTP-Schlüssel zu laden:

1. Navigieren Sie zu **Kontenadmin** > **Profile** > **Zertifikate**.
2. Klicken Sie auf **SFTP-Schlüssel laden**.
3. Klicken Sie auf der Seite **SFTP-Schlüssel laden** auf **Durchsuchen** und wählen Sie die Schlüsseldatei in Ihrem lokalen Verzeichnis aus. Die hochgeladene Datei wird für die schlüsselbasierte Authentifizierung verwendet. Das Symbol **Daten enthalten** gibt an, dass bereits ein Schlüssel hochgeladen wurde.

## FIPS-Konformität

WebSphere Partner Gateway entspricht dem Standard FIPS (Federal Information Processing Standard), d. h., dem Standard FIPS 140-2. **IBMJCEFIPS** ist der FIPS-konforme JCE-Provider. Der Provider **IBMJSSE2 JSSE** verwendet **IBM JCE** und enthält keinen Code für die Verschlüsselung; daher muss seine FIPS-Konformität nicht zertifiziert werden. Obwohl der Provider **IBMJSSEFIPS JSSE** FIPS-konform ist, sollten Sie in WebSphere Partner Gateway dennoch den Provider **IBMJSSE2** verwenden. **IBMJSSE2** ist der aktuelle Provider, der mehr Algorithmen unterstützt und über verbesserte Funktionsfähigkeit verfügt. Das Produkt kann im FIPS-Modus und im Nicht-FIPS-Modus ausgeführt werden. Ist der FIPS-Modus konfiguriert und wird ein nicht durch FIPS freigegebener Algorithmus verwendet, wird ein Fehlerereignis generiert, und die Dokumenttransaktion wird gestoppt. Der PKCS#12-Algorithmus ist nicht durch FIPS freigegeben; daher können PKCS#12-Dateien nicht im FIPS-Modus hochgeladen werden. Sie müssen ein Administrator sein, um WebSphere Partner Gateway für die Ausführung im FIPS- oder im Standardmodus zu konfigurieren. Im FIPS-Modus kann PKCS#12 im JCEKS- oder JKS-Format unter Verwendung von iKeyman auf die Konsole von WebSphere Partner Gateway hochgeladen werden.

Der FIPS-Modus unterstützt JKS-, JCEKS- und OpenPGP--Keystores. PKCS#12-Keystores werden jedoch nicht unterstützt. Über die Konsole können Sie ein Zertifikat und einen Schlüssel im JKS-, JCEKS- oder OpenPGP-Format hochladen. Wählen Sie in der Anzeige **Keystore hochladen** das Format in der Liste **Keystore-Format** aus. Die folgenden Werte sind in der Liste **Keystore-Format** verfügbar: PKCS#12, JKS, JCEKS und OpenPGP.

### WebSphere Partner Gateway für die Ausführung im FIPS-Modus konfigurieren

Gehen Sie wie folgt vor, um WebSphere Partner Gateway für die Ausführung im FIPS-Modus zu konfigurieren:

1. Legen Sie die FIPS-Provider in der Datei **java.security** fest.
2. Legen Sie die Systemeigenschaft **bcg.FIPSMode** in der Konsole von WebSphere Partner Gateway auf "true" fest.
3. Legen Sie den Provider IBMJCEFIPS in der Datei **java.security** vor dem Provider IBMJCE fest. Die Datei **java.security** befindet sich im Verzeichnis <WAS-installationsverz>/java/jre/lib/security.
4. Legen Sie die für FIPS aktivierten Socket-Factory-Klassen für die JSSE-Socket-Factory und die Server-Socket-Factory fest.
5. Starten Sie alle Server neu.

**Anmerkung:** Ein Informationsereignis wird generiert, in dem angegeben wird, dass das Produkt im FIPS-Modus ausgeführt wird.

## WebSphere Partner Gateway für die Ausführung im Standardmodus konfigurieren

Gehen Sie wie folgt vor, um WebSphere Partner Gateway für die Ausführung im Standardmodus zu konfigurieren:

1. Legen Sie die Systemeigenschaft **bcg.FIPSMode** in der Konsole von WebSphere Partner Gateway auf "False" fest.
2. Setzen Sie die Einstellungen für die JSSE-Socket-Factory, die Server-Socket-Factory und die Provider der Datei **java.security** zurück, wie nachfolgend beschrieben:
   a. Entfernen Sie die Systemeigenschaft **com.ibm.jsse2.JSSEFIPS=true** aus den Eigenschaften **Generic JVM Properties** für jeden Server.
   b. Setzen Sie die Werte der folgenden Eigenschaften auf ihre ursprünglichen Werte zurück:
      - ssl.SocketFactory.provider
      - ssl.SocketFactory.provider
   c. Setzen Sie für jede WAS-Installation den IBMJCEFIPS-Provider auf Kommentar und nummerieren Sie die Provider in der Datei **java.security** um, wobei Sie bei 1 beginnen müssen.
3. Starten Sie die Server neu.

   **Anmerkung:** Ein Informationsereignis wird generiert, in dem der Modus angegeben wird. Im Standardmodus können alle unterstützten Algorithmen einschließlich der nicht durch FIPS freigegebenen Algorithmen verwendet werden.

## IBM JSSE-Provider für den FIPS-Modus konfigurieren

Gehen Sie wie folgt vor, um die IBM JSSE-Provider für den FIPS-Modus zu konfigurieren:

1. Legen Sie die Systemeigenschaft **com.ibm.jsse2.JSSEFIPS** auf "true" fest. Legen Sie hierfür mithilfe der Administrationskonsole von WebSphere Application Server die JVM-Systemeigenschaften für den Anwendungsserver fest. Öffnen Sie die Seite <Server>/Java and Process Management/Process Definition/Java Virtual Machine und geben Sie die Eigenschaft **-Dcom.ibm.jsse2.JSSEFIPS=true** an. Diese Einstellung muss für jeden Server vorgenommen werden.
2. Legen Sie die folgenden Sicherheitseigenschaften für den IBMJSSE2-Provider fest, um alle JSSE-Anforderungen zu verarbeiten:
   - ssl.SocketFactory.provider = com.ibm.jsse2.SSLSocketFactoryImpl
   - ssl.ServerSocketFactory.provider = com.ibm.jsse2.SSLServerSocketFactoryImpl
3. Fügen Sie den den Provider IBMJCEFIPS mit dem Eintrag "com.ibm.crypto.fips.provider.IBMJCEFIPS" vor dem Provider IBMJCE zur Liste der Provider hinzu. Entfernen Sie den Provider IBMJCE nicht, da er für die Unterstützung von Keystores erforderlich ist.

   **Anmerkung:** Wenn IBMJSSE2 im FIPS-Modus ist, wird nur das TLS-Protokoll unterstützt.

## Im FIPS- und Nicht-FIPS-Modus unterstützte Algorithmen

Die folgenden Algorithmen werden im FIPS-Modus unterstützt:

- Diffie-Hellman
- RSA, DSA
- SHA-1, SHA-384, SHA-224, SHA-512
- AES, DES, TDES (Triple DES)
- FIPS 186-2 – Algorithmus für die Generierung von Pseudozufallszahlen (PRNG)
- Transport Layer Security: TLSv1
- Keystore-Format: JKS, JCEKS

Die folgenden Algorithmen werden in WebSphere Partner Gateway unterstützt:

- Asymmetrische Verschlüsselung: RSA, DSA
- Hashfunktion: SHA-1, MD5, SHA-384, SHA-224, SHA-512, RIPEMD/160
- Symmetrische Verschlüsselung: AES, DES, 3DES, RC2 (alle mit dem CBC-Modus), CAST5, Blowfish, Twofish
- PRNG: IBMSecureRandom
- Signaturalgorithmus: dsa-sha1, rsa-sha1
- Transport Layer Security: SSLv3, TLSv1
- Keystore-Format: PKCS#12, JKS, JCEKS, OpenPGP
- Algorithmen für symmetrische Verschlüsselung: AES und TripleDES mit Änderungserkennung.

  **Einschränkung:** Die Algorithmen TripleDES und AES können nur verwendet werden, wenn sowohl der Modus für die Änderungserkennung als auch der Modus für FIPS gesetzt ist.

Die folgenden Algorithmen werden nicht in FIPS, aber in in WebSphere Partner Gateway unterstützt:

- Hashfunktion: MD5, RIPEMD160
- Symmetrische Verschlüsselung: RC2, CAST5, Blowfish, Twofish
- PRNG-Provider IBMSecureRandom (alle Fälle von WebSphere Partner Gateway)
- Transport Layer Security: SSLv3
- Keystore-Format: PKCS#12

# Kapitel 14. Alerts verwalten

Die Alerts von WebSphere Partner Gateway werden dazu verwendet, wichtige Kontakte über ungewöhnliche Schwankungen im Umfang empfangener Übertragungen zu benachrichtigen oder Fehler bei der Verarbeitung von Geschäftsdokumenten zu berichten.

Eine Zusatzoption im Anzeigemodul, die Ereignisanzeige, hilft Ihnen bei der weiteren Identifizierung und Behebung von Verarbeitungsfehlern.

## Übersicht über Alerts

Ein Alert besteht aus einer textbasierten E-Mail-Nachricht, die an subskribierte Kontakte oder eine Verteilerliste für das zuständige Personal gesendet wird. Alerts basieren auf einem Systemereignis (ereignisgesteuerter Alert) oder dem erwarteten Dokumentenflussvolumen (volumenabhängiger Alert).

- Ein **volumenabhängiger Alert** benachrichtigt Sie über Zu- und Abnahmen des Übertragungsvolumens.

  Als externer Partner können Sie zum Beispiel einen volumenabhängigen Alert erstellen, der Sie benachrichtigt, wenn Sie an einem bestimmten Geschäftstag keine Übertragungen vom internen Partner empfangen. (Geben Sie unter **Volumen** die Option **Nullvolumen** und unter **Häufigkeit** die Option **Täglich** an und wählen Sie unter **Wochentage** Montag bis Freitag aus). Dieser Alert kann auf Probleme bei der Netzübertragung des internen Partners hinweisen.

  Darüber hinaus können Sie als externer Partner einen volumenabhängigen Alert erstellen, der Sie warnt, wenn die Anzahl an Übertragungen vom internen Partner die normale Rate übersteigt. Beispiel: Wenn Sie normalerweise ungefähr 1.000 Übertragungen pro Tag empfangen, können Sie das erwartete Volumen auf 1.000 und die Abweichung auf 25 % setzen. Der Alert benachrichtigt Sie, wenn Sie pro Tag mehr als 1.250 Übertragungen empfangen. Fällt das Übertragungsvolumen unter 750, werden Sie ebenfalls benachrichtigt. Dieser Alert kann auf einen erhöhten Bedarf seitens des internen Partners hinweisen, welcher im Laufe der Zeit dazu führen kann, dass Sie der Umgebung weitere Server hinzufügen müssen. Weitere Informationen zu volumenabhängigen Alerts finden Sie unter „ Volumenabhängigen Alert erstellen" auf Seite 306.

  **Anmerkung:**

  1. Volumenabhängige Alerts überwachen das Volumen hinsichtlich des Dokumenttyps, den Sie bei der Erstellung des Alerts auswählen. WebSphere Partner Gateway prüft nur Dokumente, die den im Alert ausgewählten Dokumenttyp enthalten, und generiert nur dann Alerts, wenn alle Alertbedingungen erfüllt sind.
  2. Der externe Partner kann einen volumenabhängigen Alert nur in Bezug auf das Dokumentvolumen erstellen, das an den internen Partner gesendet wird. Möchte der externe Partner einen volumenabhängigen Alert für das eingehende Dokumentvolumen konfigurieren, das vom internen Partner gesendet wird, muss der externe Partner den Hubadministrator bitten, diesen Alert im Namen des externen Partners zu konfigurieren, wobei der externe Partner als Alerteigner definiert wird. Ein interner Partner kann auch volumenabhängige Alerts für das Volumen der an externe Partner gesendeten Dokumente erstellen.

- Ein **ereignisgesteuerter Alert** benachrichtigt Sie über Fehler bei der Dokumentverarbeitung. Sie können zum Beispiel einen Alert erstellen, der Sie benachrichtigt, wenn Ihre Dokumente aufgrund von Validierungsfehlern oder des Empfangs von doppelten Dokumenten nicht verarbeitet werden können. Ferner können Sie Alerts erstellen, die Sie über den bevorstehenden Ablauf eines Zertifikats benachrichtigen.

  Zur Erstellung von ereignisgesteuerten Alerts werden vordefinierte WebSphere Partner Gateway-Ereigniscodes verwendet: Es gibt fünf Ereignistypen: Debugging, Informationen, Warnung, Fehler und Kritisch. Innerhalb eines Ereignistyps gibt es viele Ereignisse. Auf der Seite **Alert: Ereignisse** können vordefinierte Ereignisse angezeigt und ausgewählt werden. Beispiel: "240601 AS-Wiederholungsfehler" oder "108001 Kein Zertifikat". Weitere Informationen zu ereignisgesteuerten Alerts finden Sie in „ Ereignisgesteuerten Alert erstellen” auf Seite 309.

**Tipp:**

- Verwenden Sie einen volumenabhängigen Alert, um eine Benachrichtigung zu erhalten, wenn das Übertragungsvolumen des externen oder internen Partners unter die operativen Grenzwerte fällt. Dieser Alert kann auf Probleme bei der Netzübertragung des externen oder des internen Partners hinweisen.
- Verwenden Sie einen ereignisgesteuerten Alert, um eine Benachrichtigung zu erhalten, wenn Fehler bei der Dokumentverarbeitung auftreten. Sie können zum Beispiel einen ereignisgesteuerten Alert erstellen, der Sie benachrichtigt, wenn Ihre Dokumente aufgrund von Validierungsfehlern nicht verarbeitet wurden.

**Anmerkung:** Zum Senden von Alerts muss ein E-Mail-Server für die Alerts konfiguriert werden. Alerts werden auf der Seite **Attribute der Alertsteuerkomponente** konfiguriert. Klicken Sie dazu auf **Systemverwaltung** > **DocMgr-Verwaltung** > **Alertsteuerkomponente**. Weitere Informationen zum Konfigurieren des E-Mail-Servers für Alerts finden Sie im Abschnitt zur Aktualisierung von E-Mail-Adressen für Alerts im *WebSphere Partner Gateway Partnerhandbuch*.

## Alertdetails und Kontakte anzeigen oder bearbeiten

Der interne Partner kann alle Alerts unabhängig vom Alerteigner (Ersteller des Alerts) anzeigen.

1. Klicken Sie auf **Kontenadmin** > **Alerts**. Das System zeigt die Seite **Alertsuche** an.
2. Wählen Sie die Suchkriterien aus den Dropdown-Listen aus; geben Sie den Alertnamen ein. Sie können auch ohne Auswahl von Suchkriterien auf **Suchen** klicken. Das System zeigt dann alle Alerts an.
3. Klicken Sie auf **Suchen**. Das System zeigt die Seite **Alertsuche - Ergebnisse** an.
4. Klicken Sie auf das Symbol **Details anzeigen**, um die Details für einen Alert anzuzeigen.
5. Klicken Sie auf das Symbol **Bearbeiten**, um die Alertdetails zu bearbeiten.
6. Bearbeiten Sie die Informationen nach Bedarf.
7. Klicken Sie auf die Registerkarte **Benachrichtigen**.
8. Wählen Sie einen Partner (nur interner Partner oder Hubadministrator) aus. Der interne Partner kann alle Alerts unabhängig vom Alerteigner anzeigen.
9. Bearbeiten Sie gegebenenfalls die Kontakte für diesen Alert.
10. Klicken Sie auf **Speichern**.

## Nach Alerts suchen

1. Klicken Sie auf **Kontenadmin** > **Alerts**. Das System zeigt die Seite **Alertsuche** an.
2. Wählen Sie die Suchkriterien aus den Dropdown-Listen aus; geben Sie den Alertnamen ein. Sie können auch ohne Auswahl von Suchkriterien auf **Suchen** klicken. Das System zeigt dann alle Alerts an.

*Tabelle 33. Alertsuchkriterien für Partner*

| Wert | Beschreibung |
|---|---|
| Alerttyp | Volumen, Ereignis oder alle Alerttypen. |
| Alertname | Der Name des Alerts. |
| Alertstatus | Aktivierte, inaktivierte oder alle Alerts. |
| Subskribierte Kontakte | Kontakte, die einem Alert zugeordnet sind. Mögliche Optionen: **Hat Subskribenten**, **Keine Subskribenten** oder **Alle**. |
| Ergebnisse pro Seite | Steuert die Anzeige der Suchergebnisse. |

*Tabelle 34. Alertsuchkriterien für den internen Partner und den Hubadministrator*

| Wert | Beschreibung |
|---|---|
| Alerteigner | Der Ersteller des Alerts. |
| Alertpartner | Der Partner, auf den der Alert angewendet wird. |
| Alerttyp | Volumen, Ereignis oder alle Alerttypen. |
| Alertname | Der Name des Alerts. |
| Alertstatus | Aktivierte, inaktivierte oder alle Alerts. |
| Subskribierte Kontakte | Kontakte, die einem Alert zugeordnet sind. Mögliche Optionen: **Hat Subskribenten**, **Keine Subskribenten** oder **Alle**. |
| Ergebnisse pro Seite | Steuert die Anzeige der Suchergebnisse. |

3. Klicken Sie auf **Suchen**. Das System zeigt eine Liste der Alerts an, die mit Ihren Suchkriterien übereinstimmen (sofern vorhanden).

## Alert inaktivieren oder aktivieren

1. Klicken Sie auf **Kontenadmin** > **Alerts**. Das System zeigt die Seite **Alertsuche** an.
2. Wählen Sie die Suchkriterien aus den Dropdown-Listen aus; geben Sie den Alertnamen ein.
3. Klicken Sie auf **Suchen**. Das System zeigt eine Liste der Alerts an, die mit Ihren Suchkriterien übereinstimmen (sofern vorhanden).
4. Suchen Sie den Alert, und klicken Sie unter **Status** auf **Inaktiviert** oder **Aktiviert**. Nur der Hubadministrator und der Alerteigner (Ersteller des Alerts) sind zum Bearbeiten des Alertstatus berechtigt.

## Alert entfernen

1. Klicken Sie auf **Kontenadmin** > **Alerts**. Das System zeigt die Seite **Alertsuche** an.
2. Wählen Sie die Suchkriterien aus den Dropdown-Listen aus; geben Sie einen Wert für **Alertname** ein.
3. Klicken Sie auf **Suchen**. Das System zeigt eine Liste der Alerts an, die mit Ihren Suchkriterien übereinstimmen (sofern vorhanden).

4. Suchen Sie den Alert, und klicken Sie auf das Symbol **Löschen**. Nur der Hubadministrator und der Alerteigner (Ersteller des Alerts) können einen Alert entfernen.

## Neuen Kontakt zu vorhandenem Alert hinzufügen

1. Klicken Sie auf **Kontenadmin** > **Alerts**. Das System zeigt die Seite **Alertsuche** an.
2. Wählen Sie die Suchkriterien aus den Dropdown-Listen aus; geben Sie den Alertnamen ein.
3. Klicken Sie auf **Suchen**. Das System zeigt eine Liste der Alerts an, die mit Ihren Suchkriterien übereinstimmen (sofern vorhanden).
4. Klicken Sie auf das Symbol **Details anzeigen**, um die Alertdetails anzuzeigen.
5. Klicken Sie auf das Symbol **Bearbeiten**, um die Alertdetails zu bearbeiten.
6. Klicken Sie auf die Registerkarte **Benachrichtigen**.
7. Wählen Sie einen Partner (nur interner Partner oder Hubadministrator) aus.
8. Wenn der gewünschte Kontakt im Textfeld **Kontakte** aufgelistet ist, wählen Sie ihn aus und klicken Sie dann auf **Subskribieren**. Fahren Sie mit Schritt 13 fort.

   Wenn der gewünschte Kontakt im Textfeld **Kontakte** nicht aufgelistet ist, klicken Sie auf **Neu hinzufügen - Eintrag in Kontakte**. Das System zeigt das Dialogfenster **Neuen Kontakt erstellen** an.

   Der Link **Neu hinzufügen - Eintrag in Kontakte** ist nur verfügbar, wenn der Partner ein Hubbetreiber ist.
9. Geben Sie Namen, E-Mail-Adresse, Telefon- und Faxnummer des Kontakts ein.
10. Wählen Sie den Alertstatus des Kontakts aus.
    - Wählen Sie **Aktiviert** aus, um mit dem Senden von E-Mail-Nachrichten an diesen Kontakt zu beginnen, wenn das System den Alert generiert.
    - Wählen Sie **Inaktiviert** aus, um keine E-Mail-Nachrichten an diesen Kontakt zu senden, wenn das System den Alert generiert.
11. Wählen Sie die Sichtbarkeit des Kontakts aus.
    - Wählen Sie **Lokal** aus, um den Kontakt nur für Ihr Unternehmen sichtbar zu machen.
    - Wählen Sie **Global** aus, um den Kontakt für den Hubadministrator und den internen Partner sichtbar zu machen. Beide können den Kontakt für Alerts subskribieren.
12. Klicken Sie auf **Speichern**, um den Kontakt zu speichern. Klicken Sie auf **Speichern & Subskribieren**, um den Kontakt zu speichern und ihn der Liste mit Kontakten für diesen Alert hinzuzufügen.
13. Klicken Sie auf **Speichern**.

## Volumenabhängigen Alert erstellen

1. Klicken Sie auf **Kontenadmin** > **Alerts**. Das System zeigt die Seite **Alertsuche** an.
2. Klicken Sie am rechten oberen Rand der Seite auf **Erstellen**. Das System zeigt die Registerkarte zum Definieren von Alerts an.
3. Wählen Sie für **Alerttyp** den Eintrag **Volumenalert** aus (Standardeinstellung). Das System zeigt die entsprechenden Textfelder für einen Volumenalert an.
4. Geben Sie im Feld **Alertname** einen Namen für den Alert ein.

5. Geben Sie im Feld **Angepasster Geschäftstext** den entsprechenden Text ein. Wenn das Alertereignis generiert wird, wird diese Nachricht zusammen mit dem Ereignis gesendet.
6. Wählen Sie einen Alerteigner für den Alert aus.
7. Wählen Sie einen Partner mit der Berechtigung zum Erstellen eines volumenabhängigen Alerts aus (nur interner Partner oder Hubadministrator).
8. Wählen Sie **Paket**, **Protokoll** und **Dokumenttyp** aus den Dropdown-Listen aus. Die Angaben für Paket, Protokoll und Dokumenttyp müssen mit den Angaben für den Quellenpartner (extern) übereinstimmen.
9. Wählen Sie eine der drei Volumenoptionen aus (**Erwartet**, **Bereich** oder **Nullvolumen**) und fahren Sie dann mit 10 fort:
   - **Erwartet**. Wählen Sie diese Option aus, wenn ein Alert für den Fall generiert werden soll, dass das Dokumenttypvolumen von einer definierten Menge abweicht. Führen Sie die folgenden Schritte aus, um einen Alert bezüglich eines erwarteten Dokumenttypvolumens zu erstellen:
     a. Geben Sie in das Textfeld **Volumen** die Anzahl der Dokumenttypen ein, deren Empfang innerhalb des in Schritt 10 ausgewählten Zeitrahmens erwartet wird. Geben Sie nur positive Zahlen ein; wenn Sie eine negative Zahl eingeben, funktioniert der Alert nicht.
     b. Geben Sie in das Textfeld **Abweichung (%)** einen Wert für die zulässige Abweichung des Dokumenttypvolumens ein. Innerhalb dieser Abweichung wird kein Alert aktiviert. Beispiel:
        – Bei Auswahl von 20 für Volumen und 10 für die Abweichung in Prozent löst ein Dokumentenflussvolumen kleiner als 18 und größer als 22 einen Alert aus.
        – Bei Auswahl von 20 für Volumen und 0 für die Abweichung in Prozent löst ein Dokumentenflussvolumen größer/kleiner als 20 einen Alert aus.
   - **Bereich**. Bei Auswahl dieser Option wird ein Alert generiert, wenn das Dokumentenflussvolumen außerhalb eines Bereichsminimums/-maximums liegt. Führen Sie die folgenden Schritte aus, um einen Alert auf der Basis eines Wertebereichs zu erstellen:
     a. Geben Sie in das Textfeld **Min.** die Mindestanzahl an Dokumentenflüssen ein, deren Empfang innerhalb des in Schritt 10 ausgewählten Zeitrahmens erwartet wird. Ein Alert wird nur dann ausgelöst, wenn das Dokumentenflussvolumen unter diesen Wert fällt.
     b. Geben Sie in das Textfeld **Max.** die maximale Anzahl an Dokumentenflüssen ein, deren Empfang innerhalb des in Schritt 10 ausgewählten Zeitrahmens erwartet wird.

     **Anmerkung:** Die Textfelder **Min.** und **Max.** müssen bei der Erstellung eines Alerts, der auf einem Volumenbereich basiert, ausgefüllt werden.
   - **Nullvolumen**. Wählen Sie diese Option aus, um einen Alert auszulösen, wenn innerhalb des in Schritt 10 ausgewählten Zeitrahmens kein Dokumentenfluss empfangen wird.
10. Wählen Sie für den Zeitrahmen (Häufigkeit), den das System zur Überwachung des Dokumentenflussvolumens hinsichtlich der Alertgenerierung verwendet, entweder **Täglich** oder **Bereich** aus.
    - **Täglich**. Wählen Sie diese Option aus, um das Dokumentenflussvolumen an einem oder mehreren Tagen in der Woche oder im Monat zu überwachen. Wählen Sie zum Beispiel **Täglich** aus, wenn das Dokumentenflussvolumen

nur an einem oder mehreren bestimmten Tagen in der Woche (z. B. montags oder montags und donnerstags) oder im Monat (z. B. am 1. und am 15. Tag) überwacht werden soll.

- **Bereich**. Wählen Sie diese Option aus, um das Dokumentenflussvolumen zwischen zwei Tagen in der Woche oder im Monat zu überwachen. Wählen Sie zum Beispiel **Bereich** aus, um das Dokumentenflussvolumen an allen Tagen zwischen Montag und Freitag bzw. an allen Tagen zwischen dem 5. und dem 20. Tag eines jeden Monats zu überwachen.

11. Wählen Sie die **Startzeit** und die **Endzeit** (24-Stunden-Tag) der Überwachung des Dokumentenflussvolumens für die Tage aus, die im nächsten Schritt ausgewählt werden. Beachten Sie, dass das Dokumentenflussvolumen bei Auswahl eines Bereichs für die Häufigkeit von der Startzeit des ersten Tages bis zur Endzeit des letzten Tages innerhalb des Bereichs überwacht wird.
12. Wählen Sie die entsprechenden Tage innerhalb der Woche oder des Monats aus, in denen die Alertüberwachung erfolgen soll. Haben Sie als Häufigkeit **Täglich** ausgewählt, wählen Sie die tatsächlichen Tage in der Woche oder im Monat für die Alertüberwachung aus. Haben Sie als Häufigkeit **Bereich** ausgewählt, wählen Sie zwei Tage in der Woche oder im Monat aus, innerhalb derer die Alertüberwachung erfolgt.
13. Wählen Sie als Alertstatus für diesen Alert **Aktiviert** oder **Inaktiviert** aus.
14. Klicken Sie auf **Speichern**.
15. Klicken Sie auf die Registerkarte **Benachrichtigen**.
16. Klicken Sie auf das Symbol **Bearbeiten**.
17. Wählen Sie einen **Partner** (nur interner Partner oder Hubadministrator) aus.
18. Wenn der gewünschte Kontakt im Textfeld **Kontakte** aufgelistet ist, wählen Sie ihn aus und klicken Sie dann auf **Subskribieren**. Fahren Sie mit Schritt 23 fort.

    Wenn der gewünschte Kontakt im Textfeld **Kontakte** nicht aufgelistet ist, klicken Sie auf **Neu hinzufügen - Eintrag in Kontakte**. Das System zeigt das Dialogfenster **Neuen Kontakt erstellen** an.

    Beachten Sie, dass **Neu hinzufügen - Eintrag in Kontakte** nur für den Alerteigner verfügbar ist, um Kontakte zu erstellen, die dem Alerteigner zugeordnet sind. Mit dieser Funktion kann der Alerteigner keine Kontakte für Alertpartner hinzufügen.
19. Geben Sie Namen, E-Mail-Adresse, Telefon- und Faxnummer des Kontakts ein.
20. Wählen Sie den **Alertstatus** des Kontakts aus.
    - Wählen Sie **Aktiviert** aus, um mit dem Senden von E-Mail-Nachrichten an diesen Kontakt zu beginnen, wenn das System den Alert generiert.
    - Wählen Sie **Inaktiviert** aus, um keine E-Mail-Nachrichten an diesen Kontakt zu senden, wenn das System den Alert generiert.
21. Wählen Sie die Sichtbarkeit des Kontakts aus.
    - Wählen Sie **Lokal** aus, um den Kontakt nur für Ihr Unternehmen sichtbar zu machen.
    - Wählen Sie **Global** aus, um den Kontakt für den Hubadministrator und den internen Partner sichtbar zu machen. Beide können den Kontakt für Alerts subskribieren.
22. Klicken Sie auf **Speichern**, um den Kontakt zu speichern; klicken Sie auf **Speichern & Subskribieren**, um den Kontakt der Liste mit Kontakten für diesen Alert hinzuzufügen.
23. Klicken Sie auf **Speichern**.

**Anmerkung:** Änderungen für volumenabhängige Alerts, die nach dem ursprünglichen Überwachungszeitraum vorgenommen werden, werden am nächsten Tag des Überwachungszeitraums wirksam. Beispiel: Die Alertüberwachung findet mittwochs und donnerstags in der Zeit zwischen 13 - 15 Uhr statt. Am Mittwoch um 16 Uhr wird der Zeitraum für die Alertüberwachung geändert und auf 17 - 19 Uhr gesetzt. Die Alertüberwachung findet am Mittwoch nicht zwei Mal statt. Die Änderung wird erst am Donnerstag wirksam.

## Ereignisgesteuerten Alert erstellen

1. Klicken Sie auf **Kontenadmin** > **Alerts**. Das System zeigt die Seite **Alertsuche** an.
2. Klicken Sie am rechten oberen Rand der Seite auf **Erstellen**. Das System zeigt die Registerkarte zum Definieren von Alerts an.
3. Wählen Sie für **Alerttyp** den Eintrag **Ereignisalert** aus. Das System zeigt die entsprechenden Textfelder für einen ereignisgesteuerten Alert an.
4. Geben Sie einen Alertnamen für den Alert ein.
5. Geben Sie im Feld **Angepasster Geschäftstext** den entsprechenden Text ein. Wenn das Alertereignis generiert wird, wird diese Nachricht zusammen mit dem Ereignis gesendet.
6. Wählen Sie einen Alerteigner für den Alert aus.
7. Wählen Sie einen Partner aus, der den Alert auslöst. (Diese Option steht nur dem internen Partner und dem Hubadministrator zur Verfügung.) Wählen Sie die Option **Beliebiger Partner** aus, um den Alert allen Partnern im System zuzuordnen. Wenn Sie eine Alertsuche durchführen und für den Alertpartner **Beliebiger Partner** auswählen, zeigt das System alle Alerts an, die keinem bestimmten Partner zugeordnet sind.
8. Wählen Sie den Ereignistyp aus: Debugging, Informationen, Warnung, Fehler, Kritisch oder Alle.
9. Wählen Sie den Ereignisnamen aus, der den Alert aktivieren soll, z. B. "BCG240601 AS-Wiederholungsfehler" oder "108001 Kein Zertifikat". Wählen Sie eine der folgenden Optionen aus, um einen Alert zu erstellen, der Sie über den bevorstehenden Ablauf eines Zertifikats benachrichtigt:
   - BCG108005 Zertifikatablauf in 60 Tagen
   - BCG108006 Zertifikatablauf in 30 Tagen
   - BCG108007 Zertifikatablauf in 15 Tagen
   - BCG108008 Zertifikatablauf in 7 Tagen
   - BCG108009 Zertifikatablauf in 2 Tagen

   **Anmerkung:** Damit ein Ereignis hier aufgelistet wird, muss es alertfähig sein. Informationen darüber, wie Ereignisse alertfähig gemacht werden können, finden Sie in „Alertfähige Ereignisse angeben” auf Seite 316.
10. Wählen Sie den Status des Alerts aus: **Aktiviert** oder **Inaktiviert**.
11. Klicken Sie auf **Speichern**.
12. Klicken Sie auf die Registerkarte **Benachrichtigen**.
13. Wählen Sie den Benachrichtigungsmodus aus: **Alle betroffenen Beteiligten benachrichtigen** oder **Nur subskribierte Kontakte benachrichtigen**. Im Modus ***Nur subskribierte Kontakte benachrichtigen*** werden nur die subskribierten Kontakte benachrichtigt. Wird ein Alert generiert und ist der Benachrichtigungsmodus auf die Option ***Alle betroffenen Beteiligten benachrichtigen*** festgelegt, wird eine Benachrichtigung an alle Beteiligten gesendet, die mit

dem Ereignis, für das der Alert generiert wird, in Verbindung stehen. Die zugehörigen Beteiligten sind die kombinierten Kontakte des Quellenpartners, des Zielpartners und des Alerteigners.

14. Wählen Sie einen Partner (nur interner Partner oder Hubadministrator) aus.
15. Wählen Sie aus den im Textfeld **Kontakte** aufgelisteten Kontakten den gewünschten Kontakt aus und klicken Sie auf **Subskribieren**.
16. Wählen Sie den Zustellmodus aus:
    - **Alerts unverzüglich senden**. Bei Auswahl dieser Option sendet das System Alertbenachrichtigungen an den Kontakt, sobald der Alert auftritt. Verwenden Sie diese Option für kritische Alerts.
    - **Alerts stapeln nach**. Bei Auswahl dieser Option können Sie angeben, wann der Kontakt Alertbenachrichtigungen erhalten soll. Verwenden Sie diese Option für nicht kritische Alerts.

      Die beiden Optionen **Anzahl** und **Zeit** in diesem Abschnitt schließen sich nicht gegenseitig aus.

      Wenn Sie die Option **Anzahl** auswählen, müssen Sie auch die Option **Zeit** auswählen.

      – Wird die Alertanzahl (Anzahl) während des ausgewählten Zeitlimits (Zeit) erreicht, generiert das System eine Alertbenachrichtigung.
      – Wird ein Alert ausgeführt, die Alertanzahl (Anzahl) während des ausgewählten Zeitlimits (Zeit) aber nicht erreicht, generiert das System am Ende des Zeitlimits eine Alertbenachrichtigung.

      Die Option **Zeit** kann ohne die Option **Anzahl** verwendet werden; der Option **Anzahl** muss jedoch stets ein Zeitlimit (Zeit) zugeordnet werden.

      – **Anzahl**. Bei Auswahl dieser Option muss auch die Option **Zeit** verwendet werden. Geben Sie eine Zahl (n) ein. Dies ist die Anzahl der Alerts, die während des ausgewählten Zeitraums (Zeit) generiert werden, bevor das System eine Alertbenachrichtigung an den Kontakt des Alerts sendet.

        Beispiel für die Zusammenarbeit der beiden Optionen:

        Im vorliegenden Beispiel ist die Optionen **Alerts stapeln nach** auf 10 für die Anzahl (10 Alerts) und auf 2 für die Zeit (2-Stunden-Zeitraum) gesetzt. Das System hält alle Benachrichtigungen für diesen Alert zurück, bis innerhalb eines 2-Stunden-Zeitraums 10 Alerts aufgetreten sind oder das Ende des Zeitraums erreicht wurde.

        Erreicht die Alertanzahl innerhalb eines 2-Stunden-Zeitraums den Wert 10, sendet das System alle Alertbenachrichtigungen für diesen Alert an den Kontakt.

        Tritt ein Alert auf, wobei innerhalb des 2-Stunden-Zeitraums (Zeitlimit) die Anzahl 10 jedoch nicht erreicht wird, sendet das System am Ende des Zeitlimits eine Alertbenachrichtigung an den Kontakt des Alerts.
      – **Zeit**. Wählen Sie die Anzahl an Stunden (n) aus. Das System hält Alertbenachrichtigungen für n Stunden zurück. Alle n Stunden sendet das System alle zurückgehaltenen Alertbenachrichtigungen an den Kontakt.

        Wenn Sie zum Beispiel 2 eingeben, hält das System alle Benachrichtigungen für diesen Alert zurück, die innerhalb eines 2-Stunden-Intervalls auftreten. Nach Ablauf des 2-Stunden-Intervalls sendet das System alle Alertbenachrichtigungen für diesen Alert an den Kontakt.
17. Klicken Sie auf **Speichern**.

# Kapitel 15. Fehlerdatenfluss einleiten

In WebSphere Partner Gateway können sie als Administrator fehlgeschlagene Ereignisse überwachen, die beim Verarbeiten von Dokumenten auftreten. Ein Dokument kann beim Empfänger oder Document Manager fehlschlagen. Für ein fehlgeschlagenes Dokument wird das entsprechende Fehler- oder kritische Ereignis in der Ereignisengine protokolliert. Es können Alerts erstellt werden, mit denen E-Mail-Benachrichtigungen an einen oder mehrere Subskribenten gesendet werden.

Darüber hinaus kann eine Administrator einen Fehlerdokumentenfluss für interne Partner, externe Partner oder beide Partner direkt einleiten. Dieses Fehlerdokument wird auf der Basis des Fehler- oder kritischen Ereignisses für ein fehlgeschlagenes Dokument eingeleitet. Der Fehlerdokumentenfluss kann im WebSphere Partner Gateway-Format oder im Web-Service-Format vorliegen. Das Format kann in der Konfiguration des Fehlerdatenflusses konfiguriert werden.

## Konfiguration des Dokuments für den Fehlerdatenfluss

Mithilfe der Registerkarte **Fehlerdatenfluss** können Sie den Aufruf des Fehlerdatenflusses oder des Web-Services für bestimmte Fehlerereignisse festlegen. Gehen Sie dazu wie folgt vor:

1. Navigieren Sie zu **Kontenadmin** > **Fehlerdatenfluss**. In der Liste der Fehlerdatenflüsse werden für jeden Fehlerdatenfluss Symbole zum Anzeigen und Löschen dargestellt.
2. Klicken Sie auf das Symbol **Anzeigen**, um die Anzeige für die Konfiguration des Fehlerdatenflusses schreibgeschützt anzuzeigen.
3. Klicken Sie in der Anzeige der Konfiguration auf das Symbol **Bearbeiten**, um die Konfiguration des Fehlerdatenflusses zu bearbeiten.
4. Im Bearbeitungsmodus sind die folgenden Konfigurationswerte verfügbar:
   - **Name** - Der Name der Konfiguration für das Fehlerdatenflussdokument.
   - **Sendender Partner** - Klicken Sie auf **Partnersuche** und wählen Sie den Namen des Partners aus. Bei dem Partner kann es sich um einen internen oder externen Partner handeln.
   - **Partnertyp** - Wählen Sie in der Dropdown-Liste den Partnertyp aus.
   - **Fehlerereignis** - In dieser Dropdown-Liste werden nur Ereignisse mit dem Typ *Fehler* und *Kritisch* angezeigt.
   - **Typ des Fehlerdatenflusses** - Dieser Typ kann *Fehlerdatenflussdokument* oder *Web-Service aufrufen* sein.
   - **Senden an** - Wählen Sie die Empfänger des fehlgeschlagenen Dokuments aus. Mögliche Angaben sind *Absender* oder *Empfänger* oder *Beide*.
5. Klicken Sie auf **Speichern**.
6. Klicken Sie auf **Abbrechen**, wenn Sie die Operation abbrechen wollen.
7. Aktivieren Sie die B2B-Funktionalität für den Fehlerdatenfluss, der konfiguriert werden soll.
8. Wird der Web-Service aufgerufen, müssen Sie die Interaktion erstellen und die Partnerverbindung aktivieren.

Die Definitionen des Fehlerdatenflussdokuments (ErrorFlowDocument) für XML und Web-Service (WebService) werden standardmäßig in WebSphere Partner Gateway hochgeladen. Sie können diese Definitionen für Partner aktivieren und die folgenden Verbindungen erstellen:

- XML-Verbindung für ErrorFlowDocument
- ErrorFlowDocument über Webservices für Dokumentstil
- ErrorFlowDocument über Webservices für RPC-Stil

## Einschränkungen

1. Dokumente für den Fehlerdatenfluss über Web-Services haben die folgenden Einschränkungen:
   - Web-Service-Anforderungen müssen unidirektionale Anforderungen sein.
   - Ist der Bindungsstil **document**, verwendet der Eingabeparametertyp das Element **ErrorFlowDocument**, das in der Datei "BCGErrorFlowSchema.xsd" definiert ist.
   - Ist der Bindungsstil **rpc**, ist der Eingabeparametertyp **String**, und die Anzahl der Eingabeparameter ist 1.
2. Die Weiterleitung des Fehlerdatenflusses kann nicht verwendet werden, wenn eine falsche Geschäfts-ID vorliegt. Auch dann, wenn ein Dokument für den Fehlerdatenfluss für ein bestimmtes Ereignis angefordert wird und das Geschäftsdokument, das falsche IDs verwendet, mit diesem konfigurierten Ereignis fehlschlägt, kann die Weiterleitung des Fehlerdatenflusses nicht verwendet werden, weil die angegebenen Geschäfts-IDs ungültig sind.

# Kapitel 16. Konfiguration fertigstellen

Dieses Kapitel beschreibt zusätzliche Aufgaben, die Sie ausführen können, um den Hub zu konfigurieren. Es behandelt die folgenden Themen:

- „Unterstützung für große Dateien für AS-Dokumente”
- „Verwendung von APIs aktivieren”
- „Die für Ereignisse verwendeten Warteschlangen angeben” auf Seite 314
- „Alertfähige Ereignisse angeben” auf Seite 316
- „ Benutzerdefinierten Transport aktualisieren” auf Seite 316
- „Muster ” auf Seite 316

**Anmerkung:** Verwenden Sie stets die Browserinstanz, mit der Sie sich an Community Console angemeldet haben, wenn Sie Konfigurationsänderungen an WebSphere Partner Gateway vornehmen. Die gleichzeitige Verwendung mehrerer Browserinstanzen kann dazu führen, dass die Konfigurationsänderungen aufgehoben werden.

## Unterstützung für große Dateien für AS-Dokumente

Die Unterstützung für große Dateien, deren Größe im Bereich von Gigabyte liegt, wurde für AS2 und AS3 erweitert. Die maximale Größe von Dateien, die unter Verwendung von Bytefeldgruppen verarbeitet werden, ist konfigurierbar. Ist die Menge des zugeordneten Speichers größer als die Größe des verfügbaren Heapspeichers, tritt ein Fehler des Typs "OutOfMemoryError" auf. Ist der Umfang der Daten kleiner als der verfügbare Speicher kann dennoch ein Fehler des Typs "OutOfMemoryError" auftreten, wenn die Menge an zugeordnetem Speicher den verfügbaren Speicher übersteigt. Bei der Ausführung wird auf der Basis des verfügbaren Heapspeichers ermittelt, ob die konfigurierte Dateigröße unterstützt werden kann. Die maximale Dateigröße, die mithilfe von Bytefeldgruppen verwendet werden kann, wird über die Eigenschaft **bcg.maximumFileSizeForByteArrays** angegeben. Der Wert der Eigenschaft **bcg.maximumFileSizeForByteArrays** wird in MB angegeben. Übersteigt die Dateigröße den Wert für diese Eigenschaft, wird die Datei mithilfe von Datenströmen (Streams) verarbeitet. Ist die Dateigröße kleiner als der Wert dieser Eigenschaft, ist jedoch nicht ausreichend Speicher verfügbar, wird das Fehlerereignis BCG210050 generiert.

Melden Sie sich als Hubbetreiber an und navigieren Sie zur Registerkarte **Systemverwaltung** > **Gemeinsame Eigenschaften**. Überschreiben Sie den Standardwert der Eigenschaft **bcg.maximumFileSizeForByteArrays** und geben Sie die maximale Größe von Dateien an, die mit Bytefeldgruppen verwendet werden sollen. Durch das Erhöhen des Werts für diese Eigenschaft wird die Leistung verbessert.

## Verwendung von APIs aktivieren

WebSphere Partner Gateway stellt eine Gruppe von APIs bereit, mit denen auf bestimmte Funktionen zugegriffen werden kann, die üblicherweise in Community Console ausgeführt werden. Diese APIs werden im*WebSphere Partner Gateway Programmer Guide* beschrieben.

Verwenden Sie diese Prozedur, um die Verwendung der XML-basierten APIs zu aktivieren, sodass Partner API-Aufrufe auf dem WebSphere Partner Gateway-Server durchführen können:

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

**Anmerkung:** Die XML-basierte Administrator-API wird nicht weiter unterstützt.

Anstelle der Administrator-API kann auch das Migrationsprogramm verwendet werden, um Erstellungs- und Aktualisierungstasks auszuführen. Die Migrationsimportdatei enthält neue oder aktualisierte Informationen.

Die Importdatei wird durch das XML-Schema beschrieben, das im Lieferumfang des Migrationsprogramms enthalten ist. Mit einem Entwicklungstool wie Rational Application Developer können Sie eine XML-Importdatei erstellen, die mit dem Schema konform ist. Wenn Sie diese Datei mit dem Migrationsprogramm importieren, können Sie neue Partnerdefinitionen laden, einschließlich Kontakten und Geschäfts-ID für die Partner. Sie können auch vorhandene Partnerdefinitionen aktualisieren, indem Sie diese mit dem Migrationsprogramm importieren. Mit der Administrator-API können Sie außerdem einige der Konfigurationsartefakte in einem System auflisten. Durch einen vollständigen Export des Systems mithilfe des Migrationsprogramms werden Partnerfunktionalitäten, Partnerverbindungen und Empfänger (Ziele) in der exportierten xml-Datei aufgelistet.

Die Batchdatei **bcgmigrate.bat/bcgmigrate.sh** wird verwendet, um den Migrationsprozess zu starten. Wenn Sie den Befehl **bcgmigrate** ausführen, müssen Sie sicherstellen, dass Sie über die Dateiberechtigung **Ausführen** für bcgmigrate.bat bzw. bcgmigrate.sh verfügen. Dies gilt besonders für UNIX-Plattformen.

## Die für Ereignisse verwendeten Warteschlangen angeben

Sie können den Hub konfigurieren, um einer externen Warteschlange Ereignisse zuzustellen, die unter Verwendung der JMS-Konfiguration konfiguriert wurde.

Die Standard-JMS-Konfiguration wird eingerichtet, wenn Sie den Hub installieren. Sie können einige dieser Werte auf der Seite **Merkmale für Ereignisveröffentlichung** sehen.

Wenn auf eine andere JMS-Konfiguration verwiesen werden soll, geben Sie die entsprechenden Konfigurationswerte an, um die Ereignisse entweder für WebSphere Partner Gateway bzw. WAS-interne Nachrichtenwarteschlangen oder andere Nachrichtenserver zu veröffentlichen. Ändern Sie außerdem den Namen der Warteschlange, sodass er mit dem Namen der Warteschlange übereinstimmt, in der die Ereignisse veröffentlicht werden.

Gehen Sie wie folgt vor, um anzugeben, wohin die Ereignisse übermittelt werden sollten:

1. Klicken Sie im Hauptmenü auf **Systemverwaltung > DocMgr-Verwaltung > Ereignisengine > Externe Ereignisse**.

2. Klicken Sie auf das Symbol **Bearbeiten** neben **Ereigniszustellung aktivieren**.
3. Wählen Sie das Kontrollkästchen **Ereigniszustellung aktivieren** aus, um die Ereignisveröffentlichung zu aktivieren.
4. Wenn die Standardwerte für Ihre Installation korrekt sind, verändern Sie diese nicht. Die Standardwerte unterstützen die Ereignisübermittlung an die Warteschlange namens **DeliveryQ**, die vom JMS-Server bereitgestellt wird, welchen Sie während der Installation konfiguriert haben.

   Wenn Sie ändern wollen, wohin Ereignisse übermittelt werden, aktualisieren Sie die Felder. Verwenden Sie die folgenden Informationen als Referenz:

   - Geben Sie Werte für **Benutzer-ID** und **Kennwort** ein, wenn eine Benutzer-ID und ein Kennwort für den Zugriff auf die Warteschlange erforderlich sind.
   - Geben Sie für **JMS-Warteschlangenfactory-Name** den Namen der JMS-Warteschlangenverbindungsfactory von der JMS-Datei .bindings ein, die Sie verwenden.

     **Anmerkung:** In einigen Windows-Versionen vor XP müssen Sie unter Umständen den Standardwert des Felds **JMS-Warteschlangenfactory-Name** ändern, wenn Sie die Standardfunktion für Ereigniszustellung verwenden wollen. Sie müssen den Wert für **JMS-Warteschlangenfactory-Name** von `WBIC/QCF` in `WBIC\\QCF` ändern.
   - Geben Sie für **JMS-Nachrichtentyp** den Nachrichtentyp ein, der übermittelt wird. Die Auswahlmöglichkeiten sind hier **byte** oder **text**. Da die Zuordnung des JMS-Nachrichtentyps durch die Empfängerkomponente festgelegt wird, ist der Wert für den JMS-Nachrichtentyp optional.
   - Geben Sie für **JMS-Warteschlangenname** den Namen der JMS-Warteschlange ein, in der die Ereignisse veröffentlicht werden. Diese Warteschlange muss bereits in der JMS-Datei '.bindings' definiert sein, die Sie in WebSphere MQ verwenden.

     **Anmerkung:** In einigen Windows-Versionen vor XP müssen Sie unter Umständen den Standardwert des Felds **JMS-Warteschlangenname** ändern, wenn Sie die Standardfunktion für Ereigniszustellung verwenden wollen. Sie müssen den Wert für **JMS-Warteschlangenname** von `WBIC/DeliveryQ` in `WBIC\\DeliveryQ` ändern.
   - Geben Sie für **JNDI-Factory-Name** den Namen ein, der für den Zugriff auf die .bindings-Datei verwendet wird. Der Standardwert bietet Zugriff auf die Standardbindung im Dateisystem.
   - Geben Sie für **Provider-URL-Pakete** eine URL ein, die Zugriff auf die JMS-Bindungsdatei bietet. Diese URL muss dem JNDI-Factory-Name entsprechen. Dieses Feld ist optional und, wenn es leer ist, wird die Standarddateisystemposition für JMS-Bindungen verwendet.
   - Geben Sie für **Nachrichtenzeichensatz** den Zeichensatz ein, der zum Erstellen der Bytenachricht in der JMS-Warteschlange verwendet werden soll. Der Standardwert ist UTF-8. Dieses Feld ist nur für Bytenachrichten relevant.
   - Geben Sie für **JMS-Provider-URL** die URL des JMS-Providers ein. Dieses Feld ist optional und, wenn es leer ist, wird der Standard-JMS-Provider verwendet, der bei der Installation angegeben wurde.
5. Klicken Sie auf **Speichern**.

## Alertfähige Ereignisse angeben

Wenn ein Ereignis in WebSphere Partner Gateway auftritt, wird ein Ereigniscode generiert. Mit der Seite **Ereigniscodes** können Sie den alertfähigen Status des Ereigniscodes festlegen. Wenn ein Ereignis als alertfähig festgelegt wurde, wird das Ereignis in der Liste **Ereignisname** der Seite **Alert** angezeigt. Sie können dann einen Alert für das Ereignis festlegen.

Gehen Sie wie folgt vor, um anzugeben, welche Ereignisse alertfähig sein sollten:

1. Klicken Sie auf **Hubadmin > Hubkonfiguration > Ereigniscodes**. Die Seite **Ereigniscodes** wird angezeigt.
2. Gehen Sie für jedes Ereignis, das Sie alertfähig machen wollen, wie folgt vor:
   a. Klicken Sie auf das Symbol **Details anzeigen** neben dem Ereigniscode. Die Seite **Ereigniscodedetails** wird angezeigt.
   b. Wählen Sie **Alertfähig?** aus.
   c. Klicken Sie auf **Speichern**.

## Benutzerdefinierten Transport aktualisieren

Wie in Kapitel 7, „Empfänger definieren", auf Seite 59 und in Kapitel 11, „Ziele erstellen", auf Seite 227 beschrieben, können Sie eine XML-Datei hochladen, die einen benutzerdefinierten Transport beschreibt. Sie können mit **Transporttypen verwalten** die Datei hochladen. Nachdem Sie die XML-Datei hochgeladen haben, ist der Transport zur Verwendung verfügbar, wenn Sie einen Empfänger oder ein Ziel definieren.

Die XML-Datei, die den benutzerdefinierten Transport beschreibt, schließt die Attribute für den Transport mit ein. Diese Attribute werden im Abschnitt **Angepasste Transportattribute** auf der Seite für den Empfänger oder das Ziel angezeigt, wenn Sie einen benutzerdefinierten Transport angeben. Ein benutzerdefinierter Transport für ein Ziel könnte beispielsweise das Attribut **DestinationRetryCount** mit einschließen.

Der Autor der XML-Datei, die den Transport beschreibt, kann die Attribute aktualisieren, indem er die Attribute hinzufügt, löscht oder ändert. Wenn die XML-Datei geändert wurde, laden Sie die Datei mit **Transporttypen verwalten** erneut hoch. Jede Änderung an den Attributen wird auf der Seite für das Ziel oder den Empfänger wiedergegeben.

## Muster

Im Lieferumfang von WebSphere Partner Gateway sind einige Muster enthalten, die angepasste Funktionalität und Veranschaulichungen bereitstellen. Diese Pakete befinden sich unter den Ordnern **DevelopmentKits** und **Integration** in dem Verzeichnis, in das die Installation von WebSphere Partner Gateway extrahiert wurde.

Der Ordner **DevelopmentKits** enthält die folgenden Muster:

- Administrator-API: Da Administrator-APIs nicht weiter unterstützt werden, wird das Dienstprogramm für die Partnermigration verwendet, um Tasks zu erstellen und zu aktualisieren.
- Migration: Enthält Muster für das Exportieren und Importieren von Konfigurationen.

  - Exportkonfiguration: Veranschaulicht die Vorgehensweise zum Exportieren der Konfigurationen von WebSphere Partner Gateway mithilfe einer Java-Komponente unter Verwendung einer über die Befehlszeile ausgeführten Scriptdatei.
  - Importkonfiguration: Veranschaulicht die Vorgehensweise zum Importieren der Konfigurationen von WebSphere Partner Gateway mithilfe einer Java-Komponente unter Verwendung einer über die Befehlszeile ausgeführten Scriptdatei.
- Benutzerexits: Enthält Muster zum Schreiben von angepasstem Code für Benutzerexits, um Umsetzungen und Validierungen auszuführen.
  - Das Muster *EDITransTypeBusinessProcess* stellt angepasste Funktionalität für EDI-Dokumente bereit, die durch das System geleitet werden. Dieses Muster für einen Benutzerexit ist so konzipiert, dass es den EDI-Transaktionstyp aus einem EDI X12-Dokument parst. Durch das Ändern der Parsingkriterien können andere Werte extrahiert werden.
  - Das Muster *custom translation user exit* stellt die Umsetzungsfunktionalität für ein eingehendes XML-Dokument bereit.
  - Das Muster *custom validation user exit* stellt die Validierungsfunktionalität für ein eingehendes XML-Dokument bereit.
- Musterszenarios: Enthält Muster, die Richtlinien für das Einrichten eines WebSphere Partner Gateway-Systems für die unten aufgeführten Protokolle ohne Verpackung und mit AS-Verpackung bereitstellen. Für jedes Protokoll wird auch die Importdatei für die Konfiguration bereitgestellt.
  - Angepasstes XML
  - EDI-X12
  - Binäre Dokumente

Der Ordner **Integration** enthält die folgenden Muster für die Integration:

- Integration von WebSphere Transformation Extender: Muster für die Veranschaulichung der Integration mit WebSphere Transformation Extender zum Umsetzen eines XML-Dokuments in eine Flachdatei.
- Muster für WebSphere Business Integration Message Broker: Muster, mit dem veranschaulicht wird, wie WebSphere Partner Gateway mit WebSphere Business Integration Message Broker kommuniziert.
- Integration mit WebSphere Process Server: Muster, mit dem veranschaulicht wird, wie WebSphere Partner Gateway über JMS mit WebSphere Process Server integriert wird.
- Integration mit WebSphere Interchange Server: Muster, mit dem veranschaulicht wird, wie WebSphere Partner Gateway über HTTP und JMS mit Interchange Server integriert wird.

# Kapitel 17. CPP/CPA-Editor

Der CPP/CPA-Editor ist ein Eclipse-Plug-in, das die Erstellung von CPP/CPA-Dokumenten anhand einer Vorlage unterstützt und dem Benutzer die Bearbeitung mit einem Tabellenformat ermöglicht. Darüber hinaus ist es für die Daten- und Schemaprüfung zuständig.

**Voraussetzungen:**

- WID/RAD-Version 6.1 und höher ist erforderlich.
- Stellen Sie das heruntergeladene CPP/CPA-Editor-Plug-in in den EDI-Plug-in-Ordner.

Ein CPA-Dokument (CPA = Collaboration-Protocol Agreement) kann auch aus zwei CPP-Dokumenten (CPP = Collaboration-Protocol Profile) erstellt werden. CPP definiert die Funktionalität einer Partei, die elektronische Geschäftsbeziehungen mit anderen Parteien unterhält. CPA beschreibt die Vereinbarung hinsichtlich des Nachrichtenaustauschs zwischen zwei Parteien. Geben Sie für die CPP-Erstellung die Werte für einzelne XML-Elemente (einzelne XML-Elemente bestehen aus verschiedenen Attributen) über die Benutzerschnittstelle des Editors ein. Sobald das CPA-Dokument mit dem Editor erstellt wurde und der zugehörige Status AGREED lautet, dann es in WebSphere Partner Gateway importiert werden. Von den importierten Dateien werden automatisch die folgenden Elemente erstellt:

- Partner
- B2B-Ziele
- Interaktionen und Verbindungen

Darüber hinaus werden Dokumentdefinitionen automatisch definiert und die erforderliche B2B-Funktionalität wird aktiviert.

Unter Verwendung der Benutzerschnittstelle des CPP/CPA-Editors können Sie die folgenden Aktionen ausführen:

- „CPP-Dokument erstellen"
- „CPA-Dokument erstellen" auf Seite 320
- „Werte im Editor bearbeiten" auf Seite 321

Gehen Sie wie folgt vor, um den CPP/CPA-Editor als Standardeditor zu definieren:

1. Klicken Sie in der Eclipse-Plug-in-Umgebung auf das Fenstermenü und wählen Sie **Preferences** aus.
2. Klicken Sie im Fenster **Preferences** auf **General > Editor > File Association**.
3. Wählen Sie in der Liste mit den Dateitypen "*.xml" und in der Liste der zugeordneten Editoren "CPPEditor Multi – page Editor" aus.
4. Klicken Sie auf **Default**.

## CPP-Dokument erstellen

Gehen Sie wie folgt vor, um ein CPP-Dokument zu erstellen:

1. Wählen Sie in der IDE die Optionen **File** >**New** aus.
2. Wählen Sie im Fenster **New** die Optionen **CPAEditor** > **Collaboration Protocol Profile file** aus.
3. Klicken Sie auf **Next** und geben Sie die Werte des CPP/CPA-Inhabers ein.

4. Klicken Sie auf **Finish**. Die neue Datei wird unter dem angegebenen Container erstellt.
5. Wenn Sie **CPAEditor** als Standardeinstellung konfiguriert haben, müssen Sie die Werte in der Vorlage ändern. Andernfalls wird die Datei im XML-Editor geöffnet. Klicken Sie zum Öffnen der Datei im CPA-Editor mit der rechten Maustaste und wählen Sie **Open with** > **CPAEditor Multi-Page Editor** aus.
6. Geben Sie die Werte für die Attribute aller Elemente ein. Für bestimmte Attribute können Sie die entsprechenden Werte über die verschiedenen Optionen auswählen.
7. Klicken Sie auf **Save**. Daraufhin wird eine Nachricht angezeigt, in der die erfolgreiche Erstellung eines CPP-Dokuments bestätigt wird.

## CPA-Dokument erstellen

Wählen Sie eine der beiden folgenden Optionen aus:

- Fall 1: Das CPA-Dokument wird anhand einer Vorlage erstellt. Dabei können die Werte für einzelne XML-Elemente (einzelne XML-Elemente bestehen aus verschiedenen Attributen) über die Benutzerschnittstelle des Editors eingegeben werden.
- Fall 2: Das CPA-Dokument wird aus zwei CPP-Dokumenten erstellt.

Gehen Sie wie folgt vor, um ein CPA-Dokument anhand einer Vorlage zu erstellen:

1. Wählen Sie in der IDE die Optionen **File** >**New** aus.
2. Wählen Sie im Fenster **New** die Optionen **CPAEditor** > **Collaboration Protocol Agreement file** aus.
3. Klicken Sie auf **Next** und geben Sie die Werte des CPP/CPA-Inhabers ein.
4. Klicken Sie auf **Finish**. Die neue Datei wird unter dem angegebenen Container erstellt.
5. Wenn Sie **CPAEditor** als Standardeinstellung konfiguriert haben, müssen Sie die Werte in der Vorlage ändern. Andernfalls wird die Datei im XML-Editor geöffnet. Klicken Sie zum Öffnen der Datei im CPA-Editor mit der rechten Maustaste und wählen Sie **Open with** > **CPPEditor Multi-Page Editor** aus.
6. Geben Sie die Werte für die Attribute aller Elemente ein. Für bestimmte Attribute können Sie die entsprechenden Werte über die verschiedenen Optionen auswählen.
7. Klicken Sie auf **Save**. Daraufhin wird eine Nachricht angezeigt, in der die erfolgreiche Erstellung eines CPA-Dokuments bestätigt wird.

Gehen Sie wie folgt vor, um ein CPA-Dokument aus zwei CPP-Dokumenten zu erstellen:

1. Klicken Sie in der IDE auf **File** > **New** > **Other**.
2. Wählen Sie im Fenster **New** die Optionen **CPAEditor** > **Merge Collaboration Protocol Profiles** aus.
3. Klicken Sie auf **Next**.
4. Geben Sie die Werte des CPP/CPA-Inhabers sowie Pfad und Namen der CPP-Dateien ein, die zusammengeführt werden sollen.
5. Klicken Sie auf **Finish**. Die zusammengeführte Datei wird unter dem angegebenen Container erstellt.

6. Wenn Sie **CPAEditor** als Standardeinstellung konfiguriert haben, müssen Sie die Werte in der Vorlage ändern. Andernfalls wird die Datei im XML-Editor geöffnet. Klicken Sie zum Öffnen der Datei im CPA-Editor mit der rechten Maustaste und wählen Sie **Open with** > **CPPEditor Multi-Page Editor** aus.

## Werte im Editor bearbeiten

Bewegen Sie den Cursor zum Bearbeiten der Werte in der Editortabelle auf die Zelle und bearbeiten Sie die Werte. Jedem PartyInfo-Element ist ein eindeutiges partyName-Element zugeordnet. Die folgenden Unterelemente treten unter dem Element PartyInfo auf: PartyId, PartyRef, Collaboration Role, Certificate, SecurityDetails, DeliveryChannel, Transport, DocExchange und OverrideMshActionBinding. Diese Werte stehen auf verschiedenen Registerkarten des CPP/CPA-Editors zur Verfügung. PartyName dient als eindeutige Kennung, mit deren Hilfe die Unterelemente von PartyInfo dem entsprechenden PartyInfo-Element zugeordnet werden.

Beispielsweise kann ein Zertifikatelement, das ein Unterelement des PartyInfo-Elements ist, mehrmals auftreten. Das PartyInfo-Element wiederum kann in einem CPP-Dokument mehrmals auftreten.

# Kapitel 18. Web Mail Box

Die neuen Funktionen im Release von Web Mail Box stellen eine Erweiterung der vorhandenen Unterstützung von WebSphere Partner Gateway dar. Partner, Kunden und Lieferanten können nun mit dem Hub einfach unter Verwendung eines unterstützten Browsers interagieren, d. h., sie verfügen nun über die Unterstützung für webbasierte B2B-Interaktionen. Die Webversion der WebSphere Partner Gateway-Konsole wird in einem Browser geöffnet, wobei keine externe Infrastruktur (wie beispielsweise FTP-Server oder E-Mail-Einrichtungen) erforderlich ist. In dieser Version von WebSphere Partner Gateway könne die folgenden zusätzlichen Tasks ausgeführt werden:

- Dokumente für Transaktionen hochladen
- Status von Geschäftsdokumenten überwachen
- Empfangene Geschäftsdokumente herunterladen

Diese Funktion ist in erster Linie für externe Partner konzipiert, die nicht über die Infrastruktur für die Teilnahme an Transaktionen verfügen. In diesem Kapitel werden die Schritte zur Vorbereitung beschrieben, die erforderlich sind, um mit der Funktion Web Mail Box zu arbeiten.

**Anmerkung:** Dieses Release unterstützt Dokumente nur im Paket "None".

## Voraussetzungen

Damit ein externer Partner die Funktionen von Web Mail Box nutzen kann, muss der Hubadministrator die folgenden Berechtigungen erteilen:

- „Web Mail Box auf der Hubebene aktivieren”
- „Web Mail Box auf der Partnerebene aktivieren”
- „WebBoxReceiver aktivieren” auf Seite 324

### Web Mail Box auf der Hubebene aktivieren

Gehen Sie wie folgt vor, um die Berechtigungen für den Eingang und den Ausgang zu ändern:

1. Navigieren Sie zur Seite **Hubadmin** > **Konsolkonfiguration** > **Berechtigungen**.
2. Aktivieren Sie in der Liste **Berechtigung** die Einträge "Eingang" und "Ausgang".

**Anmerkung:** Dies ist eine einmalige Aktivität für den Hubadministrator.

### Web Mail Box auf der Partnerebene aktivieren

Führen Sie die folgenden Schritte für einen neuen externen Partner aus:

1. Melden Sie sich als Hubadministrator an der Konsole an.

   **Anmerkung:** Wenn Sie einen neuen externen Partner erstellen, wird automatisch eine Standardgruppe für Webbenutzer erstellt. Darüber hinaus wird die Standardgruppe für Webbenutzer auch für vorhandene Partner erstellt, wenn dieser Patch installiert wird.

2. Klicken Sie auf der Seite **Gruppen** auf das Symbol zum Anzeigen der Berechtigungen für die neu erstellte Gruppe.
3. Wählen Sie für die Eingabe und die Ausgabe die Berechtigung **Lese-/Schreibzugriff** aus.
4. Erstellen Sie einen neuen Benutzer.
5. Ordnen Sie auf der Seite **Zugehörigkeiten** den Benutzer einer Gruppe zu.

**Anmerkung:** Dies ist eine einmalige Aktivität für den Hubadministrator.

### WebBoxReceiver aktivieren

Nach der Installation der Funktion Web Mail Box muss der Hubadministrator den Empfänger aktivieren, bevor Dokumente an den internen Partner gesendet werden können. Der standardmäßige Status von WebBoxReceiver ist "Inaktiviert".

**Anmerkung:** WebBoxReceiver wird vom System erstellt und kann nicht gelöscht werden.
Führen Sie die folgenden Schritte aus, um WebBoxReceiver zu aktivieren:

1. Navigieren Sie zu **Hubadmin** > **Empfänger**.
2. Aktivieren Sie WebBoxReceiver.

**Anmerkung:** Um das Abfrageintervall für WebBoxReceiver anzupassen, können Sie das Attribut für das Abfrageintervall entsprechend ändern.

## Einschränkungen von Web Mail Box

Im Folgenden werden die Einschränkungen von Web Mail Box aufgelistet:

- Es können maximal 10 MB an interne Partner gesendet werden.

  **Anmerkung:** Abhängig vom Netz, dem Browser und dem verfügbaren Arbeitsspeicher kann dieser Wert größer oder kleiner sein.
- Der Web Box-Empfänger kann nicht gelöscht werden.
- EDI/XML-Dokumente können nicht im Binärformat gesendet werden.

# Kapitel 19. Grundlegende Beispiele

Dieser Anhang enthält Beispiele für das Konfigurieren des Hubs. Er behandelt die folgenden Themen:

- „ Basiskonfiguration – EDI-Pass-Through-Dokumente austauschen"
- „ Basiskonfiguration - Sicherheit für eingehende und ausgehende Dokumente konfigurieren" auf Seite 331
- „Basiskonfiguration erweitern" auf Seite 337

Ein separater Anhang enthält Beispiele für das Austauschen von EDI-Austauschvorgängen, die das Entfernen von Umschlägen, das Transformieren, das Versehen mit Umschlägen und das Übertragen von funktionalen Bestätigungen einschließen. Siehe Kapitel 20, „EDI-Beispiele", auf Seite 345.

Diese Beispiele sollen Ihnen eine schnelle Übersicht über die Schritte geben, die zum Konfigurieren eines Systems erforderlich sind. Wenn Sie diese Beispiele verwenden, um Ihr System zu konfigurieren, ändern Sie die spezifischen Informationen, z. B. die Namen und Geschäfts-IDs, um sie Ihren Geschäftsbedürfnissen anzupassen.

## Basiskonfiguration – EDI-Pass-Through-Dokumente austauschen

In diesem Beispiel ist die Hubkonfiguration relativ einfach gehalten: Es sind zwei Empfänger definiert (einer für Dokumente, die beim Hub von einem Partner eingehen, und einer für Dokumente, die beim Hub vom Back-End-System des internen Partners eingehen). Die Austauschvorgänge, die in diesem Beispiel konfiguriert werden, verwenden die Dokumentdefinitionen, die von WebSphere Partner Gateway bereitgestellt werden. Aus diesem Grund müssen Sie nur Interaktionen auf der Basis dieser Dokumentenflüsse erstellen. In diesem Beispiel wird kein kundenspezifisches XML verwendet.

Dieses Beispiel zeigt einen Austausch zwischen einer Back-End-Anwendung des internen Partners und einem externen Partner (Partner Zwei).

### Hub konfigurieren

Der erste Schritt bei der Konfiguration des Hubs besteht darin, die beiden Empfänger zu erstellen.

- Einen HTTP-Empfänger (namens "HttpReceiver") zum Empfangen von Dokumenten über HTTP (von Partner Zwei), die an das Back-End-System des internen Partners gesendet werden sollen.
- Einen Dateiverzeichnisempfänger (namens "FileSystemReceiver") zum Abrufen der Dokumente aus dem Dateisystem (vom Back-End-System des internen Partners), die an Partner Zwei gesendet werden sollen.

#### Empfänger definieren

Gehen Sie wie folgt vor, um einen Empfänger für den Empfang von Dokumenten über HTTP zu erstellen:

1. Klicken Sie auf **Hubadmin > Hubkonfiguration > Empfänger**.
2. Klicken Sie auf **Empfänger erstellen**.

3. Geben Sie als Empfängernamen **HttpReceiver** ein.
4. Wählen Sie in der Liste **Transport** die Option **HTTP/S** aus.
5. Verwenden Sie als Betriebsmodus den Standardwert **Produktion**.
6. Geben Sie als URI Folgendes ein: **/bcgreceiver/submit**
7. Klicken Sie auf **Speichern**.

Erstellen Sie dann einen Empfänger, um ein Verzeichnis im Dateisystem abzufragen. Durch das Erstellen des Empfängers wird automatisch ein neues Verzeichnis im Dateisystem erstellt.

Gehen Sie wie folgt vor, um den Dateisystemempfänger zu erstellen:

1. Klicken Sie auf **Hubadmin > Hubkonfiguration > Empfänger**.
2. Klicken Sie auf **Empfänger erstellen**.
3. Geben Sie als Empfängernamen **FileSystemReceiver** ein.
4. Wählen Sie in der Liste **Transport** die Option **Dateiverzeichnis** aus.
5. Verwenden Sie als standardmäßigen Betriebsmodus den Standardwert **Produktion**.
6. Geben Sie als Dokumentstammverzeichnispfad Folgendes ein: **\temp\ FileSystemReceiver**

   **Anmerkung:** Dadurch wird das Verzeichnis 'FileSystemReceiver' innerhalb des temporären Verzeichnisses erstellt. Stellen Sie sicher, dass ein Verzeichnis **temp** im Dateisystem vorhanden ist.
7. Klicken Sie auf **Speichern**.

## Dokumenttypen und Interaktionen definieren

In diesem Beispiel konfigurieren Sie den Austausch von Dokumenten, die dem EDI-X12-Standard entsprechen. In diesem Beispiel werden die Dokumente einfach durch den Hub weitergeleitet. Vom EDI-Austausch wird kein Umschlag entfernt und es tritt auch keine Transformation auf. Beispiele für das Entfernen von Umschlägen eines Austauschs, dem Transformieren der Transaktionen und dem Senden von Bestätigungen finden Sie in Kapitel 23, „Attribute”, auf Seite 437.

In diesem Abschnitt werden die folgenden Austauschvorgänge beschrieben:

- Ein EDI-X12-Dokument ohne Paket vom internen Partner an 'Partner Zwei' senden.
- Ein EDI-X12-Dokument im AS2-Paket von 'Partner Zwei' an den internen Partner senden.

Aufgrund der einbezogenen Pakete und Protokolle muss keine neue Dokumentdefinition erstellt werden. Die Pakete, Protokolle und Dokumenttypen sind im System vordefiniert.

Sie müssen allerdings Interaktionen auf der Basis dieser vordefinierten Dokumenttypen definieren.

Erstellen Sie die erste Interaktion, in der die Quelle ein ISA-formatiertes Dokument ist, das dem EDI-X12-Standard ohne Paket entspricht, und das Ziel ein ISA-formatiertes Dokument ist, das dem EDI-X12-Standard mit AS2-Paket entspricht.

1. Klicken Sie auf **Hubadmin > Hubkonfiguration > Dokumentdefinition > Interaktionen verwalten**.

2. Klicken Sie in der Anzeige **Interaktionen verwalten** auf den Link **Interaktion erstellen**.
3. Erweitern Sie in der Spalte **Quelle** Folgendes:
   a. **Paket: None**
   b. **Protokoll: EDI-X12**
4. Klicken Sie auf **Dokumenttyp: ISA**.
5. Erweitern Sie in der Spalte **Ziel** Folgendes:
   a. **Paket: AS**
   b. **Protokoll: EDI-X12**
6. Klicken Sie auf **Dokumenttyp: ISA**.
7. Wählen Sie in der Liste **Aktion** die Option **Pass-Through** aus.
8. Klicken Sie auf **Speichern**.

Erstellen Sie eine zweite Interaktion, in der das Quellenformat ein ISA-formatiertes Dokument ist, das dem EDI-X12-Standard mit AS-Paket entspricht, und das Zielformat ein ISA-formatiertes Dokument ist, das dem EDI-X12-Standard ohne Paket entspricht:

1. Klicken Sie auf den Link **Interaktion erstellen**.
2. Erweitern Sie in der Spalte **Quelle** Folgendes:
   a. **Paket: AS**
   b. **Protokoll: EDI-X12**
3. Klicken Sie auf **Dokumenttyp: ISA**.
4. Erweitern Sie in der Spalte **Ziel** Folgendes:
   a. **Paket:None**
   b. **Protokoll: EDI-X12**
5. Klicken Sie auf **Dokumenttyp:ISA**.
6. Wählen Sie in der Liste **Aktion** die Option **Pass-Through** aus.
7. Klicken Sie auf **Speichern**.

## Partner und Partnerverbindungen erstellen

In diesem Beispiel wird ein externer Partner zusätzlich zum internen Partner erstellt. Die Ziele für die Partner umfassen Standardtransporte. Es sind keine Konfigurationspunkte für die Ziele definiert.

### Partner erstellen

Erstellen Sie zwei neue Partner. Gehen Sie wie folgt vor, um den internen Partner zu definieren:

1. Klicken Sie im Hauptmenü auf **Kontenadmin**. Die Seite **Partnersuche** ist die Standardanzeige.
2. Klicken Sie auf **Erstellen**.
3. Geben Sie als Anmeldenamen des Unternehmens Folgendes ein: **CommMan**.
4. Geben Sie als Anzeigenamen des Partners Folgendes ein: **Comm Man**.
5. Wählen Sie als Partnertyp **Interner Partner** aus.
6. Klicken Sie auf **Neu** unterhalb von **Geschäfts-ID**.
7. Behalten Sie für **Typ** den Eintrag **DUNS** bei und geben Sie einen Kennungswert **123456789** ein.

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

8. Klicken Sie auf **Neu** unterhalb von **Geschäfts-ID**.
9. Wählen Sie **Unformatiert** aus und geben Sie einen Kennungswert von **12-3456789** ein.
10. Klicken Sie auf **Speichern**.

Gehen Sie wie folgt vor, um **Partner Zwei** zu definieren:

1. Klicken Sie auf **Kontenadmin > Profile > Partner**.
2. Klicken Sie auf **Erstellen**.
3. Geben Sie als Anmeldenamen des Unternehmens Folgendes ein: **partnerZwei**.
4. Geben Sie als Anzeigenamen des Partners Folgendes ein: **Partner Zwei**.
5. Wählen Sie als Partnertyp **Externer Partner** aus.
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 den internen Partner als auch 'Partner Zwei' für den Hub definiert.

Zu den nächsten Schritten gehört nun das Konfigurieren von Zielen für den internen Partner und 'Partner Zwei'.

## Ziele erstellen

Bevor Sie ein Dateiverzeichnisziel für den internen Partner erstellen, müssen Sie die Verzeichnisstruktur erstellen, die von diesem Ziel verwendet wird. Erstellen Sie ein neues Verzeichnis **FileSystemDestination** auf dem Stammlaufwerk. In diesem Verzeichnis speichert der interne Partner Dateien, die von externen Partnern empfangen wurden.

In Falle des internen Partners stellt das Ziel den Einstiegspunkt in das Back-End-System dar.

Gehen Sie wie folgt vor, um ein Ziel für den internen Partner zu erstellen:

1. Klicken Sie auf **Kontenadmin > Profile > Partner**.
2. Klicken Sie auf **Suchen**.
3. Wählen Sie **Interner Partner** aus, indem Sie auf das Symbol **Details anzeigen** klicken.
4. Klicken Sie in der horizontalen Navigationsleiste auf **Ziele**.
5. Klicken Sie auf **Erstellen**.
6. Geben Sie als Namen des Ziels **FileSystemDestination** ein.
7. Wählen Sie als **Transport** die Option **Dateiverzeichnis** aus.
8. Geben Sie als Adresse Folgendes ein: **file://C:\FileSystemDestination**.
9. Klicken Sie auf **Speichern**.

Legen Sie nun dieses neu erstellte Ziel als das Standardziel für den internen Partner fest.

1. Klicken Sie auf **Liste**, um alle für den internen Partner konfigurierten Ziele aufzulisten.
2. Klicken Sie auf **Standardziele anzeigen**.
3. Wählen Sie in der Liste **Produktion** den Eintrag **Dateisystemziel** aus.
4. Klicken Sie auf **Speichern**.

Erstellen Sie ein Ziel für 'Partner Zwei'.

1. Klicken Sie auf **Kontenadmin > Profile > Partner**.
2. Klicken Sie auf **Suchen** und wählen Sie dann Partner Zwei aus, indem Sie auf das Symbol **Details anzeigen** klicken.
3. Klicken Sie in der horizontalen Navigationsleiste auf **Ziele**.
4. Klicken Sie auf **Erstellen**.
5. Geben Sie als Namen des Ziels Folgendes ein: **HttpDestination**.
6. Wählen Sie als **Transport** die Option **HTTP/1.1** aus.
7. Geben Sie als Adresse Folgendes ein: **http://<***IP-adresse***>:80/input/AS2**. Dabei steht <*IP-adresse*> für den Computer von **Partner Zwei**.
8. Geben Sie als Benutzernamen Folgendes ein: **Comm Man**.
9. Geben Sie als Kennwort Folgendes ein: **commMan**.
10. Klicken Sie auf **Speichern**.

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

Auch für diesen Partner müssen Sie ein Standardziel definieren.

1. Klicken Sie auf **Liste** und dann auf **Standardziele anzeigen**.
2. Wählen Sie in der Liste **Produktion** den Eintrag **HttpDestination** aus.
3. Klicken Sie auf **Speichern**.

## B2B-Funktionalität konfigurieren

Definieren Sie als Nächstes die B2B-Funktionalität für den internen Partner.

1. Klicken Sie im Hauptmenü auf **Kontenadmin > Profile > Partner**.
2. Klicken Sie auf **Suchen**.
3. Wählen Sie **Interner Partner** aus, indem Sie auf das Symbol **Details anzeigen** klicken.
4. Klicken Sie auf **B2B-Funktionalität** in der horizontalen Navigationsleiste.
5. Legen Sie die Quelle und das Ziel für **Paket: None**, **Protokoll: EDI-X12** und **Dokumenttyp: ISA** fest, indem Sie die folgenden Schritte ausführen:
   a. Klicken Sie auf das Symbol **Rolle ist nicht aktiv** unter **Quelle festlegen** für **Paket: None**.
   b. Klicken Sie auf das Symbol **Rolle ist nicht aktiv** unter **Ziel festlegen** für **Paket: None**.
   c. Klicken Sie auf das Symbol **Erweitern** neben **Paket: None**.
   d. Klicken Sie auf das Symbol **Rolle ist nicht aktiv** für **Protokoll: EDI-X12 (ALL)** für die Quelle und das Ziel.
   e. Klicken Sie auf das Symbol **Erweitern** neben **Protokoll: EDI-X12 (ALL)**.
   f. Klicken Sie auf das Symbol **Rolle ist nicht aktiv** für **Dokumenttyp: ISA** für die Quelle und das Ziel.

Legen Sie dann die B2B-Funktionalität für 'Partner Zwei' fest.

1. Klicken Sie im Hauptmenü auf **Kontenadmin > Profile > Partner**.
2. Klicken Sie auf **Suchen**.
3. Wählen Sie **Partner Zwei** aus, indem Sie auf das Symbol **Details anzeigen** klicken.
4. Klicken Sie auf **B2B-Funktionalität** in der horizontalen Navigationsleiste.
5. Wählen Sie **Quelle festlegen** und **Ziel festlegen** für **Paket: AS**, **Protokoll: EDI-X12** und **Dokumenttyp: ISA** aus, indem Sie die folgenden Schritte ausführen:
   a. Klicken Sie auf das Symbol **Rolle ist nicht aktiv** unter **Quelle festlegen** für **Paket: AS**.
   b. Klicken Sie auf das Symbol **Rolle ist nicht aktiv** unter **Ziel festlegen** für **Paket: AS**.
   c. Klicken Sie auf das Symbol **Erweitern** neben **Paket: AS**.
   d. Klicken Sie auf das Symbol **Rolle ist nicht aktiv** für **Protokoll: EDI-X12 (ALL)** für die Quelle und das Ziel.
   e. Klicken Sie auf das Symbol **Erweitern** neben **Protokoll: EDI-X12 (ALL)**.
   f. Klicken Sie auf das Symbol **Rolle ist nicht aktiv** für **Dokumenttyp: ISA** für die Quelle und das Ziel.

## Partnerverbindungen definieren

Definieren Sie die Partnerverbindung für EDI-Dokumente ohne Paket, die vom internen Partner eingehen und 'Partner Zwei' zugestellt werden sollen.

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

Definieren Sie als Nächstes die Verbindung für EDI-Dokumente im AS2-Paket, die von 'Partner Zwei' eingehen und dem internen Partner ohne Paket zugestellt werden sollen. Dies ähnelt sehr der Verbindung, die Sie im vorherigen Abschnitt definiert haben, außer dass Sie auch noch AS2-Attribute konfigurieren.

1. Klicken Sie auf **Kontenadmin > Verbindungen**.
2. Wählen Sie in der Liste **Quelle** den Eintrag **Partner Zwei** aus.
3. Wählen Sie in der Liste **Ziel** den Eintrag **Interner Partner** 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) Dokumenttyp: **ISA (ALL)**
   b. **Ziel**
      1) Paket: **None (N/A)**
      2) Protokoll: **EDI-X12 (ALL)**
      3) Dokumenttyp: **ISA (ALL)**

Wählen Sie als Nächstes **Attribute** neben dem Kästchen **Paket: AS (N/A)** für **Partner Zwei** aus.

1. Bearbeiten Sie die Attribute von **Paket: AS (N/A)**, indem Sie auf der Seite abwärts blättern, und klicken Sie auf das Symbol **Erweitern** neben **Paket: AS (N/A)**.
2. Geben Sie einen Wert für **E-Mail-Adresse für AS MDN** (AS1) ein. Dies kann eine beliebige gültige E-Mail-Adresse sein.
3. Geben Sie einen Wert für **HTTP-URL für AS MDN** (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 Signaturen

## SSL-Authentifizierung für Eingangsdokumente konfigurieren

In diesem Abschnitt konfigurieren Sie die Serverauthentifizierung mit iKeyman, sodass **Partner Zwei** AS2-Dokumente über HTTPS senden kann.

Führen Sie die folgenden Schritte aus, um die Serverauthentifizierung zu konfigurieren:

1. Initiieren Sie die Anwendung iKeyman, indem Sie die Datei ikeyman.bat vom Verzeichnis /<*Produktverz*>/was/bin öffnen.
2. Öffnen Sie den Standard-Keystore des Empfängers, 'bcgSecurity.jks'. Wählen Sie in der Menüleiste **Key Database File Open** aus. Bei einer Standardinstallation befindet sich bcgSecurity.jks im folgenden Verzeichnis: <*Produktverz*>/common/security/keystore
3. Wenn Sie dazu aufgefordert werden, geben Sie das Standardkennwort für 'bcgSecurity.jks' ein. Dieses Kennwort lautet **WebAS**.
4. Wenn Sie bcgSecurity.jks zum ersten Mal öffnen, löschen Sie das Zertifikat "Dummy".

Der nächste Schritt besteht darin, ein neues selbst unterzeichnetes Zertifikat zu erstellen. Durch die Erstellung eines selbst unterzeichneten persönlichen Zertifikats werden ein privater Schlüssel und ein öffentlicher Schlüssel in der Server-Keystore-Datei erstellt.

Gehen Sie wie folgt vor, um ein neues selbst unterzeichnetes Zertifikat zu erstellen:

1. Klicken Sie auf **New Self Signed**.
2. Geben Sie dem Zertifikat eine Schlüsselbezeichnung, mit der das Zertifikat innerhalb des Keystores eindeutig gekennzeichnet ist. Verwenden Sie die Bezeichnung **selfSignedCert**.
3. Geben Sie den allgemeinen Namen des Servers ein. Dies ist die primäre, universelle Identität für das Zertifikat. Sie muss den Partner, den sie darstellt, eindeutig identifizieren.
4. Geben Sie den Namen Ihres Unternehmens ein.
5. Akzeptieren Sie alle übrigen Standardeinstellungen, und klicken Sie auf **OK**.

Angenommen, dass **Partner Zwei** eine EDI-Nachricht über AS2 mit HTTPS senden will. **Partner Zwei** muss auf das öffentliche Zertifikat verweisen, welches bei der Erstellung des selbst unterzeichneten Zertifikats mit erstellt wurde, um dies auszuführen.

Um **Partner Zwei** für die Verwendung des öffentlichen Zertifikats zu aktivieren, exportieren Sie das öffentliche Zertifikat wie folgt aus der Server-Keystore-Datei:

1. Wählen Sie das neu erstellte selbst unterzeichnete Zertifikat vom Dienstprogramm IBM Key Management (iKeyman) aus.
2. Klicken Sie auf **Extract Certificate**.
3. Ändern Sie den Datentyp in **Binary DER data**.
4. Stellen Sie den Dateinamen **commManOeffentlich** bereit, und klicken Sie auf **OK**.

Verwenden Sie iKeyman dann, um das selbst unterzeichnete Zertifikat und das private Schlüsselpaar in Form einer PKCS12-Datei zu exportieren. Diese PCKS12-Datei wird zur Verschlüsselung verwendet, dies wird in einem späteren Abschnitt beschrieben.

Gehen Sie wie folgt vor, um das selbst unterzeichnete Zertifikat und das private Schlüsselpaar zu exportieren:

1. Klicken Sie auf **Export/Import**.
2. Ändern Sie den Schlüsseldateityp in **PKCS12**.
3. Stellen Sie den Dateinamen **commManPrivat** bereit, und klicken Sie auf **OK**.
4. Geben Sie ein Kennwort ein, um die PKCS12-Zieldatei zu schützen. Bestätigen Sie das Kennwort, und klicken Sie auf **OK**.

**Anmerkung:** Stoppen und starten Sie den Empfänger erneut, damit diese Änderungen wirksam werden.

Das eingegebene Kennwort wird später verwendet, wenn Sie dieses private Zertifikat in den Hub importieren.

**Partner Zwei** muss auch einige Konfigurationsschritte ausführen, hierzu gehören das Importieren des Zertifikats und das Ändern der Adresse, an die die AS2-Dokumente gesendet werden. **Partner Zwei** muss z. B. die Adresse wie folgt ändern:

`https://<IP-adresse>:57443/bcgreceiver/submit`

Dabei steht *<IP-adresse>* für den Hub.

Das selbst unterzeichnete Zertifikat, das im Standard-Keystore des Empfängers platziert wurde, wird **Partner Zwei** jetzt immer dann angezeigt, wenn **Partner Zwei** ein Dokument über HTTPS sendet.

Um die entgegengesetzte Situation zu konfigurieren, muss **Partner Zwei** für den Hub einen SSL-Schlüssel in Form einer .der-Datei (in diesem Fall 'partnerZweiSSL-.der') bereitstellen. Falls nötig, muss **Partner Zwei** die Konfiguration auch so ändern, dass das Empfangen von Dokumenten über den HTTPS-Transport zugelassen wird.

Laden Sie die Datei partnerZweiSSL.der von **Partner Zwei** in das Profil des Hubbetreibers als Rootzertifikat. Ein Rootzertifikat ist ein Zertifikat, das von einer Zertifizierungsstelle (CA - Certifying Authority) ausgestellt wird, die für das Einrichten einer Zertifikatskette verwendet wird. In diesem Beispiel hat **Partner Zwei** das Zertifikat generiert, welches als Rootzertifikat geladen wurde, um den Hub in die Lage zu versetzen, den Absender zu erkennen und ihm zu vertrauen.

Laden Sie 'partnerZweiSSL.der' in den Hub:

1. Klicken Sie im Hauptmenü auf **Kontenadmin > Profile > Partner**.
2. Klicken Sie auf **Suchen**.
3. Wählen Sie den Hubbetreiber aus, indem Sie das Symbol **Details anzeigen** auswählen.
4. Klicken Sie auf **Zertifikate** und dann auf **Zertifikat laden**.
5. Setzen Sie den **Zertifikatstyp** auf **Root und Intermediate**.
6. Ändern Sie die Beschreibung in **Partner Zwei SSL-Zertifikat**.
7. Setzen Sie den **Status** auf **Aktiviert**.

8. Klicken Sie auf **Durchsuchen**, und navigieren Sie zum Verzeichnis, in dem Sie die Datei partnerZweiSSL.der gespeichert haben.
9. Wählen Sie das Zertifikat aus, und klicken Sie auf **Öffnen**.
10. Klicken Sie auf **Hochladen** und dann auf **Speichern**.

Ändern Sie das Ziel von Partner Zwei so, dass es HTTPS verwendet.

1. Klicken Sie auf **Kontenadmin > Profile > Partner** in der horizontalen Navigationsleiste.
2. Klicken Sie auf **Suchen**, und wählen Sie Partner Zwei aus, indem Sie auf das Symbol **Details anzeigen** klicken.
3. Klicken Sie in der horizontalen Navigationsleiste auf **Ziele**. Wählen Sie als Nächstes **HttpDestination** aus, indem Sie auf das Symbol **Details anzeigen** klicken.
4. Bearbeiten Sie es, indem Sie auf Symbol **Bearbeiten** klicken.
5. Ändern Sie den Transportwert in **HTTPS/1.1**.
6. Ändern Sie den Wert der Adresse wie folgt: **https://<***IP-adresse***>:443/input/AS2**. Dabei steht <*IP-adresse*> für das System von **Partner Zwei**.
7. Alle anderen Werte können unverändert bleiben. Klicken Sie auf **Speichern**.

## Verschlüsselung konfigurieren

Dieser Abschnitt enthält die Schritte zum Konfigurieren der Verschlüsselung.

**Partner Zwei** muss alle nötigen Konfigurationsschritte ausführen, z. B. das Importieren des öffentlichen Zertifikats und des selbst unterzeichneten Zertifikats, und die Verschlüsselung von Dokumenten konfigurieren, die zum Hub gesendet werden.

WebSphere Partner Gateway verwendet seinen privaten Schlüssel zum Entschlüsseln von Dokumenten. Um dem Hub dies zu ermöglichen, laden Sie zuerst den privaten Schlüssel, den Sie aus dem selbst unterzeichneten Zertifikat extrahiert haben, in Community Console. Führen Sie diese Aufgabe aus, wenn Sie als Hubbetreiber 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 > Partner** in der horizontalen Navigationsleiste.
2. Klicken Sie auf **Suchen**.
3. Wählen Sie den Hubbetreiber aus, indem Sie auf das Symbol **Details anzeigen** klicken.
4. Klicken Sie auf **Zertifikate** und dann auf **PKCS12 laden**.
5. Wählen Sie das Kontrollkästchen links von **Verschlüsselung** aus.
6. Ändern Sie die Beschreibung in **CommManPrivat**.
7. Wählen Sie **Aktiviert** aus.
8. Klicken Sie auf **Durchsuchen**, und navigieren Sie zum Verzeichnis, in dem die PKCS12-Datei commMannPrivat.p12 gespeichert ist.
9. Wählen Sie die Datei aus, und klicken Sie auf **Öffnen**.
10. Geben Sie das Kennwort ein, das für die PKCS12-Datei bereitgestellt wurde.
11. Übernehmen Sie den Betriebsmodus **Produktion**.

12. Klicken Sie auf **Hochladen** und dann auf **Speichern**.

Das beendet die Konfiguration, die erforderlich ist, damit ein Partner verschlüsselte Transaktionen über HTTPS an den Hub senden kann.

Im folgenden Abschnitt wird die vorherige Prozedur umgekehrt; nun sendet der Hub eine verschlüsselte EDI-Transaktion über HTTPS.

**Partner Zwei** muss ein Schlüsselpaar zur Dokumententschlüsselung generieren (in diesem Beispiel die Datei 'partnerZweiEntschlüsseln.der') und sollte das öffentliche Zertifikat für den Hub verfügbar machen.

Wie bereits erwähnt, wird der öffentliche Schlüssel vom Hub verwendet, wenn Transaktionen verschlüsselt werden, die an den Partner gesendet werden sollen. Damit dies geschehen kann, laden Sie das öffentliche Zertifikat in den Hub.

1. Klicken Sie im Hauptmenü auf **Kontenadmin > Profile > Partner**.
2. Klicken Sie auf **Suchen**.
3. Wählen Sie **Partner Zwei** aus, indem Sie auf das Symbol **Details anzeigen** klicken.
4. Klicken Sie auf **Zertifikate** in der horizontalen Navigationsleiste.
5. Klicken Sie auf **Zertifikat laden**.
6. Wählen Sie das Kontrollkästchen neben **Verschlüsselung** aus.
7. Ändern Sie die Beschreibung in **Partner Zwei verschlüsseln**.
8. Setzen Sie den Status auf **Aktiviert**.
9. Klicken Sie auf **Durchsuchen**.
10. Navigieren Sie zum Verzeichnis, in dem das Entschlüsselungszertifikat 'partnerZweiEntschlüsselt.der' gespeichert ist.
11. Wählen Sie das Zertifikat aus, und klicken Sie auf **Öffnen**.
12. Übernehmen Sie den Betriebsmodus **Produktion**.
13. Klicken Sie auf **Hochladen** und dann auf **Speichern**.

Der letzte Schritt in der Hubkonfiguration zum Senden von verschlüsselten Nachrichten über HTTPS mit AS2 besteht darin, die Partnerverbindung zu ändern, die zwischen dem internen Partner und 'Partner Zwei' vorhanden ist.

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

1. Klicken Sie in der horizontalen Navigationsleiste auf **Kontenadmin > Partnerverbindungen**.
2. Wählen Sie in der Liste **Quelle** den Eintrag **Comm Man** aus.
3. Wählen Sie in der Liste **Ziel** den Eintrag **Partner Zwei** aus.
4. Klicken Sie auf **Suchen**.
5. Klicken Sie für das Ziel auf die Schaltfläche **Attribute**.
6. Beachten Sie in der **Verbindungszusammenfassung**, dass das Attribut **AS verschlüsselt** den aktuellen Wert **Nein** hat. Bearbeiten Sie diesen Wert, indem Sie auf das Symbol **Erweitern** neben **Paket: AS (N/A)** klicken.

   **Anmerkung:** Sie müssen auf der Seite abwärts blättern, damit diese Option angezeigt wird.
7. Aktualisieren Sie in der Liste das Attribut **AS verschlüsselt** in **Ja**, und klicken Sie auf **Speichern**.

## Dokumentunterzeichnung konfigurieren

Wenn Sie eine Transaktion oder Nachricht digital unterzeichnen, verwendet WebSphere Partner Gateway Ihren privaten Schlüssel, um die Signatur zu erstellen und zu unterzeichnen. Ihr Partner, der diese Nachricht empfängt, verwendet Ihren öffentlichen Schlüssel, um die Signatur zu prüfen. Aus diesem Grund verwendet WebSphere Partner Gateway digitale Signaturen.

Dieser Abschnitt beschreibt die Schritte, die erforderlich sind, um sowohl den Hub als auch einen Partner für die Verwendung von digitalen Signaturen 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 > Partner** in der horizontalen Navigationsleiste.
2. Klicken Sie auf **Suchen**.
3. Wählen Sie **Partner Zwei** aus, indem Sie auf das Symbol **Details anzeigen** klicken.
4. Wählen Sie **Zertifikate** in der horizontalen Navigationsleiste aus.
5. Klicken Sie auf **Zertifikat laden**.
6. Wählen Sie das Kontrollkästchen neben **Digitale Signatur** aus.
7. Ändern Sie die Beschreibung in **CommMan unterzeichnend**.
8. Setzen Sie den **Status** auf **Aktiviert**.
9. Klicken Sie auf **Durchsuchen**.
10. Navigieren Sie zum Verzeichnis, in dem das digitales Zertifikat partnerZweiUnterzeichnend.der gespeichert ist, wählen Sie das Zertifikat aus, und klicken Sie auf **Öffnen**.
11. Klicken Sie auf **Hochladen** und dann auf **Speichern**.

Damit ist die Anfangskonfiguration für digitale Signaturen abgeschlossen.

Der Partner verwendet das öffentliche Zertifikat, um unterzeichnete, an den Hub gesendete Transaktionen zu authentifizieren.

Der Hub verwendet den privaten Schlüssel, um ausgehende Transaktionen, die an den Partner gesendet wurden, digital zu unterzeichnen. Zuerst aktivieren Sie den privaten Schlüssel für die digitale Signatur.

Gehen Sie wie folgt vor, um den privaten Schlüssel für die digitale Signatur zu aktivieren:

1. Klicken Sie auf **Kontenadmin > Profile > Zertifikate** in der horizontalen Navigationsleiste.
2. Klicken Sie auf das Symbol **Details anzeigen** neben **Hubbetreiber**.
3. Klicken Sie auf das Symbol **Details anzeigen** neben **CommManPrivat**.

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

4. Klicken Sie auf das Symbol **Bearbeiten**.
5. Wählen Sie das Kontrollkästchen neben **Digitale Signatur** aus.

   **Anmerkung:** Wenn mehr als ein Zertifikat für digitale Signatur verfügbar ist, würden Sie auswählen, welches das primäre bzw. das sekundäre Zertifikat ist, indem Sie **Primär** oder **Sekundär** in der Liste **Zertifikatverwendung** auswählen.
6. Klicken Sie auf **Speichern**.

Als Nächstes ändern Sie die Attribute der vorhandenen Partnerverbindung zwischen dem internen Partner und 'Partner Zwei', um unterzeichnete AS2-Transaktionen zu unterstützen.

Gehen Sie wie folgt vor, um die Attribute der Partnerverbindung zu ändern:

1. Klicken Sie in der horizontalen Navigationsleiste auf **Kontenadmin > Partnerverbindungen**.
2. Wählen Sie **Interner Partner** in der Liste **Quelle** aus.
3. Wählen Sie **Partner Zwei** in der Liste **Ziel** aus.
4. Klicken Sie auf **Suchen**.
5. Klicken Sie für **Partner Zwei** auf die Schaltfläche **Attribute**.
6. Bearbeiten Sie das Attribut **AS unterzeichnet**, indem Sie auf das Symbol **Erweitern** neben **Paket: AS (N/A)** klicken.
7. Wählen Sie **Ja** in der Liste **AS unterzeichnet** aus.
8. Klicken Sie auf **Speichern**.

Damit ist die Konfiguration abgeschlossen, die zum Senden einer unterzeichneten AS2-Transaktion von WebSphere Partner Gateway an den Partner erforderlich ist.

## Basiskonfiguration erweitern

In diesem Abschnitt erfahren Sie, wie Sie die in diesem Anhang beschriebene Basiskonfiguration ändern können. Dieser Abschnitt beschreibt unter Verwendung derselben zuvor beschriebenen Partner und der Konfiguration (ein interner Partner mit der DUNS-ID **123456789**, ein Dateiverzeichnisziel sowie ein Partner namens 'Partner Zwei' mit der DUNS-ID **987654321** und einem HTTP-Ziel), wie die Unterstützung für Folgendes hinzugefügt wird:

- Den FTP-Transport
- Angepasste XML-Dokumente
- Binärdateien (ohne Paket)

### FTP-Empfänger erstellen

Der FTP-Empfänger empfängt Dateien und übergibt sie zur Verarbeitung an Document Manager. Wie in „FTP-Server für das Empfangen von Dokumenten konfigurieren" auf Seite 35 beschrieben, müssen Sie, bevor Sie einen FTP-Empfänger 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 > Empfänger**.
2. Klicken Sie auf **Empfänger erstellen**.
3. Geben Sie die folgenden Informationen ein:
   a. Empfängername: **FTP_Receiver**
   b. Transport: **FTP-Verzeichnis**
   c. FTP-Stammverzeichnis: **C:/ftproot**
4. Klicken Sie auf **Speichern**.

# Hub für den Empfang von Binärdateien konfigurieren

Dieser Abschnitt behandelt die erforderlichen Schritte, um den Hub für den Empfang von Binärdokumenten zu konfigurieren, die **Partner Zwei** an den internen Partner senden will.

## Interaktion für Binärdokumente erstellen

Standardmäßig stellt WebSphere Partner Gateway vier Interaktionen bereit, die binäre Dokumente einschließen. Es stellt jedoch keine Interaktion für Binärdokumente im Paket **None** bereit, die an einen Partner mit dem Dokument im Paket **None** gehen. In diesem Abschnitt erstellen Sie die erforderliche Interaktion, damit Binärdokumente durch das System weitergeleitet werden können.

1. Klicken Sie auf **Hubadmin > Hubkonfiguration > Dokumentdefinition > Interaktionen verwalten**.
2. Klicken Sie in der Anzeige **Interaktionen verwalten** auf den Link **Interaktion erstellen**.
3. Klicken Sie in der Sicht **Interaktion verwalten** auf **Erstellen**.
4. Wählen Sie in der Liste **Quelle** Folgendes aus: **Paket: None Protokoll: Binary (1.0) Dokumenttyp: Binary (1.0)**.
5. Wählen Sie in der Liste **Ziel** Folgendes aus: **Paket: None Protokoll: Binary (1.0) Dokumenttyp: Binary (1.0)**.
6. Wählen Sie optional die **Transformationszuordnung** aus.
7. Wählen Sie in der Liste **Aktion** die Option **Pass-Through** aus.
8. Klicken Sie auf **Speichern**.

## B2B-Funktionalität für den internen Partner aktualisieren

Dieser Abschnitt zeigt, wie Sie den internen Partner so konfigurieren, dass er Binärdokumente akzeptieren kann.

1. Klicken Sie auf **Kontenadmin > Profile > Partner**.
2. Klicken Sie auf **Suchen**.
3. Klicken Sie auf das Symbol **Details anzeigen** neben **Comm Man**.
4. Klicken Sie auf **B2B-Funktionalität**.
5. Klicken Sie zum Aktivieren auf das Symbol **Rolle ist nicht aktiv** unter **Ziel festlegen** für **Paket: None**.
6. Klicken Sie auf das Symbol **Erweitern** neben **Paket: None**.
7. Klicken Sie auf das Symbol **Rolle ist nicht aktiv** für **Protokoll: Binary (1.0)** unter **Ziel festlegen**.
8. Klicken Sie auf das Symbol **Erweitern** neben **Protokoll: Binary (1.0)**.
9. Klicken Sie schließlich auf das Symbol **Rolle ist nicht aktiv** für **Dokumenttyp: Binary (1.0)** unter **Ziel festlegen**.

### 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 > Partner**.
2. Klicken Sie auf **Suchen**.
3. Klicken Sie auf das Symbol **Details anzeigen** neben **Partner Zwei**.
4. Klicken Sie auf **B2B-Funktionalität**.
5. Klicken Sie zum Aktivieren auf das Symbol **Rolle ist nicht aktiv** unter **Quelle festlegen** für **Paket: None**.
6. Klicken Sie auf das Symbol **Erweitern** neben **Paket: None**.
7. Klicken Sie auf das Symbol **Rolle ist nicht aktiv** für **Protokoll: Binary (1.0)** unter **Quelle festlegen**.
8. Klicken Sie auf das Symbol **Erweitern** neben **Protokoll: Binary (1.0)**.
9. Klicken Sie schließlich auf das Symbol **Rolle ist nicht aktiv** für **Dokumenttyp: Binary (1.0)** unter **Quelle festlegen**.

### Neue Partnerverbindung erstellen

Dieser Abschnitt zeigt, wie Sie eine neue Partnerverbindung zwischen dem internen Partner und 'Partner Zwei' für Binärdokumente konfigurieren können.

1. Klicken Sie auf **Kontenadmin > Verbindungen**.
2. Wählen Sie **Partner Zwei** in der Liste **Quelle** aus.
3. Wählen Sie **Interner Partner** 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.

## Hub für angepasste XML-Dokumente konfigurieren

Wie in „Angepasste XML-Dokumentverarbeitung" auf Seite 159 beschrieben, müssen Sie den Hub konfigurieren, damit er angepasste XML-Dateien weiterleiten kann. Dieser Abschnitt behandelt die erforderlichen Schritte, um Document Manager zum Weiterleiten der folgenden XML-Dokumente zu konfigurieren:

```
<?xml version="1.0" encoding="UTF-8"?>
       <!DOCTYPE Tester>
<Tester type="Test type A">
            <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**-Feldern, um die Geschäftskennungen von Absenderpartner und Zielpartner anzugeben.

### Protokolldefinitionsformat für angepasste 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 > Dokumentdefinition**.
2. Klicken Sie auf **Dokumentdefinition erstellen**.
3. Wählen Sie **Protokoll** in der Liste **Typ der Dokumentdefinition** aus.

4. Geben Sie die folgenden Informationen ein:
   a. Code: **Custom XML**
   b. Version: **1.0**
   c. Beschreibung: **Beispiel für Protokolldefinition**
5. Setzen Sie **Dokumentebene** auf **Nein**.
6. Setzen Sie **Status** auf **Aktiviert**.
7. Setzen Sie **Sichtbarkeit: Hubadministrator** auf **Ja**.
8. Setzen Sie **Sichtbarkeit: Interner Partner** auf **Ja**.
9. Setzen Sie **Sichtbarkeit: Partner** auf **Ja**.
10. Wählen Sie Folgendes aus:
    a. Paket: **AS**
    b. Paket: **None**
    c. Paket: **Backend Integration**
11. Klicken Sie auf **Speichern**.

## Dokumentdefinition 'Tester_XML' erstellen

Der zweite Schritt besteht darin, eine Dokumentdefinition für das neue Protokoll zu erstellen.

1. Klicken Sie auf **Hubadmin > Hubkonfiguration > Dokumentdefinition**.
2. Klicken Sie auf **Dokumentdefinition erstellen**.
3. Wählen Sie **Dokumenttyp** in der Liste **Typ der Dokumentdefinition** aus.
4. Geben Sie die folgenden Informationen ein:
   a. Name: **Tester_XML**
   b. Version: **1.0**
   c. Beschreibung: **Beispiel für angepassten XML-Dokumenttyp**
5. Setzen Sie **Dokumentebene** auf **Ja**.
6. Setzen Sie **Status** auf **Aktiviert**.
7. Setzen Sie **Sichtbarkeit: Hubadministrator** auf **Ja**.
8. Setzen Sie **Sichtbarkeit: Interner Partner** auf **Ja**.
9. Setzen Sie **Sichtbarkeit: Partner** auf **Ja**.
10. Klicken Sie auf das Symbol **Erweitern** neben **Paket: AS** und wählen Sie **Protokoll: CustomXML** aus.
11. Klicken Sie auf das Symbol **Erweitern** neben **Paket: None** und wählen Sie **Protokoll: CustomXML** aus.
12. Klicken Sie auf das Symbol **Erweitern** neben **Paket: Backend Integration** und wählen Sie **Protokoll: CustomXML** aus.
13. Klicken Sie auf **Speichern**.

## XML-Format 'Tester_XML' erstellen

Zuletzt erstellen Sie das XML-Format, das dem neuen Protokoll zugeordnet ist.

1. Klicken Sie auf **Hubadmin > Hubkonfiguration > XML-Formate**.
2. Klicken Sie auf **Dokumentfamilie erstellen**.
3. Geben Sie die folgenden Informationen ein, oder wählen Sie diese aus:
   a. Familienname: **Beispielfamilie**.
   b. Protokoll: **Custom XML 1.0**.
   c. Familientyp: **Root-Tag**.

d. Option für große Datei: **Keine**.
e. Familienkennung: **Tester**.

4. Klicken Sie auf **Speichern**.
5. Klicken Sie auf der Seite **Dokumentfamilie**, die daraufhin angezeigt wird, auf **XML-Format erstellen**.
6. Wählen Sie in der Liste **Dokumenttyp** die Option **&Tester_XML** aus.
7. Geben Sie als Wert für die Formatkennung **Test type A** ein.
8. Geben Sie für den XPath-Ausdruck der Formatkennung **/Tester/@type** ein.
9. Lassen Sie das Feld **Präfix-Namespace** leer (das Dokument verwendet keine Namespaces). Der Rückgabetyp ist **Text**.
10. Geben Sie in das Feld **Formatversion** und in das Feld **XPath-Ausdruck** den Wert **1** ein. Ändern Sie den Rückgabetyp in **Konstante**. Dies bedeutet, dass alle Dokumente mit der Formatkennung "Tester" über die richtige Version für eine Übereinstimmung mit diesem Format verfügen. Dies liegt daran, dass die Version für alle Dokumente 1 und die Version für dieses Format ebenfalls 1 ist. Deshalb stimmen die Versionen stets überein.
11. Geben Sie für den XPath-Ausdruck der Quellengeschäftskennung **/Tester/From** ein.
12. Geben Sie für den XPath-Ausdruck der Zielgeschäftskennung **/Tester/To** ein.
13. Das Format der restlichen Felder bleibt unverändert. Diese Felder sind optional und werden in diesem Beispiel nicht verwendet.
14. Klicken Sie auf **Speichern**.

## Interaktion für Tester_XML-Dokumente erstellen

Sie verfügen nun über ein neues Protokoll und einen neuen Dokumenttyp, mit dem Sie eine Interaktion definieren können.

1. Klicken Sie auf **Hubadmin > Hubkonfiguration > Dokumentdefinition > Interaktionen verwalten**.
2. Klicken Sie in der Anzeige **Interaktionen verwalten** auf den Link **Interaktion erstellen**.
3. Wählen Sie in der Liste **Quelle** Folgendes aus:
   a. Paket: **None**
   b. Protokoll: **Custom XML (1.0)**
   c. Dokumenttyp: **Tester_XML (1.0)**
4. Wählen Sie in der Liste **Ziel** Folgendes aus:
   a. Paket: **None**
   b. Protokoll: **Custom XML (1.0)**
   c. Dokumenttyp: **Tester_XML (1.0)**
5. Wählen Sie in der Liste **Aktion** die Option **Pass-Through** aus.
6. Klicken Sie auf **Speichern**.

## B2B-Funktionalität für den internen Partner aktualisieren

Sie müssen die B2B-Funktionalität der Partner aktualisieren, um den Austausch des angepassten XML-Dokuments zu aktivieren.

Zuerst aktivieren Sie den internen Partner für den Empfang von Tester_XML-Dokumenten (der interne Partner ist das Ziel).

1. Klicken Sie auf **Kontenadmin > Profile > Partner**.

2. Klicken Sie auf **Suchen**.
3. Wählen Sie den internen Partner aus der Liste **Partner** aus. (Beachten Sie, dass der interne Partner in diesem Beispiel über die Geschäftskennung 123456789 verfügt.)
4. Klicken Sie auf **B2B-Funktionalität**.
5. Klicken Sie zum Aktivieren auf das Symbol **Rolle ist nicht aktiv** unter **Ziel festlegen** für **Paket: None**.
6. Klicken Sie auf das Symbol **Erweitern** neben **Paket: None**.
7. Klicken Sie auf das Symbol **Rolle ist nicht aktiv** für **Protokoll: Custom XML (1.0)** unter **Ziel festlegen**.
8. Klicken Sie auf das Symbol **Erweitern** neben **Protokoll: Custom XML (1.0)**.
9. Klicken Sie schließlich auf das Symbol **Rolle ist nicht aktiv** für **Dokumenttyp: Tester_XML (1.0)** unter **Ziel festlegen**.

## B2B-Funktionalität für 'Partner Zwei' aktualisieren

Sie aktualisieren die B2B-Funktionalität von 'Partner Zwei', um den Austausch von Nachrichten mit dem neuen angepassten XML-Format zu ermöglichen.

Aktivieren Sie 'Partner Zwei' als Quelle der Tester_XML-Dokumente. (Beachten Sie, dass 'Partner Zwei' in diesem Beispiel über die Geschäftskennung 987654321 verfügt.)

1. Klicken Sie auf **Kontenadmin > Profile > Partner**.
2. Klicken Sie auf **Suchen**.
3. Wählen Sie **Partner Zwei** in der Liste **Partner** aus. (Beachten Sie, dass Partner Zwei in diesem Beispiel über die Geschäftskennung 987654321 verfügt.)
4. Klicken Sie auf **B2B-Funktionalität**.
5. Klicken Sie zum Aktivieren auf das Symbol **Rolle ist nicht aktiv** unter **Quelle festlegen** für **Paket: None**.
6. Klicken Sie auf das Symbol **Erweitern** neben **Paket: None**.
7. Klicken Sie auf das Symbol **Rolle ist nicht aktiv** für **Protokoll: Custom XML (1.0)** unter **Quelle festlegen**.
8. Klicken Sie auf das Symbol **Erweitern** neben **Protokoll: Custom XML (1.0)**.
9. Klicken Sie schließlich auf das Symbol **Rolle ist nicht aktiv** für **Dokumenttyp: Tester_XML (1.0)** unter **Quelle festlegen**.

## Neue Partnerverbindung erstellen

Erstellen Sie schließlich eine neue Partnerverbindung.

1. Klicken Sie auf **Kontenadmin > Verbindungen**.
2. Wählen Sie **Partner Zwei** in der Liste **Quelle** aus.
3. Wählen Sie **Interner Partner** in der Liste **Ziel** aus.
4. Klicken Sie auf **Suchen**.
5. Suchen Sie die Verbindung **None (N/A), Custom XML (1.0), Tester_XML (1.0)** zu **None (N/A), Custom XML (1.0), Tester_XML (1.0)** und klicken Sie auf **Aktivieren**, um sie zu aktivieren.

### Dokument mit angepasster XML weiterleiten

Kopieren Sie die Beispiel-XML vom Beginn dieses Beispiels, und fügen Sie diese in einen Texteditor ein. Speichern Sie die Datei unter einem Namen Ihrer Wahl auf der Maschine. Dann senden Sie die Datei an den Hub, indem Sie sie in dem Verzeichnis ablegen, das vom Dateiempfänger verwendet wird. In der Dokumentanzeige können Sie sehen, dass das Dokument mithilfe der dafür definierten Verbindung von 'Partner Zwei' an den internen Partner gesendet wird.

# Kapitel 20. EDI-Beispiele

Dieser Anhang enthält Beispiele für das Senden und Empfangen von EDI-Austauschvorgängen und deren Transformation in XML- und ROD-Dokumente bzw. aus XML- und ROD-Dokumenten.

Die Beispiele in diesem Anhang unterscheiden sich von denen in Kapitel 19, „Grundlegende Beispiele", auf Seite 325. Für die Beispiele in diesem Anhang werden neue Empfänger, Ziele und Profile erstellt.

**Anmerkung:** Ein Beispiel eines EDI-Austauschs, der durch den Hub ohne Entfernen von Umschlägen oder Transformation weitergeleitet wird, finden Sie in Kapitel 19, „Grundlegende Beispiele", auf Seite 325.

Jedes dieser vier Beispiele ist in sich abgeschlossen. Wenn Sie z. B. dem Beispiel für EDI zu XML folgen, werden Sie alle Schritte vom Erstellen der Ziele bis zum Aktivieren von Verbindungen für dieses Beispiel finden.

Dieser Anhang behandelt die folgenden Themen:

- „ Beispiel: EDI zu ROD"
- „ Beispiel: EDI zu XML" auf Seite 359
- „ Beispiel: XML zu EDI" auf Seite 364
- „ Beispiel: ROD zu EDI" auf Seite 372

Diese Beispiele sollen Ihnen eine schnelle Übersicht über die Schritte geben, die zum Konfigurieren eines Systems erforderlich sind. Wenn Sie diese Beispiele verwenden, um Ihr System zu konfigurieren, ändern Sie die spezifischen Informationen, z. B. die Namen und Geschäfts-IDs, um sie Ihren Geschäftsbedürfnissen anzupassen.

## Beispiel: EDI zu ROD

Dieser Abschnitt enthält ein Beispiel für das Senden einer EDI-Transaktion in einem Umschlag an den Hub, auf dem sie in ein ROD-Dokument transformiert und an den internen Partner gesendet wird.

### Umschlag vom EDI-Austausch entfernen und EDI-Austausch transformieren

In diesem Beispiel wird davon ausgegangen, dass der Zuordnungsexperte von Data Interchange Services eine Transformationszuordnung erstellt hat, die eine EDI-850-Standardtransaktion, welche mit dem Wörterbuch X12V5R1 definiert ist und der Version 5010 von X12 entspricht, nimmt und diese in ein ROD-Dokument transformiert, das von der Back-End-Anwendung des internen Partners verarbeitet wird. In diesem Beispiel heißt die Zuordnung S_DT_EDI_TO_ROD.eif.

Der Zuordnungsexperte von Data Interchange Services kann die Transformationszuordnung direkt in die WebSphere Partner Gateway-Datenbank exportieren. Alternativ hierzu kann der Zuordnungsexperte von Data Interchange Services Ihnen die

Datei senden, in dem Fall verwenden Sie das Dienstprogramm bcgDISImport, um die Datei in WebSphere Partner Gateway zu importieren. Dieser Anhang geht vom zweiten Szenario aus.

## Transformationszuordnung importieren

Dieser Abschnitt beschreibt die Schritte, die Sie beim Importieren einer Transformationszuordnung ausführen, die die EDI-Eingabe nimmt und diese in ein ROD-Format transformiert. Beim Importieren der Transformationszuordnung können Sie auch die Dokumentdefinition importieren, die der Zuordnung zugeordnet ist.

Bevor Sie die Transformationszuordnung importieren können, muss der Zuordnungsexperte von Data Interchange Services Ihnen diese zusenden. Diese Gruppe von Schritten geht davon aus, dass sich die Datei 'S_DT_EDI_TO_ROD.eif' auf Ihrem System befindet.

1. Öffnen Sie ein Befehlsfenster.
2. Geben Sie den folgenden Befehl bzw. das folgende Script ein:
   - Auf einem UNIX-System:

     ```
     <Produktverz>/bin/bcgDISImport.sh <datenbankbenutzer-id>
     <kennwort> S_DT_EDI_TO_ROD.eif
     ```

   - Auf einem Windows-System:

     ```
     <Produktverz>\bin\bcgDISImport.bat <datenbankbenutzer-id>
     <kennwort> S_DT_EDI_TO_ROD.eif
     ```

     Dabei gilt Folgendes: *<datenbankbenutzer-ID>* und *<kennwort>* sind die Werte, die Sie verwendet haben, als Sie die Datenbank als Teil der WebSphere Partner Gateway-Installation installiert haben.

## Transformationszuordnung und Dokumentdefinitionen überprüfen

Führen Sie die folgenden Schritte aus, um zu prüfen, ob die Transformationszuordnungen und Dokumentdefinitionen, die Sie importiert haben, in Community Console verfügbar sind:

1. Klicken Sie auf **Hubadmin > Hubkonfiguration > Zuordnungen > Transformationszuordnungen**.

   Die Zuordnung S_DT_EDI_TO_ROD wird angezeigt.
2. Klicken Sie auf das Symbol **Details anzeigen** neben der Zuordnung.

   Dokumentdefinitionen, denen diese Zuordnung zugeordnet ist:

*Tabelle 35. Dokumentdefinition, die der Zuordnung zugeordnet ist*

| Quelle | Ziel |
|---|---|
| Paket: N/A Protokoll: X12V5R1 (ALL)Dokumenttyp: 850 (ALL) | Paket: None Protokoll: DEMO850CL_DICTIONARY(ALL) Dokumenttyp: DEMO850CLSUW (ALL) |

Die Zuordnung S_DT_EDI_TO_ROD wurde definiert, um eine X12-850-Transaktion, die mit dem X12V5R1-Standard konform ist, in ein angepasstes Protokoll (DEMO850CL_DICTIONARY) und in einen Dokumenttyp (DEMO850CLSUW) zu transformieren.

## Empfänger konfigurieren

In diesem Abschnitt erstellen Sie einen Dateisystemverzeichnis-Empfänger für den Hub:

1. Klicken Sie auf **Hubadmin > Hubkonfiguration > Empfänger** und klicken Sie dann auf **Empfänger erstellen**.
2. Geben Sie als Empfängernamen **EDIFileTarget** ein.
3. Wählen Sie in der Liste **Transport** die Option **Dateiverzeichnis** aus.
4. Geben Sie als Stammverzeichnispfad **/Data/Manager/editarget** ein.
5. Klicken Sie auf **Speichern**.

Der Partner sendet den EDI-Austausch an diesen Empfänger.

## Interaktionen erstellen

Sie erstellen zwei Interaktionen: eine für den EDI-Umschlag und eine für die Transaktion im EDI-Umschlag.

Erstellen Sie eine Interaktion, die den EDI-Umschlag darstellt.

1. Klicken Sie auf **Hubadmin > Hubkonfiguration > Dokumentdefinition**.
2. Klicken Sie auf **Interaktion erstellen**.
3. Erweitern Sie unter **Quelle** die Einträge **Paket: None** und **Protokoll: EDI-X12** und wählen Sie **Dokumenttyp: ISA** aus.
4. Erweitern Sie unter **Ziel** die Einträge **Paket: N/A** und **Protokoll: EDI-X12** und wählen Sie **Dokumenttyp: ISA** aus.
5. Wählen Sie in der Liste **Aktion** die Option **EDI - Umschlag entfernen** aus. **Anmerkung:** In dieser Interaktion findet keine Transformation statt. Vom EDI-Austausch wird der Umschlag entfernt, wodurch die einzelne Transaktion (850) entsteht. Sie benötigen daher keine Transformationszuordnung für diese Interaktion.
6. Klicken Sie auf **Speichern**.

Erstellen Sie eine Interaktion, die über eine Quelle verfügt, die die 850-Transaktion darstellt, und ein Ziel, das das transformierte Dokument darstellt.

1. Klicken Sie auf **Hubadmin > Hubkonfiguration > Dokumentdefinition**.
2. Klicken Sie auf **Interaktion erstellen**.
3. Erweitern Sie unter **Quelle** die Einträge **Paket: N/A** und **Protokoll: X12V5R1** und wählen Sie **Dokumenttyp: 850** aus.
4. Erweitern Sie unter **Ziel** die Einträge **Paket: None** und **Protokoll: DEMO850CL_DICTIONARY** und wählen Sie **Dokumenttyp: DEMO850CLSUW** aus.
5. Wählen Sie in der Liste **Transformationszuordnung** den Eintrag **S_DT_EDI-_TO_ROD** aus.
6. Wählen Sie in der Liste **Aktion** die Option **EDI validieren und EDI konvertieren** aus.
7. Klicken Sie auf **Speichern**.

Diese Interaktion stellt die Transformation einer EDI-X12-850-Standardtransaktion in ein anderes Format dar; daher müssen Sie eine Transformationszuordnung auswählen.

## Partner erstellen

Sie haben für dieses Beispiel zwei Partner: den internen Partner (Manager) und einen externen Partner (TP1).

Erstellen Sie das Profil **Interner Partner**:

1. Klicken Sie auf **Kontenadmin > Profile > Partner** und klicken Sie auf **Erstellen**.
2. Geben Sie als Anmeldenamen des Unternehmens **ComManager** ein.
3. Geben Sie als Anzeigenamen des Partners **Manager** ein.
4. Wählen Sie als Partnertyp **Interner Partner** aus.
5. Klicken Sie auf **Neu** für die Geschäfts-ID und geben Sie `000000000` als unformatierte ID ein.

   **Anmerkung:** Stellen Sie sicher, dass Sie **Unformatiert** und nicht **DUNS** ausgewählt haben.
6. Klicken Sie erneut auf **Neu** für die Geschäfts-ID und geben Sie `01-000000000` als unformatierte ID ein.
7. Klicken Sie auf **Speichern**.

Erstellen Sie den zweiten Partner:

1. Klicken Sie auf **Kontenadmin > Profile > Partner** und klicken Sie auf **Erstellen**.
2. Geben Sie als Anmeldenamen des Unternehmens **TP1** ein.
3. Geben Sie als Anzeigenamen des Partners **TP1** ein.
4. Wählen Sie als Partnertyp **Externer Partner** aus.
5. Klicken Sie auf **Neu** für die Geschäfts-ID und geben Sie `000000001` als unformatierte ID ein.

   **Anmerkung:** Stellen Sie sicher, dass Sie **Unformatiert** und nicht **DUNS** ausgewählt haben.
6. Klicken Sie erneut auf **Neu** für die Geschäfts-ID und geben Sie `01-000000001` als unformatierte ID ein.
7. Klicken Sie auf **Speichern**.

## Ziele erstellen

Erstellen Sie in diesem Beispiel Dateiverzeichnisziele für beide Partner. Erstellen Sie zuerst ein Ziel für den Manager.

1. Klicken Sie auf **Kontenadmin > Profile > Partner** und klicken Sie auf **Suchen**.
2. Klicken Sie auf das Symbol **Details anzeigen** neben dem Profil **Manager**.
3. Klicken Sie auf **Ziele** und dann auf **Erstellen**.
4. Geben Sie die folgenden Werte für das Ziel ein. Denken Sie daran, dass das Dateiverzeichnis (der vollständige Pfad) schon auf Ihrem Dateisystem vorhanden sein muss.
   a. Geben Sie als Namen **ManagerFileDestination** ein.
   b. Wählen Sie in der Liste **Transport** die Option **Dateiverzeichnis** aus.
   c. Geben Sie als Adresse **file://Data/Manager/filedestination** ein.
   d. Klicken Sie auf **Speichern**.
5. Klicken Sie auf **Liste**, um alle Ziele für den internen Partner aufzulisten.
6. Klicken Sie auf **Standardziele anzeigen**.
7. Wählen Sie in der Liste **Produktion** das Ziel aus, das Sie in Schritt 4 erstellt haben.
8. Klicken Sie auf **Speichern**.

Erstellen Sie als Nächstes ein Ziel für den Partner.

1. Klicken Sie auf **Kontenadmin > Profile > Partner** und klicken Sie auf **Suchen**.
2. Wählen Sie den anderen Partner aus, den Sie für dieses Beispiel erstellt haben, indem Sie auf das Symbol **Details anzeigen** neben **TP1** klicken.
3. Klicken Sie auf **Ziele** und dann auf **Erstellen**.
4. Geben Sie die folgenden Werte für das Ziel ein. Denken Sie daran, dass das Dateiverzeichnis (der vollständige Pfad) schon vorhanden sein muss.
   a. Geben Sie als Namen **TP1FileDestination** ein.
   b. Wählen Sie in der Liste **Transport** die Option **Dateiverzeichnis** aus.
   c. Geben Sie als Adresse **file://Data/TP1/filedestination** ein.
   d. Klicken Sie auf **Speichern**.
5. Klicken Sie auf **Liste**, um alle Ziele für den Partner aufzulisten.
6. Klicken Sie auf **Standardziele anzeigen**.
7. Wählen Sie in der Liste **Produktion** das Ziel aus, das Sie in Schritt 4 erstellt haben.
8. Klicken Sie auf **Speichern**.

## B2B-Funktionalität konfigurieren

Aktivieren Sie die B2B-Funktionalität der beiden Partner in diesem Austausch. In diesem Beispiel stammt der EDI-Austausch vom externen Partner (TP1) und wird dem internen Partner zugestellt.

1. Klicken Sie auf **Kontenadmin > Profile > Partner**, und klicken Sie auf **Suchen**.
2. Klicken Sie auf das Symbol **Details anzeigen** für den Quellenpartner in diesem Beispiel (**TP1**).
3. Klicken Sie auf **B2B-Funktionalität**.
4. Aktivieren Sie zwei Funktionalitätsgruppen für den Quellenpartner.
   a. Aktivieren Sie zuerst die Dokumentdefinition, die den EDI-Umschlag darstellt:
      1) Klicken Sie zum Aktivieren auf das Symbol **Rolle ist nicht aktiv** unter **Quelle festlegen** für **Paket: None**.
      2) Erweitern Sie **Paket: None**.
      3) Klicken Sie auf das Symbol **Rolle ist nicht aktiv** unter **Quelle festlegen** für **Protokoll: EDI-X12 (ALL)**.
      4) Erweitern Sie **Protokoll: EDI-X12 (ALL)**.
      5) Klicken Sie auf das Symbol **Rolle ist nicht aktiv** unter **Quelle festlegen** für **Dokumenttyp: ISA (ALL)**.
   b. Aktivieren Sie danach die Dokumentdefinition, die die 850-Transaktion darstellt:
      1) Klicken Sie zum Aktivieren auf das Symbol **Rolle ist nicht aktiv** unter **Quelle festlegen** für **Paket: N/A**.
      2) Erweitern Sie **Paket: N/A**.
      3) Klicken Sie auf das Symbol **Rolle ist nicht aktiv** unter **Quelle festlegen** für **Protokoll: X12V5R1 (ALL)**.
      4) Erweitern Sie **Protokoll: X12V5R1 (ALL)**.
      5) Klicken Sie auf das Symbol **Rolle ist nicht aktiv** unter **Quelle festlegen** für **Dokumenttyp: 850**.
5. Klicken Sie auf **Kontenadmin > Profile > Partner**, und klicken Sie auf **Suchen**.
6. Klicken Sie auf das Symbol **Details anzeigen** für den Zielpartner in diesem Beispiel (**Manager**).

7. Klicken Sie auf **B2B-Funktionalität**.
8. Aktivieren Sie zwei Funktionalitätsgruppen für den Zielpartner.
   a. Aktivieren Sie zuerst die Dokumentdefinition, die den Umschlag darstellt:
      1) Klicken Sie zum Aktivieren auf das Symbol **Rolle ist nicht aktiv** unter **Ziel festlegen** für **Paket: N/A**.
      2) Erweitern Sie **Paket: N/A**.
      3) Klicken Sie auf das Symbol **Rolle ist nicht aktiv** unter **Ziel festlegen** für **Protokoll: EDI-X12 (ALL)**.
      4) Erweitern Sie **Protokoll: EDI-X12 (ALL)**.
      5) Klicken Sie auf das Symbol **Rolle ist nicht aktiv** unter **Ziel festlegen** für **Dokumenttyp: ISA (ALL)**.
   b. Aktivieren Sie als Nächstes die Dokumentdefinition, die das transformierte Dokument darstellt:
      1) Klicken Sie zum Aktivieren auf das Symbol **Rolle ist nicht aktiv** unter **Ziel festlegen** für **Paket: None**.
      2) Erweitern Sie **Paket: None**.
      3) Klicken Sie auf das Symbol **Rolle ist nicht aktiv** unter **Ziel festlegen** für **Protokoll: DEMO850CL_DICTIONARY (ALL)**.
      4) Erweitern Sie **Protokoll: DEMO850CL_DICTIONARY (ALL)**.
      5) Klicken Sie auf das Symbol **Rolle ist nicht aktiv** unter **Ziel festlegen** für **Dokumenttyp: DEMO850CLSUW(ALL)**.

## Verbindungen aktivieren

Gehen Sie wie folgt vor, um die Verbindungen zu aktivieren:

1. Klicken Sie auf **Kontenadmin > Verbindungen**.
2. Wählen Sie **TP1** in der Liste **Quelle** aus.
3. Wählen Sie **Manager** in der Liste **Ziel** aus.
4. Klicken Sie auf **Suchen**.
5. Klicken Sie auf **Aktivieren** für die Verbindung, die den Umschlag darstellt:

*Tabelle 36. Verbindung für Umschlag*

| Quelle | Ziel |
|---|---|
| Paket: None (N/A) Protokoll: EDI-X12 (ALL) Dokumenttyp: ISA (ALL) | Paket: N/A (N/A) Protokoll: EDI-X12 (ALL) Dokumenttyp: ISA (ALL) |

6. Klicken Sie auf **Aktivieren** für die Verbindung, die die 850-Transaktion darstellt, zum transformierten Dokument:

*Tabelle 37. Verbindung für EDI-Transaktion zu ROD-Dokument*

| Quelle | Ziel |
|---|---|
| Paket: N/A (N/A) Protokoll: X12V5R1Dokumenttyp: 850 (ALL) | Paket: None (N/A) Protokoll: DEMO850CL_DICTIONARY (ALL) Dokumenttyp: DEMO850CLSUW (ALL) |

## Attribute hinzufügen

Legen Sie das Attribut fest, das Dokumente mit doppelten IDs zulässt:

1. Klicken Sie auf **Hubadmin > Hubkonfiguration > Dokumentdefinition**.
2. Klicken Sie auf das Symbol **Erweitern** neben **Paket: None**.

3. Klicken Sie auf das Symbol **Attributwerte bearbeiten** neben **Protokoll: EDI-X12**.
4. Blättern Sie auf der Seite bis zum Abschnitt mit den Attributen für Dokumenttypkontexte vor. Wählen Sie in der Zeile **Dokumente mit doppelten Dokument-IDs zulassen** die Option **Ja** in der Liste aus.
5. Klicken Sie auf **Speichern**.

Wenn an dieser Stelle TP1 einen EDI-Austausch mit einer 850-Transaktion an den internen Partner gesendet hat, würde vom EDI-Austausch der Umschlag entfernt werden, wodurch eine 850-Transaktion entstände. Die 850-Transaktion wird dann in den Dokumenttyp DEMO850CLSUW transformiert und das transformierte Dokument wird an das Ziel des internen Partners gesendet.

## Dem Austausch TA1 hinzufügen

In X12 ist TA1 ein optionales Segment, mit dem der Empfang eines Austauschs bestätigt werden kann. Der Absender kann TA1 vom Empfänger anfordern, indem er das Element 14 des ISA-Austauschkontrollheaders mit **1** festlegt. Mit dem Attribut **TA1-Anforderung zulassen** können Sie in WebSphere Partner Gateway steuern, ob TA1 gesendet wird, wenn der Absender dies anfordert.

Die Zuordnung &WDI_TA1_ACK wird während der Installation von WebSphere Partner Gateway installiert, sodass Sie diese nicht importieren müssen.

### Assoziationen erstellen

Führen Sie die folgenden Schritte aus, um die Zuordnung einer Dokumentdefinition zuzuordnen:

1. Klicken Sie auf **Hubadmin > Hubkonfiguration > Zuordnungen > EDI FA-Zuordnungen**.

   Die Zuordnung &WDI_TA1_ACK wird angezeigt.
2. Klicken Sie auf das Symbol **Details anzeigen** neben der Zuordnung.

   Es werden Informationen zur Zuordnung wie auch ein Ordner für jeden Pakettyp, der auf dem System verfügbar ist, angezeigt.
3. Erstellen Sie die Assoziation zur Dokumentdefinition, indem Sie diese Schritte ausführen:
   a. Wählen Sie das Kontrollkästchen neben **Paket: None** aus und erweitern Sie den Ordner.
   b. Wählen Sie das Kontrollkästchen neben **Protokoll: EDI-X12 (ALL)** aus und erweitern Sie den Ordner.
   c. Wählen Sie das Kontrollkästchen neben **Dokumenttyp: ISA (ALL)** aus.
   d. Klicken Sie auf **Speichern**.

Sie haben eine Assoziation zwischen der Zuordnung &WDI_TA1_ACK1 und der Dokumentdefinition für den Umschlag erstellt.

### Interaktionen erstellen

Erstellen Sie eine Interaktion, die die TA1-Transaktion darstellt.

1. Klicken Sie auf **Hubadmin > Hubkonfiguration > Dokumentdefinition > Interaktionen verwalten**.
2. Klicken Sie in der Anzeige **Interaktionen verwalten** auf den Link **Interaktion erstellen**.

3. Erweitern Sie unter **Quelle** die Einträge **Paket: N/A** und **Protokoll: &X44TA1** und wählen Sie **Dokumenttyp: TA1** aus.
4. Erweitern Sie unter **Ziel** die Einträge **Paket: N/A** und **Protokoll: &X44TA1** und wählen Sie **Dokumenttyp: TA1** aus.
5. Wählen Sie in der Liste **Aktion** die Option **Pass-Through** aus.
6. Klicken Sie auf **Speichern**.

Erstellen Sie eine Interaktion mit einer Quelle, die den EDI-Umschlag darstellt, in dem TA1 enthalten sein wird.

1. Klicken Sie auf **Hubadmin > Hubkonfiguration > Dokumentdefinition > Interaktionen verwalten**.
2. Klicken Sie in der Anzeige **Interaktionen verwalten** auf den Link **Interaktion erstellen**.
3. Erweitern Sie unter **Quelle** die Einträge **Paket: N/A** und **Protokoll: EDI-X12** und wählen Sie **Dokumenttyp: ISA** aus.
4. Erweitern Sie unter **Ziel** die Einträge **Paket: None** und **Protokoll: EDI-X12** und wählen Sie **Dokumenttyp: ISA** aus.
5. Wählen Sie in der Liste **Aktion** die Option **Pass-Through** aus.
6. Klicken Sie auf **Speichern**.

## B2B-Funktionalität aktivieren

Fügen Sie als Nächstes die neu erstellten Interaktionen der B2B-Funktionalität der Partner hinzu.

1. Klicken Sie auf **Kontenadmin > Profile > Partner**, und klicken Sie auf **Suchen**.
2. Klicken Sie auf das Symbol **Details anzeigen** für den Quellenpartner in diesem Beispiel (**Manager**).

   **Anmerkung:** Denken Sie daran, dass die TA1 von dem Partner, der das ROD-Dokument empfängt, zu dem Partner fließt, der sie gesendet hat. In diesem Beispiel ist der Manager die Quelle der TA1 und der Partner TP1 ist das Ziel.
3. Klicken Sie auf **B2B-Funktionalität**.
4. Aktivieren Sie zwei Funktionalitätsgruppen für den Quellenpartner.
   a. Aktivieren Sie zuerst die Funktion für die TA1.
      1) Klicken Sie zum Aktivieren auf das Symbol **Rolle ist nicht aktiv** unter **Quelle festlegen** für **Paket: N/A**.
      2) Erweitern Sie **Paket: N/A**.
      3) Klicken Sie auf das Symbol **Rolle ist nicht aktiv** unter **Quelle festlegen** für **Protokoll: &X44TA1**.
      4) Erweitern Sie **Protokoll: &X44TA1**.
      5) Klicken Sie auf das Symbol **Rolle ist nicht aktiv** unter **Quelle festlegen** für **Dokumenttyp: TA1 (ALL)**.
   b. Aktivieren Sie als Nächstes die Funktion für den Umschlag:
      1) Klicken Sie zum Aktivieren auf das Symbol **Rolle ist nicht aktiv** unter **Quelle festlegen** für **Paket: N/A**.
      2) Erweitern Sie **Paket: N/A**.
      3) Klicken Sie auf das Symbol **Rolle ist nicht aktiv** unter **Quelle festlegen** für **Protokoll: EDI-X12**.
      4) Erweitern Sie **Protokoll: EDI-X12 (ALL)**.

5) Klicken Sie auf das Symbol **Rolle ist nicht aktiv** unter **Quelle festlegen** für **Dokumenttyp: ISA (ALL)**.

5. Klicken Sie auf **Kontenadmin > Profile > Partner**, und klicken Sie auf **Suchen**.
6. Klicken Sie auf das Symbol **Details anzeigen** für den Zielpartner in diesem Beispiel (**TP1**).
7. Klicken Sie auf **B2B-Funktionalität**.
8. Aktivieren Sie zwei Funktionalitätsgruppen für den Zielpartner.
   a. Aktivieren Sie zuerst die Dokumentdefinition, die die TA1 darstellt:
      1) Klicken Sie zum Aktivieren auf das Symbol **Rolle ist nicht aktiv** unter **Ziel festlegen** für **Paket: N/A**.
      2) Erweitern Sie **Paket: N/A**.
      3) Klicken Sie auf das Symbol **Rolle ist nicht aktiv** unter **Ziel festlegen** für **Protokoll: &X44TA1 (ALL)**.
      4) Erweitern Sie **Protokoll: &X44TA1 (ALL)**.
      5) Klicken Sie auf das Symbol **Rolle ist nicht aktiv** unter **Ziel festlegen** für **Dokumenttyp: TA1 (ALL)**.
   b. Aktivieren Sie als Nächstes die Dokumentdefinition, die den EDI-Umschlag darstellt:
      1) Klicken Sie zum Aktivieren auf das Symbol **Rolle ist nicht aktiv** unter **Ziel festlegen** für **Paket: None**.
      2) Erweitern Sie **Paket: None**.
      3) Klicken Sie auf das Symbol **Rolle ist nicht aktiv** unter **Ziel festlegen** für **Protokoll: EDI-X12 (ALL)**.
      4) Erweitern Sie **Protokoll: EDI-X12 (ALL)**.
      5) Klicken Sie auf das Symbol **Rolle ist nicht aktiv** unter **Ziel festlegen** für **Dokumenttyp: ISA (ALL)**.

## Umschlagsprofil erstellen

Sie erstellen als Nächstes das Profil für den Umschlag, der die TA1 enthalten wird:

1. Klicken Sie auf **Hubadmin > Hubkonfiguration > EDI > Umschlagsprofil**.
2. Klicken Sie auf **Erstellen**.
3. Geben Sie den Namen des Profils ein: **UmschProf1**.
4. Wählen Sie in der Liste **EDI-Standard** die Option **X12** aus.
5. Die Schaltfläche **Allgemein** ist standardmäßig ausgewählt. Geben Sie die folgenden Werte für die allgemeinen Attribute des Umschlags ein:
   - INTCTLLEN: **9**
   - GRPCTLLEN: **9**
   - TRXCTLLEN: **9**
   - MAXDOCS: **1000**
6. Klicken Sie auf **Austausch** und geben Sie die folgenden Werte für die Austauschattribute ein:
   - ISA01: **01**
   - ISA02: **ISA0000002**
   - ISA03: **02**
   - ISA04: **ISA0000004**
   - ISA11: \
   - ISA12: **00501**

- ISA15: **T**

7. Klicken Sie auf **Speichern**.

## Partnerverbindungen aktivieren

Gehen Sie wie folgt vor, um die Verbindungen zu aktivieren:

1. Klicken Sie auf **Kontenadmin > Verbindungen**.
2. Wählen Sie **Manager** in der Liste **Quelle** aus.
3. Wählen Sie **TP1** in der Liste **Ziel** aus.
4. Klicken Sie auf **Suchen**.
5. Aktivieren Sie die Verbindung, die die TA1 darstellt.

*Tabelle 38. TA1-Verbindung*

| Quelle | Ziel |
|---|---|
| Paket: N/A (N/A) Protokoll: &X44TA1 (ALL) Dokumenttyp: TA1 (ALL) | Paket: N/A (N/A) Protokoll: &X44TA1 (ALL) Dokumenttyp: TA1 (ALL) |

6. Aktivieren Sie die Verbindung, die den Umschlag darstellt:

*Tabelle 39. Verbindung für Umschlag*

| Quelle | Ziel |
|---|---|
| Paket: N/A (N/A) Protokoll: EDI-X12 (ALL) Dokumenttyp: ISA (ALL) | Paket: None (N/A) Protokoll: EDI-X12 (ALL) Dokumenttyp: ISA (ALL) |

## Attribute konfigurieren

Gehen Sie wie folgt vor, um Attribute für das Umschlagsprofil anzugeben:

1. Klicken Sie auf **Kontenadmin > Profile > Partner** und klicken Sie auf **Suchen**.
2. Wählen Sie **TP1** in der Liste aus.
3. Klicken Sie auf **B2B-Funktionalität**.
4. Klicken Sie auf das Symbol **Erweitern** neben **Paket: None**.
5. Klicken Sie auf das Symbol **Bearbeiten** neben **Protokoll: EDI-X12 (ALL)**.
6. Wählen Sie in der Zeile **TA1-Anforderung zulassen** die Option **Ja** aus.
7. Klicken Sie auf **Speichern**.
8. Klicken Sie erneut auf **B2B-Funktionalität**.
9. Klicken Sie auf das Symbol **Erweitern** neben **Paket: N/A**.
10. Klicken Sie auf das Symbol **Bearbeiten** neben **Protokoll: &X44TA1 (ALL)**.
11. Geben Sie die folgenden Attribute an:
    a. Wählen Sie in der Zeile **Umschlagsprofil** den Eintrag **UmschProf1** in der Liste aus.
    b. Geben Sie in der Zeile **Qualifikationsmerkmal für Austausch** den Wert **01** ein.
    c. Geben Sie in der Zeile **Kennung für Austausch** den Wert **000000001** ein.
    d. Geben Sie in der Zeile **Nutzungsanzeiger für Austausch** den Buchstaben **T** ein.
12. Klicken Sie auf **Speichern**.

Mit dieser Aufgabenabfolge haben Sie dem Austausch eine TA1-Bestätigung hinzugefügt. Wenn der Austausch empfangen wird, sendet WebSphere Partner Gateway

eine TA1 zurück an den Absender (TP1). Die TA1 wird in einem Umschlag gesendet, der sich nach dem Umschlagsprofil **UmschProf1** richtet.

## FA-Zuordnung hinzufügen

Dieser Abschnitt beschreibt, wie Sie eine funktionale Standardbestätigung (997) dem in „ Beispiel: EDI zu ROD" auf Seite 345 beschriebenen Dokumentenfluss hinzufügen. Die funktionale Bestätigung bietet dem Absender die Bestätigung, dass die Transaktion empfangen worden ist.

**Anmerkung:** Dieses Beispiel ähnelt „ Dem Austausch TA1 hinzufügen" auf Seite 351. Es bezieht sich jedoch nicht direkt auf das Beispiel. Stattdessen baut es auf den Aufgaben auf, die Sie in „ Beispiel: EDI zu ROD" auf Seite 345 ausgeführt haben.

WebSphere Partner Gateway enthält eine Gruppe vorinstallierter Namen für Zuordnungen der funktionalen Bestätigungen, die mit $DT_FA beginnen. Diesem folgt der Name für die funktionale Bestätigungsnachricht sowie die Version und das Release der Nachricht. Version 2 Release 4 der funktionalen Bestätigungsnachricht 997 heißt dementsprechend $DT_997V2R4. Eine Liste mit Zuordnungen, die von WebSphere Partner Gateway bereitgestellt werden, finden Sie in „Bestätigungen konfigurieren" auf Seite 223.

### Assoziationen erstellen

Führen Sie die folgenden Schritte aus, um die Zuordnung einer Dokumentdefinition zuzuordnen:

1. Klicken Sie auf **Hubadmin > Hubkonfiguration > Zuordnungen > EDI FA-Zuordnungen**.

   Die Zuordnung &DT_FA997V2R4 wird angezeigt.
2. Klicken Sie auf das Symbol **Details anzeigen** neben der Zuordnung.

   Es werden Informationen zur Zuordnung wie auch ein Ordner für jeden Pakettyp, der auf dem System verfügbar ist, angezeigt.
3. Erstellen Sie die Assoziation zur Dokumentdefinition, indem Sie diese Schritte ausführen:
   a. Wählen Sie das Kontrollkästchen neben **Paket: N/V** aus und erweitern Sie den Ordner.
   b. Wählen Sie das Kontrollkästchen neben **Protokoll: X12V5R1** aus und erweitern Sie den Ordner.
   c. Wählen Sie das Kontrollkästchen neben **Dokumenttyp: 850** aus.
   d. Klicken Sie auf **Speichern**.

Sie haben diese Zuordnung für funktionale Bestätigungen 997 dem X12-Protokoll hinzugefügt.

### Interaktionen erstellen

Erstellen Sie eine Interaktion, die die Bestätigung 997 darstellt.

1. Klicken Sie auf **Hubadmin > Hubkonfiguration > Dokumentdefinition > Interaktionen verwalten**.
2. Klicken Sie in der Anzeige **Interaktionen verwalten** auf den Link **Interaktion erstellen**.
3. Erweitern Sie unter **Quelle** die Einträge **Paket: N/A** und **Protokoll: &DT99724** und wählen Sie **Dokumenttyp: 997** aus.

4. Erweitern Sie unter **Ziel** die Einträge **Paket: N/A** und **Protokoll: &DT99724** und wählen Sie **Dokumenttyp: 997** aus.
5. Wählen Sie in der Liste **Aktion** die Option **Pass-Through** aus.
6. Klicken Sie auf **Speichern**.

Erstellen Sie eine Interaktion, die den Umschlag darstellt.

1. Klicken Sie auf **Hubadmin > Hubkonfiguration > Dokumentdefinition > Interaktionen verwalten**.
2. Klicken Sie in der Anzeige **Interaktionen verwalten** auf den Link **Interaktion erstellen**.
3. Erweitern Sie die Einträge **Paket: N/A** und **Protokoll: EDI-X12** und wählen Sie **Dokumenttyp: ISA** aus.
4. Erweitern Sie die Einträge **Paket: None** und **Protokoll: EDI-X12** und wählen Sie **Dokumenttyp: ISA** aus.
5. Wählen Sie in der Liste **Aktion** die Option **Pass-Through** aus.
6. Klicken Sie auf **Speichern**.

## B2B-Funktionalität aktivieren

Fügen Sie als Nächstes die neu erstellten Interaktionen der B2B-Funktionalität der Partner hinzu.

1. Klicken Sie auf **Kontenadmin > Profile > Partner**, und klicken Sie auf **Suchen**.
2. Klicken Sie auf das Symbol **Details anzeigen** für den Quellenpartner in diesem Beispiel (**Manager**).

   **Anmerkung:** Denken Sie daran, dass die funktionale Bestätigung von dem Partner, der das ROD-Dokument empfängt, zu dem Partner fließt, der sie gesendet hat. In diesem Beispiel ist der Manager die Quelle der funktionalen Bestätigung und der Partner TP1 ist das Ziel.
3. Klicken Sie auf **B2B-Funktionalität**.
4. Aktivieren Sie zwei Funktionalitätsgruppen für den Quellenpartner.
   a. Aktivieren Sie zuerst die Funktion für die funktionale Bestätigung.
      1) Klicken Sie zum Aktivieren auf das Symbol **Rolle ist nicht aktiv** unter **Quelle festlegen** für **Paket: N/A**.
      2) Erweitern Sie **Paket: N/A**.
      3) Klicken Sie auf das Symbol **Rolle ist nicht aktiv** unter **Quelle festlegen** für **Protokoll: &DT99724**.
      4) Erweitern Sie **Protokoll: &DT99724**.
      5) Klicken Sie auf das Symbol **Rolle ist nicht aktiv** unter **Quelle festlegen** für **Dokumenttyp: 997 (ALL)**.
   b. Aktivieren Sie als Nächstes die Funktion für den Umschlag:
      1) Klicken Sie zum Aktivieren auf das Symbol **Rolle ist nicht aktiv** unter **Quelle festlegen** für **Paket: N/A**.
      2) Erweitern Sie **Paket: N/A**.
      3) Klicken Sie auf das Symbol **Rolle ist nicht aktiv** unter **Quelle festlegen** für **Protokoll: EDI-X12**.
      4) Erweitern Sie **Protokoll: EDI-X12 (ALL)**.
      5) Klicken Sie auf das Symbol **Rolle ist nicht aktiv** unter **Quelle festlegen** für **Dokumenttyp: ISA (ALL)**.
5. Klicken Sie auf **Kontenadmin > Profile > Partner**, und klicken Sie auf **Suchen**.

6. Klicken Sie auf das Symbol **Details anzeigen** für den Zielpartner in diesem Beispiel (**TP1**).
7. Klicken Sie auf **B2B-Funktionalität**.
8. Aktivieren Sie zwei Funktionalitätsgruppen für den Zielpartner.
   a. Aktivieren Sie zuerst die Dokumentdefinition, die die funktionale Bestätigung 997 darstellt:
      1) Klicken Sie zum Aktivieren auf das Symbol **Rolle ist nicht aktiv** unter **Ziel festlegen** für **Paket: N/A**.
      2) Erweitern Sie **Paket: N/A**.
      3) Klicken Sie auf das Symbol **Rolle ist nicht aktiv** unter **Ziel festlegen** für **Protokoll: &DT99724 (ALL)**.
      4) Erweitern Sie **Protokoll: &DT99724 (ALL)**.
      5) Klicken Sie auf das Symbol **Rolle ist nicht aktiv** unter **Ziel festlegen** für **Dokumenttyp: 997 (ALL)**.
   b. Aktivieren Sie als Nächstes die Dokumentdefinition, die den EDI-Umschlag darstellt:
      1) Klicken Sie zum Aktivieren auf das Symbol **Rolle ist nicht aktiv** unter **Ziel festlegen** für **Paket: None**.
      2) Erweitern Sie **Paket: None**.
      3) Klicken Sie auf das Symbol **Rolle ist nicht aktiv** unter **Ziel festlegen** für **Protokoll: EDI-X12 (ALL)**.
      4) Erweitern Sie **Protokoll: EDI-X12 (ALL)**.
      5) Klicken Sie auf das Symbol **Rolle ist nicht aktiv** unter **Ziel festlegen** für **Dokumenttyp: ISA(ALL)**.

## Umschlagsprofil erstellen

Sie erstellen als Nächstes das Profil für den Umschlag, der die funktionale Bestätigung 997 enthalten wird: Eine funktionale Bestätigung muss, wie eine Transaktion, mit einem Umschlag versehen werden, bevor sie gesendet werden kann.

1. Klicken Sie auf **Hubadmin > Hubkonfiguration > EDI > Umschlagsprofil**.
2. Klicken Sie auf **Erstellen**.
3. Geben Sie den Namen des Profils ein: **UmschProf1**.
4. Wählen Sie in der Liste **EDI-Standard** die Option **X12** aus.
5. Die Schaltfläche **Allgemein** ist standardmäßig ausgewählt. Geben Sie die folgenden Werte für die allgemeinen Attribute des Umschlags ein:
   - INTCTLLEN: **9**
   - GRPCTLLEN: **9**
   - TRXCTLLEN: **9**
   - MAXDOCS: **1000**
6. Klicken Sie auf die Schaltfläche **Austausch** und geben Sie die folgenden Werte für die Austauschattribute ein:
   - ISA01: **01**
   - ISA02: **ISA0000002**
   - ISA03: **02**
   - ISA04: **ISA0000004**
   - ISA11: \
   - ISA12: **00501**

- ISA15: **T**

7. Klicken Sie auf **Speichern**.

## Partnerverbindungen aktivieren

Gehen Sie wie folgt vor, um die Verbindungen zu aktivieren:

1. Klicken Sie auf **Kontenadmin > Verbindungen**.
2. Wählen Sie **Manager** in der Liste **Quelle** aus.
3. Wählen Sie **TP1** in der Liste **Ziel** aus.
4. Klicken Sie auf **Suchen**.
5. Klicken Sie auf **Aktivieren** für die Verbindung, die die funktionale Bestätigung 997 darstellt:

*Tabelle 40. Verbindung für funktionale Bestätigung*

| Quelle | Ziel |
|---|---|
| Paket: N/A (N/A) Protokoll: &DT99724 (ALL) Dokumenttyp: 997 (ALL) | Paket: N/A (N/A) Protokoll: &DT99724 (ALL) Dokumenttyp: 997 (ALL) |

6. Klicken Sie auf **Aktivieren** für die Verbindung, die den EDI-Umschlag darstellt, der an den Absender des Austauschs zurückgesendet wird:

*Tabelle 41. Verbindung für Umschlag*

| Quelle | Ziel |
|---|---|
| Paket: N/A (N/A) Protokoll: EDI-X12 (ALL) Dokumenttyp: ISA (ALL) | Paket: None (N/A) Protokoll: EDI-X12 (ALL) Dokumenttyp: ISA (ALL) |

## Attribute konfigurieren

Geben Sie zuerst an, welche FA-Zuordnung verwendet werden soll:

1. Klicken Sie auf **Kontenadmin > Profile > Partner** und klicken Sie auf **Suchen**.
2. Wählen Sie **TP1** in der Liste aus.
3. Klicken Sie auf **B2B-Funktionalität**.
4. Klicken Sie auf das Symbol **Erweitern** neben **Paket: N/A**.
5. Klicken Sie auf das Symbol **Bearbeiten** neben **Protokoll: X12V5R1 (ALL)**.
6. Wählen Sie in der Zeile **FA-Zuordnung** die Option **&DT_FA997V2R4** aus.
7. Klicken Sie erneut auf **B2B-Funktionalität**.
8. Klicken Sie auf das Symbol **Erweitern** neben **Paket: N/A**.
9. Klicken Sie auf das Symbol **Bearbeiten** neben **Protokoll: &DT99724 (ALL)**.
10. Geben Sie die folgenden Attribute an:
    a. Wählen Sie in der Zeile **Umschlagsprofil** den Eintrag **UmschProf1** in der Liste aus.
    b. Geben Sie in der Zeile **Qualifikationsmerkmal für Austausch** den Wert **01** ein.
    c. Geben Sie in der Zeile **Kennung für Austausch** den Wert **000000001** ein.
    d. Geben Sie in der Zeile **Nutzungsanzeiger für Austausch** den Buchstaben **T** ein.
11. Klicken Sie auf **Speichern**.

Mit dieser Aufgabenabfolge haben Sie dem Austausch eine funktionale Bestätigung EDI-X12 997 hinzugefügt, sodass, wenn der interne Partner das Dokument emp-

fängt, er die funktionale Bestätigung 997 an den Absender (TP1) zurücksendet. Die Bestätigung 997 wird in einem Umschlag gesendet, der sich nach dem Umschlagsprofil **UmschProf1** richtet.

# Beispiel: EDI zu XML

Dieser Abschnitt enthält ein Beispiel für das Senden einer EDI-Transaktion in einem Umschlag an den Hub, auf dem sie in ein XML-Dokument transformiert und an den internen Partner gesendet wird.

In diesem Beispiel wird davon ausgegangen, dass der Zuordnungsexperte von Data Interchange Services eine Transformationszuordnung erstellt hat, die eine EDI-879-Standardtransaktion, welche mit dem Wörterbuch X12V5R1 definiert ist und der Version 5010 von X12 entspricht, nimmt und diese in ein XML-Dokument transformiert, das von der Back-End-Anwendung des internen Partners verarbeitet wird. In diesem Beispiel heißt die Zuordnung S_DT_EDI_TO_XML.eif.

Der Zuordnungsexperte von Data Interchange Services kann die Transformationszuordnung direkt in die WebSphere Partner Gateway-Datenbank exportieren. Alternativ hierzu kann der Zuordnungsexperte von Data Interchange Services Ihnen die Datei senden, in dem Fall verwenden Sie das Dienstprogramm bcgDISImport, um die Datei in WebSphere Partner Gateway zu importieren. Dieser Anhang geht vom zweiten Szenario aus.

## Transformationszuordnung importieren

Dieser Abschnitt beschreibt die Schritte, die Sie beim Importieren einer Transformationszuordnung ausführen, die die EDI-Eingabe nimmt und diese in ein XML-Format transformiert. Beim Importieren der Transformationszuordnung können Sie auch die Dokumentdefinition importieren, die der Zuordnung zugeordnet ist.

Bevor Sie die Transformationszuordnung importieren können, muss der Zuordnungsexperte von Data Interchange Services Ihnen diese zusenden. Diese Gruppe von Schritten geht davon aus, dass sich die Datei 'S_DT_EDI_TO_XML.eif' auf Ihrem System befindet.

1. Öffnen Sie ein Befehlsfenster.
2. Geben Sie den folgenden Befehl bzw. das folgende Script ein:
   - Auf einem UNIX-System:

     ```
     <Produktverz>/bin/bcgDISImport.sh <datenbankbenutzer-id>
      <kennwort> S_DT_EDI_TO_XML.eif
     ```

   - Auf einem Windows-System:

     ```
     <Produktverz>\bin\bcgDISImport.bat <datenbankbenutzer-id>
      <kennwort> S_DT_EDI_TO_XML.eif
     ```

     Dabei gilt Folgendes: <*datenbankbenutzer-ID*> und <*kennwort*> sind die Werte, die Sie verwendet haben, als Sie die Datenbank als Teil der WebSphere Partner Gateway-Installation installiert haben.

## Transformationszuordnung und Dokumentdefinitionen überprüfen

Führen Sie die folgenden Schritte aus, um zu prüfen, ob die Transformationszuordnungen und Dokumentdefinitionen, die Sie importiert haben, in Community Console verfügbar sind:

1. Klicken Sie auf **Hubadmin > Hubkonfiguration > Zuordnungen > Transformationszuordnungen**.

   Die Zuordnung S_DT_EDI_TO_XML wird angezeigt.
2. Klicken Sie auf das Symbol **Details anzeigen** neben der Zuordnung.

   Dokumentdefinitionen, denen diese Zuordnung zugeordnet ist:

*Tabelle 42. Dokumentdefinition, die der Zuordnung zugeordnet ist*

| Quelle | Ziel |
|---|---|
| Paket: N/A Protokoll: X12V5R1Dokumenttyp: 879 (ALL) | Paket: None Protokoll: FVT-XML-TEST (ALL) Dokumenttyp: WWRE_ITEMCREATIONINTERNAL (ALL) |

Die Zuordnung S_DT_EDI_TO_XML wurde definiert, um eine X12-879-Transaktion zu nehmen, die mit dem X12V4R1-Standard konform ist, und sie in ein angepasstes Protokoll transformiert.

## Empfänger konfigurieren

In diesem Abschnitt erstellen Sie einen Dateisystemverzeichnis-Empfänger für den Hub:

1. Klicken Sie auf **Hubadmin > Hubkonfiguration > Empfänger** und klicken Sie dann auf **Empfänger erstellen**.
2. Geben Sie als Empfängernamen **EDIFileTarget** ein.
3. Wählen Sie in der Liste **Transport** die Option **Dateiverzeichnis** aus.
4. Geben Sie als Stammverzeichnispfad **/Data/Manager/editarget** ein.
5. Klicken Sie auf **Speichern**.

Der Partner sendet den EDI-Austausch an diesen Empfänger.

## Interaktionen erstellen

Sie erstellen zwei Interaktionen: eine für den EDI-Umschlag und eine für die Transaktion im EDI-Umschlag.

Erstellen Sie eine Interaktion, die den EDI-Umschlag darstellt.

1. Klicken Sie auf **Hubadmin > Hubkonfiguration > Dokumentdefinition > Interaktionen verwalten**.
2. Klicken Sie in der Anzeige **Interaktionen verwalten** auf den Link **Interaktion erstellen**.
3. Erweitern Sie die Einträge **Paket: None** und **Protokoll: EDI-X12** und wählen Sie **Dokumenttyp: ISA** aus.
4. Erweitern Sie die Einträge **Paket: N/A** und **Protokoll: EDI-X12** und wählen Sie **Dokumenttyp: ISA** aus.
5. Wählen Sie in der Liste **Aktion** die Option **EDI - Umschlag entfernen** aus.

   **Anmerkung:** In dieser Interaktion findet keine Transformation statt. Vom EDI-Austausch wird der Umschlag entfernt, wodurch die einzelne Transaktion (879) entsteht. Sie benötigen daher keine Transformationszuordnung für diese Interaktion.
6. Klicken Sie auf **Speichern**.

Erstellen Sie eine Interaktion, die über eine Quelle verfügt, die die 879-Transaktion darstellt, und ein Ziel, das das transformierte Dokument darstellt.

1. Klicken Sie auf **Hubadmin > Hubkonfiguration > Dokumentdefinition > Interaktionen verwalten**.
2. Klicken Sie in der Anzeige **Interaktionen verwalten** auf den Link **Interaktion erstellen**.
3. Erweitern Sie die Einträge **Paket: N/A** und **Protokoll: X12V5R1** und wählen Sie **Dokumenttyp: 879** aus.
4. Erweitern Sie die Einträge **Paket: None** und **Protokoll: FVT-XML-TEST** und wählen Sie **Dokumenttyp: WWRE_ITEMCREATIONINTERNAL** aus.
5. Wählen Sie in der Liste **Transformationszuordnung** den Eintrag **S_DT_EDI-_TO_XML** aus.
6. Wählen Sie in der Liste **Aktion** die Option **EDI validieren und EDI konvertieren** aus.
7. Klicken Sie auf **Speichern**.

Diese Interaktion stellt die Transformation einer EDI-X12-879-Standardtransaktion in ein anderes Format dar; daher müssen Sie eine Transformationszuordnung auswählen.

## Partner erstellen

Sie haben für dieses Beispiel zwei Partner: den internen Partner (Manager) und einen externen Partner (TP1).

Erstellen Sie das Profil **Interner Partner**:

1. Klicken Sie auf **Kontenadmin > Profile > Partner** und klicken Sie auf **Erstellen**.
2. Geben Sie als Anmeldenamen des Unternehmens **ComManager** ein.
3. Geben Sie als Anzeigenamen des Partners **Manager** ein.
4. Wählen Sie als Partnertyp **Interner Partner** aus.
5. Klicken Sie auf **Neu** für die Geschäfts-ID und geben Sie `000000000` als unformatierte ID ein.

   **Anmerkung:** Stellen Sie sicher, dass Sie **Unformatiert** und nicht **DUNS** ausgewählt haben.
6. Klicken Sie erneut auf **Neu** für die Geschäfts-ID und geben Sie `01-000000000` als unformatierte ID ein.
7. Klicken Sie auf **Speichern**.

Erstellen Sie den zweiten Partner:

1. Klicken Sie auf **Kontenadmin > Profile > Partner** und klicken Sie auf **Erstellen**.
2. Geben Sie als Anmeldenamen des Unternehmens **TP1** ein.
3. Geben Sie als Anzeigenamen des Partners **TP1** ein.
4. Wählen Sie als Partnertyp **Externer Partner** aus.
5. Klicken Sie auf **Neu** für die Geschäfts-ID und geben Sie `000000001` als unformatierte ID ein.

   **Anmerkung:** Stellen Sie sicher, dass Sie **Unformatiert** und nicht **DUNS** ausgewählt haben.
6. Klicken Sie erneut auf **Neu** für die Geschäfts-ID und geben Sie `01-000000001` als unformatierte ID ein.

7. Klicken Sie auf **Speichern**.

## Ziele erstellen

Erstellen Sie in diesem Beispiel Dateiverzeichnisziele für beide Partner. Erstellen Sie zuerst ein Ziel für den Manager.

1. Klicken Sie auf **Kontenadmin > Profile > Partner** und klicken Sie auf **Suchen**.
2. Klicken Sie auf das Symbol **Details anzeigen** neben dem Profil **Manager**.
3. Klicken Sie auf **Ziele** und dann auf **Erstellen**.
4. Geben Sie die folgenden Werte für das Ziel ein. Denken Sie daran, dass das Dateiverzeichnis (der vollständige Pfad) schon auf Ihrem Dateisystem vorhanden sein muss.
   a. Geben Sie als Namen **ManagerFileDestination** ein.
   b. Wählen Sie in der Liste **Transport** die Option **Dateiverzeichnis** aus.
   c. Geben Sie als Adresse **file://Data/Manager/filedestination** ein.
   d. Klicken Sie auf **Speichern**.
5. Klicken Sie auf **Liste**, um alle Ziele für den internen Partner aufzulisten.
6. Klicken Sie auf **Standardziele anzeigen**.
7. Wählen Sie in der Liste **Produktion** das Ziel aus, das Sie in Schritt 4 erstellt haben.
8. Klicken Sie auf **Speichern**.

Erstellen Sie als Nächstes ein Ziel für den Partner.

1. Klicken Sie auf **Kontenadmin > Profile > Partner** und klicken Sie auf **Suchen**.
2. Wählen Sie den anderen Partner aus, den Sie für dieses Beispiel erstellt haben, indem Sie auf das Symbol **Details anzeigen** neben **TP1** klicken.
3. Klicken Sie auf **Ziele** und dann auf **Erstellen**.
4. Geben Sie die folgenden Werte für das Ziel ein. Denken Sie daran, dass das Dateiverzeichnis (der vollständige Pfad) schon vorhanden sein muss.
   a. Geben Sie als Namen **TP1FileDestination** ein.
   b. Wählen Sie in der Liste **Transport** die Option **Dateiverzeichnis** aus.
   c. Geben Sie als Adresse **file://Data/TP1/filedestination** ein.
   d. Klicken Sie auf **Speichern**.
5. Klicken Sie auf **Liste**, um alle Ziele für den Partner aufzulisten.
6. Klicken Sie auf **Standardziele anzeigen**.
7. Wählen Sie in der Liste **Produktion** das Ziel aus, das Sie in Schritt 4 erstellt haben.
8. Klicken Sie auf **Speichern**.

## B2B-Funktionalität konfigurieren

Aktivieren Sie die B2B-Funktionalität der beiden Partner in diesem Austausch. In diesem Beispiel stammt der EDI-Austausch vom externen Partner (TP1) und wird dem internen Partner zugestellt.

1. Klicken Sie auf **Kontenadmin > Profile > Partner**, und klicken Sie auf **Suchen**.
2. Klicken Sie auf das Symbol **Details anzeigen** für den Quellenpartner in diesem Beispiel (**TP1**).
3. Klicken Sie auf **B2B-Funktionalität**.

4. Aktivieren Sie zwei Funktionalitätsgruppen für den Quellenpartner.
   a. Aktivieren Sie zuerst die Dokumentdefinition, die den EDI-Umschlag darstellt:
      1) Klicken Sie zum Aktivieren auf das Symbol **Rolle ist nicht aktiv** unter **Quelle festlegen** für **Paket: None**.
      2) Erweitern Sie **Paket: None**.
      3) Klicken Sie auf das Symbol **Rolle ist nicht aktiv** unter **Quelle festlegen** für **Protokoll: EDI-X12 (ALL)**.
      4) Erweitern Sie **Protokoll: EDI-X12 (ALL)**.
      5) Klicken Sie auf das Symbol **Rolle ist nicht aktiv** unter **Quelle festlegen** für **Dokumenttyp: ISA (ALL)**.
   b. Aktivieren Sie als Nächstes die Dokumentdefinition, die die Transaktion darstellt:
      1) Klicken Sie zum Aktivieren auf das Symbol **Rolle ist nicht aktiv** unter **Quelle festlegen** für **Paket: N/A**.
      2) Erweitern Sie **Paket: N/A**.
      3) Klicken Sie auf das Symbol **Rolle ist nicht aktiv** unter **Quelle festlegen** für **Protokoll: X12V5R1 (ALL)**.
      4) Erweitern Sie **Protokoll: X12V5R1 (ALL)**.
      5) Klicken Sie auf das Symbol **Rolle ist nicht aktiv** unter **Quelle festlegen** für **Dokumenttyp: 879**.
5. Klicken Sie auf **Kontenadmin > Profile > Partner**, und klicken Sie auf **Suchen**.
6. Klicken Sie auf das Symbol **Details anzeigen** für den Zielpartner in diesem Beispiel (**Manager**).
7. Klicken Sie auf **B2B-Funktionalität**.
8. Aktivieren Sie zwei Funktionalitätsgruppen für den Zielpartner.
   a. Aktivieren Sie zuerst die Dokumentdefinition:
      1) Klicken Sie zum Aktivieren auf das Symbol **Rolle ist nicht aktiv** unter **Ziel festlegen** für **Paket: N/A**.
      2) Erweitern Sie **Paket: N/A**.
      3) Klicken Sie auf das Symbol **Rolle ist nicht aktiv** unter **Ziel festlegen** für **Protokoll: EDI-X12 (ALL)**.
      4) Erweitern Sie **Protokoll: EDI-X12 (ALL)**.
      5) Klicken Sie auf das Symbol **Rolle ist nicht aktiv** unter **Ziel festlegen** für **Dokumenttyp: ISA (ALL)**.
   b. Aktivieren Sie als Nächstes die Dokumentdefinition, die das transformierte Dokument darstellt:
      1) Klicken Sie zum Aktivieren auf das Symbol **Rolle ist nicht aktiv** unter **Ziel festlegen** für **Paket: None**.
      2) Erweitern Sie **Paket: None**.
      3) Klicken Sie auf das Symbol **Rolle ist nicht aktiv** unter **Ziel festlegen** für **Protokoll: FVT-XML-TEST (ALL)**.
      4) Erweitern Sie **Protokoll: FVT-XML-TEST (ALL)**.
      5) Klicken Sie auf das Symbol **Rolle ist nicht aktiv** unter **Ziel festlegen** für **Dokumenttyp: WWRE_ITEMCREATIONINTERNAL(ALL)**.

## Verbindungen aktivieren

Gehen Sie wie folgt vor, um die Verbindungen zu aktivieren:

1. Klicken Sie auf **Kontenadmin > Verbindungen**.
2. Wählen Sie **TP1** in der Liste **Quelle** aus.
3. Wählen Sie **Manager** in der Liste **Ziel** aus.
4. Klicken Sie auf **Suchen**.
5. Klicken Sie auf **Aktivieren** für die Verbindung, die den Umschlag darstellt:

*Tabelle 43. Verbindung für Umschlag*

| Quelle | Ziel |
|---|---|
| Paket: None (N/A) Protokoll: EDI-X12 (ALL) Dokumenttyp: ISA (ALL) | Paket: N/A (N/A) Protokoll: EDI-X12 (ALL) Dokumenttyp: ISA (ALL) |

6. Klicken Sie auf **Aktivieren** für die Verbindung, die die 879-Transaktion darstellt, zum transformierten Dokument:

*Tabelle 44. Verbindung für EDI-Transaktion zu XML-Dokument*

| Quelle | Ziel |
|---|---|
| Paket: N/A (N/A) Protokoll: X12V5R1 (ALL)Dokumenttyp: 879 (ALL) | Paket: None (N/A) Protokoll: FVT-XML-TEST (ALL) Dokumenttyp: WWRE_ITEMCREATIONINTERNAL (ALL) |

Wenn TP1 an dieser Stelle einen EDI-Austausch mit einer 879-Transaktion an den internen Partner sendet, wird der Umschlag vom EDI-Austausch entfernt, wodurch eine 879-Transaktion entsteht. Die 879-Transaktion wird dann transformiert und das transformierte Dokument wird an das Ziel des internen Partners gesendet.

# Beispiel: XML zu EDI

Dieser Abschnitt enthält ein Beispiel davon, wie der interne Partner ein XML-Dokument an den Hub sendet, auf dem es in eine EDI-Transaktion transformiert, in einem EDI-Austausch mit einem Umschlag versehen und an einen Partner gesendet wird.

In diesem Beispiel wird davon ausgegangen, dass der Zuordnungsexperte von Data Interchange Services eine Transformationszuordnung erstellt hat, die ein XML-Dokument in eine EDI-850-Standardtransaktion (die mit dem Wörterbuch MX12V3R1 definiert ist) transformiert, die vom Partner verarbeitet wird. In diesem Beispiel heißt die Zuordnung S_DT_XML_TO_EDI.eif.

Der Zuordnungsexperte von Data Interchange Services kann die Transformationszuordnung direkt in die WebSphere Partner Gateway-Datenbank exportieren. Alternativ hierzu kann der Zuordnungsexperte von Data Interchange Services Ihnen die Datei senden, in dem Fall verwenden Sie das Dienstprogramm bcgDISImport, um die Datei in WebSphere Partner Gateway zu importieren. Dieser Anhang geht vom zweiten Szenario aus.

## Transformationszuordnung importieren

Dieser Abschnitt beschreibt die Schritte, die Sie beim Importieren einer Transformationszuordnung ausführen, die die XML-Eingabe nimmt und diese in eine EDI-

Transaktion transformiert. Beim Importieren der Transformationszuordnung können Sie auch die Dokumentdefinition importieren, die der Zuordnung zugeordnet ist.

Bevor Sie die Transformationszuordnung importieren können, muss der Zuordnungsexperte von Data Interchange Services Ihnen diese zusenden. Diese Gruppe von Schritten geht davon aus, dass sich die Datei 'S_DT_XML_TO_EDI.eif' auf Ihrem System befindet.

1. Öffnen Sie ein Befehlsfenster.
2. Geben Sie den folgenden Befehl bzw. das folgende Script ein:
   - Auf einem UNIX-System:

     ```
     <Produktverz>/bin/bcgDISImport.sh <datenbankbenutzer-id>
      <kennwort> S_DT_XML_TO_EDI.eif
     ```

   - Auf einem Windows-System:

     ```
     <Produktverz>\bin\bcgDISImport.bat <datenbankbenutzer-id>
      <kennwort> S_DT_XML_TO_EDI.eif
     ```

     Dabei gilt Folgendes: <*datenbankbenutzer-ID*> und <*kennwort*> sind die Werte, die Sie verwendet haben, als Sie die Datenbank als Teil der WebSphere Partner Gateway-Installation installiert haben.

## Transformationszuordnung und Dokumentdefinitionen überprüfen

Führen Sie die folgenden Schritte aus, um zu prüfen, ob die Transformationszuordnungen und Dokumentdefinitionen, die Sie importiert haben, in Community Console verfügbar sind:

1. Klicken Sie auf **Hubadmin > Hubkonfiguration > Zuordnungen > Transformationszuordnungen**.

   Die Zuordnung S_DT_XML_TO_EDI wird angezeigt.
2. Klicken Sie auf das Symbol **Details anzeigen** neben der Zuordnung.

   Dokumentdefinitionen, denen diese Zuordnung zugeordnet ist:

*Tabelle 45. Dokumentdefinitionen, die der Zuordnung zugeordnet sind*

| Quelle | Ziel |
|---|---|
| Paket: None Protokoll: FVT-XML-TEST (ALL) Dokumenttyp: ICGCPO (ALL) | Paket: N/A Protokoll: MX12V3R1 (ALL) Dokumenttyp: 850 (ALL) |

Die Zuordnung S_DT_XML_TO_EDI wurde definiert, um ein XML-Dokument zu nehmen und es in eine EDI-Transaktion zu transformieren.

## Empfänger konfigurieren

In diesem Abschnitt erstellen Sie einen Dateisystemverzeichnis-Empfänger für den Hub:

1. Klicken Sie auf **Hubadmin > Hubkonfiguration > Empfänger** und klicken Sie dann auf **Empfänger erstellen**.
2. Geben Sie als Empfängernamen **XMLFileTarget** ein.
3. Wählen Sie in der Liste **Transport** die Option **Dateiverzeichnis** aus.
4. Geben Sie als Stammverzeichnispfad **/Data/Manager/xmltarget** ein.
5. Wählen Sie in der Liste **Konfigurationspunkt** die Option **Vorverarbeitung** aus.

6. Wählen Sie **com.ibm.bcg.edi.receiver.preprocesshandler.XMLSplitterHandler** in der **Verfügbarkeitsliste** aus und klicken Sie auf **Hinzufügen**, um den Handler in die **Konfigurationsliste** zu versetzen.
7. Klicken Sie auf **Speichern**.

Der interne Partner sendet das XML-Dokument an diesen Empfänger.

## Interaktionen erstellen

Sie erstellen zwei Interaktionen: eine für die Transformation XML zu EDI und eine für den EDI-Umschlag.

Erstellen Sie eine Interaktion, die über eine Quelle verfügt, die das XML-Dokument darstellt, und ein Ziel, das die transformierte 850-Transaktion darstellt.

1. Klicken Sie auf **Hubadmin > Hubkonfiguration > Dokumentdefinition > Interaktionen verwalten**.
2. Klicken Sie in der Anzeige **Interaktionen verwalten** auf den Link **Interaktion erstellen**.
3. Erweitern Sie die Einträge **Paket: None** und **Protokoll: FVT-XML-TEST** und wählen Sie **Dokumenttyp: ICGCPO** aus.
4. Erweitern Sie die Einträge **Paket: N/A** und **Protokoll: MX12V3R1** und wählen Sie **Dokumenttyp: 850** aus.
5. Wählen Sie in der Liste **Transformationszuordnung** den Eintrag **S_DT_XML_TO_EDI** aus.
6. Wählen Sie in der Liste **Aktion** die Option **XML konvertieren und EDI validieren** aus.
7. Klicken Sie auf **Speichern**.

Diese Interaktion stellt die Transformation eines XML-Dokuments in eine EDI-Transaktion dar; daher müssen Sie eine Transformationszuordnung auswählen.

Erstellen Sie eine Interaktion, die den EDI-Umschlag darstellt.

1. Klicken Sie auf **Hubadmin > Hubkonfiguration > Dokumentdefinition > Interaktionen verwalten**.
2. Klicken Sie in der Anzeige **Interaktionen verwalten** auf den Link **Interaktion erstellen**.
3. Erweitern Sie die Einträge **Paket: N/A** und **Protokoll: EDI-X12** und wählen Sie **Dokumenttyp: ISA** aus.
4. Erweitern Sie die Einträge **Paket: None** und **Protokoll: EDI-X12** und wählen Sie **Dokumenttyp: ISA** aus.
5. Wählen Sie in der Liste **Aktion** die Option **Pass-Through** aus.

   **Anmerkung:** In dieser Interaktion findet keine Transformation statt.
6. Klicken Sie auf **Speichern**.

## Partner erstellen

Sie haben für dieses Beispiel zwei Partner: den internen Partner (Manager) und einen externen Partner (TP1).

Erstellen Sie das Profil **Interner Partner**:

1. Klicken Sie auf **Kontenadmin > Profile > Partner** und klicken Sie auf **Erstellen**.
2. Geben Sie als Anmeldenamen des Unternehmens **ComManager** ein.
3. Geben Sie als Anzeigenamen des Partners **Manager** ein.
4. Wählen Sie als Partnertyp **Interner Partner** aus.
5. Klicken Sie auf **Neu** für die Geschäfts-ID und geben Sie `000000000` als unformatierte ID ein.

   **Anmerkung:** Stellen Sie sicher, dass Sie **Unformatiert** und nicht **DUNS** ausgewählt haben.
6. Klicken Sie erneut auf **Neu**, um eine neue Geschäfts-ID zu erstellen, und geben Sie `01-000000000` als unformatierte ID ein. Wenn Sie auf Neu klicken, wird auch das Textfeld "E-Mail-ID" aktiviert und angezeigt, damit Sie eine E-Mail-ID erstellen können.
7. Klicken Sie auf **Neu**, um eine neue E-Mail-ID zu erstellen, und geben Sie die E-Mail-ID im Feld "E-Mail-Kennung" ein. Wenn Sie auf **Neu** klicken, können Sie auch mehrere E-Mail-IDs erstellen.
8. Klicken Sie auf **Speichern**.

Erstellen Sie den zweiten Partner:

1. Klicken Sie auf **Kontenadmin > Profile > Partner** und klicken Sie auf **Erstellen**.
2. Geben Sie als Anmeldenamen des Unternehmens **TP1** ein.
3. Geben Sie als Anzeigenamen des Partners **TP1** ein.
4. Wählen Sie als Partnertyp **Externer Partner** aus.
5. Klicken Sie erneut auf **Neu**, um eine neue Geschäfts-ID zu erstellen, und geben Sie `01-000000000` als unformatierte ID ein. Wenn Sie auf Neu klicken, wird auch das Textfeld "E-Mail-ID" aktiviert und angezeigt, damit Sie eine E-Mail-ID erstellen können.

   **Anmerkung:** Stellen Sie sicher, dass Sie **Unformatiert** und nicht **DUNS** ausgewählt haben.
6. Klicken Sie auf **Neu**, um eine neue E-Mail-ID zu erstellen, und geben Sie die E-Mail-ID im Feld "E-Mail-Kennung" ein. Wenn Sie auf **Neu** klicken, können Sie auch mehrere E-Mail-IDs erstellen.
7. Klicken Sie auf **Speichern**.

## Ziele erstellen

Erstellen Sie in diesem Beispiel Dateiverzeichnisziele für beide Partner. Erstellen Sie zuerst ein Ziel für den Manager.

1. Klicken Sie auf **Kontenadmin > Profile > Partner** und klicken Sie auf **Suchen**.
2. Klicken Sie auf das Symbol **Details anzeigen** neben dem Profil **Manager**.
3. Klicken Sie auf **Ziele** und dann auf **Erstellen**.
4. Geben Sie die folgenden Werte für das Ziel ein. Denken Sie daran, dass das Dateiverzeichnis (der vollständige Pfad) schon auf Ihrem Dateisystem vorhanden sein muss.

a. Geben Sie als Namen **ManagerFileDestination** ein.
b. Wählen Sie in der Liste **Transport** die Option **Dateiverzeichnis** aus.
c. Geben Sie als Adresse **file://Data/Manager/filedestination** ein.
d. Klicken Sie auf **Speichern**.

5. Klicken Sie auf **Liste**, um alle Ziele für den internen Partner aufzulisten.
6. Klicken Sie auf **Standardziele anzeigen**.
7. Wählen Sie in der Liste **Produktion** das Ziel aus, das Sie in Schritt 4 auf Seite 367 erstellt haben.
8. Klicken Sie auf **Speichern**.

Erstellen Sie als Nächstes ein Ziel für den Partner.

1. Klicken Sie auf **Kontenadmin > Profile > Partner** und klicken Sie auf **Suchen**.
2. Wählen Sie den anderen Partner aus, den Sie für dieses Beispiel erstellt haben, indem Sie auf das Symbol **Details anzeigen** neben **TP1** klicken.
3. Klicken Sie auf **Ziele** und dann auf **Erstellen**.
4. Geben Sie die folgenden Werte für das Ziel ein. Denken Sie daran, dass das Dateiverzeichnis (der vollständige Pfad) schon vorhanden sein muss.
   a. Geben Sie als Namen **TP1FileDestination** ein.
   b. Wählen Sie in der Liste **Transport** die Option **Dateiverzeichnis** aus.
   c. Geben Sie als Adresse **file://Data/TP1/filedestination** ein.
   d. Klicken Sie auf **Speichern**.
5. Klicken Sie auf **Liste**, um alle Ziele für den Partner aufzulisten.
6. Klicken Sie auf **Standardziele anzeigen**.
7. Wählen Sie in der Liste **Produktion** das Ziel aus, das Sie in Schritt 4 erstellt haben.
8. Klicken Sie auf **Speichern**.

## B2B-Funktionalität konfigurieren

Aktivieren Sie die B2B-Funktionalität der beiden Partner in diesem Austausch. In diesem Beispiel stammt das XML-Dokument vom internen Partner und wird dem externen Partner zugestellt.

1. Klicken Sie auf **Kontenadmin > Profile > Partner**, und klicken Sie auf **Suchen**.
2. Klicken Sie auf das Symbol **Details anzeigen** für den Quellenpartner in diesem Beispiel (**ComMan**).
3. Klicken Sie auf **B2B-Funktionalität**.
4. Aktivieren Sie drei Funktionalitätsgruppen für den Quellenpartner.
   a. Aktivieren Sie die Dokumentdefinition, die das XML-Dokument darstellt:
      1) Klicken Sie zum Aktivieren auf das Symbol **Rolle ist nicht aktiv** unter **Quelle festlegen** für **Paket: None**.
      2) Erweitern Sie **Paket: None**.
      3) Klicken Sie auf das Symbol **Rolle ist nicht aktiv** unter **Quelle festlegen** für **Protokoll: FVT-XML-TEST (ALL)**.
      4) Erweitern Sie **Protokoll: FVT-XML-TEST (ALL)**.
      5) Klicken Sie auf das Symbol **Rolle ist nicht aktiv** unter **Quelle festlegen** für **Dokumenttyp: ICGCPO (ALL)**.
   b. Aktivieren Sie als Nächstes die Dokumentdefinition, die das transformierte Dokument darstellt:

1) Klicken Sie zum Aktivieren auf das Symbol **Rolle ist nicht aktiv** unter **Quelle festlegen** für **Paket: N/A**.
2) Erweitern Sie **Paket: N/A**.
3) Klicken Sie auf das Symbol **Rolle ist nicht aktiv** unter **Quelle festlegen** für **Protokoll: MX12V3R1 (ALL)**.
4) Erweitern Sie **Protokoll: MX12V3R1 (ALL)**.
5) Klicken Sie auf das Symbol **Rolle ist nicht aktiv** unter **Quelle festlegen** für **Dokumenttyp: 850**.

c. Aktivieren Sie dann die Dokumentdefinition, die den EDI-Umschlag darstellt:
1) Klicken Sie zum Aktivieren auf das Symbol **Rolle ist nicht aktiv** unter **Quelle festlegen** für **Paket: N/A**.
2) Erweitern Sie **Paket: N/A**.
3) Klicken Sie auf das Symbol **Rolle ist nicht aktiv** unter **Quelle festlegen** für **Protokoll: EDI-X12 (ALL)**.
4) Erweitern Sie **Protokoll: EDI-X12 (ALL)**.
5) Klicken Sie auf das Symbol **Rolle ist nicht aktiv** unter **Quelle festlegen** für **Dokumenttyp: ISA (ALL)**.

5. Klicken Sie auf **Kontenadmin > Profile > Partner**, und klicken Sie auf **Suchen**.
6. Klicken Sie auf das Symbol **Details anzeigen** für den Zielpartner in diesem Beispiel (**TP1**).
7. Klicken Sie auf **B2B-Funktionalität**.
8. Aktivieren Sie zwei Funktionalitätsgruppen für den Zielpartner.
a. Aktivieren Sie zuerst die Dokumentdefinition, die die EDI-850-Transaktion darstellt:
1) Klicken Sie zum Aktivieren auf das Symbol **Rolle ist nicht aktiv** unter **Ziel festlegen** für **Paket: N/A**.
2) Erweitern Sie **Paket: N/A**.
3) Klicken Sie auf das Symbol **Rolle ist nicht aktiv** unter **Ziel festlegen** für **Protokoll: MX12V3R1 (ALL)**.
4) Erweitern Sie **Protokoll: MX12V3R1 (ALL)**.
5) Klicken Sie auf das Symbol **Rolle ist nicht aktiv** unter **Ziel festlegen** für **Dokumenttyp: 850 (ALL)**.

b. Aktivieren Sie als Nächstes die Dokumentdefinition:
1) Klicken Sie zum Aktivieren auf das Symbol **Rolle ist nicht aktiv** unter **Ziel festlegen** für **Paket: None**.
2) Erweitern Sie **Paket: None**.
3) Klicken Sie auf das Symbol **Rolle ist nicht aktiv** unter **Ziel festlegen** für **Protokoll: EDI-X12 (ALL)**.
4) Erweitern Sie **Protokoll: EDI-X12 (ALL)**.
5) Klicken Sie auf das Symbol **Rolle ist nicht aktiv** unter **Ziel festlegen** für **Dokumenttyp: ISA(ALL)**.

## Umschlagsprofil erstellen

Sie erstellen als Nächstes das Profil für den Umschlag, der die transformierte 850-Transaktion enthalten wird:

1. Klicken Sie auf **Hubadmin > Hubkonfiguration > EDI > Umschlagsprofil**.
2. Klicken Sie auf **Erstellen**.

3. Geben Sie den Namen des Profils ein: **UmschProf1**.
4. Wählen Sie in der Liste **EDI-Standard** die Option **X12** aus.
5. Die Schaltfläche **Allgemein** ist standardmäßig ausgewählt. Geben Sie die folgenden Werte für die allgemeinen Attribute des Umschlags ein:
   - INTCTLLEN: **9**
   - GRPCTLLEN: **9**
   - TRXCTLLEN: **9**
   - MAXDOCS: **1000**
6. Klicken Sie auf **Austausch** und geben Sie die folgenden Werte für die Austauschattribute ein:
   - ISA01: **01**
   - ISA02: **ISA0000002**
   - ISA03: **02**
   - ISA04: **ISA0000004**
   - ISA11: **U**
   - ISA12: **00301**
   - ISA15: **T**
7. Klicken Sie auf **Speichern**.

## XML-Format erstellen

In diesem Abschnitt erstellen Sie das angepasste XML-Format.

1. Klicken Sie auf **Hubadmin > Hubkonfiguration > XML-Formate**.
2. Klicken Sie auf **XML-Format erstellen**.
3. Wählen Sie als **Routing-Format** das Format **FVT-XML-TEST ALL** aus.
4. Wählen Sie für **Dateityp** den Eintrag **XML** aus.
5. Wählen Sie als Kennungstyp **Root-Tag** aus und geben Sie **MMDoc** ein.
6. Wählen Sie als Quellengeschäfts-ID **Konstante** aus und geben Sie **000000000** ein.
7. Wählen Sie als Zielgeschäfts-ID **Konstante** aus und geben Sie **000000001** ein.
8. Wählen Sie als Quellendokumenttyp **Konstante** aus und geben Sie **ICGCPO** ein.
9. Wählen Sie als Quellendokumenttyp-Version **Konstante** aus und geben Sie **ALLE** ein.
10. Klicken Sie auf **Speichern**.

## Verbindungen aktivieren

Aktivieren Sie die Partnerverbindungen:

1. Klicken Sie auf **Kontenadmin > Verbindungen**.
2. Wählen Sie **Manager** in der Liste **Quelle** aus.
3. Wählen Sie **TP1** in der Liste **Ziel** aus.
4. Klicken Sie auf **Suchen**.
5. Klicken Sie auf **Aktivieren** für die folgende Verbindung:

*Tabelle 46. Verbindung für XML-Dokument zu EDI-Transaktion*

| Quelle | Ziel |
|---|---|
| Paket: None (N/A) Protokoll: FVT-XML-TEST (ALL) Dokumenttyp: ICGCPO (ALL) | Paket: N/A (N/A) Protokoll: MX12V3R1 (ALL) Dokumenttyp: 850 (ALL) |

6. Klicken Sie auf **Aktivieren** für die Verbindung, die den EDI-Umschlag darstellt:

*Tabelle 47. Verbindung für EDI-Umschlag*

| Quelle | Ziel |
|---|---|
| Paket: N/A (N/A) Protokoll: EDI-X12 (ALL) Dokumenttyp: ISA (ALL) | Paket: None (N/A) Protokoll: EDI-X12 (ALL) Dokumenttyp: ISA (ALL) |

## Attribute konfigurieren

Konfigurieren Sie die Attribute für die B2B-Funktionalität des Zielpartners (TP1) und des Quellenpartners (Manager):

1. Klicken Sie auf **Kontenadmin > Profile > Partner** und klicken Sie auf **Suchen**.
2. Klicken Sie zum Auswählen auf das Symbol **Details anzeigen** neben **TPI**.
3. Klicken Sie auf **B2B-Funktionalität**.
4. Klicken Sie auf das Symbol **Erweitern** neben **Paket: N/A**.
5. Klicken Sie auf das Symbol **Bearbeiten** neben **Protokoll: MX12V3R1**.
6. Geben Sie die folgenden Attribute an:
   a. Wählen Sie in der Zeile **Umschlagsprofil** den Eintrag **UmschProf1** in der Liste aus.
   b. Geben Sie in der Zeile **Qualifikationsmerkmal für Austausch** den Wert **01** ein.
   c. Geben Sie in der Zeile **Kennung für Austausch** den Wert **000000001** ein.
   d. Geben Sie in der Zeile **Nutzungsanzeiger für Austausch** den Buchstaben **T** ein.
7. Klicken Sie auf **Speichern**.
8. Klicken Sie auf **Kontenadmin > Profile > Partner** und klicken Sie auf **Suchen**.
9. Klicken Sie zum Auswählen auf das Symbol **Details anzeigen** neben **Manager**.
10. Klicken Sie auf **B2B-Funktionalität**.
11. Klicken Sie auf das Symbol **Erweitern** neben **Paket: N/A**.
12. Klicken Sie auf das Symbol **Bearbeiten** neben **Protokoll: MX12V3R1 (ALL)**.
13. Geben Sie die folgenden Attribute an:
    a. Geben Sie in der Zeile **Qualifikationsmerkmal für Austausch** den Wert **01** ein.
    b. Geben Sie in der Zeile **Kennung für Austausch** den Wert **000000000** ein.
    c. Geben Sie in der Zeile **Nutzungsanzeiger für Austausch** den Buchstaben **T** ein.
14. Klicken Sie auf **Speichern**.

Wenn der Quellenpartner (der interne Partner) jetzt ein XML-Dokument an den Partner sendet, wird es auf dem Hub in eine EDI-Transaktion konvertiert, mit einem Umschlag versehen und dann an das Ziel des Partners gesendet.

# Beispiel: ROD zu EDI

Dieser Abschnitt enthält ein Beispiel davon, wie der interne Partner ein ROD-Dokument an den Hub sendet, auf dem es in eine EDI-Transaktion transformiert, in einem EDI-Austausch mit einem Umschlag versehen und an einen Partner gesendet wird.

In diesem Beispiel wird davon ausgegangen, dass der Zuordnungsexperte von Data Interchange Services eine Transformationszuordnung erstellt hat, die ein ROD-Dokument in eine EDI-850-Standardtransaktion (die mit dem Wörterbuch X12V5R1 definiert ist und der Version 5010 von X12 entspricht) transformiert, die vom Partner verarbeitet wird. In diesem Beispiel heißt die Zuordnung S_DT_ROD_TO_EDI.eif.

Der Zuordnungsexperte von Data Interchange Services kann die Transformationszuordnung direkt in die WebSphere Partner Gateway-Datenbank exportieren. Alternativ hierzu kann der Zuordnungsexperte von Data Interchange Services Ihnen die Datei senden, in dem Fall verwenden Sie das Dienstprogramm bcgDISImport, um die Datei in WebSphere Partner Gateway zu importieren. Dieser Anhang geht vom zweiten Szenario aus.

## Transformationszuordnung importieren

Dieser Abschnitt beschreibt die Schritte, die Sie beim Importieren einer Transformationszuordnung ausführen, die die ROD-Eingabe nimmt und diese in eine X12-Transaktion transformiert. Beim Importieren der Transformationszuordnung können Sie auch die Dokumentdefinition importieren, die der Zuordnung zugeordnet ist.

Bevor Sie die Transformationszuordnung importieren können, muss der Zuordnungsexperte von Data Interchange Services Ihnen diese zusenden. Diese Gruppe von Schritten geht davon aus, dass sich die Datei 'S_DT_ROD_TO_EDI.eif' auf Ihrem System befindet.

1. Öffnen Sie ein Befehlsfenster.
2. Geben Sie den folgenden Befehl bzw. das folgende Script ein:
   - Auf einem UNIX-System:

     ```
     <Produktverz>/bin/bcgDISImport.sh <datenbankbenutzer-id>
      <kennwort> S_DT_ROD_TO_EDI.eif
     ```

   - Auf einem Windows-System:

     ```
     <Produktverz>\bin\bcgDISImport.bat <datenbankbenutzer-id>
      <kennwort> S_DT_ROD_TO_EDI.eif
     ```

     Dabei gilt Folgendes: *<datenbankbenutzer-ID>* und *<kennwort>* sind die Werte, die Sie verwendet haben, als Sie die Datenbank als Teil der WebSphere Partner Gateway-Installation installiert haben.

## Transformationszuordnung und Dokumentdefinitionen überprüfen

Führen Sie die folgenden Schritte aus, um zu prüfen, ob die Transformationszuordnungen und Dokumentdefinitionen, die Sie importiert haben, in Community Console verfügbar sind:

1. Klicken Sie auf **Hubadmin > Hubkonfiguration > Zuordnungen > Transformationszuordnungen**.

Die Zuordnung S_DT_ROD_TO_EDI wird angezeigt.

2. Klicken Sie auf das Symbol **Details anzeigen** neben der Zuordnung.
   Dokumentdefinitionen, denen diese Zuordnung zugeordnet ist:

*Tabelle 48. Dokumentdefinitionen, die der Zuordnung zugeordnet sind*

| Quelle | Ziel |
|---|---|
| Paket: None Protokoll: ROD-TO-EDI_DICT (ALL) Dokumenttyp: DTROD-TO-EDI_ROD (ALL) | Paket: N/A Protokoll: X12V5R1(ALL) Dokumenttyp: 850 (ALL) |

Die Zuordnung S_DT_ROD_TO_EDI wurde definiert, um ein ROD-Dokument, das dem Wörterbuch ROD-TO-EDI_DICT zugeordnet ist, zu nehmen und dieses in eine X12-850-Transaktion zu transformieren, die mit dem X12V5R1-Standard konform ist.

## Empfänger konfigurieren

In diesem Abschnitt erstellen Sie einen Dateisystemverzeichnis-Empfänger für den Hub:

1. Klicken Sie auf **Hubadmin > Hubkonfiguration > Empfänger** und klicken Sie dann auf **Empfänger erstellen**.
2. Geben Sie als Empfängernamen **RODFileTarget** ein.
3. Wählen Sie in der Liste **Transport** die Option **Dateiverzeichnis** aus.
4. Geben Sie als Stammverzeichnispfad **/Data/Manager/rodtarget** ein.
5. Wählen Sie in der Liste **Konfigurationspunkt** die Option **Vorverarbeitung** aus.
6. Wählen Sie **com.ibm.bcg.edi.receiver.preprocesshandler.RODSplitterHandler** in der **Verfügbarkeitsliste** aus und klicken Sie auf **Hinzufügen**, um den Handler in die **Konfigurationsliste** zu versetzen.
7. Wählen Sie **com.ibm.bcg.edi.receiver.preprocesshandler.RODSplitterHandler** in der **Konfigurationsliste** aus und klicken Sie auf **Konfigurieren**.
8. Fügen Sie die in der Tabelle gezeigten Werte hinzu:

*Tabelle 49. Attribute für den ROD-Verteilerhandler*

| Feld | Wert |
|---|---|
| From Packaging Name | None |
| From Packaging Version | N/A |
| From Protocol Name | ROD-TO-EDI_DICT |
| From Protocol Version | ALL |
| From Process Code | DTROD-TO-EDI_ROD |
| From Process Version | ALL |
| METADICTIONARY | ROD-TO-EDI_DICT |
| METADOCUMENT | DTROD-TO-EDI_ROD |
| METASYNTAX | rod |
| ENCODING | ascii |
| BCG_BATCHDOCS | ON |

9. Klicken Sie auf **Festlegen**.

10. Klicken Sie auf **Speichern**.

Der interne Partner sendet das ROD-Dokument an dieses Ziel.

## Interaktionen erstellen

Sie erstellen zwei Interaktionen: eine für den EDI-Umschlag, der vom Hub gesendet wird, und eine für die Transformation des ROD-Dokuments in EDI.

Erstellen Sie eine Interaktion, die über eine Quelle verfügt, die das ROD-Dokument darstellt, und ein Ziel, das das X12-Dokument darstellt.

1. Klicken Sie auf **Hubadmin > Hubkonfiguration > Dokumentdefinition > Interaktionen verwalten**.
2. Klicken Sie in der Anzeige **Interaktionen verwalten** auf den Link **Interaktion erstellen**.
3. Erweitern Sie den Eintrag **Paket: None** und **Protokoll: ROD-TO-EDI_DICT** und wählen Sie **DTROD-TO-EDI_ROD** aus.
4. Erweitern Sie die Einträge **Paket: N/A** und **Protokoll: X12V5R1** und wählen Sie **Dokumenttyp: 850** aus.
5. Wählen Sie in der Liste **Transformationszuordnung** den Eintrag **S_DT_ROD-_TO_EDI** aus.
6. Wählen Sie in der Liste **Aktion** die Option **ROD konvertieren und EDI validieren** aus.
7. Klicken Sie auf **Speichern**.

Diese Interaktion stellt die Transformation eines ROD-Dokuments in eine X12-Standardtransaktion dar; daher müssen Sie eine Transformationszuordnung auswählen.

Erstellen Sie eine Interaktion, die den EDI-Umschlag darstellt.

1. Klicken Sie auf **Hubadmin > Hubkonfiguration > Dokumentdefinition > Interaktionen verwalten**.
2. Klicken Sie in der Anzeige **Interaktionen verwalten** auf den Link **Interaktion erstellen**.
3. Erweitern Sie die Einträge **Paket: N/A** und **Protokoll: EDI-X12** und wählen Sie **Dokumenttyp: ISA** aus.
4. Erweitern Sie die Einträge **Paket: None** und **Protokoll: EDI-X12** und wählen Sie **Dokumenttyp: ISA** aus.
5. Wählen Sie in der Liste **Aktion** die Option **Pass-Through** aus.

   **Anmerkung:** In dieser Interaktion findet keine Transformation statt. In dieser Interaktion wird der EDI-Austausch mit einem Umschlag versehen.
6. Klicken Sie auf **Speichern**.

## Partner erstellen

Sie haben für dieses Beispiel zwei Partner: den internen Partner (Manager) und einen externen Partner (TP1).

Erstellen Sie das Profil **Interner Partner**:

1. Klicken Sie auf **Kontenadmin > Profile > Partner** und klicken Sie auf **Erstellen**.
2. Geben Sie als Anmeldenamen des Unternehmens **ComManager** ein.

3. Geben Sie als Anzeigenamen des Partners **Manager** ein.
4. Wählen Sie als Partnertyp **Interner Partner** aus.
5. Klicken Sie auf **Neu** für die Geschäfts-ID und geben Sie `000000000` als unformatierte ID ein.

   **Anmerkung:** Stellen Sie sicher, dass Sie **Unformatiert** und nicht **DUNS** ausgewählt haben.
6. Klicken Sie erneut auf **Neu** für die Geschäfts-ID und geben Sie `01-000000000` als unformatierte ID ein.
7. Klicken Sie auf **Speichern**.

Erstellen Sie den zweiten Partner:

1. Klicken Sie auf **Kontenadmin > Profile > Partner** und klicken Sie auf **Erstellen**.
2. Geben Sie als Anmeldenamen des Unternehmens **TP1** ein.
3. Geben Sie als Anzeigenamen des Partners **TP1** ein.
4. Wählen Sie als Partnertyp **Externer Partner** aus.
5. Klicken Sie auf **Neu** für die Geschäfts-ID und geben Sie `000000001` als unformatierte ID ein.

   **Anmerkung:** Stellen Sie sicher, dass Sie **Unformatiert** und nicht **DUNS** ausgewählt haben.
6. Klicken Sie erneut auf **Neu** für die Geschäfts-ID und geben Sie `01-000000001` als unformatierte ID ein.
7. Klicken Sie auf **Speichern**.

## Ziele erstellen

Erstellen Sie in diesem Beispiel Dateiverzeichnisziele für beide Partner. Erstellen Sie zuerst ein Ziel für den Manager.

1. Klicken Sie auf **Kontenadmin > Profile > Partner** und klicken Sie auf **Suchen**.
2. Klicken Sie auf das Symbol **Details anzeigen** neben dem Profil **Manager**.
3. Klicken Sie auf **Ziele** und dann auf **Erstellen**.
4. Geben Sie die folgenden Werte für das Ziel ein. Denken Sie daran, dass das Dateiverzeichnis (der vollständige Pfad) schon auf Ihrem Dateisystem vorhanden sein muss.
   a. Geben Sie als Namen **ManagerFileDestination** ein.
   b. Wählen Sie in der Liste **Transport** die Option **Dateiverzeichnis** aus.
   c. Geben Sie als Adresse **file://Data/Manager/filedestination** ein.
   d. Klicken Sie auf **Speichern**.
5. Klicken Sie auf **Liste**, um alle Ziele für den internen Partner aufzulisten.
6. Klicken Sie auf **Standardziele anzeigen**.
7. Wählen Sie in der Liste **Produktion** das Ziel aus, das Sie in Schritt 4 erstellt haben.
8. Klicken Sie auf **Speichern**.

Erstellen Sie als Nächstes ein Ziel für den Partner.

1. Klicken Sie auf **Kontenadmin > Profile > Partner** und klicken Sie auf **Suchen**.
2. Wählen Sie den anderen Partner aus, den Sie für dieses Beispiel erstellt haben, indem Sie auf das Symbol **Details anzeigen** neben **TP1** klicken.

3. Klicken Sie auf **Ziele** und dann auf **Erstellen**.
4. Geben Sie die folgenden Werte für das Ziel ein. Denken Sie daran, dass das Dateiverzeichnis (der vollständige Pfad) schon vorhanden sein muss.
   a. Geben Sie als Namen **TP1FileDestination** ein.
   b. Wählen Sie in der Liste **Transport** die Option **Dateiverzeichnis** aus.
   c. Geben Sie als Adresse **file://Data/TP1/filedestination** ein.
   d. Klicken Sie auf **Speichern**.
5. Klicken Sie auf **Liste**, um alle Ziele für den Partner aufzulisten.
6. Klicken Sie auf **Standardziele anzeigen**.
7. Wählen Sie in der Liste **Produktion** das Ziel aus, das Sie in Schritt 4 erstellt haben.
8. Klicken Sie auf **Speichern**.

## B2B-Funktionalität konfigurieren

Aktivieren Sie die B2B-Funktionalität der beiden Partner in diesem Austausch. In diesem Beispiel stammt das ROD-Dokument vom internen Partner und wird dem externen JPartner (TP1) zugestellt.

1. Klicken Sie auf **Kontenadmin > Profile > Partner**, und klicken Sie auf **Suchen**.
2. Klicken Sie auf das Symbol **Details anzeigen** für den Quellenpartner in diesem Beispiel (**Manager**).
3. Klicken Sie auf **B2B-Funktionalität**.
4. Aktivieren Sie zwei Funktionalitätsgruppen für den Quellenpartner.
   a. Aktivieren Sie zuerst die Dokumentdefinition, die das ROD-Dokument darstellt:
      1) Klicken Sie zum Aktivieren auf das Symbol **Rolle ist nicht aktiv** unter **Quelle festlegen** für **Paket: None**.
      2) Erweitern Sie **Paket: None**.
      3) Klicken Sie auf das Symbol **Rolle ist nicht aktiv** unter **Quelle festlegen** für **Protokoll: ROD-TO-EDI_DICT (ALL)**.
      4) Erweitern Sie **Protokoll: ROD-TO-EDI_DICT (ALL)**.
      5) Klicken Sie auf das Symbol **Rolle ist nicht aktiv** unter **Quelle festlegen** für **Dokumenttyp: DTROD-TO-EDI_ROD (ALL)**.
   b. Aktivieren Sie als Nächstes die Dokumentdefinition, die den EDI-Umschlag darstellt:
      1) Klicken Sie zum Aktivieren auf das Symbol **Rolle ist nicht aktiv** unter **Quelle festlegen** für **Paket: N/A**.
      2) Erweitern Sie **Paket: N/A**.
      3) Klicken Sie auf das Symbol **Rolle ist nicht aktiv** unter **Quelle festlegen** für **Protokoll: EDI-X12 (ALL)**.
      4) Erweitern Sie **Protokoll: EDI-X12 (ALL)**.
      5) Klicken Sie auf das Symbol **Rolle ist nicht aktiv** unter **Quelle festlegen** für **Dokumenttyp: ISA (ALL)**.
5. Klicken Sie auf **Kontenadmin > Profile > Partner**, und klicken Sie auf **Suchen**.
6. Klicken Sie auf das Symbol **Details anzeigen** für den Zielpartner in diesem Beispiel (**TP1**).
7. Klicken Sie auf **B2B-Funktionalität**.
8. Aktivieren Sie zwei Funktionalitätsgruppen für den Zielpartner.

a. Aktivieren Sie zuerst die Dokumentdefinition, die die EDI-850-Transaktion darstellt:
   1) Klicken Sie zum Aktivieren auf das Symbol **Rolle ist nicht aktiv** unter **Ziel festlegen** für **Paket: N/A**.
   2) Erweitern Sie **Paket: N/A**.
   3) Klicken Sie auf das Symbol **Rolle ist nicht aktiv** unter **Ziel festlegen** für **Protokoll: X12V5R1 (ALL)**.
   4) Erweitern Sie **Protokoll: X12V5R1 (ALL)**.
   5) Klicken Sie auf das Symbol **Rolle ist nicht aktiv** unter **Ziel festlegen** für **Dokumenttyp: 850 (ALL)**.

b. Aktivieren Sie als Nächstes die Dokumentdefinition, die den Umschlag darstellt:
   1) Klicken Sie zum Aktivieren auf das Symbol **Rolle ist nicht aktiv** unter **Ziel festlegen** für **Paket: None**.
   2) Erweitern Sie **Paket: None**.
   3) Klicken Sie auf das Symbol **Rolle ist nicht aktiv** unter **Ziel festlegen** für **Protokoll: EDI-X12 (ALL)**.
   4) Erweitern Sie **Protokoll: EDI-X12 (ALL)**.
   5) Klicken Sie auf das Symbol **Rolle ist nicht aktiv** unter **Ziel festlegen** für **Dokumenttyp: ISA (ALL)**.

## Umschlagsprofil erstellen

Sie erstellen als Nächstes das Profil für den Umschlag, der die transformierte 850-Transaktion enthalten wird:

1. Klicken Sie auf **Hubadmin > Hubkonfiguration > EDI > Umschlagsprofil**.
2. Klicken Sie auf **Erstellen**.
3. Geben Sie den Namen des Profils ein: **UmschProf1**.
4. Wählen Sie in der Liste **EDI-Standard** die Option **X12** aus.
5. Die Schaltfläche **Allgemein** ist standardmäßig ausgewählt. Geben Sie die folgenden Werte für die allgemeinen Attribute des Umschlags ein:
   - INTCTLLEN: **9**
   - GRPCTLLEN: **9**
   - TRXCTLLEN: **9**
   - MAXDOCS: **1000**
6. Klicken Sie auf die Schaltfläche **Austausch** und geben Sie die folgenden Werte für die Austauschattribute ein:
   - ISA01: **01**
   - ISA02: **ISA0000002**
   - ISA03: **02**
   - ISA04: **ISA0000004**
   - ISA11: \
   - ISA12: **00501**
   - ISA15: **T**
7. Klicken Sie auf **Speichern**.

## Verbindungen aktivieren

Gehen Sie wie folgt vor, um die Verbindungen zu aktivieren:

1. Klicken Sie auf **Kontenadmin > Verbindungen**.
2. Wählen Sie **Manager** in der Liste **Quelle** aus.
3. Wählen Sie **TP1** in der Liste **Ziel** aus.
4. Klicken Sie auf **Suchen**.
5. Klicken Sie auf **Aktivieren** für die Verbindung, die die Verbindung vom ROD-Dokument zur EDI-Transaktion darstellt:

*Tabelle 50. Verbindung für ROD zu EDI*

| Quelle | Ziel |
|---|---|
| Paket: N/A (N/A) Protokoll: ROD-TO-EDI_DICT (ALL) Dokumenttyp: DTROD-TO-EDI_ROD (ALL) | Paket: None (N/A) Protokoll: X12V5R1 (ALL) Dokumenttyp: 850 |

6. Klicken Sie auf **Aktivieren** für die Verbindung, die den Umschlag darstellt:

*Tabelle 51. Verbindung für Umschlag*

| Quelle | Ziel |
|---|---|
| Paket: None (N/A) Protokoll: EDI-X12 (ALL) Dokumenttyp: ISA (ALL) | Paket: N/A (N/A) Protokoll: EDI-X12 (ALL) Dokumenttyp: ISA (ALL) |

## Attribute konfigurieren

Gehen Sie wie folgt vor, um Attribute für das Umschlagsprofil anzugeben:

1. Klicken Sie auf **Kontenadmin > Profile > Partner** und klicken Sie auf **Suchen**.
2. Wählen Sie **TP1** in der Liste aus.
3. Klicken Sie auf **B2B-Funktionalität**.
4. Klicken Sie auf das Symbol **Erweitern** neben **Paket: N/A**.
5. Klicken Sie auf das Symbol **Bearbeiten** neben **Protokoll: X12V5R1**.
6. Geben Sie die folgenden Attribute an:
   a. Wählen Sie in der Zeile **Umschlagsprofil** den Eintrag **UmschProf1** in der Liste aus.
   b. Geben Sie in der Zeile **Qualifikationsmerkmal für Austausch** den Wert **01** ein.
   c. Geben Sie in der Zeile **Kennung für Austausch** den Wert **000000001** ein.
   d. Geben Sie in der Zeile **Nutzungsanzeiger für Austausch** den Buchstaben **T** ein.
7. Klicken Sie auf **Speichern**.

Wenn der interne Partner jetzt ein ROD-Dokument an den Hub sendet, wird das Dokument in eine 850-Transaktion transformiert, welche dann mit einem Umschlag versehen und an das Ziel des Partners gesendet wird.

# Kapitel 21. Zusätzliche RosettaNet-Informationen

Dieser Anhang enthält weitere Informationen zur RosettaNet-Unterstützung. Er behandelt die folgenden Themen:

- „PIPs inaktivieren"
- „ Fehlerbenachrichtigung bereitstellen"
- „PIP-Dokumentdefinitionspakete erstellen" auf Seite 381
- „PIP-Dokumentdefinitionspakete" auf Seite 393

## PIPs inaktivieren

Nachdem ein PIP-Paket in WebSphere Partner Gateway hochgeladen wurde, kann es nicht mehr entfernt werden. Sie können jedoch den PIP inaktivieren, sodass er nicht mehr verwendet werden kann.

Führen Sie die folgenden Schritte aus, um einen PIP für die Kommunikation mit allen Partnern zu inaktivieren:

1. Klicken Sie auf **Hubadmin > Hubkonfiguration > Dokumentdefinition**.
2. Erweitern Sie die Dokumentdefinitionen, um den Dokumenttyp des PIP anzuzeigen, den Sie inaktivieren wollen.
3. Klicken Sie in der Spalte **Status** des Pakets auf **Aktiviert**. Die Spalte **Status** zeigt jetzt **Inaktiviert** an, und WebSphere Partner Gateway kann die Dokumentdefinition für den PIP nicht mehr verwenden.

Um eine PIP-Kommunikation mit einem bestimmten Partner zu inaktivieren, inaktivieren Sie die Verbindung mit dem Partner, die für den PIP definiert wurde.

## Fehlerbenachrichtigung bereitstellen

### 0A1 PIP

Wenn ein Fehler während der Verarbeitung einer PIP-Nachricht auftritt, verwendet WebSphere Partner Gateway den 0A1 PIP als Mechanismus, um den Fehler an den Partner bzw. das Back-End-System zu übertragen, der bzw. das die Nachricht gesendet hat. Angenommen, ein Back-End-System initiiert z. B. einen 3A4 PIP. WebSphere Partner Gateway verarbeitet die RNSC-Nachricht und sendet eine RosettaNet-Nachricht an einen Partner. WebSphere Partner Gateway wartet auf die Antwort auf die RosettaNet-Nachricht, bis die Wartezeit das Zeitlimit erreicht. Nachdem dies geschehen ist, erstellt WebSphere Partner Gateway einen 0A1 PIP und sendet ihn an den Partner. Der 0A1 PIP gibt die Ausnahmebedingung an, sodass der Partner dann den Fehler des 3A4 PIP kompensieren kann.

Zum Bereitstellen der Fehlerbenachrichtigung laden Sie ein 0A1-Paket hoch und erstellen eine PIP-Verbindung zu dem Partner, der dieses Paket verwendet.

### Kontaktinformationen aktualisieren

Zum Ändern der RosettaNet-Kontaktinformationen mit dem 0A1 PIP müssen Sie die Datei BCG.Properties bearbeiten, die sich im Verzeichnis <*Produktverz*>/router/lib/config befindet.

Diese Felder füllen die Kontaktinformationen im 0A1 PIP aus. Ein Wert für Fax ist optional (der Wert kann leer sein), aber die restlichen Werte sind erforderlich.

- **bcg.0A1.fromContactName**
- **bcg.0A1.fromEMailAddr**
- **bcg.0A1.fromPhoneNbr**
- **bcg.0A1.fromFaxNbr**

Die Telefonnummern sind auf eine Länge von 30 Byte begrenzt. Die übrigen Felder sind ohne Längenbegrenzung. Wenn die Werte geändert wurden, muss Document Manager erneut gestartet werden.

## RosettaNet-Attributwerte bearbeiten

Zur RosettaNet-Unterstützung verfügt eine Dokumentdefinition für den Aktionstyp über eine besondere Gruppe von Attributen. Diese Attribute stellen Informationen bereit, mit denen die PIP-Nachricht validiert wird, um die im PIP verwendeten Rollen und Services sowie die Antwort auf die Aktion zu definieren. Die PIP-Pakete, die von WebSphere Partner Gateway bereitgestellt werden, definieren automatisch Werte für diese Attribute und Sie müssen diese normalerweise nicht ändern.

Führen Sie die folgenden Schritte aus, um die RosettaNet-Attribute einer Dokumentdefinition für Aktionen zu bearbeiten:

1. Klicken Sie auf **Hubadmin > Hubkonfiguration > Dokumentdefinition**.
2. Klicken Sie auf die Symbole **Erweitern**, um einen Knoten individuell zur entsprechenden Dokumentdefinitionsebene zu erweitern, oder wählen Sie **Alle** aus, um die gesamte Baumstruktur zu erweitern.
3. Die Spalte **Aktionen** enthält für jede Aktion ein Symbol **RosettaNet-Attributwerte bearbeiten**. Klicken Sie auf dieses Symbol, um die RosettaNet-Attribute der Aktion zu bearbeiten. Community Console zeigt eine Liste der definierten Attribute unter **RosettaNet-Attribute** an.
4. Vervollständigen Sie die folgenden Parameter unter **RosettaNet-Attribute**. (Diese Attribute sind automatisch definiert, wenn ein PIP auf das System hochgeladen wird.)

*Tabelle 52. 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 Partners oder Back-End-Systems, der bzw. das die Nachricht sendet. |
| Empfängerservice | Enthält den Netzkomponentenservicenamen des Partners oder Back-End-Systems, der bzw. das die Nachricht empfängt. |
| Absenderrolle | Enthält den Rollennamen des Partners oder Back-End-Systems, der bzw. das die Nachricht sendet. |
| Empfängerrolle | Enthält den Rollennamen des Partners oder Back-End-Systems, der bzw. das die Nachricht empfängt. |
| Root-Tag | Enthält den Namen des Root-Elements im XML-Dokument, das dem PIP zugeordnet ist. |
| Antwort aus Aktionsname | Gibt die nächste Aktion an, die im PIP ausgeführt werden soll. |

**Anmerkung:** Wenn die Konsole die Nachricht `Keine Attribute gefunden` anzeigt, sind die Attribute nicht definiert worden.

5. Wenn die Konsole diese Nachricht für eine Definition der unteren Ebene anzeigt, kann die Definition dennoch funktionieren, da sie die Attribute von der Definition der höheren Ebene übernimmt. Das Hinzufügen von Attributen und ihren Werten überschreibt die übernommenen Attribute und ändert die Funktion der Dokumentdefinition.
6. Klicken Sie auf **Speichern**.

## PIP-Dokumentdefinitionspakete erstellen

Da RosettaNet von Zeit zu Zeit PIPs hinzufügt, müssen Sie möglicherweise Ihre eigenen PIP-Pakete erstellen, um diese neuen PIPs zu unterstützen oder um Upgrades für PIPs zu unterstützen. Die Prozeduren in diesem Abschnitt beschreiben, mit Ausnahme der angegeben Stellen, wie das PIP-Dokumentdefinitionspaket für PIP 5C4 V01.03.00 erstellt wird. WebSphere Partner Gateway stellt ein PIP-Dokumentdefinitionspaket für PIP 5C4 V01.02.00 bereit. Die Prozeduren dokumentieren daher tatsächlich, wie ein Upgrade ausgeführt wird. Das Erstellen eines PIP-Dokumentdefinitionspakets ist allerdings ähnlich, 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-Dokumentdefinitionspakets umfasst die folgenden Prozeduren:

- XSD-Dateien erstellen
- XML-Datei erstellen
- Pakete erstellen

## XSD-Dateien erstellen

Ein PIP-Dokumentdefinitionspaket 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 391.

Führen Sie die folgenden Schritte aus, um die XSD-Dateien für das PIP-Dokumentdefinitionspaket zu erstellen:

1. Importieren oder laden Sie die DTD-Datei in einen XML-Editor, wie z. B. WebSphere Studio Application Developer. Laden Sie z. B. die Datei '5C4_MS_V01_03_RegistrationStatusNotification.dtd'.
2. Konvertieren Sie mit dem XML-Editor die DTD-Datei in ein XML-Schema. Die folgenden Schritte beschreiben, wie Sie dies mit Application Developer ausführen:
   a. Öffnen Sie in der Anzeige **Navigation** der Perspektive **XML** das Projekt mit der importierten DTD-Datei.
   b. Klicken Sie mit der rechten Maustaste auf die DTD-Datei und wählen Sie **Generieren > XML-Schema** aus.
   c. Geben Sie in der Anzeige **Generieren** die Position ein, bzw. wählen Sie diese dort aus, wo Sie die neue XSD-Datei speichern wollen. Geben Sie in das Feld **Dateiname** den Namen der neuen XSD-Datei ein. Im vorliegenden Beispiel würden Sie einen Namen, wie z. B. 'BCG_5C4RegistrationStatusNotification_V01.03.xsd', eingeben.
   d. Klicken Sie auf **Fertigstellen**.
3. Kompensieren Sie die Elemente, die über mehrere Kardinalitätswerte in den RosettaNet-XML-Richtlinien verfügen, indem Sie der neuen XSD-Datei Spezifikationen hinzufügen. Die Richtlinien stellen die Elemente in der Nachricht mit einer Baumstruktur dar und zeigen die Kardinalität jedes Elements links neben dem Element an.

   Im Allgemeinen stimmen die Elemente in den Richtlinien mit den Definitionen der Elemente in der DTD-Datei überein. Die Richtlinien könnten jedoch einige Elemente enthalten, die denselben Namen aber unterschiedliche Kardinalitäten haben. Da die DTD-Datei in diesem Fall nicht die Kardinalität zur Verfügung stellen kann, müssen Sie die XSD-Datei modifizieren. Die Richtliniendatei '5C4_MG_V01_03_00_RegistrationStatusNotification.htm' hat z. B. eine Definition für **ContactInformation** in Zeile 15, die über fünf untergeordnete Elemente mit den folgenden Kardinalitäten verfügt:

   1 contactName

   0..1 EmailAddress

   0..1 facsimileNumber

   0..1 PhysicalLocation

   0..1 telephoneNumber

   Die Definition für **ContactInformation** in Zeile 150 verfügt über vier untergeordnete Elemente mit den folgenden Kardinalitäten:

   1 contactName

   1 EmailAddress

   0..1 facsimileNumber

   1 telephoneNumber

   In der XSD-Datei verfügt aber jedes untergeordnete Element von **ContactInformation** über eine Kardinalität, die beiden Definitionen entspricht:

```
<xsd:element name="ContactInformation">
    <xsd:complexType>
      <xsd:sequence>
          <xsd:element ref="contactName"/>
          <xsd:element maxOccurs="1" minOccurs="0" ref="EmailAddress"/>
            <xsd:element maxOccurs="1" minOccurs="0" ref="facsimileNumber"/>
            <xsd:element maxOccurs="1" minOccurs="0" ref="PhysicalLocation"/>
            <xsd:element maxOccurs="1" minOccurs="0" ref="telephoneNumber"/>
      </xsd:sequence>
  </xsd:complexType>
</xsd:element>
```

Wenn Sie das PIP-Dokumentdefinitionspaket auf einer anderen Version des Pakets basierend aktualisieren und Sie eine Definition von der anderen Version wiederverwenden wollen, führen Sie die folgenden Schritte für jede dieser Definitionen aus:

a. Löschen Sie die Definition des Elements. Löschen Sie z. B. das Element **ContactInformation**.

b. Öffnen Sie das PIP-Dokumentdefinitionspaket der Version, die ersetzt wird. Öffnen Sie z. B. die Datei 'BCG_Package_RNIFV02.00_5C4V01.02.zip'.

c. Suchen Sie die Definition, die Sie wiederverwenden wollen. Die Definition von **ContactInformation_type7** in der Datei 'BCG_ContactInformation_Types.xsd' stimmt z. B. mit der Definition überein, die Sie für Zeile 15 der Richtlinien benötigen.

```
<xsd:complexType name="ContactInformation_type7">
    <xsd:sequence>
        <xsd:element name="contactName" type="common_FreeFormText_R"/>
        <xsd:element name="EmailAddress" type="common_EmailAddres_R"
                minOccurs="0"/>
        <xsd:element name="facsimileNumber"
                type="common_CommunicationsNumber_R" minOccurs="0"/>
        <xsd:element name="PhysicalLocation"
                type="PhysicalLocation_type1" minOccurs="0" />
        <xsd:element name="telephoneNumber"
                type="common_CommunicationsNumber_R minOccurs="0" />
    </xsd:sequence>
</xsd:complexType>
```

d. Erstellen Sie in der neuen XSD-Datei, die Sie für das aktualisierte PIP-Dokumentdefinitionspaket erstellen, einen Verweis auf die XSD-Datei, die die wiederzuverwendende Definition enthält. Erstellen Sie z. B. einen Verweis auf 'BCG_ContactInformation_Types.xsd' in der Datei 'BCG_5C4RegistrationStatusNotification_V01.03.xsd' wie folgt:

```
<xsd:include schemaLocation="BCG_ContactInformation_Types.xsd"/>
```

e. Löschen Sie in der neuen XSD-Datei das Attribut **ref** jedes Elements, das auf das gelöschte Element verweist. Fügen Sie ein Attribut **type** hinzu, das auf die wiederzuverwendende Definition verweist. Löschen Sie z. B. im Element **productProviderFieldApplicationEngineer** den Verweis *ref="Contact Information"* und fügen Sie die folgenden Informationen hinzu:

```
name="ContactInformation"
 type="ContactInformation_type7"
```

Wenn Sie ein PIP-Dokumentdefinitionspaket erstellen oder ein PIP-Dokumentdefinitionspaket upgraden, aber die benötigte Definition nicht in der anderen Version vorhanden ist, führen Sie die folgenden Schritte für jede Instanz des Elements aus, das Sie in den Richtlinien gefunden haben:

a. Löschen Sie die Definition des Elements. Löschen Sie z. B. das Element **ContactInformation**.

b. Erstellen Sie die Ersetzungsdefinition. Erstellen Sie z. B. die Definition **ContactInformation_localType1** so, dass diese mit der Definition in Zeile 15 der Richtlinien übereinstimmt.

```
<xsd:complexType name="ContactInformation_localType1">
    <xsd:sequence>
        <xsd:element ref="contactName"/>
        <xsd:element maxOccurs="1" minOccurs="0" ref="EmailAddress"/>
          <xsd:element maxOccurs="1" minOccurs="0"
                ref="facsimileNumber"/>
          <xsd:element maxOccurs="1" minOccurs="0"
                ref="PhysicalLocation"/>
          <xsd:element maxOccurs="1" minOccurs="0"
                ref="telephoneNumber"/>
    </xsd:sequence>
</xsd:complexType>
```

c. Löschen Sie für jedes Element, das auf das gelöschte Element verweist, sein Attribut **ref** und fügen Sie ein Attribut **type** hinzu, das auf den entsprechenden komplexen Typ verweist, welchen Sie im vorherigen Schritt definiert haben. Löschen Sie z. B. im Element **productProviderFieldApplicationEngineer** den Verweis *ref="Contact Information"* und fügen Sie die folgenden Informationen hinzu:

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

Abb. 35 zeigt das Element **productProviderFieldApplicationEngineer**, bevor es geändert wird.

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

*Abbildung 35. Element* **productProviderFieldApplicationEngineer** *vor der Änderung*

Abb. 36 zeigt das Element **productProviderFieldApplicationEngineer**, nachdem es geändert wurde.

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

*Abbildung 36. Element* **productProviderFieldApplicationEngineer** *nach der Änderung*

4. Geben Sie die Aufzählungswerte für Elemente an, die nur über spezifische Werte verfügen können. Die Richtlinien definieren die Aufzählungswerte in den Tabellen des Abschnitts **Guideline Information** (Richtlinieninformationen).

   In einer PIP 5C4 V01.03.00-Nachricht kann z. B. **GlobalRegistrationComplexityLevelCode** nur über die folgenden Werte verfügen: **Above average (Über dem Durchschnitt), Average (Durchschnitt), Maximum (Maximum), Minimum (Minimum), None (Kein) und Some (Einiges)**.

Wenn Sie das PIP-Dokumentdefinitionspaket basierend auf einer anderen Version des Pakets aktualisieren und eine Gruppe von Aufzählungswerten von der anderen Version wiederverwenden wollen, führen Sie die folgenden Schritte für jede dieser Gruppen aus:

a. Löschen Sie die Definition für das Element. Löschen Sie z. B. das Element **GlobalRegistrationComplexityLevelCode**:

b. Öffnen Sie das PIP-Dokumentdefinitionspaket der Version, die ersetzt wird. Öffnen Sie z. B. die Datei 'BCG_Package_RNIFV02.00_5C4V01.02.zip'.

c. Suchen Sie die Definition mit den Aufzählungswerten, die Sie wiederverwenden wollen. Die Definition **_GlobalRegistrationComplexityLevelCode** in der Datei 'BCG_GlobalRegistrationComplexityLevelCode.xsd' enthält die Aufzählungswertdefinitionen, die durch die Tabelle **Entity Instances** (Entitätsinstanzen) definiert werden.

```
<xsd:simpleType name="_GlobalRegistrationComplexityLevelCode">
    <xsd:restriction base="xsd:string">
        <xsd:enumeration value="Above average"/>
        <xsd:enumeration value="Average"/>
        <xsd:enumeration value="Maximum"/>
        <xsd:enumeration value="Minimum"/>
        <xsd:enumeration value="None"/>
        <xsd:enumeration value="Some"/>
      </xsd:restriction>
</xsd:simpleType>
```

d. Erstellen Sie in der neuen XSD-Datei, die Sie für das aktualisierte PIP-Dokumentdefinitionspaket erstellen, einen Verweis auf die XSD-Datei, die die wiederzuverwendende Definition enthält. Erstellen Sie z. B. einen Verweis auf 'BCG_GlobalRegistrationComplexityLevelCode.xsd' in der Datei 'BCG_5C4RegistrationStatusNotification_V01.03.xsd' wie folgt:

```
<xsd:include schemaLocation=
    "BCG_GlobalRegistrationComplexityLevelCode_Types.xsd" />
```

e. Löschen Sie in der neuen XSD-Datei das Attribut **ref** jedes Elements, das auf das gelöschte Element verweist. Fügen Sie ein Attribut **type** hinzu, das auf die wiederzuverwendende Definition verweist. Löschen Sie z. B. im Element **DesignAssemblyInformation** den Verweis *ref*=”GlobalRegistrationComplexityLevelCode” und fügen Sie die folgenden Informationen hinzu:

```
         name="GlobalRegistrationComplexityLevelCode"
type="_GlobalRegistrationComplexityLevelCode"
```

Wenn Sie ein PIP-Dokumentdefinitionspaket erstellen oder ein PIP-Dokumentdefinitionspaket upgraden, die benötigten Aufzählungswertdefinitionen aber nicht in der anderen Version vorhanden sind, führen Sie die folgenden Schritte für jedes Element mit Aufzählungswerten in den Richtlinien aus:

a. Löschen Sie die Definition des Elements. Löschen Sie z. B. das Element **GlobalRegistrationComplexityLevelCode**.

b. Erstellen Sie die Ersetzungsdefinition. Erstellen Sie z. B. die Definition **GlobalRegistrationComplexityLevelCode_localType** und schließen Sie die Aufzählungswertdefinitionen, wie von der Tabelle beschrieben, mit ein.

```
<xsd:simpleType
        name="GlobalRegistrationComplexityLevelCode_localType">
    <xsd:restriction base="xsd:string">
        <xsd:enumeration value="Above average"/>
        <xsd:enumeration value="Average"/>
        <xsd:enumeration value="Maximum"/>
        <xsd:enumeration value="Minimum"/>
```

```
            <xsd:enumeration value="None"/>
            <xsd:enumeration value="Some"/>
          </xsd:restriction>
      </xsd:simpleType>
```

c. Löschen Sie für jedes Element, das auf das gelöschte Element verweist, sein Attribut **ref** und fügen Sie ein Attribut **type** hinzu, das auf den entsprechenden komplexen Typ verweist, welchen Sie im vorherigen Schritt definiert haben. Löschen Sie z. B. *ref="GlobalRegistrationComplexityLevelCode"* und fügen Sie die folgenden Informationen hinzu:

```
         name="GlobalRegistrationComplexityLevelCode"
type="GlobalRegistrationComplexityLevelCode_localType"
```

Abb. 37 zeigt das Element **DesignAssemblyInformation**, bevor es geändert wird.

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

*Abbildung 37. Element* **DesignAssemblyInformation** *vor der Änderung*

Abb. 38 auf Seite 387 zeigt das Element **DesignAssemblyInformation**, nachdem es geändert wurde.

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

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

*Abbildung 38. Element* **DesignAssemblyInformation** *nach der Änderung*

5. Legen Sie **Data Type** (Datentyp), **Min** (minimale Länge) und **Max** (maximale Länge) und **Representation** (Darstellung) von **Data Entities** (Datenentitäten) fest. Die RosettaNet-XML-Nachrichtenrichtlinien stellen diese Informationen in der Tabelle **Fundamental Business Data Entities** (Grundlegende Geschäftsdatenentitäten) bereit.

   Wenn Sie das PIP-Dokumentdefinitionspaket basierend auf einer anderen Version des Pakets aktualisieren und eine Datenentitätsdefinition von der anderen Version wiederverwenden wollen, führen Sie die folgenden Schritte für jede Gruppe aus:

   a. Löschen Sie die Definition für das Datenentitätselement. Löschen Sie z. B. das Element **DateStamp**.
   b. Öffnen Sie das PIP-Dokumentdefinitionspaket 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-Dokumentdefinitionspaket erstellen, einen Verweis auf die XSD-Datei, die die wiederzuverwendende Definition enthält. Erstellen Sie z. B. einen Verweis auf 'BCG_common.xsd' in der Datei 'BCG_5C4RegistrationStatusNotification_V01.03.xsd' wie folgt:

      ```
      <xsd:include schemaLocation="BCG_common.xsd" />
      ```

   e. Löschen Sie in der neuen XSD-Datei das Attribut **ref** jedes Elements, das auf das gelöschte Element verweist. Fügen Sie ein Attribut **type** hinzu, das auf die wiederzuverwendende Definition verweist. Löschen Sie z. B. im Element **DesignAssemblyInformation** den Verweis *ref*=”DateStamp” und fügen Sie die folgenden Informationen hinzu:

```
name="DateStamp" type="_common_DateStamp_R"
```

Wenn Sie ein PIP-Dokumentdefinitionspaket erstellen oder ein PIP-Dokumentdefinitionspaket upgraden, die benötigte Datenentitätsdefinition aber nicht in der anderen Version vorhanden ist, führen Sie die folgenden Schritte für jedes Datenentitätselement aus:

a. Löschen Sie die Definition des Elements. Löschen Sie z. B. das Element **DateStamp**.

b. Erstellen Sie die Ersetzungsdefinition. Verwenden Sie z. B. die Informationen zum Datentyp, zur minimalen Länge und zur maximalen Länge sowie zur Darstellung, um die Definition **DateStamp_localType** zu erstellen.

```
<xsd:simpleType name="DateStamp_localType">
    <xsd:restriction base="xsd:string">
        <xsd:pattern value="[0-9]{8}Z" />
      </xsd:restriction>
</xsd:simpleType>
```

c. Löschen Sie für jedes Element, das auf das gelöschte Element verweist, sein Attribut **ref** und fügen Sie ein Attribut **type** hinzu, das auf den entsprechenden komplexen Typ verweist, welchen Sie im vorherigen Schritt definiert haben. Löschen Sie z. B. *ref="DateStamp"* und fügen Sie die folgenden Informationen hinzu:

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

Abb. 39 zeigt das Element **beginDate**, bevor es geändert wird.

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

*Abbildung 39. Element* **beginDate** *vor der Änderung*

Abb. 40 zeigt das Element **beginDate**, nachdem es geändert wurde.

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

*Abbildung 40. Element* **beginDate** *nach der Änderung*

## XML-Datei erstellen

Nachdem Sie die XSD-Dateien für Ihr PIP-Dokumentdefinitionspaket erstellt haben, können Sie nun die XML-Datei für das Paket **RNIF** und die XML-Datei für das Paket **Backend Integration** erstellen. Diese Pakete heißen z. B. 'BCG_Package_RNIFV02.00_5C4V01.03.zip' und 'BCG_Package_RNSC1.0_RNIFV02.00_5C4V01.03.zip'. Die folgende Prozedur beschreibt, wie Sie die XML-Datei für das RNIF-Paket erstellen:

1. Extrahieren Sie die XML-Datei aus einer RNIF-PIP-Dokumentdefinitionspaketdatei. Wenn Sie ein Upgrade durchführen, extrahieren Sie die Datei von der vorherigen Version des Pakets (z. B. 'BCG_Package_RNIFV02.00_5C4V01.02.zip'). Wenn Sie ein neues Paket erstellen, extrahieren Sie die Datei aus einem PIP-Dokumentdefinitionspaket, das dem zu

erstellenden Paket gleicht. Wenn Sie z. B. ein Paket erstellen, um einen Doppelaktions-PIP zu unterstützen, kopieren Sie die XML-Datei von einem anderen Doppelaktions-PIP-Paket.

2. Kopieren Sie die Datei und benennen Sie diese entsprechend um (z. B. 'BCG_RNIFV02.00_5C4V01.03.xml').
3. Aktualisieren Sie in der neuen Datei die Elemente, die Informationen zum PIP enthalten. Die folgende Tabelle listet z. B. die Informationen auf, die Sie im 5C4 PIP-Beispiel aktualisieren müssen. Beachten Sie, dass die Informationen mehr als einmal in der Datei vorkommen könnten. Stellen Sie sicher, dass Sie alle Instanzen aktualisieren.

*Tabelle 53. 5C4 PIP-Aktualisierungsinformationen*

| **Zu ändernde Informationen** | **Alter Wert** | **Neuer Wert** |
|---|---|---|
| PIP-ID | 5C4 | 5C4 |
| PIP-Version | V01.02 | V01.03 |
| Der Name der Anforderungsnachrichten-DTD-Datei ohne Dateierweiterung | 5C4_MS_V01_02_ RegistrationStatusNotification | 5C4_MS_V01_03_ RegistrationStatusNotification |
| Der Name der Bestätigungsnachrichten-DTD-Datei ohne Dateierweiterung (nur für Doppelaktions-PIPs) | N/A | N/A |
| Der Name der Anforderungsnachrichten-XSD-Datei ohne Dateierweiterung | BCG_5C4RegistrationStatus Notification_V01.02 | BCG_5C4RegistrationStatus Notification_V01.03 |
| Der Name der Bestätigungsnachrichten-ohne Dateierweiterung (nur für Doppelaktions-PIPs) | N/A XSD-Datei | N/A |
| Root-Elementname in der XSD-Datei für die Anforderungsnachricht | Pip5C4RegistrationStatus Notification | Pip5C4RegistrationStatus Notification |
| Root-Elementname 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 54. 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 |

*Tabelle 54. 5C4 PIP-Aktualisierungsinformationen von der PIP-Spezifikation (Forts.)*

| Zu aktualisierende Informationen | Beschreibung | Wert im 5C4-Paket |
|---|---|---|
| Responderrollenname | Angegeben in Tabelle 3-1 | Demand Creator |
| Anforderungs-aktionsname | Angegeben in Tabelle 4-2 | Registration Status Notification |
| Bestätigungsaktions-name | Angegeben in Tabelle 4-2 (nur für Doppelaktions-PIPs) | N/A |

5. Aktualisieren Sie die Paketattributwerte. Wenn Sie eine Aktualisierung durchführen, vergleichen Sie die Spezifikationen für die Versionen, da Sie diese Werte unter Umständen nicht aktualisieren müssen.

   **Anmerkung:** Wenn Sie das Paket **Backend Integration** erstellen, überspringen Sie diesen Schritt und fahren Sie mit Schritt 6 fort.

*Tabelle 55. 5C4 PIP-Attributaktualisierungen*

| Zu aktualisierende Informationen | Beschrei-bung | Wert im 5C4-Paket | Elementpfad in der XML-Datei |
|---|---|---|---|
| NonRepudiation Required | Angegeben in Tabelle 3-3 | N | ns1:Package ns1:Protocol ns1:Process ns1:Attribute (sein ATTRIBUTEKEY ist NonRepudiationRequired) ns1:AttributeValue AttributePickListItem ATTRVALUEKEY |
| NonRepudiationOf Receipt | Angegeben in Tabelle 3-3 | N | ns1:Package ns1:Protocol ns1:Process ns1:Attribute (sein ATTRIBUTEKEY ist NonRepudiationOfReceipt) ns1:AttributeValue AttributePickListItem ATTRVALUEKEY |
| DigitalSignature Required | Angegeben in Tabelle 5-1 | Y | ns1:Package ns1:Protocol ns1:Process ns1:Attribute (sein ATTRIBUTEKEY ist DigitalSignatureRequired) ns1:AttributeValue AttributePickListItem ATTRVALUEKEY |
| TimeToAcknowledge | Angegeben in Tabelle 3-3 | 2 (120 min) | ns1:Package ns1:Protocol ns1:Process ns1:Attribute (sein ATTRIBUTEKEY ist TimeToAcknowledge) ns1:AttributeValue ATTRVALUE |
| TimeToPerform | Angegeben in Tabelle 3-3 | 2 (120 min) | ns1:Package ns1:Protocol ns1:Process ns1:Attribute (sein ATTRIBUTEKEY ist TimeToPerform) ns1:AttributeValue ATTRVALUE |
| RetryCount | Angegeben in Tabelle 3-3 | 3 | ns1:Package ns1:Protocol ns1:Process ns1:Attribute (sein ATTRIBUTEKEY ist RetryCount) ns1:AttributeValue ATTRVALUE |

6. Aktualisieren Sie die Elemente **ns1:Package/ns1:Protocol/GuidelineMap**, um nicht mehr verwendete XSD-Dateien zu entfernen und um jede XSD-Datei hinzuzufügen, die Sie erstellt oder auf die Sie verwiesen haben.

Zur Erstellung des Pakets **Backend Integration** wiederholen Sie Schritt 1 auf Seite 388 bis 6 auf Seite 390, mit Ausnahme der folgenden Unterschiede:

- Extrahieren Sie in Schritt 1 auf Seite 388 die XML-Datei aus dem Paket **Backend Integration** (z. B. BCG_Package_RNSC1.0_RNIFV02.00_5C4V01.02.zip).
- Führen Sie Schritt 5 auf Seite 390 nicht aus.

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

### Paket erstellen

Führen Sie die folgenden Schritte aus, um das RNIF-Paket zu erstellen:

1. Erstellen Sie ein Verzeichnis 'GuidelineMaps' und kopieren Sie die XSD-Dateien des Pakets in dieses Verzeichnis.
2. Erstellen Sie ein Verzeichnis Packages und kopieren Sie die RNIF-XML-Datei in dieses Verzeichnis.
3. Gehen Sie in das übergeordnete Verzeichnis und erstellen Sie ein PIP-Dokumentdefinitionspaket (ZIP-Datei), das die Verzeichnisse 'GuidelineMaps' und 'Packages' enthält. Sie müssen die Verzeichnisstruktur in der ZIP-Datei beibehalten.

Zur Erstellung des Pakets **Backend Integration** führen Sie die Schritte 1 bis 3 aus, aber verwenden Sie die Backend Integration-XML-Datei anstelle der RNIF-Datei.

Nachdem Sie das PIP-Paket erstellt haben, können Sie es mit der in „RNIF- und PIP-Dokumenttyppakete" auf Seite 114 beschriebenen Prozedur hochladen.

## Informationen zur Validierung

WebSphere Partner Gateway validiert den Service-Content einer RosettaNet-Nachricht mithilfe von Validierungszuordnungen. Diese Validierungszuordnungen definieren die Struktur einer gültigen Nachricht und definieren die Kardinalität, das Format und die gültigen Werte (Aufzählung) der Elemente in der Nachricht. In jedem PIP-Dokumentdefinitionspaket stellt WebSphere Partner Gateway die Validierungszuordnungen als XSD-Dateien im Verzeichnis 'GuidelineMaps' bereit.

Da RosettaNet das Format einer PIP-Nachricht angibt, müssen Sie in der Regel die Validierungszuordnungen nicht anpassen. Wenn Sie dies jedoch tun, finden Sie in „PIP-Dokumentdefinitionspakete erstellen" auf Seite 381 Informationen zu den Schritten, die zum Upgraden der XSD-Dateien nötig sind, mit denen die Nachrichten validiert werden, und dazu, wie Sie ein angepasstes PIP-Dokumentdefinitionspaket erstellen.

### Kardinalität

Die Kardinalität bestimmt, wie häufig ein bestimmtes Element in einer Nachricht angezeigt werden kann oder muss. In den Validierungszuordnungen bestimmen die Attribute **minOccurs** und **maxOccurs** die Kardinalität des Attributs, wie im folgenden Beispiel aus der Datei 'BCG_5C4RegistrationStatusNotification_V01.02.xsd' gezeigt wird:

```
<xsd:element name="GeographicRegion" type="GeographicRegionType"
    minOccurs="0"/>
```

Wenn WebSphere Partner Gateway nicht die Kardinalität eines Elements überprüfen muss, sind die Werte für die Attribute **minOccurs** und **maxOccurs** des Elements in den Validierungszuordnungen mit "0" und "unbounded" angegeben, wie im Beispiel dargestellt:

```
<xsd:element name="DesignRegistrationIdentification"
        type="DesignRegistrationIdentificationType2"
    minOccurs="0" maxOccurs="unbounded"/>
```

## Format

Das Format bestimmt die Anordnung bzw. das Layout der Daten für den Typ eines Elements. In den Validierungszuordnungen verfügt der Typ über mindestens eine Einschränkung, wie in den folgenden Beispielen dargestellt:

### Beispiel 1

```
<xsd:simpleType name="_common_LineNumber_R">
    <xsd:restriction base="xsd:string">
        <xsd:minLength value="1" />
        <xsd:maxLength value="6" />
      </xsd:restriction>
</xsd:simpleType>
```

Alle Elemente des Typs **_common_LineNumber_R** in einer Nachricht müssen Zeichenfolgen (string) sein und 1 bis 6 Zeichen lang sein.

### Beispiel 2

```
<xsd:simpleType name="_GlobalLocationIdentifier">
    <xsd:restriction base="xsd:string">
        <xsd:pattern value="[0-9]{9}.{1,4}" />
      </xsd:restriction>
</xsd:simpleType>
```

Alle Elemente des Typs **_GlobalLocationIdentifier** in einer Nachricht müssen Zeichenfolgen (string) sein und über neun numerische Datenzeichen gefolgt von einem bis vier alphanumerischen Datenzeichen verfügen. Die minimale Länge beträgt daher 10 Zeichen und die maximale Länge sind 13 Zeichen.

### Beispiel 3

```
<xsd:element name="DayOfMonth">
    <xsd:simpleType>
        <xsd:restriction base="xsd:positiveInteger">
            <xsd:totalDigits value="2" />
            <xsd:minInclusive value="1" />
            <xsd:maxInclusive value="31" />
        </xsd:restriction>
    </xsd:simpleType>
</xsd:element>
```

Alle Elemente des Typs **_DayofMonth** in einer Nachricht müssen positive ganze Zahlen (positiveInteger) sein und über ein oder zwei Zeichen verfügen und einen Wert von 1 bis inklusive 31 haben.

## Aufzählung

Die Aufzählung bestimmt die gültigen Werte für ein Element. In den Validierungszuordnungen verfügt der Typ des Elements über mindestens eine Aufzählungseinschränkung, wie in dem folgenden Beispiel dargestellt:

```
<xsd:simpleType name="_local_GlobalDesignRegistrationNotificationCode">
    <xsd:restriction base="xsd:string">
        <xsd:enumeration value="Initial" />
        <xsd:enumeration value="Update" />
      </xsd:restriction>
</xsd:simpleType>
```

Alle Elemente des Typs **_local_GlobalDesignRegistrationNotificationCode** in einer Nachricht dürfen nur "Initial" oder "Update" als Werte haben.

# PIP-Dokumentdefinitionspakete

Die folgenden Abschnitte zeigen die PIP-Dokumentdefinitionspakete, die von WebSphere Partner Gateway für jeden PIP bereitgestellt werden. In jedem Paket ist eine XML-Datei in einem Verzeichnis 'Packages' enthalten, und es sind mehrere XSD-Dateien in einem Verzeichnis 'GuidelineMaps' enthalten, die alle PIP-Dokumentdefinitionspakete für den PIP gemeinsam haben.

## 0A1 Notification of Failure V1.0

Der folgende Abschnitt beschreibt den Inhalt für den PIP **0A1 Notification of Failure V1.0**.

### Inhalt der Paketdatei

Die folgende Tabelle zeigt die ZIP-Dateien und entsprechenden XML-Dateien für den PIP **0A1 Notification of Failure V1.0**. Die Richtlinienzuordnungen, die für alle Versionen gleich sind, werden im nachfolgenden Abschnitt gezeigt.

*Tabelle 56. ZIP- und XML-Dateien für PIP '0A1 Notification of Failure V1.0'*

| ZIP-Dateiname | XML-Dateiname |
|---|---|
| BCG_Package_RNIF1.1_0A11.0.zip | BCG_RNIF1.1_0A11.0.xml |
| BCG_Package_RNSC1.0_RNIF1.1_0A11.0.zip | BCG_RNSC1.0_RNIF1.1_0A11.0.xml |

### Inhalt der Richtlinienzuordnungen

Dieser Abschnitt listet den Inhalt der Richtlinienzuordnungen für **0A1 Notification of Failure V1.0** auf:

- 0A1FailureNotification_1.0.xml
- BCG_0A1FailureNotification_1.0.xsd
- BCG_common.xsd
- BCG_GlobalPartnerClassificationCode.xsd
- BCG_GlobalPartnerRoleClassificationCode.xsd
- BCG_string_len_0.xsd
- BCG_xml.xsd

## 0A1 Notification of Failure V02.00

Der folgende Abschnitt beschreibt den Inhalt für den PIP **0A1 Notification of Failure V02.00**.

### Inhalt der Paketdatei

Die folgende Tabelle zeigt die ZIP-Dateien und entsprechenden XML-Dateien für den PIP **0A1 Notification of Failure V02.00**. Die Richtlinienzuordnungen, die für alle Versionen gleich sind, werden im nachfolgenden Abschnitt gezeigt.

*Tabelle 57. ZIP- und XML-Dateien für PIP '0A1 Notification of Failure V02.00'*

| ZIP-Dateiname | XML-Dateiname |
|---|---|
| BCG_Package_RNIFV02.00_0A1V02.00.zip | BCG_RNIFV02.00_0A1V02.00.xml |
| BCG_Package_RNSC1.0_RNIFV02.00_0A1V02.00.zip | BCG_RNSC1.0_RNIFV02.00_0A1V02.00.xml |

### Inhalt der Richtlinienzuordnungen

Dieser Abschnitt listet den Inhalt der Richtlinienzuordnungen für **0A1 Notification of Failure V02.00** auf:

- 0A1FailureNotification_V02.00.xml
- BCG_0A1FailureNotification_V02.00.xsd
- BCG_common.xsd
- BCG_GlobalPartnerClassificationCode.xsd
- BCG_GlobalPartnerRoleClassificationCode.xsd
- BCG_string_len_0.xsd
- BCG_xml.xsd

## 2A1 Distribute New Product Information

Der folgende Abschnitt beschreibt den Inhalt für den PIP **2A1 Distribute New Product Information**.

### Inhalt der Paketdatei

Die folgende Tabelle zeigt die ZIP-Dateien und entsprechenden XML-Dateien für den PIP **2A1 Distribute New Product Information**. Die Richtlinienzuordnungen, die für alle Versionen gleich sind, werden im nachfolgenden Abschnitt gezeigt.

*Tabelle 58. ZIP- und XML-Dateien für '2A1 Distribute New Product Information'*

| ZIP-Dateiname | XML-Dateiname |
|---|---|
| BCG_Package_RNIF1.1_2A1V02.00.zip | BCG_RNIF1.1_2A1V02.00.xml |
| BCG_Package_RNIFV02.00_2A1V02.00.zip | BCG_RNIFV02.00_2A1V02.00.xml |
| BCG_Package_RNSC1.0_RNIF1.1_2A1V02.00.zip | BCG_RNSC1.0_RNIF1.1_2A1V02.00.xml |
| BCG_Package_RNSC1.0_RNIFV02.00_2A1V02.00.zip | BCG_RNSC1.0_RNIFV02.00_2A1V02.00.xml |

### Inhalt der Richtlinienzuordnungen

Dieser Abschnitt listet den Inhalt der Richtlinienzuordnungen für **2A1 Distribute New Product Information** auf:

- BCG_2A1ProductCatalogInformationNotification_V02.00.xsd
- BCG_BusinessDescription_Types.xsd
- BCG_BusinessDescription_Types_V422.xsd
- BCG_BusinessDescription_Types_V43.xsd
- BCG_BusinessTaxIdentifier_Types.xsd

- BCG_common.xsd
- BCG_common_V422.xsd
- BCG_common_V43.xsd
- BCG_ContactInformation_Types.xsd
- BCG_ContactInformation_Types_V422.xsd
- BCG_ContactInformation_Types_V43.xsd
- BCG_GlobalCountryCode.xsd
- BCG_GlobalCurrencyCode.xsd
- BCG_GlobalDocumentReferenceTypeCode.xsd
- BCG_GlobalIntervalCode.xsd
- BCG_GlobalLeadTimeClassificationCode_V43.xsd
- BCG_GlobalMonetaryAmountTypeCode.xsd
- BCG_GlobalPackageTypeCode_V422.xsd
- BCG_GlobalPartnerClassificationCode_V43.xsd
- BCG_GlobalPartnerRoleClassificationCode_V422.xsd
- BCG_GlobalPriceTypeCode_V43.xsd
- BCG_GlobalProductAssociationCode_V43.xsd
- BCG_GlobalProductLifeCycleStatusCode.xsd
- BCG_GlobalProductProcurementTypeCode_V43.xsd
- BCG_GlobalProductTypeCode_V43.xsd
- BCG_GlobalProductUnitofMeasureCode_V43.xsd
- BCG_GlobalProprietaryProductIdentificationTypeCode_V43.xsd
- BCG_GlobalStandardClassificationSchemeCode_V43.xsd
- BCG_GlobalWarrantyTypeCode_V43.xsd
- BCG_InvoiceChargeTypeCode_V422.xsd
- BCG_NationalExportControlClassificationCode.xsd
- BCG_PartnerDescription_Types_V43.xsd
- BCG_PhysicalAddress_Types.xsd
- BCG_PhysicalAddress_Types_V422.xsd
- BCG_string_len_0.xsd
- BCG_xml.xsd

## 2A12 Distribute Product Master

Der folgende Abschnitt beschreibt den Inhalt für den PIP **2A12 Distribute Product Master**.

### Inhalt der Paketdatei

Die folgende Tabelle zeigt die ZIP-Dateien und entsprechenden XML-Dateien für den PIP **2A12 Distribute Product Master**. Die Richtlinienzuordnungen, die für alle Versionen gleich sind, werden im nachfolgenden Abschnitt gezeigt.

*Tabelle 59. ZIP- und XML-Dateien für '2A12 Distribute Product Master'*

| ZIP-Dateiname | XML-Dateiname |
|---|---|
| BCG_Package_RNIF1.1_2A12V01.03.zip | BCG_RNIF1.1_2A12V01.03.xml |
| BCG_Package_RNIFV02.00_2A12V01.03.zip | BCG_RNIFV02.00_2A12V01.03.xml |
| BCG_Package_RNSC1.0_RNIF1.1_2A12V01.03.zip | BCG_RNSC1.0_RNIF1.1_2A12V01.03.xml |

*Tabelle 59. ZIP- und XML-Dateien für '2A12 Distribute Product Master' (Forts.)*

| ZIP-Dateiname | XML-Dateiname |
|---|---|
| BCG_Package_RNSC1.0_RNIFV02.00_2A12V01.03.zip | BCG_RNSC1.0_RNIFV02.00_2A12V01.03.xml |

### Inhalt der Richtlinienzuordnungen

Dieser Abschnitt listet den Inhalt der Richtlinienzuordnungen für **2A12 Distribute Product Master** auf:

- BCG_2A12ProductMasterNotification_V01.03.xsd
- BCG_BusinessDescription_Types.xsd
- BCG_BusinessTaxIdentifier_Types.xsd
- BCG_common.xsd
- BCG_ContactInformation_Types.xsd
- BCG_GlobalAssemblyLevelCode.xsd
- BCG_GlobalCountryCode.xsd
- BCG_GlobalIntervalCode.xsd
- BCG_GlobalLeadTimeClassificationCode.xsd
- BCG_GlobalPartnerClassificationCode.xsd
- BCG_GlobalPartnerRoleClassificationCode.xsd
- BCG_GlobalProductLifeCycleStatusCode.xsd
- BCG_GlobalProductProcurementTypeCode.xsd
- BCG_GlobalProductUnitOfMeasureCode.xsd
- BCG_PartnerDescription_Types.xsd
- BCG_PhysicalAddress_Types.xsd
- BCG_string_len_0.xsd
- BCG_xml.xsd

## 3A1 Request Quote

Der folgende Abschnitt beschreibt den Inhalt des PIP **3A1 Request Quote**.

### Inhalt der Paketdatei

Die folgende Tabelle zeigt die ZIP-Dateien und entsprechenden XML-Dateien für den PIP **3A1 Request Quote**. Die Richtlinienzuordnungen, die für alle Versionen gleich sind, werden im nachfolgenden Abschnitt gezeigt.

*Tabelle 60. ZIP- und XML-Dateien für PIP '3A1 Request Quote'*

| ZIP-Dateiname | XML-Dateiname |
|---|---|
| BCG_Package_RNIF1.1_3A1V02.00.zip | BCG_RNIF1.1_3A1V02.00.xml |
| BCG_Package_RNIFV02.00_3A1V02.00.zip | BCG_RNIFV02.00_3A1V02.00.xml |
| BCG_Package_RNSC1.0_RNIF1.1_3A1V02.00.zip | BCG_RNSC1.0_RNIF1.1_3A1V02.00.xml |
| BCG_Package_RNSC1.0_RNIFV02.00_3A1V02.00.zip | BCG_RNSC1.0_RNIFV02.00_3A1V02.00.xml |

### Inhalt der Richtlinienzuordnungen

Dieser Abschnitt listet den Inhalt der Richtlinienzuordnungen für **3A1 Request Quote** auf:

- BCG_3A1QuoteConfirmation_V02.00.xsd
- BCG_3A1QuoteRequest_V02.00.xsd
- BCG_BusinessDescription_Types.xsd
- BCG_BusinessTaxIdentifier_Types.xsd
- BCG_common.xsd
- BCG_ContactInformation_Types.xsd
- BCG_GlobalCountryCode.xsd
- BCG_GlobalCurrencyCode.xsd
- BCG_GlobalGovernmentPriorityRatingCode.xsd
- BCG_GlobalMonetaryAmountTypeCode.xsd
- BCG_GlobalPartnerClassificationCode.xsd
- BCG_GlobalPartnerRoleClassificationCode.xsd
- BCG_GlobalProductSubstitutionReasonCode.xsd
- BCG_GlobalProductTermsCode.xsd
- BCG_GlobalProductUnitOfMeasureCode.xsd
- BCG_GlobalQuoteLineItemStatusCode.xsd
- BCG_GlobalQuoteTypeCode.xsd
- BCG_GlobalStockIndicatorCode.xsd
- BCG_GlobalTaxExemptionCode.xsd
- BCG_PartnerDescription_Types.xsd
- BCG_PhysicalAddress_Types.xsd
- BCG_string_len_0.xsd
- BCG_xml.xsd

## 3A2 Request Price and Availability

Der folgende Abschnitt beschreibt den Inhalt des PIP **3A2 Request Price and Availability**.

### Inhalt der Paketdatei

Die folgende Tabelle zeigt die ZIP-Dateien und die entsprechenden XML-Dateien für den PIP **3A2 Request Price and Availability**. Die Richtlinienzuordnungen, die für alle Versionen gleich sind, werden im nachfolgenden Abschnitt gezeigt.

*Tabelle 61. ZIP- und XML-Dateien für '3A2 Request Price and Availability'*

| ZIP-Dateiname | XML-Dateiname |
|---|---|
| BCG_Package_RNIF1.1_3A2R02.01.zip | BCG_RNIF1.1_3A2R02.01.xml |
| BCG_Package_RNIFV02.00_3A2R02.01.zip | BCG_RNIFV02.00_3A2R02.01.xml |
| BCG_Package_RNSC1.0_RNIF1.1_3A2R02.01.zip | BCG_RNSC1.0_RNIF1.1_3A2R02.01.xml |
| BCG_Package_RNSC1.0_RNIFV02.00_3A2R02.01.zip | BCG_RNSC1.0_RNIFV02.00_3A2R02.01.xml |

### Inhalt der Richtlinienzuordnungen

Dieser Abschnitt listet den Inhalt der Richtlinienzuordnungen für **3A2 Request Price and Availability** auf:

- BCG_3A2PriceAndAvailabilityRequest_R02.01.xsd
- BCG_3A2PriceAndAvailabilityResponse_R02.01.xsd

- BCG_BusinessDescription_Types.xsd
- BCG_BusinessTaxIdentifier_Types.xsd
- BCG_common.xsd
- BCG_ContactInformation_Types.xsd
- BCG_GlobalCountryCode.xsd
- BCG_GlobalCurrencyCode.xsd
- BCG_GlobalCustomerAuthorizationCode.xsd
- BCG_GlobalPartnerClassificationCode.xsd
- BCG_GlobalPricingTypeCode.xsd
- BCG_GlobalProductAvailabilityCode.xsd
- BCG_GlobalProductStatusCode.xsd
- BCG_GlobalProductSubstitutionReasonCode.xsd
- BCG_GlobalProductUnitOfMeasureCode.xsd
- BCG_PartnerDescription_Types.xsd
- BCG_PhysicalAddress_Types.xsd
- BCG_string_len_0.xsd
- BCG_xml.xsd

## 3A4 Request Purchase Order V02.00

Der folgende Abschnitt beschreibt den Inhalt des PIP **3A4 Request Purchase Order V02.00**.

### Inhalt der Paketdatei

Die folgende Tabelle zeigt die ZIP-Dateien und entsprechenden XML-Dateien für den PIP **3A4 Request Purchase Order**. Die Richtlinienzuordnungen, die für alle Versionen gleich sind, werden im nachfolgenden Abschnitt gezeigt.

*Tabelle 62. ZIP- und XML-Dateien für '3A4 Request Purchase Order'*

| ZIP-Dateiname | XML-Dateiname |
|---|---|
| BCG_Package_RNIF1.1_3A4V02.00.zip | BCG_RNIF1.1_3A4V02.00.xml |
| BCG_Package_RNIFV02.00_3A4V02.00.zip | BCG_RNIFV02.00_3A4V02.00.xml |
| BCG_Package_RNSC1.0_RNIF1.1_3A4V02.00.zip | BCG_RNSC1.0_RNIF1.1_3A4V02.00.xml |
| BCG_Package_RNSC1.0_RNIFV02.00_3A4V02.00.zip | BCG_RNSC1.0_RNIFV02.00_3A4V02.00.xml |

### Inhalt der Richtlinienzuordnungen

Dieser Abschnitt listet den Inhalt der Richtlinienzuordnungen für **3A4 Request Purchase Order** auf:

- BCG_3A4PurchaseOrderConfirmation_V02.00.xsd
- BCG_3A4PurchaseOrderRequest_V02.00.xsd
- BCG_BusinessDescription_Types.xsd
- BCG_BusinessDescription_Types_V422.xsd
- BCG_BusinessTaxIdentifier_Types.xsd
- BCG_common.xsd
- BCG_common_V422.xsd
- BCG_ContactInformation_Types.xsd

- BCG_GlobalAccountClassificationCode.xsd
- BCG_GlobalConfirmationTypeCode.xsd
- BCG_GlobalCountryCode.xsd
- BCG_GlobalCreditCardClassificationCode.xsd
- BCG_GlobalCurrencyCode.xsd
- BCG_GlobalDocumentReferenceTypeCode.xsd
- BCG_GlobalDocumentReferenceTypeCode_V422.xsd
- BCG_GlobalFinanceTermsCode.xsd
- BCG_GlobalGovernmentPriorityRatingCode.xsd
- BCG_GlobalMonetaryAmountTypeCode.xsd
- BCG_GlobalPartnerClassificationCode.xsd
- BCG_GlobalPartnerRoleClassificationCode_V422.xsd
- BCG_GlobalPaymentConditionCode.xsd
- BCG_GlobalPriceUnitOfMeasureCode.xsd
- BCG_GlobalProductSubstitutionReasonCode.xsd
- BCG_GlobalProductUnitOfMeasureCode.xsd
- BCG_GlobalPurchaseOrderAcknowledgmentReasonCode.xsd
- BCG_GlobalPurchaseOrderFillPriorityCode.xsd
- BCG_GlobalPurchaseOrderStatusCode.xsd
- BCG_GlobalPurchaseOrderTypeCode.xsd
- BCG_GlobalShipmentTermsCode.xsd
- BCG_GlobalShipmentTermsCode_V422.xsd
- BCG_GlobalShippingServiceLevelCode.xsd
- BCG_GlobalSpecialFulfillmentRequestCode.xsd
- BCG_GlobalSpecialHandlingCode_V422.xsd
- BCG_GlobalTaxExemptionCode.xsd
- BCG_GlobalTaxExemptionCode_V422.xsd
- BCG_InvoiceChargeTypeCode.xsd
- BCG_PartnerDescription_Types.xsd
- BCG_PhysicalAddress_Types.xsd
- BCG_PhysicalAddress_Types_V422.xsd
- BCG_string_len_0.xsd
- BCG_xml.xsd

## 3A4 Request Purchase Order V02.02

Der folgende Abschnitt beschreibt den Inhalt des PIP **3A4 Request Purchase Order V02.02**.

### Inhalt der Paketdatei

Die folgende Tabelle zeigt die ZIP-Dateien und entsprechenden XML-Dateien für den PIP **3A4 Request Purchase Order**. Die Richtlinienzuordnungen, die für alle Versionen gleich sind, werden im nachfolgenden Abschnitt gezeigt.

*Tabelle 63. ZIP- und XML-Dateien für '3A4 Request Purchase Order'*

| ZIP-Dateiname | XML-Dateiname |
|---|---|
| BCG_Package_RNIF1.1_3A4V02.02.zip | BCG_RNIF1.1_3A4V02.02.xml |

*Tabelle 63. ZIP- und XML-Dateien für '3A4 Request Purchase Order' (Forts.)*

| ZIP-Dateiname | XML-Dateiname |
|---|---|
| BCG_Package_RNIFV02.00_3A4V02.02.zip | BCG_RNIFV02.00_3A4V02.02.xml |
| BCG_Package_RNSC1.0_RNIF1.1_3A4V02.02.zip | BCG_RNSC1.0_RNIF1.1_3A4V02.02.xml |
| BCG_Package_RNSC1.0_RNIFV02.00_3A4V02.02.zip | BCG_RNSC1.0_RNIFV02.00_3A4V02.02.xml |

## Inhalt der Richtlinienzuordnungen

Dieser Abschnitt listet den Inhalt der Richtlinienzuordnungen für **3A4 Request Purchase Order** auf:

- BCG_3A4PurchaseOrderConfirmation_V02.02.xsd
- BCG_3A4PurchaseOrderRequest_V02.02.xsd
- BCG_BusinessDescription_Types.xsd
- BCG_BusinessTaxIdentifier_Types.xsd
- BCG_common.xsd
- BCG_ContactInformation_Types.xsd
- BCG_GlobalAccountClassificationCode.xsd
- BCG_GlobalConfirmationTypeCode.xsd
- BCG_GlobalCountryCode.xsd
- BCG_GlobalCreditCardClassificationCode.xsd
- BCG_GlobalCurrencyCode.xsd
- BCG_GlobalDocumentReferenceTypeCode.xsd
- BCG_GlobalFinanceTermsCode.xsd
- BCG_GlobalGovernmentPriorityRatingCode.xsd
- BCG_GlobalMonetaryAmountTypeCode.xsd
- BCG_GlobalPartnerClassificationCode.xsd
- BCG_GlobalPartnerRoleClassificationCode.xsd
- BCG_GlobalPaymentConditionCode.xsd
- BCG_GlobalPriceUnitOfMeasureCode.xsd
- BCG_GlobalProductSubstitutionReasonCode.xsd
- BCG_GlobalProductUnitOfMeasureCode.xsd
- BCG_GlobalPurchaseOrderAcknowledgmentReasonCode.xsd
- BCG_GlobalPurchaseOrderFillPriorityCode.xsd
- BCG_GlobalPurchaseOrderStatusCode.xsd
- BCG_GlobalPurchaseOrderTypeCode.xsd
- BCG_GlobalShipmentTermsCode.xsd
- BCG_GlobalShippingServiceLevelCode.xsd
- BCG_GlobalSpecialFulfillmentRequestCode.xsd
- BCG_GlobalSpecialHandlingCode.xsd
- BCG_GlobalTaxExemptionCode.xsd
- BCG_InvoiceChargeTypeCode.xsd
- BCG_PartnerDescription_Types.xsd
- BCG_PhysicalAddress_Types.xsd
- BCG_string_len_0.xsd
- BCG_xml.xsd

# 3A5 Query Order Status

Der folgende Abschnitt beschreibt den Inhalt des PIP **3A5 Query Order Status**.

## Inhalt der Paketdatei

Die folgende Tabelle zeigt die ZIP-Dateien und entsprechenden XML-Dateien für den PIP **3A5 Query Order Status**. Die Richtlinienzuordnungen, die für alle Versionen gleich sind, werden im nachfolgenden Abschnitt gezeigt.

*Tabelle 64. ZIP- und XML-Dateien für '3A5 Query Order Status'*

| ZIP-Dateiname | XML-Dateiname |
|---|---|
| BCG_Package_RNIF1.1_3A5R02.00.zip | BCG_RNIF1.1_3A5R02.00.xml |
| BCG_Package_RNIFV02.00_3A5R02.00.zip | BCG_RNIFV02.00_3A5R02.00.xml |
| BCG_Package_RNSC1.0_RNIF1.1_3A5R02.00.zip | BCG_RNSC1.0_RNIF1.1_3A5R02.00.xml |
| BCG_Package_RNSC1.0_RNIFV02.00_3A5R02.00.zip | BCG_RNSC1.0_RNIFV02.00_3A5R02.00.xml |

## Inhalt der Richtlinienzuordnungen

Dieser Abschnitt listet den Inhalt der Richtlinienzuordnungen für **3A5 Query Order Status** auf:

- BCG_3A5PurchaseOrderStatusQuery_R02.00.xsd
- BCG_3A5PurchaseOrderStatusResponse_R02.00.xsd
- BCG_BusinessDescription_Types.xsd
- BCG_BusinessTaxIdentifier_Types.xsd
- BCG_common.xsd
- BCG_ContactInformation_Types.xsd
- BCG_GlobalAccountClassificationCode.xsd
- BCG_GlobalCountryCode.xsd
- BCG_GlobalCreditCardClassificationCode.xsd
- BCG_GlobalCurrencyCode.xsd
- BCG_GlobalCustomerTypeCode.xsd
- BCG_GlobalDocumentReferenceTypeCode.xsd
- BCG_GlobalFinanceTermsCode.xsd
- BCG_GlobalFreeOnBoardCode.xsd
- BCG_GlobalGovernmentPriorityRatingCode.xsd
- BCG_GlobalLineItemStatusCode.xsd
- BCG_GlobalOrderQuantityTypeCode.xsd
- BCG_GlobalPartnerClassificationCode.xsd
- BCG_GlobalPartnerRoleClassificationCode.xsd
- BCG_GlobalProductSubstitutionReasonCode.xsd
- BCG_GlobalProductUnitOfMeasureCode.xsd
- BCG_GlobalPurchaseOrderAcknowledgmentReasonCode.xsd
- BCG_GlobalPurchaseOrderFillPriority
- BCG_GlobalPurchaseOrderStatusCode.xsd
- BCG_GlobalPurchaseOrderTypeCode.xsd
- BCG_GlobalShipmentTermsCode.xsd
- BCG_GlobalShippingServiceLevelCode.xsd

- BCG_GlobalSpecialFulfillmentRequestCode.xsd
- BCG_GlobalSpecialHandlingCode.xsd
- BCG_GlobalTaxExemptionCode.xsd
- BCG_GlobalTransportEventCode.xsd
- BCG_PartnerDescription_Types.xsd
- BCG_PhysicalAddress_Types.xsd
- BCG_string_len_0.xsd
- BCG_xml.xsd

## 3A6 Distribute Order Status

Der folgende Abschnitt beschreibt den Inhalt des PIP **3A6 Distribute Order Status**.

### Inhalt der Paketdatei

Die folgende Tabelle zeigt die ZIP-Dateien und entsprechenden XML-Dateien für den PIP **3A6 Distribute Order Status**. Die Richtlinienzuordnungen, die für alle Versionen gleich sind, werden im nachfolgenden Abschnitt gezeigt.

*Tabelle 65. ZIP- und XML-Dateien für '3A6 Distribute Order Status'*

| ZIP-Dateiname | XML-Dateiname |
|---|---|
| BCG_Package_RNIF1.1_3A6V02.02.zip | BCG_RNIF1.1_3A6V02.02.xml |
| BCG_Package_RNIFV02.00_3A6V02.02.zip | BCG_RNIFV02.00_3A6V02.02.xml |
| BCG_Package_RNSC1.0_RNIF1.1_3A6V02.02.zip | BCG_RNSC1.0_RNIF1.1_3A6V02.02.xml |
| BCG_Package_RNSC1.0_RNIFV02.00_3A6V02.02.zip | BCG_RNSC1.0_RNIFV02.00_3A6V02.02.xml |

### Inhalt der Richtlinienzuordnungen

Dieser Abschnitt listet den Inhalt der Richtlinienzuordnungen für **3A6 Distribute Order Status** auf:

- BCG_3A6PurchaseOrderStatusNotification_V02.02.xsd
- BCG_BusinessDescription_Types.xsd
- BCG_BusinessTaxIdentifier_Types.xsd
- BCG_common.xsd
- BCG_ContactInformation_Types.xsd
- BCG_GlobalAccountClassificationCode.xsd
- BCG_GlobalCountryCode.xsd
- BCG_GlobalCreditCardClassificationCode.xsd
- BCG_GlobalCurrencyCode.xsd
- BCG_GlobalDocumentReferenceTypeCode.xsd
- BCG_GlobalFinanceTermsCode.xsd
- BCG_GlobalGovernmentPriorityRatingCode.xsd
- BCG_GlobalLineItemStatusCode.xsd
- BCG_GlobalMonetaryAmountTypeCode.xsd
- BCG_GlobalNotificationReasonCode.xsd
- BCG_GlobalOrderQuantityTypeCode.xsd
- BCG_GlobalPartnerClassificationCode.xsd
- BCG_GlobalPartnerRoleClassificationCode.xsd

- BCG_GlobalPaymentConditionCode.xsd
- BCG_GlobalPriceUnitOfMeasureCode.xsd
- BCG_GlobalProductSubstitutionReasonCode.xsd
- BCG_GlobalProductUnitOfMeasureCode.xsd
- BCG_GlobalPurchaseOrderAcknowledgmentReasonCode.xsd
- BCG_GlobalPurchaseOrderFillPriorityCode.xsd
- BCG_GlobalPurchaseOrderStatusCode.xsd
- BCG_GlobalPurchaseOrderTypeCode.xsd
- BCG_GlobalShipmentTermsCode.xsd
- BCG_GlobalShippingServiceLevelCode.xsd
- BCG_GlobalSpecialFulfillmentRequestCode.xsd
- BCG_GlobalSpecialHandlingCode.xsd
- BCG_GlobalTaxExemptionCode.xsd
- BCG_GlobalTrackingReferenceTypeCode.xsd
- BCG_InvoiceChargeTypeCode.xsd
- BCG_PartnerDescription_Types.xsd
- BCG_PhysicalAddress_Types.xsd
- BCG_string_len_0.xsd
- BCG_xml.xsd

## 3A7 Notify of Purchase Order Update

Der folgende Abschnitt beschreibt den Inhalt des PIP **3A7 Notify of Purchase Order Update**.

### Inhalt der Paketdatei

Die folgende Tabelle zeigt die ZIP-Dateien und entsprechenden XML-Dateien für den PIP **3A7 Notify of Purchase Order Update**. Die Richtlinienzuordnungen, die für alle Versionen gleich sind, werden im nachfolgenden Abschnitt gezeigt.

*Tabelle 66. ZIP- und XML-Dateien für '3A7 Notify of Purchase Order Update'*

| ZIP-Dateiname | XML-Dateiname |
|---|---|
| BCG_Package_RNIF1.1_3A7V02.02.zip | BCG_RNIF1.1_3A7V02.02.xml |
| BCG_Package_RNIFV02.00_3A7V02.02.zip | BCG_RNIFV02.00_3A7V02.02.xml |
| BCG_Package_RNSC1.0_RNIF1.1_3A7V02.02.zip | BCG_RNSC1.0_RNIF1.1_3A7V02.02.xml |
| BCG_Package_RNSC1.0_RNIFV02.00_3A7V02.02.zip | BCG_RNSC1.0_RNIFV02.00_3A7V02.02.xml |

### Inhalt der Richtlinienzuordnungen

Dieser Abschnitt listet den Inhalt der Richtlinienzuordnungen für **3A7 Notify of Purchase Order Update** auf:

- BCG_3A7PurchaseOrderUpdateNotification_V02.02.xsd
- BCG_BusinessDescription_Types.xsd
- BCG_BusinessTaxIdentifier_Types.xsd
- BCG_common.xsd
- BCG_ContactInformation_Types.xsd
- BCG_GlobalAccountClassificationCode.xsd

- BCG_GlobalActionCode.xsd
- BCG_GlobalConfirmationTypeCode.xsd
- BCG_GlobalCountryCode.xsd
- BCG_GlobalCreditCardClassificationCode.xsd
- BCG_GlobalCurrencyCode.xsd
- BCG_GlobalDocumentReferenceTypeCode.xsd
- BCG_GlobalFinanceTermsCode.xsd
- BCG_GlobalGovernmentPriorityRatingCode.xsd
- BCG_GlobalMonetaryAmountTypeCode.xsd
- BCG_GlobalPartnerClassificationCode.xsd
- BCG_GlobalPartnerRoleClassificationCode.xsd
- BCG_GlobalPaymentConditionCode.xsd
- BCG_GlobalPriceUnitOfMeasureCode.xsd
- BCG_GlobalProductSubstitutionReasonCode.xsd
- BCG_GlobalProductUnitOfMeasureCode.xsd
- BCG_GlobalPurchaseOrderAcknowledgmentReasonCode.xsd
- BCG_GlobalPurchaseOrderFillPriorityCode.xsd
- BCG_GlobalPurchaseOrderStatusCode.xsd
- BCG_GlobalPurchaseOrderTypeCode.xsd
- BCG_GlobalShipmentTermsCode.xsd
- BCG_GlobalShippingServiceLevelCode.xsd
- BCG_GlobalSpecialFulfillmentRequestCode.xsd
- BCG_GlobalSpecialHandlingCode.xsd
- BCG_GlobalTaxExemptionCode.xsd
- BCG_InvoiceChargeTypeCode.xsd
- BCG_PartnerDescription_Types.xsd
- BCG_PhysicalAddress_Types.xsd
- BCG_string_len_0.xsd
- BCG_xml.xsd

## 3A8 Request Purchase Order Change V01.02

Der folgende Abschnitt beschreibt den Inhalt des PIP **3A8 Request Purchase Order Change V01.02**.

### Inhalt der Paketdatei

Die folgende Tabelle zeigt die ZIP-Dateien und entsprechenden XML-Dateien für den PIP **3A8 Request Purchase Order Change**. Die Richtlinienzuordnungen, die für alle Versionen gleich sind, werden im nachfolgenden Abschnitt gezeigt.

*Tabelle 67. ZIP- und XML-Dateien für '3A8 Request Purchase Order Change'*

| ZIP-Dateiname | XML-Dateiname |
|---|---|
| BCG_Package_RNIF1.1_3A8V01.02.zip | BCG_RNIF1.1_3A8V01.02.xml |
| BCG_Package_RNIFV02.00_3A8V01.02.zip | BCG_RNIFV02.00_3A8V01.02.xml |
| BCG_Package_RNSC1.0_RNIF1.1_3A8V01.02.zip | BCG_RNSC1.0_RNIF1.1_3A8V01.02.xml |
| BCG_Package_RNSC1.0_RNIFV02.00_3A8V01.02.zip | BCG_RNSC1.0_RNIFV02.00_3A8V01.02.xml |

### Inhalt der Richtlinienzuordnungen

Dieser Abschnitt listet den Inhalt der Richtlinienzuordnungen für **3A8 Request Purchase Order Change** auf:

- BCG_3A8PurchaseOrderChangeConfirmation_V01.02.xsd
- BCG_3A8PurchaseOrderChangeRequest_V01.02.xsd
- BCG_BusinessDescription_Types.xsd
- BCG_BusinessTaxIdentifier_Types.xsd
- BCG_common.xsd
- BCG_ContactInformation_Types.xsd
- BCG_GlobalAccountClassificationCode.xsd
- BCG_GlobalActionCode.xsd
- BCG_GlobalConfirmationTypeCode.xsd
- BCG_GlobalCountryCode.xsd
- BCG_GlobalCreditCardClassificationCode.xsd
- BCG_GlobalCurrencyCode.xsd
- BCG_GlobalDocumentReferenceTypeCode.xsd
- BCG_GlobalFinanceTermsCode.xsd
- BCG_GlobalGovernmentPriorityRatingCode.xsd
- BCG_GlobalMonetaryAmountTypeCode.xsd
- BCG_GlobalPartnerClassificationCode.xsd
- BCG_GlobalPartnerRoleClassificationCode.xsd
- BCG_GlobalPaymentConditionCode.xsd
- BCG_GlobalPriceUnitOfMeasureCode.xsd
- BCG_GlobalProductSubstitutionReasonCode.xsd
- BCG_GlobalProductUnitOfMeasureCode.xsd
- BCG_GlobalPurchaseOrderAcknowledgmentReasonCode.xsd
- BCG_GlobalPurchaseOrderFillPriorityCode.xsd
- BCG_GlobalPurchaseOrderStatusCode.xsd
- BCG_GlobalPurchaseOrderTypeCode.xsd
- BCG_GlobalShipmentTermsCode.xsd
- BCG_GlobalShippingServiceLevelCode.xsd
- BCG_GlobalSpecialFulfillmentRequestCode.xsd
- BCG_GlobalSpecialHandlingCode.xsd
- BCG_GlobalTaxExemptionCode.xsd
- BCG_InvoiceChargeTypeCode.xsd
- BCG_PartnerDescription_Types.xsd
- BCG_PhysicalAddress_Types.xsd
- BCG_string_len_0.xsd
- BCG_xml.xsd

## 3A8 Request Purchase Order Change V01.03

Der folgende Abschnitt beschreibt den Inhalt des PIP **3A8 Request Purchase Order Change V01.03**.

## Inhalt der Paketdatei

Die folgende Tabelle zeigt die ZIP-Dateien und entsprechenden XML-Dateien für den PIP **3A8 Request Purchase Order Change**. Die Richtlinienzuordnungen, die für alle Versionen gleich sind, werden im nachfolgenden Abschnitt gezeigt.

*Tabelle 68. ZIP- und XML-Dateien für '3A8 Request Purchase Order Change'*

| ZIP-Dateiname | XML-Dateiname |
|---|---|
| BCG_Package_RNIF1.1_3A8V01.03.zip | BCG_RNIF1.1_3A8V01.03.xml |
| BCG_Package_RNIFV02.00_3A8V01.03.zip | BCG_RNIFV02.00_3A8V01.03.xml |
| BCG_Package_RNSC1.0_RNIF1.1_3A8V01.03.zip | BCG_RNSC1.0_RNIF1.1_3A8V01.03.xml |
| BCG_Package_RNSC1.0_RNIFV02.00_3A8V01.03.zip | BCG_RNSC1.0_RNIFV02.00_3A8V01.03.xml |

## Inhalt der Richtlinienzuordnungen

Dieser Abschnitt listet den Inhalt der Richtlinienzuordnungen für **3A8 Request Purchase Order Change** auf:

- BCG_3A8PurchaseOrderChangeConfirmation_V01.03.xsd
- BCG_3A8PurchaseOrderChangeRequest_V01.03.xsd
- BCG_BusinessDescription_Types.xsd
- BCG_BusinessDescription_Types_V43.xsd
- BCG_BusinessTaxIdentifier_Types.xsd
- BCG_common.xsd
- BCG_common_V422.xsd
- BCG_common_V43.xsd
- BCG_ContactInformation_Types.xsd
- BCG_GlobalAccountClassificationCode.xsd
- BCG_GlobalActionCode.xsd
- BCG_GlobalConfirmationTypeCode.xsd
- BCG_GlobalCountryCode.xsd
- BCG_GlobalCreditCardClassificationCode.xsd
- BCG_GlobalCurrencyCode.xsd
- BCG_GlobalDocumentReferenceTypeCode.xsd
- BCG_GlobalFinanceTermsCode.xsd
- BCG_GlobalFreeOnBoardCode_V422.xsd
- BCG_GlobalGovernmentPriorityRatingCode.xsd
- BCG_GlobalMonetaryAmountTypeCode.xsd
- BCG_GlobalPartnerClassificationCode_V43.xsd
- BCG_GlobalPartnerRoleClassificationCode_V43.xsd
- BCG_GlobalPaymentConditionCode.xsd
- BCG_GlobalProductSubstitutionReasonCode.xsd
- BCG_GlobalProductUnitOfMeasureCode_V43.xsd
- BCG_GlobalPurchaseOrderAcknowledgmentReasonCode.xsd
- BCG_GlobalPurchaseOrderFillPriorityCode.xsd
- BCG_GlobalPurchaseOrderStatusCode.xsd
- BCG_GlobalPurchaseOrderTypeCode.xsd

- BCG_GlobalShipmentTermsCode.xsd
- BCG_GlobalShippingServiceLevelCode.xsd
- BCG_GlobalSpecialFulfillmentRequestCode.xsd
- BCG_GlobalSpecialHandlingCode_V43.xsd
- BCG_GlobalTaxExemptionCode.xsd
- BCG_GlobalTransportEventCode.xsd
- BCG_InvoiceChargeTypeCode_V422.xsd
- BCG_PartnerDescription_Types.xsd
- BCG_PartnerDescription_Types_V43.xsd
- BCG_PhysicalAddress_Types.xsd
- BCG_string_len_0.xsd
- BCG_xml.xsd

## 3A9 Request Purchase Order Cancellation

Der folgende Abschnitt beschreibt den Inhalt des PIP **3A9 Request Purchase Order Cancellation**.

### Inhalt der Paketdatei

Die folgende Tabelle zeigt die ZIP-Dateien und entsprechenden XML-Dateien für den PIP **3A9 Request Purchase Order Cancellation**. Die Richtlinienzuordnungen, die für alle Versionen gleich sind, werden im nachfolgenden Abschnitt gezeigt.

*Tabelle 69. ZIP- und XML-Dateien für '3A9 Request Purchase Order Cancellation'*

| ZIP-Dateiname | XML-Dateiname |
|---|---|
| BCG_Package_RNIF1.1_3A9V01.01.zip | BCG_RNIF1.1_3A9V01.01.xml |
| BCG_Package_RNIFV02.00_3A9V01.01.zip | BCG_RNIFV02.00_3A9V01.01.xml |
| BCG_Package_RNSC1.0_RNIF1.1_3A9V01.01.zip | BCG_RNSC1.0_RNIF1.1_3A9V01.01.xml |
| BCG_Package_RNSC1.0_RNIFV02.00_3A9V01.01.zip | BCG_RNSC1.0_RNIFV02.00_3A9V01.01.xml |

### Inhalt der Richtlinienzuordnungen

Dieser Abschnitt listet den Inhalt der Richtlinienzuordnungen für **3A9 Request Purchase Order Cancellation** auf:

- BCG_3A9PurchaseOrderCancellationConfirmation_V01.01.xsd
- BCG_3A9PurchaseOrderCancellationRequest_V01.01.xsd
- BCG_BusinessDescription_Types.xsd
- BCG_BusinessTaxIdentifier_Types.xsd
- BCG_common.xsd
- BCG_ContactInformation_Types.xsd
- BCG_GlobalCountryCode.xsd
- BCG_GlobalPartnerClassificationCode.xsd
- BCG_GlobalPurchaseOrderCancellationCode.xsd
- BCG_GlobalPurchaseOrderCancellationResponseCode.xsd
- BCG_PartnerDescription_Types.xsd
- BCG_PhysicalAddress_Types.xsd
- BCG_string_len_0.xsd
- BCG_xml.xsd

# 3B2 Notify of Advance Shipment

Der folgende Abschnitt beschreibt den Inhalt des PIP **3B2 Notify of Advance Shipment**.

## Inhalt der Paketdatei

Die folgende Tabelle zeigt die ZIP-Dateien und entsprechenden XML-Dateien für den PIP **3B2 Notify of Advance Shipment**. Die Richtlinienzuordnungen, die für alle Versionen gleich sind, werden im nachfolgenden Abschnitt gezeigt.

*Tabelle 70. ZIP- und XML-Dateien für* **3B2 Notify of Advance Shipment**

| ZIP-Dateiname | XML-Dateiname |
|---|---|
| BCG_Package_RNIF1.1_3B2V01.01.zip | BCG_RNIF1.1_3B2V01.01.xml |
| BCG_Package_RNIFV02.00_3B2V01.01.zip | BCG_RNIFV02.00_3B2V01.01.xml |
| BCG_Package_RNSC1.0_RNIF1.1_3B2V01.01.zip | BCG_RNSC1.0_RNIF1.1_3B2V01.01.xml |
| BCG_Package_RNSC1.0_RNIFV02.00_3B2V01.01.zip | BCG_RNSC1.0_RNIFV02.00_3B2V01.01.xml |

## Inhalt der Richtlinienzuordnungen

Dieser Abschnitt listet den Inhalt der Richtlinienzuordnungen für **3B2 Notify of Advance Shipment** auf:

- BCG_3B2AdvanceShipmentNotification_V01.01.xsd
- BCG_BusinessDescription_Types.xsd
- BCG_BusinessTaxIdentifier_Types.xsd
- BCG_common.xsd
- BCG_ContactInformation_Types.xsd
- BCG_GlobalCountryCode.xsd
- BCG_GlobalDocumentReferenceTypeCode.xsd
- BCG_GlobalIncotermsCode.xsd
- BCG_GlobalLotQuantityClassificationCode.xsd
- BCG_GlobalPackageTypeCode.xsd
- BCG_GlobalPartnerClassificationCode.xsd
- BCG_GlobalPhysicalUnitOfMeasureCode.xsd
- BCG_GlobalProductUnitOfMeasureCode.xsd
- BCG_GlobalShipDateCode.xsd
- BCG_GlobalShipmentChangeDispositionCode.xsd
- BCG_GlobalShipmentModeCode.xsd
- BCG_GlobalShippingServiceLevelCode.xsd
- BCG_GlobalTrackingReferenceTypeCode.xsd
- BCG_NationalExportControlClassificationCode.xsd
- BCG_PartnerDescription_Types.xsd
- BCG_PhysicalAddress_Types.xsd
- BCG_string_len_0.xsd
- BCG_xml.xsd

# 3B3 Distribute Shipment Status

Der folgende Abschnitt beschreibt den Inhalt des PIP **3B3 Distribute Shipment Status**.

## Inhalt der Paketdatei

Die folgende Tabelle zeigt die ZIP-Dateien und entsprechenden XML-Dateien für den PIP **3B3 Distribute Shipment Status**. Die Richtlinienzuordnungen, die für alle Versionen gleich sind, werden im nachfolgenden Abschnitt gezeigt.

*Tabelle 71. ZIP- und XML-Dateien für* **3B3 Distribute Shipment Status**

| ZIP-Dateiname | XML-Dateiname |
|---|---|
| BCG_Package_RNIF1.1_3B3R01.00.zip | BCG_RNIF1.1_3B3R01.00.xml |
| BCG_Package_RNIFV02.00_3B3R01.00.zip | BCG_RNIFV02.00_3B3R01.00.xml |
| BCG_Package_RNSC1.0_RNIF1.1_3B3R01.00.zip | BCG_RNSC1.0_RNIF1.1_3B3R01.00.xml |
| BCG_Package_RNSC1.0_RNIFV02.00_3B3R01.00.zip | BCG_RNSC1.0_RNIFV02.00_3B3R01.00.xml |

## Inhalt der Richtlinienzuordnungen

Dieser Abschnitt listet den Inhalt der Richtlinienzuordnungen für **3B3 Distribute Shipment Status** auf:

- 3B3 Distribute Shipment Status_R01.00.xsd
- BCG_BusinessDescription_Types.xsd
- BCG_BusinessDescription_Types_V422.xsd
- BCG_BusinessDescription_Types_V43.xsd
- BCG_BusinessTaxIdentifier_Types.xsd
- BCG_common_V422.xsd
- BCG_common_V43.xsd
- BCG_ContactInformation_Types.xsd
- BCG_ContactInformation_Types_V422.xsd
- BCG_ContactInformation_Types_V43.xsd
- BCG_GlobalCountryCode.xsd
- BCG_GlobalDocumentReferenceTypeCode_V43.xsd
- BCG_GlobalPartnerClassificationCode_V43.xsd
- BCG_GlobalShipmentDispositionCode.xsd
- BCG_GlobalShipmentModeCode.xsd
- BCG_GlobalShipmentStatusCode_V43.xsd
- BCG_GlobalShipmentStatusReportingLevelCode_V43.xsd
- BCG_GlobalTrackingReferenceTypeCode.xsd
- BCG_PartnerDescription_Types_V43.xsd
- BCG_PhysicalAddress_Types.xsd
- BCG_PhysicalAddress_Types_V422.xsd
- BCG_PhysicalAddress_Types_V423.xsd
- BCG_string_len_0.xsd
- BCG_xml.xsd

# 3B11 Notify of Shipping Order

Der folgende Abschnitt beschreibt den Inhalt des PIP **3B11 Notify of Shipping Order**.

## Inhalt der Paketdatei

Die folgende Tabelle zeigt die ZIP-Dateien und entsprechenden XML-Dateien für den PIP **3B11 Notify of Shipping Order**. Die Richtlinienzuordnungen, die für alle Versionen gleich sind, werden im nachfolgenden Abschnitt gezeigt.

*Tabelle 72. ZIP- und XML-Dateien für* **3B11 Notify of Shipping Order**

| ZIP-Dateiname | XML-Dateiname |
|---|---|
| BCG_Package_RNIF1.1_3B11R01.00A.zip | BCG_RNIF1.1_3B11R01.00A.xml |
| BCG_Package_RNIFV02.00_3B11R01.00A.zip | BCG_RNIFV02.00_3B11R01.00A.xml |
| BCG_Package_RNSC1.0_RNIF1.1_3B11R01.00A.zip | BCG_RNSC1.0_RNIF1.1_3B11R01.00A.xml |
| BCG_Package_RNSC1.0_RNIFV02.00_3B11R01.00A.zip | BCG_RNSC1.0_RNIFV02.00_3B11R01.00A.xml |

## Inhalt der Richtlinienzuordnungen

Dieser Abschnitt listet den Inhalt der Richtlinienzuordnungen für **3B11 Notify of Shipping Order** auf:

- 3B11 ShippingOrderNotification_R01.00A.xsd
- BCG_BusinessDescription_Types.xsd
- BCG_BusinessDescription_Types_V422.xsd
- BCG_BusinessTaxIdentifier_Types.xsd
- BCG_common.xsd
- BCG_ContactInformation_Types.xsd
- BCG_ContactInformation_Types_V422.xsd
- BCG_GlobalCountryCode.xsd
- BCG_GlobalCurrencyCode.xsd
- BCG_GlobalDocumentReferenceTypeCode_V422.xsd
- BCG_GlobalFreightPaymentTermsCode_V422.xsd
- BCG_GlobalIncotermsCode.xsd
- BCG_GlobalOrderAdminCode_V422.xsd
- BCG_GlobalPartnerClassificationCode.xsd
- BCG_GlobalPartnerRoleClassificationCode.xsd
- BCG_GlobalProductUnitOfMeasureCode.xsd
- BCG_GlobalShipDateCode.xsd
- BCG_GlobalShipmentModeCode.xsd
- BCG_GlobalShippingServiceLevelCode.xsd
- BCG_GlobalSpecialHandlingCode.xsd
- BCG_GlobalWarrantyTypeCode_V43.xsd
- BCG_PartnerDescription_Types.xsd
- BCG_PartnerDescription_Types_V422.xsd
- BCG_PhysicalAddress_Types.xsd
- BCG_string_len_0.xsd
- BCG_xml.xsd

# 3B12 Request Shipping Order

Der folgende Abschnitt beschreibt den Inhalt des PIP **3B12 Request of Shipping Order**.

## Inhalt der Paketdatei

Die folgende Tabelle zeigt die ZIP-Dateien und entsprechenden XML-Dateien für den PIP **3B12 Request Shipping Order**. Die Richtlinienzuordnungen, die für alle Versionen gleich sind, werden im nachfolgenden Abschnitt gezeigt.

*Tabelle 73. ZIP- und XML-Dateien für* **3B12 Request Shipping Order**

| ZIP-Dateiname | XML-Dateiname |
|---|---|
| BCG_Package_RNIF1.1_3B12V01.01.zip | BCG_RNIF1.1_3B12V01.01.xml |
| BCG_Package_RNIFV02.00_3B12V01.01.zip | BCG_RNIFV02.00_3B12V01.01.xml |
| BCG_Package_RNSC1.0_RNIF1.1_3B12V01.01.zip | BCG_RNSC1.0_RNIF1.1_3B12V01.01.xml |
| BCG_Package_RNSC1.0_RNIFV02.00_3B12V01.01.zip | BCG_RNSC1.0_RNIFV02.00_3B12V01.01.xml |

## Inhalt der Richtlinienzuordnungen

Dieser Abschnitt listet den Inhalt der Richtlinienzuordnungen für **3B12 Request Shipping Order** auf:

- BCG_3B12ShippingOrderConfirmation_V01.01.xsd
- BCG_3B12ShippingOrderRequest_V01.01.xsd
- BCG_BusinessTaxIdentifier_Types.xsd
- BCG_common.xsd
- BCG_common_V422.xsd
- BCG_ContactInformation_Types.xsd
- BCG_ContactInformation_Types_V422.xsd
- BCG_GlobalCountryCode.xsd
- BCG_GlobalCurrencyCode.xsd
- BCG_GlobalDocumentReferenceTypeCode.xsd
- BCG_GlobalIncotermsCode.xsd
- BCG_GlobalPackageTypeCode.xsd
- BCG_GlobalPartnerClassificationCode.xsd
- BCG_GlobalPartnerRoleClassificationCode.xsd
- BCG_GlobalPhysicalUnitOfMeasureCode.xsd
- BCG_GlobalProductUnitOfMeasureCode.xsd
- BCG_GlobalShipDateCode.xsd
- BCG_GlobalShippingServiceLevelCode.xsd
- BCG_GlobalSpecialHandlingCode.xsd
- BCG_PartnerDescription_Types.xsd
- BCG_PartnerDescription_Types_V422.xsd
- BCG_PhysicalAddress_Types.xsd
- BCG_string_len_0.xsd
- BCG_xml.xsd

# 3B13 Notify of Shipping Order Confirmation

Der folgende Abschnitt beschreibt den Inhalt des PIP **3B13 Notify of Shipping Order Confirmation**.

## Inhalt der Paketdatei

Die folgende Tabelle zeigt die ZIP-Dateien und entsprechenden XML-Dateien für den PIP **3B13 Notify of Shipping Order Confirmation**. Die Richtlinienzuordnungen, die für alle Versionen gleich sind, werden im nachfolgenden Abschnitt gezeigt.

*Tabelle 74. ZIP- und XML-Dateien für* **3B13 Notify of Shipping Order Confirmation**

| ZIP-Dateiname | XML-Dateiname |
|---|---|
| BCG_Package_RNIF1.1_3B13V01.01.zip | BCG_RNIF1.1_3B13V01.01.xml |
| BCG_Package_RNIFV02.00_3B13V01.01.zip | BCG_RNIFV02.00_3B13V01.01.xml |
| BCG_Package_RNSC1.0_RNIF1.1_3B13V01.01.zip | BCG_RNSC1.0_RNIF1.1_3B13V01.01.xml |
| BCG_Package_RNSC1.0_RNIFV02.00_3B13V01.01.zip | BCG_RNSC1.0_RNIFV02.00_3B13V01.01.xml |

## Inhalt der Richtlinienzuordnungen

Dieser Abschnitt listet den Inhalt der Richtlinienzuordnungen für **3B13 Notify of Shipping Order Confirmation** auf:

- BCG_3B13ShippingOrderConfirmationNotification_V01.01.xsd
- BCG_BusinessDescription_Types.xsd
- BCG_BusinessTaxIdentifier_Types.xsd
- BCG_common.xsd
- BCG_common_V422.xsd
- BCG_ContactInformation_Types.xsd
- BCG_GlobalCountryCode.xsd
- BCG_GlobalCurrencyCode.xsd
- BCG_GlobalDocumentReferenceTypeCode.xsd
- BCG_GlobalPartnerClassificationCode.xsd
- BCG_GlobalPartnerRoleClassificationCode.xsd
- BCG_GlobalPhysicalUnitOfMeasureCode.xsd
- BCG_GlobalProductUnitOfMeasureCode.xsd
- BCG_GlobalShipDateCode.xsd
- BCG_GlobalShippingServiceLevelCode.xsd
- BCG_GlobalSpecialHandlingCode.xsd
- BCG_GlobalTrackingReferenceTypeCode.xsd
- BCG_PartnerDescription_Types.xsd
- BCG_PhysicalAddress_Types.xsd
- BCG_string_len_0.xsd
- BCG_xml.xsd

# 3B14 Request Shipping Order Cancellation

Der folgende Abschnitt beschreibt den Inhalt des PIP **3B14 Request Shipping Order Cancellation**.

### Inhalt der Paketdatei

Die folgende Tabelle zeigt die ZIP-Dateien und entsprechenden XML-Dateien für den PIP **3B14 Request Shipping Order Cancellation**. Die Richtlinienzuordnungen, die für alle Versionen gleich sind, werden im nachfolgenden Abschnitt gezeigt.

*Tabelle 75. ZIP- und XML-Dateien für* **3B14 Request Shipping Order Cancellation**

| ZIP-Dateiname | XML-Dateiname |
|---|---|
| BCG_Package_RNIF1.1_3B14V01.00.zip | BCG_RNIF1.1_3B14V01.00.xml |
| BCG_Package_RNIFV02.00_3B14V01.00.zip | BCG_RNIFV02.00_3B14V01.00.xml |
| BCG_Package_RNSC1.0_RNIF1.1_3B14V01.00.zip | BCG_RNSC1.0_RNIF1.1_3B14V01.00.xml |
| BCG_Package_RNSC1.0_RNIFV02.00_3B14V01.00.zip | BCG_RNSC1.0_RNIFV02.00_3B14V01.00.xml |

### Inhalt der Richtlinienzuordnungen

Dieser Abschnitt listet den Inhalt der Richtlinienzuordnungen für **3B14 Request Shipping Order Cancellation** auf:

- 3B14_ShippingOrderCancellationConfirmation_V01.00.xsd
- 3B14_ShippingOrderCancellationRequest_V01.00.xsd
- BCG_common.xsd
- BCG_common_V422.xsd
- BCG_ContactInformation_Types.xsd
- BCG_GlobalDocumentReferenceTypeCode.xsd
- BCG_GlobalOrderAdminCode_V22.xsd
- BCG_GlobalPartnerRoleClassificationCode.xsd
- BCG_GlobalPartnerRoleClassificationCode_V43.xsd
- BCG_GlobalShippingOrderCancellationStatusReasonCode_V43.xsd
- BCG_PartnerDescription_Types.xsd
- BCG_PartnerDescription_Types_V43.xsd
- BCG_string_len_0.xsd
- BCG_xml.xsd

## 3B18 Notify of Shipping Documentation

Der folgende Abschnitt beschreibt den Inhalt des PIP **3B18 Notify of Shipping Documentation**.

### Inhalt der Paketdatei

Die folgende Tabelle zeigt die ZIP-Dateien und entsprechenden XML-Dateien für den PIP **3B18 Notify of Shipping Documentation**. Die Richtlinienzuordnungen, die für alle Versionen gleich sind, werden im nachfolgenden Abschnitt gezeigt.

*Tabelle 76. ZIP- und XML-Dateien für* **3B18 Notify of Shipping Documentation**

| ZIP-Dateiname | XML-Dateiname |
|---|---|
| BCG_Package_RNIF1.1_3B18V01.00.zip | BCG_RNIF1.1_3B18V01.00.xml |
| BCG_Package_RNIFV02.00_3B18V01.00.zip | BCG_RNIFV02.00_3B18V01.00.xml |
| BCG_Package_RNSC1.0_RNIF1.1_3B18V01.00.zip | BCG_RNSC1.0_RNIF1.1_3B18V01.00.xml |
| BCG_Package_RNSC1.0_RNIFV02.00_3B18V01.00.zip | BCG_RNSC1.0_RNIFV02.00_3B18V01.00.xml |

### Inhalt der Richtlinienzuordnungen

Dieser Abschnitt listet den Inhalt der Richtlinienzuordnungen für **3B18 Notify of Shipping Documentation** auf:

- BCG_3B18ShippingDocumentationNotification_V01.00.xsd
- BCG_BusinessDescription_Types.xsd
- BCG_BusinessDescription_Types_V422.xsd
- BCG_common_V422.xsd
- BCG_ContactInformation_Types.xsd
- BCG_GlobalCountryCode.xsd
- BCG_GlobalCurrencyCode.xsd
- BCG_GlobalDocumentReferenceTypeCode.xsd
- BCG_GlobalFreeOnBoardCode_V422.xsd
- BCG_GlobalFreightPaymentTermsCode_V422.xsd
- BCG_GlobalIncotermsCode.xsd
- BCG_GlobalMonetaryAmountTypeCode.xsd
- BCG_GlobalOrderAdminCode_V422.xsd
- BCG_GlobalPackageTypeCode_V422.xsd
- BCG_GlobalPartnerClassificationCode_V422.xsd
- BCG_GlobalPartnerRoleClassificationCode_V422.xsd
- BCG_GlobalPaymentTermsCode.xsd
- BCG_GlobalPhysicalUnitOfMeasureCode_V422.xsd
- BCG_GlobalPortIdentifierAuthorityCode_V422.xsd
- BCG_GlobalPortTypeCode_V422.xsd
- BCG_GlobalProductUnitOfMeasureCode.xsd
- BCG_GlobalShipDateCode.xsd
- BCG_GlobalShipmentModeCode.xsd
- BCG_GlobalShippingDocumentCode_V422.xsd
- BCG_GlobalShippingServiceLevelCode.xsd
- BCG_GlobalSpecialHandlingCode_V422.xsd
- BCG_GlobalTrackingReferenceTypeCode.xsd
- BCG_InvoiceChargeTypeCode_V422.xsd
- BCG_NationalExportControlClassificationCode.xsd
- BCG_PhysicalAddress_Types.xsd
- BCG_string_len_0.xsd
- BCG_xml.xsd

## 3C1 Return Product

Der folgende Abschnitt beschreibt den Inhalt des PIP **3C1 Return Product**.

### Inhalt der Paketdatei

Die folgende Tabelle zeigt die ZIP-Dateien und entsprechenden XML-Dateien für den PIP **3C1 Return Product**. Die Richtlinienzuordnungen, die für alle Versionen gleich sind, werden im nachfolgenden Abschnitt gezeigt.

*Tabelle 77. ZIP- und XML-Dateien für* **3C1 Return Product**

| ZIP-Dateiname | XML-Dateiname |
|---|---|
| BCG_Package_RNIF1.1_3C1V01.00.zip | BCG_RNIF1.1_3C1V01.00.xml |
| BCG_Package_RNIFV02.00_3C1V01.00.zip | BCG_RNIFV02.00_3C1V01.00.xml |
| BCG_Package_RNSC1.0_RNIF1.1_3C1V01.00.zip | BCG_RNSC1.0_RNIF1.1_3C1V01.00.xml |
| BCG_Package_RNSC1.0_RNIFV02.00_3C1V01.00.zip | BCG_RNSC1.0_RNIFV02.00_3C1V01.00.xml |

### Inhalt der Richtlinienzuordnungen

Dieser Abschnitt listet den Inhalt der Richtlinienzuordnungen für **3C1 Return Product** auf:

- BCG_3C1ReturnProductConfirmation_V01.00.xsd
- BCG_3C1ReturnProductRequest_V01.00.xsd
- BCG_BusinessDescription_Types.xsd
- BCG_BusinessDescription_Types_V43.xsd
- BCG_common.xsd
- BCG_common_V422.xsd
- BCG_common_V43.xsd
- BCG_ContactInformation_Types.xsd
- BCG_GlobalCurrencyCode.xsd
- BCG_GlobalDocumentReferenceTypeCode.xsd
- BCG_GlobalFailureTypeCode_V43.xsd
- BCG_GlobalPartnerClassificationCode_V43.xsd
- BCG_GlobalPartnerRoleClassificationCode_V43.xsd
- BCG_GlobalProductUnitOfMeasureCode_V43.xsd
- BCG_GlobalShippingServiceLevelCode.xsd
- BCG_PartnerDescription_Types.xsd
- BCG_PartnerDescription_Types_V43.xsd
- BCG_PhysicalAddress_Types.xsd
- BCG_string_len_0.xsd
- BCG_xml.xsd

## 3C3 Notify of Invoice

Der folgende Abschnitt beschreibt den Inhalt des PIP **3C3 Notify of Invoice**.

### Inhalt der Paketdatei

Die folgende Tabelle zeigt die ZIP-Dateien und entsprechenden XML-Dateien für den PIP **3C3 Notify of Invoice**. Die Richtlinienzuordnungen, die für alle Versionen gleich sind, werden im nachfolgenden Abschnitt gezeigt.

*Tabelle 78. ZIP- und XML-Dateien für* **3C3 Notify of Invoice**

| ZIP-Dateiname | XML-Dateiname |
|---|---|
| BCG_Package_RNIF1.1_3C3V01.01.zip | BCG_RNIF1.1_3C3V01.01.xml |
| BCG_Package_RNIFV02.00_3C3V01.01.zip | BCG_RNIFV02.00_3C3V01.01.xml |
| BCG_Package_RNSC1.0_RNIF1.1_3C3V01.01.zip | BCG_RNSC1.0_RNIF1.1_3C3V01.01.xml |

*Tabelle 78. ZIP- und XML-Dateien für* **3C3 Notify of Invoice** *(Forts.)*

| ZIP-Dateiname | XML-Dateiname |
|---|---|
| BCG_Package_RNSC1.0_RNIFV02.00_3C3V01.01.zip | BCG_RNSC1.0_RNIFV02.00_3C3V01.01.xml |

### Inhalt der Richtlinienzuordnungen

Dieser Abschnitt listet den Inhalt der Richtlinienzuordnungen für **3C3 Notify of Invoice** auf:

- BCG_3C3InvoiceNotification_V01.01.xsd
- BCG_BusinessDescription_Types.xsd
- BCG_BusinessTaxIdentifier_Types.xsd
- BCG_common.xsd
- BCG_ContactInformation_Types.xsd
- BCG_GlobalCountryCode.xsd
- BCG_GlobalCurrencyCode.xsd
- BCG_GlobalDocumentTypeCode.xsd
- BCG_GlobalMonetaryAmountTypeCode.xsd
- BCG_GlobalPartnerClassificationCode.xsd
- BCG_GlobalPartnerRoleClassificationCode.xsd
- BCG_GlobalPaymentTermsCode.xsd
- BCG_GlobalProductUnitOfMeasureCode.xsd
- BCG_GlobalSaleTypeCode.xsd
- BCG_GlobalShipmentTermsCode.xsd
- BCG_GlobalShippingServiceLevelCode.xsd
- BCG_GlobalSpecialHandlingCode.xsd
- BCG_InvoiceChargeTypeCode.xsd
- BCG_NationalExportControlClassificationCode.xsd
- BCG_PartnerDescription_Types.xsd
- BCG_PhysicalAddress_Types.xsd
- BCG_string_len_0.xsd
- BCG_xml.xsd

## 3C4 Notify of Invoice Reject

Der folgende Abschnitt beschreibt den Inhalt des PIP **3C4 Notify of Invoice Reject**.

### Inhalt der Paketdatei

Die folgende Tabelle zeigt die ZIP-Dateien und entsprechenden XML-Dateien für den PIP **3C4 Notify of Invoice Reject**. Die Richtlinienzuordnungen, die für alle Versionen gleich sind, werden im nachfolgenden Abschnitt gezeigt.

*Tabelle 79. ZIP- und XML-Dateien für* **3C4 Notify of Invoice Reject**

| ZIP-Dateiname | XML-Dateiname |
|---|---|
| BCG_Package_RNIF1.1_3C4V01.00.zip | BCG_RNIF1.1_3C4V01.00.xml |
| BCG_Package_RNIFV02.00_3C4V01.00.zip | BCG_RNIFV02.00_3C4V01.00.xml |
| BCG_Package_RNSC1.0_RNIF1.1_3C4V01.00.zip | BCG_RNSC1.0_RNIF1.1_3C4V01.00.xml |

*Tabelle 79. ZIP- und XML-Dateien für* **3C4 Notify of Invoice Reject** *(Forts.)*

| ZIP-Dateiname | XML-Dateiname |
|---|---|
| BCG_Package_RNSC1.0_RNIFV02.00_3C4V01.00.zip | BCG_RNSC1.0_RNIFV02.00_3C4V01.00.xml |

### Inhalt der Richtlinienzuordnungen

Dieser Abschnitt listet den Inhalt der Richtlinienzuordnungen für **3C4 Notify of Invoice Reject** auf:

- BCG_3C4InvoiceRejectNotification_V01.00.xsd
- BCG_BusinessDescription_Types.xsd
- BCG_BusinessTaxIdentifier_Types.xsd
- BCG_common.xsd
- BCG_ContactInformation_Types.xsd
- BCG_GlobalCountryCode.xsd
- BCG_GlobalInvoiceRejectionCode.xsd
- BCG_GlobalMonetaryAmountTypeCode.xsd
- BCG_GlobalPartnerClassificationCode.xsd
- BCG_PartnerDescription_Types.xsd
- BCG_PhysicalAddress_Types.xsd
- BCG_string_len_0.xsd
- BCG_xml.xsd

## 3C6 Notify of Remittance Advice

Der folgende Abschnitt beschreibt den Inhalt des PIP **3C6 Notify of Remittance Advice**.

### Inhalt der Paketdatei

Die folgende Tabelle zeigt die ZIP-Dateien und entsprechenden XML-Dateien für den PIP **3C6 Notify of Remittance Advice**. Die Richtlinienzuordnungen, die für alle Versionen gleich sind, werden im nachfolgenden Abschnitt gezeigt.

*Tabelle 80. ZIP- und XML-Dateien für* **3C6 Notify of Remittance Advice**

| ZIP-Dateiname | XML-Dateiname |
|---|---|
| BCG_Package_RNIF1.1_3C6V01.00.zip | BCG_RNIF1.1_3C6V01.00.xml |
| BCG_Package_RNIFV02.00_3C6V01.00.zip | BCG_RNIFV02.00_3C6V01.00.xml |
| BCG_Package_RNSC1.0_RNIF1.1_3C6V01.00.zip | BCG_RNSC1.0_RNIF1.1_3C6V01.00.xml |
| BCG_Package_RNSC1.0_RNIFV02.00_3C6V01.00.zip | BCG_RNSC1.0_RNIFV02.00_3C6V01.00.xml |

### Inhalt der Richtlinienzuordnungen

Dieser Abschnitt listet den Inhalt der Richtlinienzuordnungen für **3C6 Notify of Remittance Advice** auf:

- BCG_3C6RemittanceAdviceNotification_V01.00.xsd
- BCG_BusinessDescription_Types.xsd
- BCG_BusinessTaxIdentifier_Types.xsd
- BCG_common.xsd

- BCG_ContactInformation_Types.xsd
- BCG_GlobalCountryCode.xsd
- BCG_GlobalCurrencyCode.xsd
- BCG_GlobalDocumentTypeCode.xsd
- BCG_GlobalFinancialAdjustmentReasonCode.xsd
- BCG_GlobalInvoiceRejectionCode.xsd
- BCG_GlobalMonetaryAmountTypeCode.xsd
- BCG_GlobalPartnerClassificationCode.xsd
- BCG_GlobalPaymentMethodCode.xsd
- BCG_PartnerDescription_Types.xsd
- BCG_PhysicalAddress_Types.xsd
- BCG_string_len_0.xsd
- BCG_xml.xsd

## 3C7 Notify of Self-Billing Invoice

Der folgende Abschnitt beschreibt den Inhalt des PIP **3C7 Notify of Self-Billing Invoice**.

### Inhalt der Paketdatei

Die folgende Tabelle zeigt die ZIP-Dateien und entsprechenden XML-Dateien für den PIP **3C7 Notify of Self-Billing Invoice**. Die Richtlinienzuordnungen, die für alle Versionen gleich sind, werden im nachfolgenden Abschnitt gezeigt.

*Tabelle 81. ZIP- und XML-Dateien für* **3C7 Notify of Self-Billing Invoice**

| ZIP-Dateiname | XML-Dateiname |
|---|---|
| BCG_Package_RNIF1.1_3C7V01.00.zip | BCG_RNIF1.1_3C7V01.00.xml |
| BCG_Package_RNIFV02.00_3C7V01.00.zip | BCG_RNIFV02.00_3C7V01.00.xml |
| BCG_Package_RNSC1.0_RNIF1.1_3C7V01.00.zip | BCG_RNSC1.0_RNIF1.1_3C7V01.00.xml |
| BCG_Package_RNSC1.0_RNIFV02.00_3C7V01.00.zip | BCG_RNSC1.0_RNIFV02.00_3C7V01.00.xml |

### Inhalt der Richtlinienzuordnungen

Dieser Abschnitt listet den Inhalt der Richtlinienzuordnungen für **3C7 Notify of Self-Billing Invoice** auf:

- BCG_3C7SelfBillingInvoiceNotification_V01.00.xsd
- BCG_BusinessDescription_Types.xsd
- BCG_BusinessDescription_Types_V422.xsd
- BCG_BusinessTaxIdentifier_Types.xsd
- BCG_common.xsd
- BCG_common_V422.xsd
- BCG_ContactInformation_Types.xsd
- BCG_GlobalCountryCode.xsd
- BCG_GlobalCurrencyCode.xsd
- BCG_GlobalDocumentReferenceTypeCode.xsd
- BCG_GlobalDocumentTypeCode.xsd
- BCG_GlobalDocumentTypeCode_V422.xsd

- BCG_GlobalMonetaryAmountTypeCode.xsd
- BCG_GlobalPartnerClassificationCode.xsd
- BCG_GlobalPartnerRoleClassificationCode.xsd
- BCG_GlobalPaymentTermsCode.xsd
- BCG_GlobalProductUnitOfMeasureCode.xsd
- BCG_GlobalSaleTypeCode.xsd
- BCG_GlobalShipmentTermsCode.xsd
- BCG_GlobalShippingServiceLevelCode.xsd
- BCG_InvoiceChargeTypeCode.xsd
- BCG_NationalExportControlClassificationCode.xsd
- BCG_PartnerDescription_Types.xsd
- BCG_PhysicalAddress_Types.xsd
- BCG_string_len_0.xsd
- BCG_xml.xsd

## 3D8 Distribute Work in Process

Der folgende Abschnitt beschreibt den Inhalt des PIP **3D8 Distribute Work in Process**.

### Inhalt der Paketdatei

Die folgende Tabelle zeigt die ZIP-Dateien und entsprechenden XML-Dateien für den PIP **3D8 Distribute Work in Process**. Die Richtlinienzuordnungen, die für alle Versionen gleich sind, werden im nachfolgenden Abschnitt gezeigt.

*Tabelle 82. ZIP- und XML-Dateien für* **3D8 Distribute Work in Process**

| ZIP-Dateiname | XML-Dateiname |
|---|---|
| BCG_Package_RNIF1.1_3D8V01.00.zip | BCG_RNIF1.1_3D8V01.00.xml |
| BCG_Package_RNIFV02.00_3D8V01.00.zip | BCG_RNIFV02.00_3D8V01.00.xml |
| BCG_Package_RNSC1.0_RNIF1.1_3D8V01.00.zip | BCG_RNSC1.0_RNIF1.1_3D8V01.00.xml |
| BCG_Package_RNSC1.0_RNIFV02.00_3D8V01.00.zip | BCG_RNSC1.0_RNIFV02.00_3D8V01.00.xml |

### Inhalt der Richtlinienzuordnungen

Dieser Abschnitt listet den Inhalt der Richtlinienzuordnungen für **3D8 Distribute Work in Process** auf:

- BCG_3D8WorkInProcessNotification_V01.00.xsd
- BCG_BusinessDescription_Types.xsd
- BCG_BusinessTaxIdentifier_Types.xsd
- BCG_common.xsd
- BCG_ContactInformation_Types.xsd
- BCG_GlobalCountryCode.xsd
- BCG_GlobalDocumentReferenceTypeCode.xsd
- BCG_GlobalLotCode.xsd
- BCG_GlobalLotQuantityClassificationCode.xsd
- BCG_GlobalLotStatusCode.xsd
- BCG_GlobalPartnerClassificationCode.xsd

- BCG_GlobalPriorityCode.xsd
- BCG_GlobalProductUnitOfMeasureCode.xsd
- BCG_GlobalWorkInProcessLocationCode.xsd
- BCG_GlobalWorkInProcessPartTypeCode.xsd
- BCG_PartnerDescription_Types.xsd
- BCG_PhysicalAddress_Types.xsd
- BCG_string_len_0.xsd
- BCG_xml.xsd

## 4A1 Notify of Strategic Forecast

Der folgende Abschnitt beschreibt den Inhalt des PIP **4A1 Notify of Strategic Forecast**.

### Inhalt der Paketdatei

Die folgende Tabelle zeigt die ZIP-Dateien und entsprechenden XML-Dateien für den PIP **4A1 Notify of Strategic Forecast**. Die Richtlinienzuordnungen, die für alle Versionen gleich sind, werden im nachfolgenden Abschnitt gezeigt.

*Tabelle 83. ZIP- und XML-Dateien für '4A1 Notify of Strategic Forecast'*

| ZIP-Dateiname | XML-Dateiname |
|---|---|
| BCG_Package_RNIF1.1_4A1V02.00.zip | BCG_RNIF1.1_4A1V02.00.xml |
| BCG_Package_RNIFV02.00_4A1V02.00.zip | BCG_RNIFV02.00_4A1V02.00.xml |
| BCG_Package_RNSC1.0_RNIF1.1_4A1V02.00.zip | BCG_RNSC1.0_RNIF1.1_4A1V02.00.xml |
| BCG_Package_RNSC1.0_RNIFV02.00_4A1V02.00.zip | BCG_RNSC1.0_RNIFV02.00_4A1V02.00.xml |

### Inhalt der Richtlinienzuordnungen

Dieser Abschnitt listet den Inhalt der Richtlinienzuordnungen für **4A1 Notify of Strategic Forecast** auf:

- BCG_4A1StrategicForecastNotification_V02.00.xsd
- BCG_BusinessDescription_Types.xsd
- BCG_BusinessTaxIdentifier_Types.xsd
- BCG_common.xsd
- BCG_ContactInformation_Types.xsd
- BCG_GlobalCountryCode.xsd
- BCG_GlobalCurrencyCode.xsd
- BCG_GlobalForecastEventCode.xsd
- BCG_GlobalForecastIntervalCode.xsd
- BCG_GlobalForecastTypeCode.xsd
- BCG_GlobalPartnerClassificationCode.xsd
- BCG_GlobalPartnerReferenceTypeCode.xsd
- BCG_GlobalProductUnitOfMeasureCode.xsd
- BCG_PartnerDescription_Types.xsd
- BCG_PhysicalAddress_Types.xsd
- BCG_StrategicForecastQuantityTypeCode.xsd
- BCG_string_len_0.xsd
- BCG_xml.xsd

# 4A3 Notify of Threshold Release Forecast

Der folgende Abschnitt beschreibt den Inhalt des PIP **4A3 Notify of Threshold Release Forecast**.

## Inhalt der Paketdatei

Die folgende Tabelle zeigt die ZIP-Dateien und entsprechenden XML-Dateien für den PIP **4A3 Notify of Threshold Release Forecast**. Die Richtlinienzuordnungen, die für alle Versionen gleich sind, werden im nachfolgenden Abschnitt gezeigt.

*Tabelle 84. ZIP- und XML-Dateien für '4A3 Notify of Threshold Release Forecast'*

| ZIP-Dateiname | XML-Dateiname |
|---|---|
| BCG_Package_RNIF1.1_4A3V02.00.zip | BCG_RNIF1.1_4A3V02.00.xml |
| BCG_Package_RNIFV02.00_4A3V02.00.zip | BCG_RNIFV02.00_4A3V02.00.xml |
| BCG_Package_RNSC1.0_RNIF1.1_4A3V02.00.zip | BCG_RNSC1.0_RNIF1.1_4A3V02.00.xml |
| BCG_Package_RNSC1.0_RNIFV02.00_4A3V02.00.zip | BCG_RNSC1.0_RNIFV02.00_4A3V02.00.xml |

## Inhalt der Richtlinienzuordnungen

Dieser Abschnitt listet den Inhalt der Richtlinienzuordnungen für **4A3 Notify of Threshold Release Forecast** auf:

- BCG_4A3ThresholdReleaseForecastNotification_V02.00.xsd
- BCG_BusinessDescription_Types.xsd
- BCG_BusinessTaxIdentifier_Types.xsd
- BCG_common.xsd
- BCG_ContactInformation_Types.xsd
- BCG_GlobalCountryCode.xsd
- BCG_GlobalCurrencyCode.xsd
- BCG_GlobalForecastEventCode.xsd
- BCG_GlobalForecastIntervalCode.xsd
- BCG_GlobalForecastInventoryTypeCode.xsd
- BCG_GlobalForecastReferenceTypeCode.xsd
- BCG_GlobalPartnerClassificationCode.xsd
- BCG_GlobalPartnerReferenceTypeCode.xsd
- BCG_GlobalProductUnitOfMeasureCode.xsd
- BCG_OrderForecastQuantityTypeCode.xsd
- BCG_PartnerDescription_Types.xsd
- BCG_PhysicalAddress_Types.xsd
- BCG_string_len_0.xsd
- BCG_xml.xsd

# 4A4 Notify of Planning Release Forecast

Der folgende Abschnitt beschreibt den Inhalt des PIP **4A4 Notify of Planning Release Forecast**.

### Inhalt der Paketdatei

Die folgende Tabelle zeigt die ZIP-Dateien und entsprechenden XML-Dateien für den PIP **4A4 Notify of Planning Release Forecast**. Die Richtlinienzuordnungen, die für alle Versionen gleich sind, werden im nachfolgenden Abschnitt gezeigt.

*Tabelle 85. ZIP- und XML-Dateien für '4A4 Notify of Planning Release Forecast'*

| ZIP-Dateiname | XML-Dateiname |
|---|---|
| BCG_Package_RNIF1.1_4A4R02.00A.zip | BCG_RNIF1.1_4A4R02.00A.xml |
| BCG_Package_RNIFV02.00_4A4R02.00A.zip | BCG_RNIFV02.00_4A4R02.00A.xml |
| BCG_Package_RNSC1.0_RNIF1.1_4A4R02.00A.zip | BCG_RNSC1.0_RNIF1.1_4A4R02.00A.xml |
| BCG_Package_RNSC1.0_RNIFV02.00_4A4R02.00A.zip | BCG_RNSC1.0_RNIFV02.00_4A4R02.00A.xml |

### Inhalt der Richtlinienzuordnungen

Dieser Abschnitt listet den Inhalt der Richtlinienzuordnungen für **4A4 Notify of Planning Release Forecast** auf:

- BCG_4A4PlanningReleaseForecastNotification_R02.00A.xsd
- BCG_BusinessDescription_Types.xsd
- BCG_BusinessTaxIdentifier_Types.xsd
- BCG_common.xsd
- BCG_ContactInformation_Types.xsd
- BCG_GlobalCountryCode.xsd
- BCG_GlobalCurrencyCode.xsd
- BCG_GlobalForecastInventoryTypeCode.xsd
- BCG_GlobalForecastQuantityTypeCode_V422.xsd
- BCG_GlobalForecastReferenceTypeCode.xsd
- BCG_GlobalIntervalCode.xsd
- BCG_GlobalPartnerClassificationCode.xsd
- BCG_GlobalPartnerReferenceTypeCode.xsd
- BCG_GlobalProductUnitOfMeasureCode.xsd
- BCG_GlobalTransportEventCode.xsd
- BCG_PartnerDescription_Types.xsd
- BCG_PhysicalAddress_Types.xsd
- BCG_PhysicalAddress_Types_V422.xsd
- BCG_string_len_0.xsd
- BCG_xml.xsd

## 4A5 Notify of Forecast Reply

Der folgende Abschnitt beschreibt den Inhalt des PIP **4A5 Notify of Forecast Reply**.

### Inhalt der Paketdatei

Die folgende Tabelle zeigt die ZIP-Dateien und entsprechenden XML-Dateien für den PIP **4A5 Notify of Forecast Reply**. Die Richtlinienzuordnungen, die für alle Versionen gleich sind, werden im nachfolgenden Abschnitt gezeigt.

*Tabelle 86. ZIP- und XML-Dateien für '4A5 Notify of Forecast Reply'*

| ZIP-Dateiname | XML-Dateiname |
|---|---|
| BCG_Package_RNIF1.1_4A5V02.00.zip | BCG_RNIF1.1_4A5V02.00.xml |
| BCG_Package_RNIFV02.00_4A5V02.00.zip | BCG_RNIFV02.00_4A5V02.00.xml |
| BCG_Package_RNSC1.0_RNIF1.1_34A5V02.00.zip | BCG_RNSC1.0_RNIF1.1_34A5V02.00.xml |
| BCG_Package_RNSC1.0_RNIFV02.00_4A5V02.00.zip | BCG_RNSC1.0_RNIFV02.00_4A5V02.00.xml |

### Inhalt der Richtlinienzuordnungen

Dieser Abschnitt listet den Inhalt der Richtlinienzuordnungen für **4A5 Notify of Forecast Reply** auf:

- BCG_4A5ForecastReplyNotification_V02.00.xsd
- BCG_BusinessDescription_Types.xsd
- BCG_BusinessTaxIdentifier_Types.xsd
- BCG_common.xsd
- BCG_ContactInformation_Types.xsd
- BCG_ForecastReplyQuantityTypeCode.xsd
- BCG_GlobalCountryCode.xsd
- BCG_GlobalCurrencyCode.xsd
- BCG_GlobalForecastEventCode.xsd
- BCG_GlobalForecastIntervalCode.xsd
- BCG_GlobalForecastInventoryTypeCode.xsd
- BCG_GlobalForecastReferenceTypeCode.xsd
- BCG_GlobalForecastResponseCode.xsd
- BCG_GlobalForecastRevisionReasonCode.xsd
- BCG_GlobalPartnerClassificationCode.xsd
- BCG_GlobalPartnerReferenceTypeCode.xsd
- BCG_GlobalProductUnitOfMeasureCode.xsd
- BCG_PartnerDescription_Types.xsd
- BCG_PhysicalAddress_Types.xsd
- BCG_string_len_0.xsd
- BCG_xml.xsd

## 4B2 Notify of Shipment Receipt

Der folgende Abschnitt beschreibt den Inhalt des PIP **4B2 Notify of Shipment Receipt**.

### Inhalt der Paketdatei

Die folgende Tabelle zeigt die ZIP-Dateien und entsprechenden XML-Dateien für den PIP **4B2 Notify of Shipment Receipt**. Die Richtlinienzuordnungen, die für alle Versionen gleich sind, werden im nachfolgenden Abschnitt gezeigt.

*Tabelle 87. ZIP- und XML-Dateien für* **4B2 Notify of Shipment Receipt**

| ZIP-Dateiname | XML-Dateiname |
|---|---|
| BCG_Package_RNIF1.1_4B2V01.00.zip | BCG_RNIF1.1_4B2V01.00.xml |
| BCG_Package_RNIFV02.00_4B2V01.00.zip | BCG_RNIFV02.00_4B2V01.00.xml |
| BCG_Package_RNSC1.0_RNIF1.1_4B2V01.00.zip | BCG_RNSC1.0_RNIF1.1_4B2V01.00.xml |
| BCG_Package_RNSC1.0_RNIFV02.00_4B2V01.00.zip | BCG_RNSC1.0_RNIFV02.00_4B2V01.00.xml |

### Inhalt der Richtlinienzuordnungen

Dieser Abschnitt listet den Inhalt der Richtlinienzuordnungen für **4B2 Notify of Shipment Receipt** auf:

- BCG_4B2ShipmentReceiptNotification_V01.00.xsd
- BCG_BusinessDescription_Types.xsd
- BCG_BusinessTaxIdentifier_Types.xsd
- BCG_common.xsd
- BCG_ContactInformation_Types.xsd
- BCG_GlobalCountryCode.xsd
- BCG_GlobalDocumentReferenceTypeCode.xsd
- BCG_GlobalLotDiscrepancyReasonCode.xsd
- BCG_GlobalPartnerClassificationCode.xsd
- BCG_GlobalPartnerRoleClassificationCode.xsd
- BCG_GlobalProductUnitOfMeasureCode.xsd
- BCG_GlobalReceivingDiscrepancyCode.xsd
- BCG_GlobalReceivingDiscrepancyReasonCode.xsd
- BCG_GlobalSpecialFulfillmentRequestCode.xsd
- BCG_GlobalSpecialHandlingCode.xsd
- BCG_GlobalTrackingReferenceTypeCode.xsd
- BCG_PartnerDescription_Types.xsd
- BCG_PhysicalAddress_Types.xsd
- BCG_string_len_0.xsd
- BCG_xml.xsd

## 4B3 Notify of Consumption

Der folgende Abschnitt beschreibt den Inhalt des PIP **4B3 Notify of Consumption**.

### Inhalt der Paketdatei

Die folgende Tabelle zeigt die ZIP-Dateien und entsprechenden XML-Dateien für den PIP **4B3 Notify of Consumption**. Die Richtlinienzuordnungen, die für alle Versionen gleich sind, werden im nachfolgenden Abschnitt gezeigt.

*Tabelle 88. ZIP- und XML-Dateien für* **4B3 Notify of Consumption**

| ZIP-Dateiname | XML-Dateiname |
|---|---|
| BCG_Package_RNIF1.1_4B3V01.00.zip | BCG_RNIF1.1_4B3V01.00.xml |
| BCG_Package_RNIFV02.00_4B3V01.00.zip | BCG_RNIFV02.00_4B3V01.00.xml |
| BCG_Package_RNSC1.0_RNIF1.1_4B3V01.00.zip | BCG_RNSC1.0_RNIF1.1_4B3V01.00.xml |

*Tabelle 88. ZIP- und XML-Dateien für* **4B3 Notify of Consumption** *(Forts.)*

| ZIP-Dateiname | XML-Dateiname |
|---|---|
| BCG_Package_RNSC1.0_RNIFV02.00_4B3V01.00.zip | BCG_RNSC1.0_RNIFV02.00_4B3V01.00.xml |

### Inhalt der Richtlinienzuordnungen

Dieser Abschnitt listet den Inhalt der Richtlinienzuordnungen für **4B3 Notify of Consumption** auf:

- BCG_4B3ConsumptionNotification_V01.00.xsd
- BCG_BusinessDescription_Types.xsd
- BCG_BusinessDescription_Types_V422.xsd
- BCG_BusinessDescription_Types_V43.xsd
- BCG_BusinessTaxIdentifier_Types.xsd
- BCG_common.xsd
- BCG_common_V43.xsd
- BCG_ContactInformation_Types.xsd
- BCG_ContactInformation_Types_V422.xsd
- BCG_ContactInformation_Types_V43.xsd
- BCG_GlobalCountryCode.xsd
- BCG_GlobalCurrencyCode.xsd
- BCG_GlobalDocumentReferenceTypeCode_V43.xsd
- BCG_GlobalInventoryCode_V43.xsd
- BCG_GlobalPartnerClassificationCode_V422.xsd
- BCG_GlobalPartnerClassificationCode_V43.xsd
- BCG_GlobalProductUnitOfMeasureCode.xsd
- BCG_PartnerDescription_Types_V43.xsd
- BCG_PhysicalAddress_Types.xsd
- BCG_string_len_0.xsd
- BCG_xml.xsd

## 4C1 Distribute Inventory Report V02.01

Der folgende Abschnitt beschreibt den Inhalt für den PIP **4C1 Distribute Inventory Report V02.01**.

### Inhalt der Paketdatei

Die folgende Tabelle zeigt die ZIP-Dateien und entsprechenden XML-Dateien für den PIP **4C1 Distribute Inventory Report**. Die Richtlinienzuordnungen, die für alle Versionen gleich sind, werden im nachfolgenden Abschnitt gezeigt.

*Tabelle 89. ZIP- und XML-Dateien für* **4C1 Distribute Inventory Report**

| ZIP-Dateiname | XML-Dateiname |
|---|---|
| BCG_Package_RNIF1.1_4C1V02.01.zip | BCG_RNIF1.1_4C1V02.01.xml |
| BCG_Package_RNIFV02.00_4C1V02.01.zip | BCG_RNIFV02.00_4C1V02.01.xml |
| BCG_Package_RNSC1.0_RNIF1.1_4C1V02.01.zip | BCG_RNSC1.0_RNIF1.1_4C1V02.01.xml |
| BCG_Package_RNSC1.0_RNIFV02.00_4C1V02.01.zip | BCG_RNSC1.0_RNIFV02.00_4C1V02.01.xml |

### Inhalt der Richtlinienzuordnungen

Dieser Abschnitt listet den Inhalt der Richtlinienzuordnungen für **4C1 Distribute Inventory Report** auf:

- BCG_4C1InventoryReportNotification_V02.01.xsd
- BCG_BusinessDescription_Types.xsd
- BCG_BusinessTaxIdentifier_Types.xsd
- BCG_common.xsd
- BCG_common_V422.xsd
- BCG_ContactInformation_Types.xsd
- BCG_ContactInformation_Types_V422.xsd
- BCG_GlobalCountryCode.xsd
- BCG_GlobalDocumentReferenceTypeCode.xsd
- BCG_GlobalInventoryCode.xsd
- BCG_GlobalPartnerClassificationCode.xsd
- BCG_GlobalPartnerRoleClassificationCode.xsd
- BCG_GlobalProductUnitOfMeasureCode.xsd
- BCG_PhysicalAddress_Types.xsd
- BCG_PhysicalAddress_Types_V422.xsd
- BCG_string_len_0.xsd
- BCG_xml.xsd

## 4C1 Distribute Inventory Report V02.03

Im folgenden Abschnitt wird der Inhalt des PIP **4C1 Distribute Inventory Report V02.03** beschrieben.

### Inhalt der Paketdatei

Die folgende Tabelle zeigt die ZIP-Dateien und entsprechenden XML-Dateien für den PIP **4C1 Distribute Inventory Report** an. Die Richtlinienzuordnungen, die für alle Versionen gleich sind, werden im nachfolgenden Abschnitt dargestellt.

*Tabelle 90. ZIP- und XML-Dateien für* **4C1 Distribute Inventory Report**

| ZIP-Dateiname | XML-Dateiname |
|---|---|
| BCG_Package_RNIF1.1_4C1V02.03.zip | BCG_RNIF1.1_4C1V02.03.xml |
| BCG_Package_RNIFV02.00_4C1V02.03.zip | BCG_RNIFV02.00_4C1V02.03.xml |
| BCG_Package_RNSC1.0_RNIF1.1_4C1V02.03.zip | BCG_RNSC1.0_RNIF1.1_4C1V02.03.xml |
| BCG_Package_RNSC1.0_RNIFV02.00_4C1V02.03.zip | BCG_RNSC1.0_RNIFV02.00_4C1V02.03.xml |

### Inhalt der Richtlinienzuordnungen

Dieser Abschnitt listet den Inhalt der Richtlinienzuordnungen für **4C1 Distribute Inventory Report** auf:

- BCG_4C1InventoryReportNotification_V02.03.xsd
- BCG_BusinessDescription_Types.xsd
- BCG_BusinessTaxIdentifier_Types.xsd
- BCG_common.xsd
- BCG_ContactInformation_Types.xsd

- BCG_GlobalCountryCode.xsd
- BCG_GlobalDocumentReferenceTypeCode.xsd
- BCG_GlobalInventoryCode.xsd
- BCG_GlobalPartnerClassificationCode.xsd
- BCG_GlobalPartnerRoleClassificationCode.xsd
- BCG_GlobalProductUnitOfMeasureCode.xsd
- BCG_PhysicalAddress_Types.xsd
- BCG_string_len_0.xsd
- BCG_xml.xsd

## 5C1 Distribute Product List

Der folgende Abschnitt beschreibt den Inhalt für den PIP **5C1 Distribute Product List**.

### Inhalt der Paketdatei

Die folgende Tabelle zeigt die ZIP-Dateien und entsprechenden XML-Dateien für den PIP **5C1 Distribute Product List**. Die Richtlinienzuordnungen, die für alle Versionen gleich sind, werden im nachfolgenden Abschnitt gezeigt.

*Tabelle 91. ZIP- und XML-Dateien für* **5C1 Distribute Product List**

| ZIP-Dateiname | XML-Dateiname |
|---|---|
| BCG_Package_RNIF1.1_5C1V01.00.zip | BCG_RNIF1.1_5C1V01.00.xml |
| BCG_Package_RNIFV02.00_5C1V01.00.zip | BCG_RNIFV02.00_5C1V01.00.xml |
| BCG_Package_RNSC1.0_RNIF1.1_5C1V01.00.zip | BCG_RNSC1.0_RNIF1.1_5C1V01.00.xml |
| BCG_Package_RNSC1.0_RNIFV02.00_5C1V01.00.zip | BCG_RNSC1.0_RNIFV02.00_5C1V01.00.xml |

### Inhalt der Richtlinienzuordnungen

Dieser Abschnitt listet den Inhalt der Richtlinienzuordnungen für **5C1 Distribute Product List** auf:

- BCG_5C1ProductListNotification_V01.00.xsd
- BCG_BusinessDescription_Types.xsd
- BCG_BusinessTaxIdentifier_Types.xsd
- BCG_common.xsd
- BCG_ContactInformation_Types.xsd
- BCG_GlobalCountryCode.xsd
- BCG_GlobalCurrencyCode.xsd
- BCG_GlobalPartnerClassificationCode.xsd
- BCG_GlobalPartnerRoleClassificationCode.xsd
- BCG_GlobalPriceTypeCode.xsd
- BCG_PartnerDescription_Types.xsd
- BCG_PhysicalAddress_Types.xsd
- BCG_string_len_0.xsd
- BCG_xml.xsd

# 5C2 Request Design Registration

Der folgende Abschnitt beschreibt den Inhalt des PIP **5C2 Request Design Registration**.

## Inhalt der Paketdatei

Die folgende Tabelle zeigt die ZIP-Dateien und entsprechenden XML-Dateien für den PIP **5C2 Request Design Registration**. Die Richtlinienzuordnungen, die für alle Versionen gleich sind, werden im nachfolgenden Abschnitt gezeigt.

*Tabelle 92. ZIP- und XML-Dateien für* **5C2 Request Design Registration**

| ZIP-Dateiname | XML-Dateiname |
|---|---|
| BCG_Package_RNIF1.1_5C2V01.00.zip | BCG_RNIF1.1_5C2V01.00.xml |
| BCG_Package_RNIFV02.00_5C2V01.00.zip | BCG_RNIFV02.00_5C2V01.00.xml |
| BCG_Package_RNSC1.0_RNIF1.1_5C2V01.00.zip | BCG_RNSC1.0_RNIF1.1_5C2V01.00.xml |
| BCG_Package_RNSC1.0_RNIFV02.00_5C2V01.00.zip | BCG_RNSC1.0_RNIFV02.00_5C2V01.00.xml |

## Inhalt der Richtlinienzuordnungen

Dieser Abschnitt listet den Inhalt der Richtlinienzuordnungen für **5C2 Request Design Registration** auf:

- BCG_5C2DesignRegistrationConfirmation_V01.00.xsd
- BCG_5C2DesignRegistrationRequest_V01.00.xsd
- BCG_BusinessDescription_Types.xsd
- BCG_common.xsd
- BCG_common_V422.xsd
- BCG_common_V43.xsd
- BCG_ContactInformation_Types.xsd
- BCG_DesignWinStatusReasonCode_V43.xsd
- BCG_GlobalAttachmentDescriptionCode_V422.xsd
- BCG_GlobalCountryCode.xsd
- BCG_GlobalCurrencyCode.xsd
- BCG_GlobalDocumentReferenceTypeCode.xsd
- BCG_GlobalMimeTypeQualifierCode_V43.xsd
- BCG_GlobalMonetaryAmountTypeCode.xsd
- BCG_GlobalPartnerClassificationCode_V43.xsd
- BCG_GlobalPartnerRoleClassificationCode_V43.xsd
- BCG_GlobalPriceTypeCode_V43.xsd
- BCG_GlobalRegistrationComplexityLevelCode.xsd
- BCG_GlobalRegistrationInvolvementLevelCode.xsd
- BCG_InvoiceChargeTypeCode_V422.xsd
- BCG_PartnerDescription_Types.xsd
- BCG_PartnerDescription_Types_V43.xsd
- BCG_PhysicalAddress_Types.xsd
- BCG_string_len_0.xsd
- BCG_xml.xsd

## 5C4 Distribute Registration Status

Der folgende Abschnitt beschreibt den Inhalt des PIP **5C4 Distribute Registration Status**.

### Inhalt der Paketdatei

Die folgende Tabelle zeigt die ZIP-Dateien und entsprechenden XML-Dateien für den PIP **5C4 Distribute Registration Status**. Die Richtlinienzuordnungen, die für alle Versionen gleich sind, werden im nachfolgenden Abschnitt gezeigt.

*Tabelle 93. ZIP- und XML-Dateien für* **5C4 Distribute Registration Status**

| ZIP-Dateiname | XML-Dateiname |
|---|---|
| BCG_Package_RNIF1.1_5C4V01.02.zip | BCG_RNIF1.1_5C4V01.02.xml |
| BCG_Package_RNIFV02.00_5C4V01.02.zip | BCG_RNIFV02.00_5C4V01.02.xml |
| BCG_Package_RNSC1.0_RNIF1.1_5C4V01.023.zip | BCG_RNSC1.0_RNIF1.1_5C4V01.023.xml |
| BCG_Package_RNSC1.0_RNIFV02.00_5C4V01.02.zip | BCG_RNSC1.0_RNIFV02.00_5C4V01.02.xml |

### Inhalt der Richtlinienzuordnungen

Dieser Abschnitt listet den Inhalt der Richtlinienzuordnungen für **5C4 Distribute Registration Status** auf:

- BCG_5C4RegistrationStatusNotification_V01.02.xsd
- BCG_BusinessDescription_Types.xsd
- BCG_BusinessTaxIdentifier_Types.xsd
- BCG_common.xsd
- BCG_ContactInformation_Types.xsd
- BCG_GlobalCountryCode.xsd
- BCG_GlobalPartnerClassificationCode.xsd
- BCG_GlobalPartnerRoleClassificationCode.xsd
- BCG_GlobalRegistrationComplexityLevelCode.xsd
- BCG_GlobalRegistrationInvolvementLevelCode.xsd
- BCG_PartnerDescription_Types.xsd
- BCG_PhysicalAddress_Types.xsd
- BCG_string_len_0.xsd
- BCG_xml.xsd

## 5D1 Request Ship From Stock And Debit Authorization

Der folgende Abschnitt beschreibt den Inhalt des PIP **5D1 Request Ship From Stock And Debit Authorization**.

### Inhalt der Paketdatei

Die folgende Tabelle zeigt die ZIP-Dateien und entsprechenden XML-Dateien für den PIP **5D1 Request Ship From Stock And Debit Authorization**. Die Richtlinienzuordnungen, die für alle Versionen gleich sind, werden im nachfolgenden Abschnitt gezeigt.

*Tabelle 94. ZIP- und XML-Dateien für* **5D1 Request Ship From Stock And Debit Authorization**

| ZIP-Dateiname | XML-Dateiname |
|---|---|
| BCG_Package_RNIF1.1_5D1V01.00.zip | BCG_RNIF1.1_5D1V01.00.xml |
| BCG_Package_RNIFV02.00_5D1V01.00.zip | BCG_RNIFV02.00_5D1V01.00.xml |
| BCG_Package_RNSC1.0_RNIF1.1_5D1V01.00.zip | BCG_RNSC1.0_RNIF1.1_5D1V01.00.xml |
| BCG_Package_RNSC1.0_RNIFV02.00_5D1V01.00.zip | BCG_RNSC1.0_RNIFV02.00_5D1V01.00.xml |

### Inhalt der Richtlinienzuordnungen

Dieser Abschnitt listet den Inhalt der Richtlinienzuordnungen für **5D1 Request Ship From Stock And Debit Authorization** auf:

- BCG_5D1ShipFromStockAndDebitAuthorizationConfirmation_V01.00.xsd
- BCG_5D1ShipFromStockAndDebitAuthorizationRequest_V01.00.xsd
- BCG_BusinessDescription_Types.xsd
- BCG_BusinessTaxIdentifier_Types.xsd
- BCG_common.xsd
- BCG_ContactInformation_Types.xsd
- BCG_GlobalCountryCode.xsd
- BCG_GlobalCurrencyCode.xsd
- BCG_GlobalDocumentReferenceTypeCode.xsd
- BCG_GlobalPartnerClassificationCode.xsd
- BCG_GlobalPartnerRoleClassificationCode.xsd
- BCG_GlobalPriceTypeCode.xsd
- BCG_GlobalProductUnitOfMeasureCode.xsd
- BCG_GlobalShipFromStockAndDebitAuthorizationRejectionCode.xsd
- BCG_PartnerDescription_Types.xsd
- BCG_PhysicalAddress_Types.xsd
- BCG_string_len_0.xsd
- BCG_xml.xsd

## 6C1 Query Service Entitlement

Der folgende Abschnitt beschreibt den Inhalt des PIP **6C1 Query Service Entitlement**.

### Inhalt der Paketdatei

Die folgende Tabelle zeigt die ZIP-Dateien und entsprechenden XML-Dateien für den PIP **6C1 Query Service Entitlement**. Die Richtlinienzuordnungen, die für alle Versionen gleich sind, werden im nachfolgenden Abschnitt gezeigt.

*Tabelle 95. ZIP- und XML-Dateien für* **6C1 Query Service Entitlement**

| ZIP-Dateiname | XML-Dateiname |
|---|---|
| BCG_Package_RNIF1.1_6C1V01.00.zip | BCG_RNIF1.1_6C1V01.00.xml |
| BCG_Package_RNIFV02.00_6C1V01.00.zip | BCG_RNIFV02.00_6C1V01.00.xml |
| BCG_Package_RNSC1.0_RNIF1.1_6C1V01.00.zip | BCG_RNSC1.0_RNIF1.1_6C1V01.00.xml |
| BCG_Package_RNSC1.0_RNIFV02.00_6C1V01.00.zip | BCG_RNSC1.0_RNIFV02.00_6C1V01.00.xml |

### Inhalt der Richtlinienzuordnungen

Dieser Abschnitt listet den Inhalt der Richtlinienzuordnungen für **6C1 Query Service Entitlement** auf:

- BCG_6C1ServiceEntitlementQuery_V01.00.xsd
- BCG_6C1ServiceEntitlementStatusResponse_V01.00.xsd
- BCG_common_V43.xsd
- BCG_ContactInformation_Types.xsd
- BCG_ContactInformation_Types_V43.xsd
- BCG_GlobalCurrencyCode.xsd
- BCG_GlobalNotificationCode_V43.xsd
- BCG_GlobalPartnerClassificationCode_V43.xsd
- BCG_GlobalPaymentTypeCode_V43.xsd
- BCG_GlobalServiceDeliveryMethodCode_V43.xsd
- BCG_GlobalShippingServiceLevelCode.xsd
- BCG_GlobalWarrantyMethodCode_V43.xsd
- BCG_GlobalWarrantyProgramCode_V43.xsd
- BCG_GlobalWarrantyTypeCode_V43.xsd
- BCG_PartnerDescription_Types_V43.xsd
- BCG_string_len_0.xsd
- BCG_xml.xsd

## 6C2 Request Warranty Claim

Der folgende Abschnitt beschreibt den Inhalt des PIP **6C2 Request Warranty Claim**.

### Inhalt der Paketdatei

Die folgende Tabelle zeigt die ZIP-Dateien und entsprechenden XML-Dateien für den PIP **6C2 Request Warranty Claim**. Die Richtlinienzuordnungen, die für alle Versionen gleich sind, werden im nachfolgenden Abschnitt gezeigt.

*Tabelle 96. ZIP- und XML-Dateien für* **6C2 Request Warranty Claim**

| ZIP-Dateiname | XML-Dateiname |
|---|---|
| BCG_Package_RNIF1.1_6C2V01.00.zip | BCG_RNIF1.1_6C2V01.00.xml |
| BCG_Package_RNIFV02.00_6C2V01.00.zip | BCG_RNIFV02.00_6C2V01.00.xml |
| BCG_Package_RNSC1.0_RNIF1.1_6C2V01.00.zip | BCG_RNSC1.0_RNIF1.1_6C2V01.00.xml |
| BCG_Package_RNSC1.0_RNIFV02.00_6C2V01.00.zip | BCG_RNSC1.0_RNIFV02.00_6C2V01.00.xml |

### Inhalt der Richtlinienzuordnungen

Dieser Abschnitt listet den Inhalt der Richtlinienzuordnungen für **6C2 Request Warranty Claim** auf:

- BCG_6C2WarrantyClaimConfirmation_V01.00.xsd
- BCG_6CWarrantyClaimRequest_V01.00.xsd
- BCG_common.xsd
- BCG_ContactInformation_Types.xsd
- BCG_GlobalCurrencyCode.xsd

- BCG_GlobalDocumentReferenceTypeCode.xsd
- BCG_GlobalFailureTypeCode_V43.xsd
- BCG_GlobalOperatingSystemCode_V43.xsd
- BCG_GlobalPartnerClassificationCode_V43.xsd
- BCG_GlobalPartnerRoleClassificationCode_V43.xsd
- BCG_GlobalPaymentTypeCode_V43.xsd
- BCG_GlobalServiceDeliveryMethodCode_V43.xsd
- BCG_GlobalWarrantyTypeCode_V43.xsd
- BCG_PartnerDescription_Types_V43.xsd
- BCG_string_len_0.xsd
- BCG_xml.xsd

## 7B1 Distribute Work in Process

Der folgende Abschnitt beschreibt den Inhalt des PIP **7B1 Distribute Work in Process**.

### Inhalt der Paketdatei

Die folgende Tabelle zeigt die ZIP-Dateien und entsprechenden XML-Dateien für den PIP **7B1 Distribute Work in Process**. Die Richtlinienzuordnungen, die für alle Versionen gleich sind, werden im nachfolgenden Abschnitt gezeigt.

*Tabelle 97. ZIP- und XML-Dateien für* **7B1 Distribute Work in Process**

| ZIP-Dateiname | XML-Dateiname |
|---|---|
| BCG_Package_RNIF1.1_7B1V01.00.zip | BCG_RNIF1.1_7B1V01.00.xml |
| BCG_Package_RNIFV02.00_37B1V01.00.zip | BCG_RNIFV02.00_37B1V01.00.xml |
| BCG_Package_RNSC1.0_RNIF1.1_7B1V01.00.zip | BCG_RNSC1.0_RNIF1.1_7B1V01.00.xml |
| BCG_Package_RNSC1.0_RNIFV02.00_7B1V01.00.zip | BCG_RNSC1.0_RNIFV02.00_7B1V01.00.xml |

### Inhalt der Richtlinienzuordnungen

Dieser Abschnitt listet den Inhalt der Richtlinienzuordnungen für **7B1 Distribute Work in Process** auf:

- BCG_7B1WorkInProcessNotification_V01.00.xsd
- BCG_BusinessDescription_Types.xsd
- BCG_BusinessTaxIdentifier_Types.xsd
- BCG_common.xsd
- BCG_ContactInformation_Types.xsd
- BCG_GlobalChangeReasonCode.xsd
- BCG_GlobalCountryCode.xsd
- BCG_GlobalDocumentReferenceTypeCode.xsd
- BCG_GlobalEquipmentTypeCode.xsd
- BCG_GlobalLotCode.xsd
- BCG_GlobalLotQuantityClassificationCode.xsd
- BCG_GlobalLotStatusCode.xsd
- BCG_GlobalPartnerClassificationCode.xsd
- BCG_GlobalPartnerRoleClassificationCode.xsd

- BCG_GlobalPriorityCode.xsd
- BCG_GlobalProductUnitOfMeasureCode.xsd
- BCG_GlobalWorkInProcessLocationCode.xsd
- BCG_GlobalWorkInProcessPartTypeCode.xsd
- BCG_GlobalWorkInProcessQuantityChangeCode.xsd
- BCG_GlobalWorkInProcessTypeCode.xsd
- BCG_PartnerDescription_Types.xsd
- BCG_PhysicalAddress_Types.xsd
- BCG_string_len_0.xsd
- BCG_xml.xsd

## 7B5 Notify Of Manufacturing Work Order

Der folgende Abschnitt beschreibt den Inhalt des PIP **7B5 Notify Of Manufacturing Work Order**.

### Inhalt der Paketdatei

Die folgende Tabelle zeigt die ZIP-Dateien und entsprechenden XML-Dateien für den PIP **7B5 Notify Of Manufacturing Work Order**. Die Richtlinienzuordnungen, die für alle Versionen gleich sind, werden im nachfolgenden Abschnitt gezeigt.

*Tabelle 98. ZIP- und XML-Dateien für* **7B5 Notify Of Manufacturing Work Order**

| ZIP-Dateiname | XML-Dateiname |
|---|---|
| BCG_Package_RNIF1.1_7B5V01.00.zip | BCG_RNIF1.1_7B5V01.00.xml |
| BCG_Package_RNIFV02.00_7B5V01.00.zip | BCG_RNIFV02.00_7B5V01.00.xml |
| BCG_Package_RNSC1.0_RNIF1.1_7B5V01.00.zip | BCG_RNSC1.0_RNIF1.1_7B5V01.00.xml |
| BCG_Package_RNSC1.0_RNIFV02.00_7B5V01.00.zip | BCG_RNSC1.0_RNIFV02.00_7B5V01.00.xml |

### Inhalt der Richtlinienzuordnungen

Dieser Abschnitt listet den Inhalt der Richtlinienzuordnungen für **7B5 Notify Of Manufacturing Work Order** auf:

- BCG_7B5NotifyOfManufacturingWorkOrder_V01.00.xsd
- BCG_BusinessDescription_Types.xsd
- BCG_BusinessTaxIdentifier_Types.xsd
- BCG_common.xsd
- BCG_ContactInformation_Types.xsd
- BCG_GlobalAttachmentDescriptionCode_V422.xsd
- BCG_GlobalBusinessActionCode_V422.xsd
- BCG_GlobalChangeReasonCode.xsd
- BCG_GlobalCountryCode.xsd
- BCG_GlobalDevicePackageTypeCode_V422.xsd
- BCG_GlobalDocumentReferenceTypeCode.xsd
- BCG_GlobalLineItemStatusCode.xsd
- BCG_GlobalLotCode.xsd
- BCG_GlobalMimeTypeQualifierCode_V422.xsd
- BCG_GlobalPackageTypeCode.xsd

- BCG_GlobalPartnerClassificationCode.xsd
- BCG_GlobalPartnerRoleClassificationCode.xsd
- BCG_GlobalPhysicalUnitOfMeasureCode.xsd
- BCG_GlobalPriorityCode.xsd
- BCG_GlobalProductUnitOfMeasureCode.xsd
- BCG_GlobalWorkInProcessLocationCode.xsd
- BCG_PartnerDescription_Types.xsd
- BCG_PhysicalAddress_Types.xsd
- BCG_string_len_0.xsd
- BCG_xml.xsd

## 7B6 Notify Of Manufacturing Work Order Reply

Der folgende Abschnitt beschreibt den Inhalt des PIP **7B6 Notify Of Manufacturing Work Order Reply**.

### Inhalt der Paketdatei

Die folgende Tabelle zeigt die ZIP-Dateien und entsprechenden XML-Dateien für den PIP **7B6 Notify Of Manufacturing Work Order Reply**. Die Richtlinienzuordnungen, die für alle Versionen gleich sind, werden im nachfolgenden Abschnitt gezeigt.

*Tabelle 99. ZIP- und XML-Dateien für* **7B6 Notify Of Manufacturing Work Order Reply**

| ZIP-Dateiname | XML-Dateiname |
|---|---|
| BCG_Package_RNIF1.1_7B6V01.00.zip | BCG_RNIF1.1_7B6V01.00.xml |
| BCG_Package_RNIFV02.00_7B6V01.00.zip | BCG_RNIFV02.00_7B6V01.00.xml |
| BCG_Package_RNSC1.0_RNIF1.1_7B6V01.00.zip | BCG_RNSC1.0_RNIF1.1_7B6V01.00.xml |
| BCG_Package_RNSC1.0_RNIFV02.00_7B6V01.00.zip | BCG_RNSC1.0_RNIFV02.00_7B6V01.00.xml |

### Inhalt der Richtlinienzuordnungen

Dieser Abschnitt listet den Inhalt der Richtlinienzuordnungen für **7B6 Notify Of Manufacturing Work Order Reply** auf:

- BCG_7B6NotifyOfManufacturingWorkOrderReply_V01.00.xsd
- BCG_BusinessDescription_Types.xsd
- BCG_BusinessTaxIdentifier_Types.xsd
- BCG_common.xsd
- BCG_ContactInformation_Types.xsd
- BCG_GlobalChangeReasonCode.xsd
- BCG_GlobalCountryCode.xsd
- BCG_GlobalDocumentReferenceTypeCode.xsd
- BCG_GlobalLineItemStatusCode.xsd
- BCG_GlobalPartnerClassificationCode.xsd
- BCG_GlobalPartnerRoleClassificationCode.xsd
- BCG_GlobalProductUnitOfMeasureCode.xsd
- BCG_PartnerDescription_Types.xsd
- BCG_PhysicalAddress_Types.xsd
- BCG_string_len_0.xsd
- BCG_xml.xsd

# Kapitel 22. Zusätzliche CIDX-Informationen

Dieser Anhang enthält zusätzliche Informationen zur CIDX-Unterstützung. Er behandelt die folgenden Themen:

## Unterstützung für CIDX-Prozessaktivierung

CIDX stellt zwei Mechanismen zur Prozessaktivierung bereit:

- **Nachrichtenbasierte Aktivierung:** Die Dokumentverknüpfung basiert auf <RequestingDocumentIdentifier> und <ThisDocumentIdentifier>.
- **Framework-basierte Aktivierung:** Die Dokumentverknüpfung basiert auf der Service-Header-Semantik von RNIF 1.1.

Bei nachrichtenbasierter Aktivierung sind für ChemXML-Transaktionen Einzelaktions-PIP-Pakete erforderlich. Bei Framework-basierter Aktivierung sind für ChemXML-Transaktionen Doppelaktions-PIP-Pakete erforderlich. WebSphere Partner Gateway unterstützt beide Formen der Prozessaktivierung. WebSphere Partner Gateway stellt Einzelaktions-PIP-Pakete für "E41 Order Create" und "E42 Order Response" zur Verfügung.

## CIDX-Dokumentdefinitionspakete erstellen

Zur Unterstützung weiterer CIDX-Nachrichten müssen Sie möglicherweise eigene CIDX-Nachrichten erstellen. Die Vorgehensweise für die Erstellung neuer CIDX-Dokumentdefinitionspakete entspricht der Vorgehensweise bei RosettaNet.

Weitere Informationen zu RosettaNet finden Sie in Kapitel 21, „Zusätzliche RosettaNet-Informationen”, auf Seite 379.

# Kapitel 23. Attribute

In diesem Anhang werden die Attribute beschrieben, die Sie über Community Console festlegen können. Die folgenden Attribute werden beschrieben:

- „EDI-Attribute"
- „AS-Attribute" auf Seite 451
- „RosettaNet-Attribute" auf Seite 456
- „Backend Integration-Attribut" auf Seite 459
- „ebMS-Attribute" auf Seite 459
- „Allgemeine Attribute" auf Seite 468
- „OpenPGP-Attribute" auf Seite 470

## EDI-Attribute

Dieser Abschnitt enthält eine Beschreibung der EDI-Attribute, die Sie verwenden können, während Sie Ihre EDI-Austauschvorgänge konfigurieren. Einige dieser Attribute sind in der Steuerzeichenfolge vordefiniert, die die Transformationszuordnung darstellt, die dem EDI-Dokument zugeordnet ist. Die in der Steuerzeichenfolge festgelegten Werte (auf dem Data Interchange Services-Client) überschreiben jeden Wert, den Sie in Community Console eingeben.

### Attribute für Umschlagsprofil

Sie können verschiedene Attribute für ein EDI-Umschlagsprofil festlegen. Die verfügbaren Attribute hängen vom EDI-Typ ab. Im Allgemeinen entsprechen die Attribute einem EDI-Standard und die zulässigen Werte hängen vom EDI-Standard ab, den das Umschlagsprofil darstellt.

Für keines der Attribute ist ein Wert erforderlich. Für einige der Attribute wird ein Standardwert verwendet, wenn Sie keinen Wert eingeben. Die Tabellen in diesem Abschnitt listen die Attribute, denen Standardwerte zugeordnet sind, und deren Standardwerte auf.

**Anmerkung:** Die Merkmale des Umschlagsprofils, die nicht aufgelistet sind, verfügen über keine Standardwerte. Der von Ihnen angegebene Textwert wird verwendet, wenn er nicht von generischen oder spezifischen Umschlagsmerkmalen überschrieben werden, die in der Zuordnung oder in einer Verbindung festgelegt sind.

#### X12-Attribute

Die Tabellen in diesem Abschnitt listen die X12-Attribute auf, für die Standardwerte bereitgestellt sind.

##### Allgemeine Attribute

Tabelle 100 auf Seite 438 listet die allgemeinen Attribute auf, für die Standardwerte bereitgestellt werden.

*Tabelle 100. Allgemeine Attribute*

| Feldname | Erforderlich | Beschreibung | Standardwert |
|---|---|---|---|
| INTCTLLEN (Länge der Austausch-kontrollnummer) | Nein | Definiert eine bestimmte Länge für die Austauschkontrollnummer. Falls Sie einen Wert eingeben, muss dieser eine ganze Zahl sein.<br><br>Wenn Sie keinen Wert eingeben, wird die Standardlänge verwendet. | 9 |
| GRPCTLLEN (Länge der Gruppenkontrollnummer) | Nein | Definiert eine bestimmte Länge für die Gruppenkontrollnummer. Falls Sie einen Wert eingeben, muss dieser eine ganze Zahl sein.<br><br>Wenn Sie keinen Wert eingeben, wird die Standardlänge verwendet. | 9 |
| TRXCTLLEN (Länge der Transaktions-kontrollnummer) | Nein | Definiert eine bestimmte Länge für die Transaktionskontrollnummer. Falls Sie einen Wert eingeben, muss dieser eine ganze Zahl sein.<br><br>Wenn Sie keinen Wert eingeben, wird die Standardlänge verwendet. | 9 |
| ENVTYPE (Umschlagstyp) | Nein | Dieses Attribut wird nicht vom Benutzer festgelegt, sondern vom Umschlagsprofiltyp abgeleitet, der erstellt wird. | X12 |
| MAXDOCS (Max. Anzahl an Transaktionen) | Nein | Maximale Anzahl an Transaktionen in einem Umschlag. Falls Sie einen Wert eingeben, muss dieser eine ganze Zahl sein. | Keine maximale Anzahl |
| CTLNUMFLAG (Kontrollnummern nach Transaktions-ID) | Nein | **Ja** gibt an, dass separate Gruppen mit Kontrollnummern auf der Basis des EDI-Transaktionstyps aufbewahrt werden.<br><br>**Nein** gibt an, dass eine allgemeine Gruppe mit Kontrollnummern für jeden EDI-Transaktionstyp verwendet werden soll. | Nein |

## Austauschattribute

Es sind keine X12-Austauschattribute erforderlich und die Attribute verfügen über keine Standardwerte.

*Tabelle 101. Gruppenattribute*

| Feldname | Erforderlich | Beschreibung | Standardwert |
|---|---|---|---|
| GS01 (ID der funktionalen Gruppe) | Nein | Die Gruppen-ID. | Der Standardwert kommt aus dem Header der Steuerzeichenfolge. Sie können diesen Wert auf dem Data Interchange Services-Client anzeigen, indem Sie sich die Spalte **Funktionsgruppe** auf der Seite **EDI-Dokumentdefinitionen** ansehen. |
| GS08 (Gruppenversion) | Nein | Die Gruppenversion. | Der Standardwert gilt pro Standard. |

## Gruppenattribute

Tabelle 101 listet die Gruppenattribute auf, für die Standardwerte bereitgestellt sind.

### Transaktion, Attribute

Es sind keine Transaktionsattribute erforderlich. Die Attribute verfügen über keine Standardwerte.

## UCS-Attribute

Dieser Abschnitt listet auf, ob Standardwerte auf einen UCS-Austausch, eine UCS-Gruppe und eine UCS-Transaktion angewendet werden.

### Allgemeine Attribute

Tabelle 102 listet die allgemeinen Attribute auf, für die Standardwerte bereitgestellt werden.

*Tabelle 102. Allgemeine Attribute*

| Feldname | Erforderlich | Beschreibung | Standardwert |
|---|---|---|---|
| INTCTLLEN (Länge der Austausch-kontrollnummer) | Nein | Definiert eine bestimmte Länge für die Austauschkontrollnummer. Falls Sie einen Wert eingeben, muss dieser eine ganze Zahl sein.<br><br>Wenn Sie keinen Wert eingeben, wird die Standardlänge verwendet. | 5 |
| GRPCTLLEN (Länge der Gruppenkontrollnummer) | Nein | Definiert eine bestimmte Länge für die Gruppenkontrollnummer. Falls Sie einen Wert eingeben, muss dieser eine ganze Zahl sein.<br><br>Wenn Sie keinen Wert eingeben, wird die Standardlänge verwendet. | 9 |
| TRXCTLLEN (Länge der Transaktions-kontrollnummer) | Nein | Definiert eine bestimmte Länge für die Transaktionskontrollnummer. Falls Sie einen Wert eingeben, muss dieser eine ganze Zahl sein.<br><br>Wenn Sie keinen Wert eingeben, wird die Standardlänge verwendet. | 9 |
| ENVTYPE (Umschlagstyp) | Nein | Dieses Attribut wird nicht vom Hubadmin festgelegt, sondern wird von dem Umschlagsprofiltyp abgeleitet, der erstellt wird. | UCS |
| MAXDOCS (Max. Anzahl an Transaktionen) | Nein | Maximale Anzahl an Transaktionen in einem Umschlag. Falls Sie einen Wert eingeben, muss dieser eine ganze Zahl sein. | Keine maximale Anzahl |
| CTLNUMFLAG (Kontrollnummern nach Transaktions-ID) | Nein | **Ja** gibt an, dass separate Gruppen mit Kontrollnummern auf der Basis des EDI-Transaktionstyps aufbewahrt werden.<br><br>**Nein** gibt an, dass eine allgemeine Gruppe mit Kontrollnummern für jeden EDI-Transaktionstyp verwendet werden soll. | Nein |

### Austauschattribute

Es sind keine Austauschattribute erforderlich. Die Attribute verfügen über keine Standardwerte.

### Gruppenattribute

Tabelle 103 listet die Gruppenattribute auf, für die Standardwerte bereitgestellt sind.

*Tabelle 103. Gruppenattribute*

| Feldname | Erforderlich | Beschreibung | Standardwert |
|---|---|---|---|
| GS01 (ID der funktionalen Gruppe) | Nein | Die Gruppen-ID. | Der Standardwert kommt aus dem Header der Steuerzeichenfolge. Sie können diesen Wert auf dem Data Interchange Services-Client anzeigen, indem Sie sich die Spalte **Funktionsgruppe** auf der Seite **EDI-Dokumentdefinitionen** ansehen. |
| GS08 (Gruppenversion) | Nein | Die Gruppenversion. | Der Standardwert gilt pro Standard. |

### Transaktion, Attribute

Es sind keine Transaktionsattribute erforderlich. Die Attribute verfügen über keine Standardwerte.

## EDIFACT-Attribute

Dieser Abschnitt listet auf, ob Standardwerte auf einen EDIFACT-Austausch, eine EDIFACT-Gruppe und eine EDIFACT-Nachricht angewendet werden.

### Allgemeine Attribute

Tabelle 104 listet die allgemeinen Attribute auf, für die Standardwerte bereitgestellt werden.

*Tabelle 104. Allgemeine Attribute*

| Feldname | Erforderlich | Beschreibung | Standardwert |
|---|---|---|---|
| INTCTLLEN (Länge der Austauschkontrollnummer) | Nein | Definiert eine bestimmte Länge für die Austauschkontrollnummer. Falls Sie einen Wert eingeben, muss dieser eine ganze Zahl sein.<br><br>Wenn Sie keinen Wert eingeben, wird die Standardlänge verwendet. | 9 |
| GRPCTLLEN (Länge der Gruppenkontrollnummer) | Nein | Definiert eine bestimmte Länge für die Gruppenkontrollnummer. Falls Sie einen Wert eingeben, muss dieser eine ganze Zahl sein.<br><br>Wenn Sie keinen Wert eingeben, wird die Standardlänge verwendet. | 9 |
| TRXCTLLEN (Länge der Transaktionskontrollnummer) | Nein | Definiert eine bestimmte Länge für die Transaktionskontrollnummer. Falls Sie einen Wert eingeben, muss dieser eine ganze Zahl sein.<br><br>Wenn Sie keinen Wert eingeben, wird die Standardlänge verwendet. | 9 |
| ENVTYPE (Umschlagstyp) | Nein | Dieses Attribut wird nicht vom Hubadmin festgelegt, sondern wird von dem Umschlagsprofiltyp abgeleitet, der erstellt wird. | EDIFACT |

*Tabelle 104. Allgemeine Attribute (Forts.)*

| Feldname | Erforderlich | Beschreibung | Standardwert |
|---|---|---|---|
| EDIFACTGRP (Gruppen für EDI erstellen) | Nein | Dieser Wert ist nur für EDIFACT-Umschlagstypen. (Die Gruppenebene ist in EDIFACT veraltet.)<br><br>**Ja** gibt an, dass funktionale Gruppen (UNG/UNE-Segmente) für EDIFACT DATA erstellt werden sollen.<br><br>**Nein** gibt an, dass sie nicht erstellt werden sollen. | Nein |
| MAXDOCS (Max. Anzahl an Transaktionen) | Nein | Maximale Anzahl an Transaktionen in einem Umschlag. Falls Sie einen Wert eingeben, muss dieser eine ganze Zahl sein. | Keine maximale Anzahl |
| CTLNUMFLAG (Kontrollnummern nach Transaktions-ID) | Nein | **Ja** gibt an, dass separate Gruppen mit Kontrollnummern auf der Basis des EDI-Transaktionstyps aufbewahrt werden.<br><br>**Nein** gibt an, dass eine allgemeine Gruppe mit Kontrollnummern für jeden EDI-Transaktionstyp verwendet werden soll. | Nein |

## Austauschattribute

Es sind keine Austauschattribute erforderlich. Die Attribute verfügen über keine Standardwerte.

## Gruppenattribute

Tabelle 105 listet die Gruppenattribute auf, für die Standardwerte bereitgestellt sind.

*Tabelle 105. Gruppenattribute*

| Feldname | Erforderlich | Beschreibung | Standardwert |
|---|---|---|---|
| UNG01 (ID der funktionalen Gruppe) | Nein | Die Gruppen-ID. | Der Standardwert kommt aus dem Header der Steuerzeichenfolge. Sie können diesen Wert auf dem Data Interchange Services-Client anzeigen, indem Sie sich die Spalte **Funktionsgruppe** auf der Seite **EDI-Dokumentdefinitionen** ansehen. |

## Nachrichtenattribute

Tabelle 106 listet die Nachrichtenattribute auf, für die Standardwerte bereitgestellt sind.

*Tabelle 106. Nachrichtenattribute*

| Feldname | Erforderlich | Beschreibung | Standardwert |
|---|---|---|---|
| UNH0201 (Nachrichtentyp) | Nein | Der Nachrichtentyp. | Der Standardwert kommt aus dem Header der Steuerzeichenfolge. Sie können diesen Wert auf dem Data Interchange Services-Client anzeigen, indem Sie sich die Seite **EDI-Dokumentdefinitionen** ansehen. |
| UNH0202 (Nachrichtenversion) | Nein | Die Version der Nachricht. | D |
| UNH0203 (Nachrichtenrelease) | Nein | Der Release der Nachricht. | Pro Standard |

*Tabelle 106. Nachrichtenattribute (Forts.)*

| Feldname | Erforderlich | Beschreibung | Standardwert |
|---|---|---|---|
| UNH0204 (Kontrollierende Stelle) | Nein | Der Code, der eine kontrollierende Stelle angibt. | UN |

# Dokumentdefinitions- und Verbindungsattribute

In diesem Abschnitt werden Dokumentdefinitionsattribute für den Umschlag aufgelistet. Einige dieser Attribute können nur, wie angegeben, auf der Protokoll- oder Verbindungsebene festgelegt werden.

## Trennzeichen- und Begrenzerattribute

Dieser Abschnitt listet die Zeichen auf, die als Begrenzer oder Trennzeichen in einem EDI-Austausch verwendet werden. Tabelle 107 zeigt das Attribut, wie es in Community Console angezeigt wird, den entsprechenden Begriff in X12 und EDIFACT (ISO 9735 Version 4, Release 1), ob das Attribut erforderlich ist, und eine Beschreibung des Attributs. Im Anschluss an die Tabelle wird ein Beispiel aufgeführt, wie diese Zeichen in einem EDI-Dokument angezeigt werden.

### Attributbeschreibungen

Die Trennzeichen- und Begrenzerattribute werden in Tabelle 107 aufgelistet.

**Anmerkung:** Einige Zeichen (wie angegeben) können Hexadezimalwerte sein. Diese können Unicode-Werte oder Werte eines anderen Codierungstyps sein. Verwenden Sie für Unicode das Format \unnnn. Bei einer anderen Codierung verwenden Sie das Format 0xnn.

*Tabelle 107. Attribute für Umschlagsprofil*

| Attribut | X12-Begriff | EDIFACT-Begriff | Beschreibung |
|---|---|---|---|
| Segmentbegrenzer | Segmentabschlusszeichen | Segmentabschlusszeichen | Dies ist ein einzelnes Zeichen, das am letzten Zeichen eines Segments angezeigt wird. Das Zeichen kann ein Hexadezimalwert sein.<br><br>Der Standardwert basiert auf dem EDI-Typ.<br><br>**X12** ~ (Tilde)<br><br>**EDIFACT**<br>' (einfaches Anführungszeichen)<br><br>**UCS** ~ (Tilde) |
| Begrenzer für Datenelemente | Trennzeichen für Datenelemente | Trennzeichen für Datenelemente | Dies ist ein einzelnes Zeichen, das die Datenelemente eines Segments trennt. Das Zeichen kann ein Hexadezimalwert sein.<br><br>Der Standardwert basiert auf dem EDI-Typ.<br><br>**X12** * (Stern)<br><br>**EDIFACT**<br>+ (Pluszeichen)<br><br>**UCS** * (Stern) |

*Tabelle 107. Attribute für Umschlagsprofil (Forts.)*

| Attribut | X12-Begriff | EDIFACT-Begriff | Beschreibung |
|---|---|---|---|
| Begrenzer für Unterelemente | Trennzeichen für Komponenten-elemente | Trennzeichen für Komponenten-datenelemente | Dies ist ein einzelnes Zeichen, das die Komponentenelemente eines zusammengesetzten Datenelements trennt. Das Zeichen kann ein Hexadezimalwert sein.<br><br>Der Standardwert basiert auf dem EDI-Typ.<br><br>**X12** \ (Backslash)<br><br>**EDIFACT**<br>: (Doppelpunkt)<br><br>**UCS** \ (Backslash) |
| Freigabezeichen | | Freigabezeichen | Dies ist ein einzelnes Zeichen, das die Bedeutung des nächsten Zeichens überschreibt, und ermöglicht, dass ein Trennzeichen in einem Datenelement angezeigt wird. Das Zeichen kann ein Hexadezimalwert sein. Es wird nur auf EDIFACT angewendet.<br><br>**EDIFACT**<br>? (Fragezeichen) |
| Trennzeichen für wiederholte Datenelemente | Wiederholungs-trennzeichen | Wiederholungs-trennzeichen | Dies ist ein einzelnes Zeichen, das die Instanzen eines wiederholten Datenelements trennt. Dieses Zeichen kann ein Hexadezimalwert sein.<br><br>Der Standardwert basiert auf dem EDI-Typ für X12 oder EDIFACT.<br><br>**X12** ^ (Zirkumflex)<br><br>**EDIFACT**<br>* (Stern) |
| Dezimalschreib-weise | | Dezimalschreib-weise (veraltet) | Dieses Attribut wurde im Dezimalformat oder beim Parsing verwendet und ist jetzt veraltet. Es kann nur ein Punkt bzw. nur ein Komma sein.<br><br>Der Standardwert ist ein Punkt. |

## Beispiel für EDI-Struktur

Dieser Abschnitt zeigt einen einfachen EDI-Austausch und wie die in Tabelle 107 auf Seite 442 beschriebenen Attribute in einem Austausch verwendet werden.

Eine EDI-Nachricht besteht aus einer Gruppe von Segmenten in einer besonderen Reihenfolge. Ein Segment besteht aus einer Gruppe von Elementen. In einem Segment kann ein Element ein einfaches Datenelement sein, das nur ein Informationselement enthält. Ein Element kann außerdem ein zusammengesetztes Datenelement sein, das zwei oder mehr einfache Datenelemente enthält. Die einfachen Elemente, die ein zusammengesetztes Element ausmachen, heißen Komponentendatenelemente.

Es gibt keine Verschachtelung von zusammengesetzten Datenelementen. Ein zusammengesetztes Element kann nur einfache Datenelemente, keine anderen Kombinationen enthalten. Obwohl dies hier nicht gezeigt wird, kann ein Komponentendatenelement auch als wiederholtes Datenelement definiert werden.

Betrachten Sie das folgende Beispiel:

```
ABC*123*AA\BB\CC*001^002^003*star?*power~
```

In diesem Beispiel gilt Folgendes:

- "ABC" ist der Segmentname (EDIFACT bezeichnet dies als "Segment-Tag"); dies würde als "ABC-Segment" bezeichnet werden.
- "*" (Stern) ist das Datenelementtrennzeichen.

  Der entsprechende Attributname in Community Console lautet **Segmentbegrenzer**.
- "123" ist das erste Datenelement, ein einfaches Datenelement, in manchen Kontexten könnte es auch als ABC01 bezeichnet werden.
- "AA\BB\CC" ist das zweite Datenelement (ABC02), es ist ein zusammengesetztes Element, das aus Komponentendatenelemente
  - "\" (Backslash) ist das Komponentendatenelement-Trennzeichen.

    Der entsprechende Attributname in Community Console lautet **Begrenzer für Datenelemente**.
  - "AA" ist das erste Komponentendatenelement von ABC02 (welches auch als ABC0201 bezeichnet werden könnte).
  - "BB" ist das zweite Komponentendatenelement von ABC02 (ABC0202).
  - "CC" ist das dritte Komponentendatenelement von ABC02 (ABC0203).
- "001^002^003" ist das dritte Datenelement (ABC03), es ist ein wiederholtes Datenelement.
  - "^" (Zirkumflex) ist das Wiederholungstrennzeichen.

    Der entsprechende Attributname in Community Console lautet **Zeichen für wiederholte Datenelemente**.
  - "001","002","003" sind die Wiederholungen (alle könnten als ABC03 bezeichnet werden).
- "star?*power" ist das vierte Datenelement (ABC04).
  - "?" (Fragezeichen) ist das Freigabezeichen und bedeutet, der nachfolgende Stern wird nicht als Trennzeichen für Datenelemente behandelt.
  - "star*power" ist der Ergebniswert von ABC04.
- "~" (Tilde) ist das Segmentabschlusszeichen.

  Der entsprechende Attributname in Community Console lautet **Segmentbegrenzer**.

## Zusätzliche EDI-Attribute

In diesem Abschnitt werden zusätzliche EDI-Attribute aufgelistet, die Sie auf der Dokumentdefinitions- oder auf der Verbindungsebene festlegen können.

*Tabelle 108. Zusätzliche EDI-Attribute*

| Attribut | Erforderlich | Beschreibung | Einschränkungen | Standardwert |
|---|---|---|---|---|
| Segmentausgabe | Nein | Wenn dies in der EDI/XML-Transformation verwendet wird, zeigt dies an, ob ein Zeilenumbruch nach jedem EDI-Segment oder jedem XML-Element auftreten soll.<br><br>**Wichtig:**<br>1. Verwenden Sie immer einen aus nur einem Zeichen bestehenden Begrenzer.<br>2. Wenn Sie eine Kombination der Zeichenbegrenzer "/r/n" verwenden und der Zeichenbegrenzer "/r" an der Position des Segmentbegrenzers im Austauschheader gefunden wird, wird der Zeichenbegrenzer "/n" ignoriert.<br>3. Ändern Sie die Typenbaumstruktur entsprechend. | Beschränkt auf Protokoll oder Verbindung | Ja |
| Dokumente mit doppelten Dokument-IDs zulassen | Nein | **Ja** gibt an, dass doppelte Dokument-IDs (Austauschkontrollnummern) zulässig sind.<br><br>**Nein** gibt an, dass doppelte Austauschkontrollnummern als Fehler behandelt werden sollen. | Beschränkt auf Protokoll oder Verbindung | Nein |
| Höchste Fehlerkategorie bei der Umsetzung | Nein | Gibt die maximale Anzahl Fehler an, die während einer Transformation auftreten können, bevor die Transformation fehlschlägt.<br><br>Gültige Werte sind 0, 1 oder 2.<br><br>Wenn die Transformationszuordnung einen Fehlerbefehl enthält, um einen benutzerdefinierten Fehler anzuzeigen, und der Ebenenparameter des Fehlerbefehls größer als dieser Wert ist, schlägt die Transformation fehl. | Beschränkt auf Protokoll oder Verbindung | 0 |
| EDI FA-Zuordnungen | Nein | Stellt die Zuordnung bereit, die für das Konvertieren der internen generischen FA in die bestimmte FA verwendet werden soll.<br>**Anmerkung:** Sie wählen dieses Attribut in einer Liste mit Zuordnungen aus, die als FA-Zuordnungen (Zuordnungstyp “K”) angegeben sind. | Beschränkt auf Protokoll oder Verbindung | |
| Umschlagsprofil | Ja | Der Name des EDI-Umschlagsprofils, der für das Versehen mit einem Umschlag verwendet werden soll. Alle Umschlagsprofile, die Sie definiert haben, sind in der Liste verfügbar. | | |
| XMLNS aktiv | Nein | Führen Sie eine Namespaceverarbeitung für das Eingabe-XML-Dokument aus. Dieses Attribut wird vom XML-Transfomationsschritt verwendet.<br><br>Gültige Werte sind **Ja** oder **Nein**. | | Schema: Ja<br>DTD: Nein |

*Tabelle 108. Zusätzliche EDI-Attribute (Forts.)*

| Attribut | Erforderlich | Beschreibung | Einschränkungen | Standardwert |
|---|---|---|---|---|
| Höchste Validierungsfehlerkategorie | Nein | Die höchste akzeptable Validierungsfehlerkategorie (die Fehlerkategorie zum Akzeptieren bevor die Transaktion als "failed" (fehlgeschlagen) betrachtet wird).<br><br>Gültige Werte sind 0, 1 oder 2.<br><br>**0** Nur Validierung ohne Fehler zulassen.<br><br>**1** Keine Dokumente fehlschlagen lassen, die nur einfache Elementvalidierungsfehler aufweisen.<br><br>**2** Keine Dokumente fehlschlagen lassen, die Element- oder Segmentvalidierungsfehler aufweisen. | | 0 |
| Stufe der Validierung | Nein | Zeigt die Überprüfungsstufe an, die auf der Transaktionsebene ausgeführt werden soll. Ein Wert von 2 bedeutet, dass die Werte verwendet werden, die für die Attribute **Alphanumerische Validierungstabelle** und **Validierungstabelle für Zeichensatz** festgelegt wurden. Dieses Attribut wird auch auf das Attribut **Detaillierte Validierung des Segments** angewendet, wenn für dieses Attribut **Ja** festgelegt wurde.<br><br>Gültige Werte sind 0, 1 oder 2.<br><br>**0** Nur Basisvalidierung ausführen, wie z. B. das Überprüfen auf fehlende obligatorische Elemente und Segmente sowie auf Mindest- und Höchstlängen. Kein Validieren von Elementwerten für die Datentypen oder Codelisten, die in der Transaktionsdefinition angegeben sind.<br><br>**1** Validierung der Stufe 0 ausführen und validieren der Elementwerte für die Codelisten, die für das Datenelement angegeben sind.<br><br>**2** Validierung der Stufe 1 ausführen und validieren, ob der Elementwert für den Datentyp des Elements korrekt ist. | | 0 |
| Validierungstabelle für Zeichensatz | Nein | Gibt die Tabelle an, die für die Zeichensatzvalidierung verwendet werden soll. Diese Tabelle wird nur verwendet, wenn das Attribut **Stufe der Validierung** den Wert 2 hat.<br><br>Dieses Attribut bezieht sich auf die virtuelle Codelistentabelle. Der Benutzer kann neue Codelisten auf der Registerkarte **Codelisten** des Zuordnungsbereichs im Data Interchange Services-Client erstellen. Dieser Bereich enthält außerdem Codelisten, die für andere Zwecke verwendet werden, wie z. B. die Validierung bestimmter EDI-Elemente. | | CHARSET |

*Tabelle 108. Zusätzliche EDI-Attribute (Forts.)*

| Attribut | Erforderlich | Beschreibung | Einschränkungen | Standardwert |
|---|---|---|---|---|
| Alphanumerische Validierungstabelle | Nein | Gibt die Tabelle an, die für die alphanumerische Validierung verwendet werden soll. Diese Tabelle wird nur verwendet, wenn das Attribut **Stufe der Validierung** den Wert 2 hat.<br><br>Das Attribut bezieht sich auf die virtuellen Codelistentabellen. Der Benutzer kann neue Codelisten auf der Registerkarte **Codelisten** des Zuordnungsbereichs im Data Interchange Services-Client erstellen. Dieser Bereich enthält außerdem Codelisten, die für andere Zwecke verwendet werden, wie z. B. die Validierung bestimmter EDI-Elemente. | | ALPHANUM |
| Informationen auf Gruppenebene nur in funktionaler Bestätigung generieren | Nein | Dieses Attribut gilt für EDI-X12. Die Werte sind **Ja** oder **Nein**.<br><br>**Ja** Informationen auf Gruppenebene nur für funktionale Bestätigung generieren<br><br>**Nein** Vollständiges funktionales Bestätigungsdetail für jede einzelne Transaktion und Segmente und Elemente in einer Transaktion generieren. | Beschränkt auf Protokoll oder Verbindung | Nein |
| Jahr für Jahrhundertsteuerung | Nein | Wenn Datumsangaben von zweistelligen Jahresangaben in vierstellige Jahresangaben konvertiert werden, wird bei zweistelligen Jahresangaben nach diesem Wert ein Jahrhundertwert von “19” angenommen. Bei zweistelligen Jahresangaben gleich oder vor diesem Wert wird von einem Jahrhundertwert von “20” ausgegangen.<br><br>Der gültige Bereich ist 0-99. | Beschränkt auf Protokoll oder Verbindung | 10 |

*Tabelle 108. Zusätzliche EDI-Attribute (Forts.)*

| Attribut | Erforderlich | Beschreibung | Einschränkungen | Standardwert |
|---|---|---|---|---|
| Detaillierte Validierung des Segments | Nein | Dieses Attribut gilt für die folgenden Segmentheader und -trailer.<br>• X12<br>– ISA, IEA<br>– GS, GE<br>– ST, SE<br>• EDIFACT<br>– UNA<br>– UNB, UNZ<br>– UNG, UNE<br>– UNH, UNT<br>• UNTUCS<br>– BG, EG<br>– GS, GE<br>– ST, SE<br><br>Gültige Werte sind **Ja** oder **Nein**.<br><br>**Ja** Detaillierte Umschlagssegmentvalidierung ausführen. Die Überprüfungstiefe wird vom Attribut **Stufe der Validierung** gesteuert.<br><br>**Nein** Detaillierte Umschlagssegmentvalidierung nicht ausführen. | Beschränkt auf Protokoll oder Verbindung | Nein |
| TA1-Anforderung zulassen | Nein | Generierung einer TA1-Anforderung zulassen, wenn dies im Austauschumschlagsegment angegeben ist. Gilt nur für EDI-X12.<br><br>Wenn auf **Ja** gesetzt, wird eine TA1 generiert, falls dies im Austauschumschlagsegment angegeben ist.<br><br>Wenn auf **Nein** gesetzt, wird keine TA1 generiert, selbst wenn dies im Austauschumschlagsegment angegeben ist. | Beschränkt auf Protokoll oder Verbindung | Ja |
| Umschlag bei Fehlern löschen | Nein | Dieses Attribut wird bei vielgestaltiger Verarbeitung verwendet.<br><br>Im Falle eines Stapels, der durch das Entfernen des Umschlags entstanden ist, gibt dieses Attribut an, ob der gesamte Stapel gelöscht werden soll, wenn eine der Transaktionen fehlschlägt.<br><br>Gültige Werte sind **Ja** und **Nein**. | Beschränkt auf Protokoll oder Verbindung | Nein |

*Tabelle 108. Zusätzliche EDI-Attribute (Forts.)*

| Attribut | Erforderlich | Beschreibung | Einschränkungen | Standardwert |
|---|---|---|---|---|
| Qualifikationsmerkmal1 für Verbindungsprofil | Nein | Dieses Attribut wird vom Programm zur Umschlaggenerierung verwendet, um zu ermitteln, welches Profil für eine Austauschverbindung verwendet werden soll. Transaktionen mit verschiedenen Werten für dieses Attribut werden in verschiedene Austauschvorgänge gestellt. | | |
| Qualifikationsmerkmal für Austausch | Nein | Der Code, mit dem das Format der Kennung für Austausch vom Absender oder Empfänger angegeben wird. | | |
| Kennung für Austausch | Nein | Gibt den spezifischen Absender oder Empfänger des Dokuments an. Der eingegebene Datentyp wird vom Attribut **Qualifikationsmerkmal für Austausch** bestimmt. | | |
| Nutzungsanzeiger für Austausch | Nein | Gibt an, ob die konvertierten Quellendokumente als Produktions-, Test- oder Informationsdokumente klassifiziert werden.<br><br>Gültige Werte sind **P**, **T** und **I**. | | |
| Kennung für Absender der Gruppenanwendung | Nein | Gibt den spezifischen Absender der Transaktion an. Dieses Attribut, wenn es von den Handelspartnern festgesetzt wurde, ermöglicht die Adressierung innerhalb eines Unternehmens. | | |
| Kennung für Empfänger der Gruppenanwendung | Nein | Gibt den spezifischen Empfänger oder die spezifische Anwendung der Transaktion an. Dieses Attribut, wenn es von den Handelspartnern festgesetzt wurde, ermöglicht die Adressierung innerhalb eines Unternehmens. | | |
| Umgekehrtes Routing für Austausch | Nein | Gibt die Adresse an, an die der Empfänger alle Antworten richten soll. | | |
| Routing-Adresse für Austausch | Nein | Der Unteradressencode für vorwärts gerichtetes Routing. | | |
| Qualifikationsmerkmal für Absender der Gruppenanwendung | Nein | Der Code, mit dem das Format der Kennung für Absender der Gruppenanwendung angegeben wird. | | |
| Qualifikationsmerkmal für Empfänger der Gruppenanwendung | Nein | Der Code, mit dem das Format der Kennung für Empfänger der Gruppenanwendung angegeben wird. | | |
| Kennwort für Gruppenanwendung | Nein | Dieses Attribut definiert Sicherheitsinformationen. | | |

*Tabelle 108. Zusätzliche EDI-Attribute (Forts.)*

| Attribut | Erforderlich | Beschreibung | Einschränkungen | Standardwert |
|---|---|---|---|---|
| Zeitlimit für erforderliche funktionale Bestätigung (FA) | | Zeit (in Minuten) nach dem Senden einer Transaktion, während der eine funktionale Bestätigung (Functional Acknowledgment - FA) zurückgegeben werden muss. Wird dieser Wert leer gelassen, ist keine funktionale Bestätigung erforderlich. | | |

## Data Interchange Services-Clientmerkmale

Dieser Abschnitt listet die Merkmale auf, die als Teil der Transformationszuordnung im Data Interchange Services-Client und ihren entsprechenden WebSphere Partner Gateway-Attributen festgelegt werden können.

*Tabelle 109. Zuordnung der Merkmale und ihrer entsprechenden Attribute*

| Data Interchange Services-Clientmerkmal | Überschreibt WebSphere Partner Gateway-Attribut |
|---|---|
| AckReq | Bestätigung angefordert |
| Alphanum | Alphanumerische Validierungstabelle |
| Charset | Validierungstabelle für Zeichensatz |
| CtlNumFlag | Kontrollnummern nach Transaktions-IDs |
| EdiDecNot (Dezimalschreibweise) | Dezimalschreibweise |
| EdiDeDlm (Datenelementtrennzeichen) | Begrenzer für Datenelemente |
| EdiDeSep (wiederholtes Datenelementtrennzeichen) | Trennzeichen für wiederholte Datenelemente |
| EdifactGrp | Gruppen für EDI erstellen |
| EdiRlsChar (Freigabezeichen) | Freigabezeichen |
| EdiSeDlm (Komponentendatenelement-Trennzeichen) | Begrenzer für Unterelemente |
| EdiSegDlm (Segmentabschlusszeichen) | Segmentbegrenzer |
| EnvProfName | Umschlagsprofil |
| EnvType | Umschlagstyp |
| MaxDocs | Max. Anzahl an Transaktionen |
| Reroute | Umgekehrtes Routing für Austausch |
| SegOutput | Segmentausgabe |
| ValLevel | Stufe der Validierung |
| ValErrLevel | Höchste Validierungsfehlerkategorie |
| ValMap | Validierungszuordnung |

Tabelle 110 listet zusätzliche Data Interchange Services-Clientmerkmale und deren zugeordnete WebSphere Partner Gateway-Attribute auf.

*Tabelle 110. Data Interchange Services-Clientmerkmale und deren zugeordnete Attribute*

| Data Interchange Services-Clientmerkmal | Überschreibt WebSphere Partner Gateway-Attribut |
|---|---|
| IchgCtlNum | Austauschkontrollnummer |
| IchgSndrQl | Qualifikationsmerkmal für Absender des Austauschs |

*Tabelle 110. Data Interchange Services-Clientmerkmale und deren zugeordnete Attribute (Forts.)*

| Data Interchange Services-Clientmerkmal | Überschreibt WebSphere Partner Gateway-Attribut |
|---|---|
| IchgSndrId | Austauschabsender-ID |
| IchgRcvrQl | Qualifikationsmerkmal für Empfänger des Austauschs |
| IchgRcvrId | Austauschempfänger-ID |
| IchgDate | Datum für Austausch |
| IchgTime | Zeit für Austausch |
| IchgPswd | Kennwort für Austausch |
| IchgUsgInd | Nutzungsanzeiger für Austausch |
| IchgAppRef | Anwendungsreferenz für Austausch |
| IchgVerRel | Version und Release für Austausch |
| IchgGrpCnt | Anzahl von Gruppen im Austausch |
| IchgCtlTotal | Kontrollsumme vom Austauschtrailersegment |
| IchgTrxCnt | Anzahl von Dokumenten im Austausch |
| GrpCtlNum | Kontrollnummer der Gruppe |
| GrpFuncGrpId | ID der funktionalen Gruppe |
| GrpAppSndrId | Kennung für Absender der Gruppenanwendung |
| GrpAppRcvrId | Kennung für Empfänger der Gruppenanwendung |
| GrpDate | Gruppendatum |
| GrpTime | Gruppenzeit |
| GrpPswd | Gruppenkennwort |
| GrpVer Gruppenversion. | Gruppenversion |
| GrpRel Gruppenrelease. | Gruppenrelease |
| GrpTrxCnt | Anzahl von Dokumenten in der Gruppe |
| TrxCtlNum | Kontrollnummer der Transaktion |
| TrxCode | Transaktionscode |
| TrxVer | Transaktionsversion |
| TrxRel | Transaktionsrelease |
| TrxSegCnt | Anzahl EDI-Segmente im Dokument |

## AS-Attribute

Dieser Abschnitt beschreibt die AS-Attribute.

*Tabelle 111. AS-Attribute*

| Attribut | Erforderlich | Beschreibung | Einschränkungen | Standardwert |
|---|---|---|---|---|
| Bestätigungszeit (in Min.) | Nein | Die Wartezeit für eine MDN-Bestätigung, bevor die ursprüngliche Anforderung erneut gesendet wird. Dieses Attribut funktioniert in Verbindung mit **Wiederholungszähler**. Die Einheiten werden in Minuten angegeben. | Beschränkt auf Paket oder Verbindung | 30 |

*Tabelle 111. AS-Attribute (Forts.)*

| Attribut | Erforderlich | Beschreibung | Einschränkungen | Standardwert |
|---|---|---|---|---|
| Wiederholungszähler | Nein | Gibt an, wie oft eine Anforderung gesendet werden soll, wenn kein MDN empfangen wird. Dieses Attribut wird in Verbindung mit **Bestätigungszeit** verwendet.<br><br>Wenn für dieses Attribut z. B. 3 festgelegt wurde, kann die Anforderung theoretisch viermal gesendet werden: das erste Mal und dann drei Wiederholungen. | Beschränkt auf Paket oder Verbindung | 3 |
| AS-Komprimierung vor Unterzeichnung | Nein | Gibt an, ob die AS-Komprimierung auf sowohl die Nutzdaten als auch die Signatur oder nur auf die Nutzdaten angewendet wird.<br><br>Wenn Sie **Ja** auswählen, werden die Nutzdaten komprimiert, bevor die Nachricht unterzeichnet wird. Dieses Attribut wird in Verbindung mit **AS komprimiert** verwendet. | Beschränkt auf Paket oder Verbindung | Ja |
| AS komprimiert | Nein | Die Daten komprimieren. Dieses Attribut wird in Verbindung mit **AS-Komprimierung vor Unterzeichnung** verwendet. | Beschränkt auf Paket oder Verbindung | Nein |
| AS verschlüsselt | Nein | Dieses Attribut gilt für AS2 und gibt die URL an, an die ein Partner eine asynchrone MDN senden soll. Dieses Attribut wird in Verbindung mit dem Attribut **AS-MDN asynchron** verwendet; ein Wert ist jedoch auch für synchrone MDNs erforderlich. | Beschränkt auf Paket oder Verbindung | Nein |
| HTTP-URL für AS MDN | Ja, falls das Attribut **AS-MDN asynchron** auf **Ja** gesetzt ist und Sie AS2 verwenden. | Dieses Attribut gilt für AS2 und gibt die URL an, an die ein Partner eine asynchrone MDN senden soll. Dieses Attribut wird in Verbindung mit dem Attribut **AS-MDN asynchron** verwendet; ein Wert ist jedoch auch für synchrone MDNs erforderlich. | Beschränkt auf Paket oder Verbindung | |
| E-Mail-Adresse für AS MDN | Ja, falls das Attribut **AS-MDN asynchron** auf **Ja** gesetzt ist und Sie AS1 verwenden. | Gibt die E-Mail-Adresse für den zu verwendenden Partner an, wenn Sie eine asynchrone MDN senden. Dieses Attribut wird in Verbindung mit dem Attribut **AS-MDN angefordert** verwendet. Der Wert von **E-Mail-Adresse für AS MDN** wird im Feld "Disposition-notification-to" (Dispositionsbenachrichtigung an) verwendet.<br><br>Für AS1 wird dieses Attribut in Verbindung mit dem Attribut **AS-MDN asynchron** im Format mailto:xxx@company.com verwendet.<br><br>Auch für AS2 ist für dieses Attribut ein Wert erforderlich, obwohl die E-Mail-Adresse selbst nicht verwendet wird. | Beschränkt auf Paket oder Verbindung | |

*Tabelle 111. AS-Attribute (Forts.)*

| Attribut | Erforderlich | Beschreibung | Einschränkungen | Standardwert |
|---|---|---|---|---|
| AS-MDN asynchron | Nein | Gibt an, ob die MDN synchron oder asynchron zurückgegeben werden soll. Der Wert dieses Attributs beeinflusst, ob das Attribut **HTTP-URL für AS MDN** oder das Attribut **E-Mail-Adresse für AS MDN** verwendet wird.<br><br>Gültige Werte sind **Ja** und **Nein**.<br><br>**Ja** Asynchron<br><br>**Nein** Synchron<br><br>Wenn für dieses Attribut **Ja** festgelegt ist, wird das Feld "receipt-delivery-option" (Empfangszustellungsoption) basierend auf dem Attribut **HTTP-URL für AS MDN** (für AS2) oder dem Attribut **E-Mail-Adresse für AS MDN** (für AS1) gefüllt. | Beschränkt auf Paket oder Verbindung | Ja |
| AS-MDN angefordert | Nein | Gibt an, ob eine MDN-Antwort erforderlich ist. Wenn für das Attribut **Ja** festgelegt ist, bewirkt dies, dass der Header “transport Disposition-notification-to” (Transport für Dispositionsbenachrichtigung an) mit dem Wert vom Attribut **E-Mail-Adresse für AS MDN** gefüllt wird.<br><br>Gültige Werte sind **Ja** und **Nein**.<br><br>**Ja** Eine MDN anfordern.<br><br>**Nein** Keine MDN anfordern. | Beschränkt auf Paket oder Verbindung | Ja |
| AS Message Digest Algorithm | Nein | Der Nachrichtenauszugsalgorithmus, der beim Unterzeichnen verwendet wird. Dieses Attribut wird in Verbindung mit den Attributen **AS unterzeichnet** und **AS MDN unterzeichnet** verwendet.<br><br>Bei unterzeichneten MDNs wird dieser Wert verwendet, um den Header “Disposition-notification-options: signed-receipt-micalg” (Dispositionsbenachrichtigungsoptionen: unterzeichneter Empfangs-MIC-Algorithmus) zu füllen. | Beschränkt auf Paket oder Verbindung | sha1 |

*Tabelle 111. AS-Attribute (Forts.)*

| Attribut | Erforderlich | Beschreibung | Einschränkungen | Standardwert |
|---|---|---|---|---|
| AS MDN unterzeichnet | Nein | Gibt an, ob die Anforderung erfordert, dass eine unterzeichnete MDN zurückgegeben wird. Dieses Attribut wird in Verbindung mit **AS-MDN angefordert** verwendet.<br><br>Wenn der Wert **Ja** lautet, wird "Disposition-notification-options: signed-receipt-protocol" (Dispositionsbenachrichtigungsoptionen: unterzeichnetes Empfangsprotokoll) gefüllt.<br><br>Gültige Werte sind **Ja** und **Nein**.<br><br>**Ja** Unterzeichnete MDN angefordert.<br><br>**Nein** Keine unterzeichnete MDN angefordert.<br><br>Wenn für dieses Attribut **Ja** festgelegt ist, muss die vom Partner gesendete MDN unterzeichnet sein.<br><br>Wenn für dieses Attribut **Nein** festgelegt ist, kann die MDN unterzeichnet bzw. nicht unterzeichnet sein. | Beschränkt auf Paket oder Verbindung | Nein |
| AS unterzeichnet | Nein | Gibt an, ob das Dokument unterzeichnet werden soll.<br><br>Dies gibt für die Seite "AN" eines Austauschs an, wenn Sie Dokumente an einen Partner senden, ob das Dokument unterzeichnet werden soll.<br><br>Für die Seite "VON" des Austauschs, wenn Sie Dokumente von einem Partner empfangen, muss eine vom Partner gesendete AS-Anforderung unterzeichnet werden, falls für das Attribut **Ja** festgelegt ist. Wenn für das Attribut **Nein** festgelegt ist, kann das Dokument vom Partner unterzeichnet bzw. nicht unterzeichnet sein.<br><br>**Ja** Das Dokument unterzeichnen.<br><br>**Nein** Ein unterzeichnetes Dokument ist nicht erforderlich. | Beschränkt auf Paket oder Verbindung | Nein |
| Unbestreitbarkeit erforderlich | Nein | Gibt an, ob das Dokument im Unbestreitbarkeitsspeicher gespeichert werden muss. Wird auf das Dokument als Quelle und als Ziel angewendet.<br><br>Ja: Das Dokument wird im Unbestreitbarkeitsspeicher gespeichert.<br><br>Nein: Das Dokument wird nicht im Unbestreitbarkeitsspeicher gespeichert. | Beschränkt auf Paket oder Verbindung | Ja |

*Tabelle 111. AS-Attribute (Forts.)*

| Attribut | Erforderlich | Beschreibung | Einschränkungen | Standardwert |
|---|---|---|---|---|
| Nachrichtenspeicherung erforderlich | Nein | Gibt an, ob das Dokument im Nachrichtenspeicher gespeichert werden muss. Dieses Attribut gilt für das Quellen- und das Zieldokument.<br><br>Ja: Das Dokument wird im Nachrichtenspeicher gespeichert.<br><br>Nein: Das Dokument wird nicht im Nachrichtenspeicher gespeichert. | Beschränkt auf Paket oder Verbindung | Ja |
| AS-Geschäfts-ID | Nein | Die AS-Geschäfts-ID, die im Header "AS2-To" oder im Header "AS3-To" verwendet werden soll. Wenn kein Wert bereitgestellt ist, verwendet WebSphere Partner Gateway die Geschäfts-ID des Empfängers, die im Quellendokument verwendet wird.<br>**Anmerkung:** Der Header "AS2-From" bzw. "AS3-From" wird über das Attribut "AS-Geschäfts-ID" der Quellendokumentdefinition oder, falls keine Definition vorliegt, vom ursprünglichen Quellendokument festgelegt, das von WebSphere Partner Gateway empfangen wurde und als AS gesendet wird. | Beschränkt auf Paket oder Verbindung | |
| FTP-Adresse für AS MDN | **Ja** für AS3, wenn das Attribut **AS-MDN angefordert** auf **Ja** gesetzt ist. | Die FTP-Adresse für AS MDN, die bei Anforderung einer MDN verwendet wird. Dieses Attribut wird in Verbindung mit dem Attribut **AS-MDN angefordert** verwendet. Der Wert von **FTP-Adresse für AS MDN** wird im Feld "Disposition-notification-to" (Dispositionsbenachrichtigung an) verwendet. Das folgende Format ist erforderlich: `ftp://benutzername:pwd@host.com:port/ordnername.` | Beschränkt auf Paket oder Verbindung | Nein |
| Signaturalgorithmus | Ja, wenn "Digitale Signatur erforderlich" auf "Ja" gesetzt ist. | Der zum Signieren des Dokuments verwendete Algorithmus. Dieses Attribut wird nur dann verwendet, wenn der Attributwert "Digitale Signatur erforderlich" auf "Ja" gesetzt ist. | | dsa-sha1 |
| Verschlüsselungsalgorithmus | Ja, wenn der Attributwert "Verschlüsselung erforderlich" auf "Ja" gesetzt ist. | Der zum Verschlüsseln der Nutzdaten verwendete Algorithmus. Dieser Wert wird in Verbindung mit dem Attribut "Verschlüsselungsprotokoll" verwendet.<br><br>Dieses Attribut wird nur dann verwendet, wenn der Attributwert "Verschlüsselung erforderlich" auf "Ja" gesetzt ist. | | AES-128 |

*Tabelle 111. AS-Attribute (Forts.)*

| Attribut | Erforderlich | Beschreibung | Einschränkungen | Standardwert |
|---|---|---|---|---|
| Verschlüsselungsprotokoll | Nein | Das zum Verschlüsseln der Nutzdaten verwendete Protokoll. Gültige Werte sind "XMLEncryption" und "SMIME".<br><br>Dieses Attribut wird nur dann verwendet, wenn der Attributwert "Verschlüsselung erforderlich" auf "Ja" gesetzt ist. Wenn "Verschlüsselung erforderlich" auf "Ja" gesetzt ist und für dieses Attribut kein Wert angegeben wurde, schlägt das Dokument fehl. | | XMLEncryption |

## RosettaNet-Attribute

Dieser Abschnitt beschreibt die RosettaNet-Attribute.

*Tabelle 112. RosettaNet-Attribute*

| Attribut | Erforderlich | Beschreibung | Einschränkungen | Standardwert |
|---|---|---|---|---|
| Bestätigungszeit | Ja | Die Wartezeit für eine Empfangsbestätigung, bevor die ursprüngliche Anforderung erneut gesendet wird. Dieses Attribut funktioniert in Verbindung mit **Wiederholungszähler**. Die Einheiten werden in Minuten angegeben.<br><br>Der Standardwert wird aus dem RosettaNet-PIP-Spezifikationsdokument bezogen. | Beschränkt auf Paket oder Verbindung | 120 |
| Ausführungszeit | Ja | Die Wartezeit für eine Antwort auf eine Aktionsanforderung, bevor eine Fehlerbenachrichtigung gesendet wird. | Beschränkt auf Paket oder Verbindung | |
| Wiederholungszähler | Ja | Gibt an, wie oft eine Anforderung gesendet werden soll, wenn keine Empfangsbestätigung empfangen wurde. Dieses Attribut wird in Verbindung mit **Bestätigungszeit** verwendet.<br><br>Mit einer Einstellung von z. B. 3 kann die Anforderung theoretisch viermal gesendet werden: das erste Mal und die drei Wiederholungen.<br><br>Der Standardwert wird aus dem RosettaNet-PIP-Spezifikationsdokument bezogen. | Beschränkt auf Paket oder Verbindung | 3 |
| Digitale Signatur erforderlich | Nein | Gibt an, ob die PIP-Nachricht eine digitale Signatur erfordert.<br><br>Der Standardwert wird aus dem RosettaNet-PIP-Spezifikationsdokument bezogen. | Beschränkt auf Paket oder Verbindung | Ja |

*Tabelle 112. RosettaNet-Attribute (Forts.)*

| Attribut | Erforderlich | Beschreibung | Einschränkungen | Standardwert |
|---|---|---|---|---|
| Unbestreitbarkeit erforderlich | Nein | Gibt an, ob das Dokument im Unbestreitbarkeitsspeicher gespeichert werden muss. Wird auf das Dokument als Quelle und als Ziel angewendet.<br><br>Ja: Das Dokument wird im Unbestreitbarkeitsspeicher gespeichert.<br><br>Nein: Das Dokument wird nicht im Unbestreitbarkeitsspeicher gespeichert. | Beschränkt auf Paket oder Verbindung | Ja |
| Nachrichtenspeicherung erforderlich | Nein | Gibt an, ob das Dokument im Nachrichtenspeicher gespeichert werden muss. Dieses Attribut gilt für das Quellen- und das Zieldokument.<br><br>Ja: Das Dokument wird im Nachrichtenspeicher gespeichert.<br><br>Nein: Das Dokument wird nicht im Nachrichtenspeicher gespeichert. | Beschränkt auf Paket oder Verbindung | Ja |
| Unbestreitbarkeit des Empfangs | Nein | Gibt an, ob das Dokument der Empfangsbestätigung im Unbestreitbarkeitsspeicher gespeichert werden soll.<br><br>Der Standardwert wird aus dem RosettaNet-PIP-Spezifikationsdokument bezogen. | Beschränkt auf Paket oder Verbindung | Ja |
| Sync unterstützt | | Gibt an, ob der PIP (Partner Interface Process) die synchrone Übertragung unterstützt.<br><br>Der Standardwert wird bereitgestellt basierend auf der PIP-Spezifikation. | Beschränkt auf Paket oder Verbindung<br><br>Dieses Attribut ist nur für RNIF 2.0 verfügbar. | |
| Sync-Bestätigung erforderlich | | Gibt an, ob der PIP eine synchrone Empfangsbestätigung erfordert.<br><br>Der Standardwert wird bereitgestellt basierend auf der PIP-Spezifikation. | Beschränkt auf Paket oder Verbindung<br><br>Dieses Attribut ist nur für RNIF 2.0 verfügbar. | |
| Globaler Lieferkettencode | Für RNIF 1.1 erforderlich | Der Code, der die Lieferkette für die Funktion des Partners angibt.<br><br>Gültige Werte:<br>• Elektronische Komponenten<br>• Informationstechnologie<br>• Halbleiterfertigung | Beschränkt auf Paket oder Verbindung | |

*Tabelle 112. RosettaNet-Attribute (Forts.)*

| Attribut | Erforderlich | Beschreibung | Einschränkungen | Standardwert |
|---|---|---|---|---|
| Verschlüsselung | | Dieses Attribut gibt an, ob eine Verschlüsselung ausgeführt werden soll.<br>**Anmerkung:** Dies entspricht nicht der SSL-Verschlüsselung.<br><br>Dies gibt für die Seite "AN" eines Austauschs an, wenn Sie Dokumente an einen Partner senden, ob das Dokument verschlüsselt werden soll.<br><br>Für die Seite "VON" eines Austauschs, wenn Sie Dokumente von einem Partner empfangen, muss eine vom Partner gesendete RNIF-Anforderung verschlüsselt werden, falls für das Attribut **Ja** festgelegt ist. Wenn für das Attribut **Nein** festgelegt ist, kann das Dokument vom Partner verschlüsselt bzw. unverschlüsselt sein.<br><br>Gültige Werte:<br><br>**Keine** Eine Verschlüsselung ist nicht erforderlich.<br><br>**Nutzdaten**<br>Nur RosettaNet Service Content verschlüsseln.<br><br>**Nutzdaten und Container**<br>RosettaNet Service Content und den Service-Header zusammen verschlüsseln. | Beschränkt auf Paket oder Verbindung<br><br>Dieses Attribut ist nur für RNIF 2.0 verfügbar. | Kein Standardwert |
| Text des Nachrichtenstandards | Nein | Der Standard, dem der Service-Content entsprechen muss. Dieser Wert muss nur dann definiert werden, wenn es sich um keine RosettaNet Service Content-Nachricht handelt. | | Kein Standardwert |
| Version des Nachrichtenstandards | Nein | Die Version des Standards, der der Service-Content entsprechen muss. Dieser Wert muss nur dann definiert werden, wenn es sich um keine RosettaNet Service Content-Nachricht handelt. | | Kein Standardwert |
| PIP - Kennung für Nutzdatenbindung | Nein | Diese partnerdefinierte PIP-Bindungskennung ist eine eindeutige Kennung zwischen den Handelspartnern. Dieses Attribut wird nur dann gesetzt, wenn es sich um einen Nicht-RosettaNet Service Content handelt. | | Kein Standardwert |
| FromGlobalPartner-ClassificationCode | Ja, für RNIF 1.1-Schemata | Der Code, der die Funktion eines Partners in der Lieferkette angibt. Nur dann erforderlich, wenn RNIF 1.1 für schemabasierte PIPs verwendet wird. Dieser Wert muss bei Verwendung von schemabasierten PIPs auch für 0A1 PIPs angegeben werden. | | Kein Standardwert |

*Tabelle 112. RosettaNet-Attribute (Forts.)*

| Attribut | Erforderlich | Beschreibung | Einschränkungen | Standardwert |
|---|---|---|---|---|
| ToGlobalPartnerClassificationCode | Ja, für RNIF 1.1-Schemata | Der Code, der die Funktion eines Partners in der Lieferkette angibt. Nur dann erforderlich, wenn RNIF 1.1 für schemabasierte PIPs verwendet wird. Dieser Wert muss bei Verwendung von schemabasierten PIPs auch für 0A1 PIPs angegeben werden. | | Kein Standardwert |
| RN-Nachrichtenauszugsalgorithmus | Nein | Dieses Attribut wird nur dann verwendet, wenn das Attribut "Digitale Unterschrift erforderlich" auf **Ja** gesetzt ist. Legt den Nachrichtenauszugsalgorithmus fest, der für die digitale Signatur verwendet wird. Die zulässigen Werte sind **SHA1** und **MD5**. | | SHA1 |
| RN-Verschlüsselungsalgorithmus | Nein | Dieses Attribut wird nur dann verwendet, wenn das Attribut "Verschlüsselung" auf "Nutzdaten" oder "Nutzdaten und Container" gesetzt ist. Zulässige Werte sind "Triple DES" und "RC2-40". | | Triple DES |

## Backend Integration-Attribut

Dieser Abschnitt beschreibt das Attribut, das dem Paket **Backend Integration** zugeordnet ist.

*Tabelle 113. Backend Integration-Attribut*

| Attribut | Beschreibung | Standardwert |
|---|---|---|
| Umschlagsmarkierung | Dieses Attribut gibt an, ob das Dokument mit einem XML-Umschlag versehen werden soll.<br><br>Gültige Werte sind **Ja** und **Nein**. | Nein |

## ebMS-Attribute

Dieser Abschnitt beschreibt die ebMS-Attribute.

*Tabelle 114. ebMS-Attribute*

| Attribut | Erforderlich | Beschreibung | Einschränkungen | Standardwert |
|---|---|---|---|---|
| Bestätigungszeit (in Min.) | Nein | Die Wartezeit für eine Bestätigung, bevor die ursprüngliche Anforderung erneut gesendet wird. Dieses Attribut funktioniert in Verbindung mit **Wiederholungszähler**. Die Einheiten werden in Minuten angegeben. | Beschränkt auf Paket oder Verbindung | 30 |

*Tabelle 114. ebMS-Attribute (Forts.)*

| Attribut | Erforderlich | Beschreibung | Einschränkungen | Standardwert |
|---|---|---|---|---|
| Wiederholungszähler | Nein | Gibt an, wie oft eine Anforderung gesendet werden soll, wenn keine Bestätigung empfangen wird. Dieses Attribut wird in Verbindung mit **Bestätigungszeit** verwendet.<br><br>Wenn für dieses Attribut z. B. 3 festgelegt wurde, kann die Anforderung theoretisch viermal gesendet werden: das erste Mal und dann drei Wiederholungen. | Beschränkt auf Paket oder Verbindung | 3 |
| Unbestreitbarkeit erforderlich | Nein | Gibt an, ob das Dokument im Unbestreitbarkeitsspeicher gespeichert werden muss. Wird auf das Dokument als Quelle und als Ziel angewendet.<br><br>Ja: Das Dokument wird im Unbestreitbarkeitsspeicher gespeichert.<br><br>Nein: Das Dokument wird nicht im Unbestreitbarkeitsspeicher gespeichert. | Beschränkt auf Paket oder Verbindung | Ja |
| Nachrichtenspeicherung erforderlich | Nein | Gibt an, ob das Dokument im Nachrichtenspeicher gespeichert werden muss. Dieses Attribut gilt für das Quellen- und das Zieldokument.<br><br>Ja: Das Dokument wird im Nachrichtenspeicher gespeichert.<br><br>Nein: Das Dokument wird nicht im Nachrichtenspeicher gespeichert. | Beschränkt auf Paket oder Verbindung | Ja |
| Unbestreitbarkeit des Empfangs | Nein | Gibt an, ob das Dokument der Empfangsbestätigung im Unbestreitbarkeitsspeicher gespeichert werden soll. | Beschränkt auf Paket oder Verbindung | Ja |

*Tabelle 114. ebMS-Attribute (Forts.)*

| Attribut | Erforderlich | Beschreibung | Einschränkungen | Standardwert |
|---|---|---|---|---|
| Bestätigung angefordert | Nein | Gültige Werte sind "Immer", "Pro_Nachricht" und "Nie".<br><br>Bei Auswahl von "Immer" wird beim Senden eines ebMS-Dokuments eine Bestätigung angefordert, indem das Element "acknowledgmentRequested" in das ebMS-SOAP-Dokument eingefügt wird.<br><br>Für den Absender bedeutet die Auswahl von "Pro_Nachricht" oder "Nie", dass keine Bestätigung angefordert wird. Wenn ein ebMS-Dokument empfangen wird und der Wert auf "Immer" gesetzt ist, muss das eingehende Dokument eine Bestätigung anfordern, da es sonst fehlschlägt.<br><br>Wenn der Wert auf dem Empfängerhub auf "Pro_Nachricht" gesetzt ist, schlägt das Dokument nicht fehl, unabhängig davon, ob das Dokument eine Bestätigung anfordert oder nicht. Wenn der Wert auf "Nie" gesetzt ist, sollte das eingehende ebMS-Dokument niemals eine Bestätigung anfordern. | | Nie |
| Bestätigung mit Signatur angefordert | Nein | Gültige Werte sind "Immer", "Pro_Nachricht" und "Nie".<br><br>"Immer" gibt an, dass eine Bestätigung mit Signatur angefordert wird. Bei Auswahl von "Pro_Nachricht" und "Nie" besteht die Möglichkeit, dass eine Bestätigung ohne Signatur angefordert wird. Dieses Attribut wird in Verbindung mit dem Attribut "AcknowledgementRequested" verwendet.<br><br>Wenn der Wert des Attributs "AcknowledgementRequested" auf "Pro_Nachricht" oder "Nie" gesetzt ist, wird dieses Attribut nicht in Betracht gezogen.<br><br>Wenn kein Wert vorhanden ist, wird "Nie" verwendet. Dieses Attribut wird nur beim Senden eines Dokuments verwendet. Für empfangene Dokumente wird es nicht verwendet. | | Nie |

*Tabelle 114. ebMS-Attribute (Forts.)*

| Attribut | Erforderlich | Beschreibung | Einschränkungen | Standardwert |
|---|---|---|---|---|
| Actor | Nein | Dieses Attribut muss in einer ebMS 2.0-Implementierung nicht gesetzt werden. Das Attribut "Actor" wird bei Anforderung einer Sync-Bestätigung benötigt. Es wird in das ebMS-SOAP-Dokument eingefügt.<br><br>Die ebMS 2.0-Spezifikation empfiehlt einen konstanten Wert (http://schemas.xmlsoap.org/soap/actor/next) für dieses Attribut (Standardwert). Für diese Einstellung wird gesorgt, und der Benutzer muss diesen Attributwert jedenfalls nicht setzen. Die Verwendung ist für zukünftige Implementierungen vorgesehen. | | http://schemas.xmlsoap.org/soap/actor/next |
| Komprimierung erforderlich | Nein | Gültige Werte sind "Ja" und "Nein". Wenn die ebMS-Nutzdaten komprimiert werden sollen, muss der Wert auf "Ja" gesetzt werden. Ist keine Komprimierung erforderlich, wird der Wert nicht angegeben oder auf "Nein" gesetzt. | | Nein |
| Doppelter Ausschluss | Nein | Wenn dieser Attributwert beim Senden einer ebMS-Nachricht auf "Immer" gesetzt ist, wird das Element "DuplicateElimination" in das ebMS-SOAP-Dokument eingefügt. Das Vorhandensein des Elements "DuplicateElimination" in einem ebMS-SOAP-Dokument gibt an, dass der Empfängerhub die ebMS-Nutzdaten nicht an das Back-End zustellt, wenn das ebMS-Dokument ein Duplikat ist.<br>**Anmerkung:** Bei einem SOAP-Dokument werden die Werte "Pro Nachricht" und "Nie" nicht in das Element "DuplicateElimination" eingefügt.<br><br>Ist der Wert beim Empfang eines ebMS-Dokuments auf "Immer" gesetzt, muss das Element "DuplicateElimination" im ebMS-SOAP-Dokument vorhanden sein, sonst schlägt das Dokument fehl. Ist der Wert auf "Pro Nachricht" gesetzt und ist für das empfangene Dokument das Element "duplicateElimination" gesetzt, muss die Duplikatprüfung ausgeführt werden.<br><br>Wenn der Attributwert für ein empfangenes ebMS-Dokument auf "Immer" gesetzt und das Element "DuplicateElimination" vorhanden ist, wird das Dokument überprüft, um festzustellen, ob es sich um ein Duplikat handelt. Wenn das Dokument ein Duplikat ist, schlägt das Dokument fehl.<br><br>Wenn der Wert auf "Nie" gesetzt ist und das Element "DuplicateElimination" im SOAP-Dokument vorhanden ist, schlägt das Dokument fehl.<br><br>Wenn kein Wert vorhanden ist, wird "Nie" verwendet. | | Nie |

*Tabelle 114. ebMS-Attribute (Forts.)*

| Attribut | Erforderlich | Beschreibung | Einschränkungen | Standardwert |
|---|---|---|---|---|
| Bestandteile verschlüsseln | Nein | Der Wert für dieses Attribut ist eine Liste mit durch Semikolon getrennten Inhaltstypen für Nutzdaten. Beispiel: Bei Verwendung von application/xml;text/xml;application/binary:application/edi werden Nutzdaten mit diesen Inhaltstypen verschlüsselt.<br><br>Dieses Attribut wird nur dann verwendet, wenn der Attributwert "Verschlüsselung erforderlich" auf "Ja" gesetzt ist. | | application/xml;text/xml;application/EDI-X12;application/EDI-CONSENT;application/EDIFACT;application/binary;application/octet-stream |
| MIME-Parameter für Verschlüsselung | Nein | Ein optionales Attribut, das verwendet wird, um dem verschlüsselten Dokument zusätzliche Parameter als MimeMultipart-Header hinzuzufügen. Wird auf alle verschlüsselten Nutzdaten angewendet. Beispielwert: smime-type=”enveloped-data” or type=”text/xml” version=”1.0.”<br><br>Dieses Attribut wird nur dann verwendet, wenn der Attributwert "Verschlüsselung erforderlich" auf "Ja" gesetzt ist. | | Kein Standardwert<br><br>**Anmerkung:** Diese Variable wird in der aktuellen Implementierung nicht verwendet. Die Definition dieser Variablen hat keine Auswirkungen auf die Laufzeit. |
| MIME-Typ für Verschlüsselung | Nein | Wird in der aktuellen Implementierung nicht verwendet. | | Kein Standardwert |
| Verschlüsselung erforderlich | Nein | Gültige Werte sind "Ja" und "Nein". Bei Auswahl von "Ja" werden die Nutzdaten verschlüsselt. Dieses Attribut wird in Verbindung mit "Bestandteile verschlüsseln" verwendet.<br>**Anmerkung:** Wenn "Verschlüsselung erforderlich" auf "Ja" gesetzt ist und für "Bestandteile verschlüsseln" keine Inhaltstypen konfiguriert sind, wird nichts verschlüsselt. | | |
| Verschlüsselungstransformation | Nein | Wird in der aktuellen Implementierung nicht verwendet. | | Kein Standardwert<br><br>**Anmerkung:** Diese Variable wird in der aktuellen Implementierung nicht verwendet. Die Definition dieser Variablen hat keine Auswirkungen auf die Laufzeit. |

*Tabelle 114. ebMS-Attribute (Forts.)*

| Attribut | Erforderlich | Beschreibung | Einschränkungen | Standardwert |
|---|---|---|---|---|
| Von Signatur ausschließen | Nein | Der Wert für dieses Attribut ist eine Liste von durch Semikolon getrennten Inhaltstypen, z. B. `application/binary;application/octet-stream`. Nutzdaten mit diesem Inhaltstyp werden nicht in die Signatur eingefügt.<br><br>Dieses Attribut wird nur dann verwendet, wenn der Attributwert "Digitale Signatur erforderlich" auf "Ja" gesetzt ist. | | Keine Einträge, Signatur wird auf alle Nutzdaten angewendet. |
| Hashfunktion | Nein | Hashalgorithmus, der beim Hashing der Nutzdaten während des Signierens in der XML-Signatur verwendet werden soll. Dieses Attribut wird nur dann verwendet, wenn der Attributwert "Digitale Signatur erforderlich" auf "Ja" gesetzt ist.<br><br>Als Hashalgorithmus für ebMS wird nur SHA1 unterstützt. Auch wenn in der Verbindung für ebMS-Dokumente ein anderer Hashalgorithmus festgelegt ist, wird dennoch SHA1 als Hashalgorithmus verwendet. | | SHA1 |
| Semantik der Nachrichtenreihenfolge | Nein | Gültige Werte sind "Garantiert" und "Nicht_garantiert". Wenn der Wert beim Senden eines Dokuments auf "Garantiert" gesetzt ist, wird das Element "MessageOrder" in das SOAP-Dokument eingefügt. Identifiziert der empfangende Hub das Element im SOAP-Dokument, wird sichergestellt, dass die Nutzdaten nacheinander an das Back-End gesendet werden.<br><br>Wenn dieses Attribut für ein empfangenes Dokument auf "Garantiert" gesetzt ist, muss das eingehende ebMS-Dokument das Element "MessageOrder" enthalten. Andernfalls schlägt das Dokument fehl. In diesem Fall wird an den Partner eine Fehlernachricht mit dem Fehlercode "Inkonsistente Nachricht" gesendet. | | Nicht_garantiert |
| Rolle | Nein | Beim Senden eines ebMS-Dokuments wird dieser Attributwert als Wert für das Rollenelement im ebMS-SOAP-Dokument verwendet.<br><br>Beim Empfang eines ebMS-Dokuments wird dieser Attributwert mit dem Wert für das Rollenelement im ebMS-SOAP-Dokument verglichen. Wenn die Werte nicht übereinstimmen (oder wenn der Attributwert leer ist), schlägt das Dokument fehl. In diesem Fall wird an den Partner eine Fehlernachricht mit dem Fehlercode "Inkonsistente Nachricht" gesendet. | | Kein Standardwert |

*Tabelle 114. ebMS-Attribute (Forts.)*

| Attribut | Erforderlich | Beschreibung | Einschränkungen | Standardwert |
|---|---|---|---|---|
| Dauer der Persistenz | Nein | Die Zeit in Minuten, während der das Dokument bestehen bleiben soll, z. B. 1440 für 24 Stunden.<br><br>Beim Senden eines Dokuments wird mit "Dauer der Persistenz" die Lebensdauer unter Verwendung der folgenden Formel berechnet: Lebensdauer = Dauer der Persistenz + (Anz. der Wiederholungen * Wiederholungsintervall).<br><br>Beim Empfang eines Dokuments wird "Dauer der Persistenz" zur Verhinderung von Duplikaten verwendet. Beim Empfang eines Dokuments mit doppelter Nachrichten-ID wird überprüft, ob das Attribut "Dauer der Persistenz" für das frühere Dokument abgelaufen ist. Ist "Dauer der Persistenz" nicht abgelaufen, wird das Dokument als Duplikat markiert; ansonsten wird es nicht als Duplikat markiert.<br><br>Wenn kein Eintrag vorhanden ist, wird standardmäßig der Wert 0 verwendet. | | 0 |
| Bestandteile verpacken | Nein | Wird in der aktuellen Implementierung nicht verwendet. | | Kein Standardwert<br><br>**Anmerkung:** Diese Variable wird in der aktuellen Implementierung nicht verwendet. Die Definition dieser Variablen hat keine Auswirkungen auf die Laufzeit. |
| MIME-Parameter für Paket | Nein | Wird in der aktuellen Implementierung nicht verwendet. | | Kein Standardwert<br><br>**Anmerkung:** Diese Variable wird in der aktuellen Implementierung nicht verwendet. Die Definition dieser Variablen hat keine Auswirkungen auf die Laufzeit. |

*Tabelle 114. ebMS-Attribute (Forts.)*

| Attribut | Erforderlich | Beschreibung | Einschränkungen | Standardwert |
|---|---|---|---|---|
| Verschlüsselungsalgorithmus | Ja, wenn der Attributwert "Verschlüsselung erforderlich" auf "Ja" gesetzt ist. | Der zum Verschlüsseln der Nutzdaten verwendete Algorithmus. Dieser Wert wird in Verbindung mit dem Attribut "Verschlüsselungsprotokoll" verwendet.<br><br>Dieses Attribut wird nur dann verwendet, wenn der Attributwert "Verschlüsselung erforderlich" auf "Ja" gesetzt ist. | | AES-128 |
| Verschlüsselungsprotokoll | Nein | Das zum Verschlüsseln der Nutzdaten verwendete Protokoll. Gültige Werte sind "XMLEncryption" und "SMIME".<br><br>Dieses Attribut wird nur dann verwendet, wenn der Attributwert "Verschlüsselung erforderlich" auf "Ja" gesetzt ist. Wenn "Verschlüsselung erforderlich" auf "Ja" gesetzt ist und für dieses Attribut kein Wert angegeben wurde, schlägt das Dokument fehl. | | XMLEncryption |
| Wiederholungsintervall | Nein | Für ein gesendetes Dokument das Zeitintervall in Minuten, in dem auf eine Bestätigung gewartet wird, bevor das ebMS-Dokument erneut gesendet wird. ebMS-Dokumente werden nur dann erneut gesendet, wenn eine Bestätigung angefordert wurde und der Partner während des Wiederholungsintervalls keine Bestätigung empfangen hat.<br><br>Der Wert 0 gibt an, dass keine Wiederholungen zulässig sind. Dieses Attribut wird in Verbindung mit dem Attribut "Wiederholungszähler" verwendet. | | 270 |
| Signaturalgorithmus | Ja, wenn "Digitale Signatur erforderlich" auf "Ja" gesetzt ist. | Der zum Signieren des Dokuments verwendete Algorithmus. Dieses Attribut wird nur dann verwendet, wenn der Attributwert "Digitale Signatur erforderlich" auf "Ja" gesetzt ist.<br>**Anmerkung:** In ebMS wird 'hmac-sha1' nicht unterstützt. | | dsa-sha1 |
| Signaturtransformation | Nein | Der Transformationsalgorithmus zum Transformieren der Nutzdaten, bevor die XML-Signatur erstellt wird. Dieses Attribut wird nur dann verwendet, wenn der Attributwert "Digitale Signatur erforderlich" auf "Ja" gesetzt ist. | | Kein Standardwert |

*Tabelle 114. ebMS-Attribute (Forts.)*

| Attribut | Erforderlich | Beschreibung | Einschränkungen | Standardwert |
|---|---|---|---|---|
| Synchroner Antwortmodus | Nein | Der Typ der synchronen Antwort, der für das gesendete Dokument erforderlich ist.<br><br>Die folgenden Werte können gesetzt werden:<br>• **MSHSignalsOnly** - Es werden nur Dokumente mit MSH-Bestätigung/-Fehler über eine synchrone Verbindung gesendet. Die Geschäftsantwort und die Geschäftssignaldokumente werden asynchron zurückgegeben.<br>• **signalsOnly** - Es werden nur Geschäftssignaldokumente und MSH-Dokumente über eine synchrone Verbindung gesendet. Die Geschäftsantwort wird asynchron zurückgegeben.<br>• **responseOnly** - Es werden nur Geschäftsantworten und MSH-Dokumente über eine synchrone Verbindung gesendet. Geschäftssignaldokumente werden nicht zurückgegeben.<br>• **signalsAndResponse** - Es werden nur Geschäftsantworten und Geschäftssignaldokumente über eine synchrone Verbindung gesendet.<br>• **Keine** - Keine synchronen Antwortdokumente vom Empfänger. | | Keine |
| Verständlichkeitsprüfung erforderlich | Nein | Der Wert dieses Attributs wird als Wert des Headers "x-aux-IntelligibleCheckRequired" an das Back-End gesendet. Gültige Werte sind "Ja" und "Nein". Dieses Attribut teilt dem Back-End mit, dass die Empfangsbestätigung nur dann gesendet werden soll, wenn das ebXML-Dokument mit den Nutzdaten fehlerfrei ist. Die Interpretation des Werts obliegt dem Back-End. | | Nein |
| Kanonisierungsmethode | Nein | Der Kanonisierungsalgorithmus, der verwendet wird, bevor die XML-Signatur erstellt wird. Dieses Attribut wird nur dann verwendet, wenn der Attributwert "Digitale Signatur erforderlich" auf "Ja" gesetzt ist. | | INCLUSIVE_ WITH_ COMMENTS |
| Zu komprimierende Bestandteile | Nein | Die Liste der durch Semikolon getrennten Inhaltstypen der Nutzdaten, die komprimiert werden sollen. Wenn beispielsweise die Nutzdaten mit den Inhaltstypen "text/xml" und "application/edi" komprimiert werden müssen, lautet der Wert für dieses Attribut "text/xml;application/edi". Sind keine Einträge vorhanden, werden die Nutzdaten auch dann nicht komprimiert, wenn "Komprimierung erforderlich" auf "Ja" gesetzt ist.<br><br>Dieses Attribut wird nur dann verwendet, wenn der Attributwert "Komprimierung erforderlich" auf "Ja" gesetzt ist. | | application/xml; text/xml;application/EDI-X12; application/EDI-CONSENT; application/EDIFACT |

*Tabelle 114. ebMS-Attribute (Forts.)*

| Attribut | Erforderlich | Beschreibung | Einschränkungen | Standardwert |
|---|---|---|---|---|
| Servicetyp | Ja, wenn das Serviceelement (Dokumenttyp) keine URI ist. | Beim Senden eines ebMS-Dokuments muss der Wert des ebMSService-Elements in der ebMS-SOAP-Nachricht eine URI oder eine Zeichenfolge sein. Im Falle einer Zeichenfolge ist dieses Typattribut erforderlich. Wenn das Serviceelement (Dokumenttyp) keine URI ist, wird der Attributwert von "Servicetyp" als Typattributwert im ebMS-Dokument verwendet. | | Kein Standardwert |

## Allgemeine Attribute

Dieser Abschnitt beschreibt die allgemeinen Attribute.

*Tabelle 115. Allgemeine Attribute*

| Attribut | Erforderlich | Beschreibung | Einschränkungen | Standardwert |
|---|---|---|---|---|
| Validierungszuordnung | Nein | Die Validierungszuordnung, die zum Validieren des Dokuments verwendet wird. Die Aktion, die während der Laufzeit verwendet wird, muss einen Validierungsschritt beinhalten, der dieses Attribut verwendet. Nur Validierungszuordnungen, die hochgeladen und dem Dokumenttyp zugeordnet wurden, können ausgewählt werden. | Beschränkt auf Paket oder Verbindung | Kein Standardwert |
| Benutzerattribut 1 | Nein | Zur Verwendung in benutzerdefinierten Exits. Der Wert wird vom Ersteller des benutzerdefinierten Exits festgelegt. Diese werden im Geschäftsdokumentobjekt gesetzt, wobei das Attribut "bcg.ro.user.User01" entweder ein Absenderpräfix (Quellendokument) oder ein Empfängerpräfix (Zieldokument) ist. | | Kein Standardwert |
| Benutzerattribut 2 | Nein | Zur Verwendung in benutzerdefinierten Exits. Der Wert wird vom Ersteller des benutzerdefinierten Exits festgelegt. Diese werden im Geschäftsdokumentobjekt gesetzt, wobei das Attribut "bcg.ro.user.User02" entweder ein Absenderpräfix (Quellendokument) oder ein Empfängerpräfix (Zieldokument) ist. | | Kein Standardwert |
| Benutzerattribut 3 | Nein | Zur Verwendung in benutzerdefinierten Exits. Der Wert wird vom Ersteller des benutzerdefinierten Exits festgelegt. Diese werden im Geschäftsdokumentobjekt gesetzt, wobei das Attribut "bcg.ro.user.User03" entweder ein Absenderpräfix (Quellendokument) oder ein Empfängerpräfix (Zieldokument) ist. | | Kein Standardwert |

*Tabelle 115. Allgemeine Attribute (Forts.)*

| Attribut | Erforderlich | Beschreibung | Einschränkungen | Standardwert |
|---|---|---|---|---|
| Benutzerattribut 4 | Nein | Zur Verwendung in benutzerdefinierten Exits. Der Wert wird vom Ersteller des benutzerdefinierten Exits festgelegt. Diese werden im Geschäftsdokumentobjekt gesetzt, wobei das Attribut "bcg.ro.user.User04" entweder ein Absenderpräfix (Quellendokument) oder ein Empfängerpräfix (Zieldokument) ist. | | Kein Standardwert |
| Benutzerattribut 5 | Nein | Zur Verwendung in benutzerdefinierten Exits. Der Wert wird vom Ersteller des benutzerdefinierten Exits festgelegt. Diese werden im Geschäftsdokumentobjekt gesetzt, wobei das Attribut "bcg.ro.user.User05" entweder ein Absenderpräfix (Quellendokument) oder ein Empfängerpräfix (Zieldokument) ist. | | Kein Standardwert |
| Benutzerattribut 6 | Nein | Zur Verwendung in benutzerdefinierten Exits. Der Wert wird vom Ersteller des benutzerdefinierten Exits festgelegt. Diese werden im Geschäftsdokumentobjekt gesetzt, wobei das Attribut "bcg.ro.user.User06" entweder ein Absenderpräfix (Quellendokument) oder ein Empfängerpräfix (Zieldokument) ist. | | Kein Standardwert |
| Benutzerattribut 7 | Nein | Zur Verwendung in benutzerdefinierten Exits. Der Wert wird vom Ersteller des benutzerdefinierten Exits festgelegt. Diese werden im Geschäftsdokumentobjekt gesetzt, wobei das Attribut "bcg.ro.user.User07" entweder ein Absenderpräfix (Quellendokument) oder ein Empfängerpräfix (Zieldokument) ist. | | Kein Standardwert |
| Benutzerattribut 8 | Nein | Zur Verwendung in benutzerdefinierten Exits. Der Wert wird vom Ersteller des benutzerdefinierten Exits festgelegt. Diese werden im Geschäftsdokumentobjekt gesetzt, wobei das Attribut "bcg.ro.user.User08" entweder ein Absenderpräfix (Quellendokument) oder ein Empfängerpräfix (Zieldokument) ist. | | Kein Standardwert |
| Benutzerattribut 9 | Nein | Zur Verwendung in benutzerdefinierten Exits. Der Wert wird vom Ersteller des benutzerdefinierten Exits festgelegt. Diese werden im Geschäftsdokumentobjekt gesetzt, wobei das Attribut "bcg.ro.user.User09" entweder ein Absenderpräfix (Quellendokument) oder ein Empfängerpräfix (Zieldokument) ist. | | Kein Standardwert |

*Tabelle 115. Allgemeine Attribute (Forts.)*

| Attribut | Erforderlich | Beschreibung | Einschränkungen | Standardwert |
|---|---|---|---|---|
| Benutzerattribut 10 | Nein | Zur Verwendung in benutzerdefinierten Exits. Der Wert wird vom Ersteller des benutzerdefinierten Exits festgelegt. Diese werden im Geschäftsdokumentobjekt gesetzt, wobei das Attribut "bcg.ro.user.User10" entweder ein Absenderpräfix (Quellendokument) oder ein Empfängerpräfix (Zieldokument) ist. | | Kein Standardwert |

## OpenPGP-Attribute

Nachdem Sie eine Verbindung zwischen einem internen und einem externen Partner hergestellt haben, können Sie die Verbindungsattribute definieren. Dies wird im vorliegenden Thema beschrieben.

Aktivieren Sie auf der Seite **Verbindungen verwalten** eine Verbindung und klicken Sie auf der Zielseite der B2B-Funktionalität auf **Attribute**, um die Werte für OpenPGP-spezifische Verbindungsattribute festzulegen.

Die folgenden OpenPGP-Verbindungsattribute können festgelegt werden:

*Tabelle 116. OpenPGP-Attribute*

| Attribut | Erforderlich | Beschreibung | Standardwert |
|---|---|---|---|
| OpenPGP-Format verwenden | Ja | Legen Sie die Zielseite der B2B-Funktionalität auf der Seite "Verbindungen verwalten" auf "Wahr", wenn Sie das OpenPGP-Format verwenden wollen. | Kein Standardwert |
| Verschlüsselung erforderlich | Optional | Dieses Attribut kann verwendet werden, um die Nutzdaten zu verschlüsseln. Setzen Sie den Wert auf "Ja", wenn Nutzdaten verschlüsselt werden sollen. | Kein Standardwert |
| Vorgabe für den symmetrischen Algorithmus | Obligatorisch | Dieses Attribut gibt den bevorzugten Verschlüsselungsalgorithmus für die OpenPGP-Verschlüsselung an. Wählen Sie den bevorzugten symmetrischen Algorithmus in der Dropdown-Liste aus. Ist das Attribut **Verschlüsselung erforderlich** auf "Wahr" gesetzt, ist eine Angabe in diesem Attribut obligatorisch. | Kein Standardwert |
| Änderungserkennung | Optional; wird nur zusammen mit der Verschlüsselung ausgewählt. | Setzen Sie dieses Attribut auf "Wahr", wenn eine Prüfung der Nachrichtenintegrität ausgeführt werden soll. Bei dieser Einstellung wird überprüft, ob die Nachricht während der Übertragung manipuliert wurde. | Kein Standardwert |
| Komprimierung erforderlich | Optional | Dieses Attribut kann verwendet werden, um die Nutzdaten zu komprimieren. Setzen Sie das Attribut auf "Ja", wenn die Komprimierung verwendet werden soll. | Kein Standardwert |
| Vorgabe für den Komprimierungsalgorithmus | Obligatorisch | Dieses Attribut gibt den bevorzugten Komprimierungsalgorithmus für OpenPGP an. Wählen Sie den bevorzugten Komprimierungsalgorithmus in der Dropdown-Liste aus. Ist das Attribut **Komprimierung erforderlich** auf "Wahr" gesetzt, ist eine Angabe in diesem Attribut obligatorisch. | Kein Standardwert |

*Tabelle 116. OpenPGP-Attribute (Forts.)*

| Attribut | Erforderlich | Beschreibung | Standard-wert |
|---|---|---|---|
| Armor | Optional | OpenPGP codiert Daten in ASCII-Armor. Es schließt die Radix-64-codierten Daten in spezielle Header ein, damit OpenPGP die Daten später wiederherstellen kann. ASCII-Armor wird auch verwendet, um unaufbereitete Binärdaten bei der Übertragung über die Verbindung zu schützen. Wenn Sie dieses Attribut auf der Zielseite der Verbindung auf "Wahr" setzen, wird Armor beim Packen des Dokuments ausgeführt. Die Angabe eines Werts für dieses Attribut ist optional. | Kein Standardwert |

# Bemerkungen

Die vorliegenden Informationen wurden für Produkte und Services entwickelt, die auf dem deutschen Markt angeboten werden.

Möglicherweise bietet IBM die in dieser Dokumentation beschriebenen Produkte, Services oder Funktionen in anderen Ländern nicht an. Informationen über die gegenwärtig im jeweiligen Land verfügbaren Produkte und Services sind beim zuständigen IBM Ansprechpartner erhältlich. Hinweise auf IBM Lizenzprogramme oder andere IBM Produkte bedeuten nicht, dass nur Programme, Produkte oder Services von IBM verwendet werden können. Anstelle der IBM Produkte, Programme oder Services können auch andere, ihnen äquivalente Produkte, Programme oder Services verwendet werden, solange diese keine gewerblichen oder andere Schutzrechte von IBM verletzen. Die Verantwortung für den Betrieb von Produkten, Programmen und Services anderer Anbieter 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® Director of Licensing*
*IBM Europe, Middle East & Africa*
*Tour Descartes*
*2, avenue Gambetta*
*92066 Paris La Defense*
*France*

Trotz sorgfältiger Bearbeitung können technische Ungenauigkeiten oder Druckfehler in dieser Veröffentlichung nicht ausgeschlossen werden. Die hier enthaltenen Informationen werden in regelmäßigen Zeitabständen aktualisiert und als Neuausgabe veröffentlicht. 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 werden lediglich als Service für den Kunden bereitgestellt 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 unabhängig voneinander 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 dieser Informationen kann unter Umständen von bestimmten Bedingungen - in einigen Fällen auch von der Zahlung einer Gebühr - abhängig sein.

Die Lieferung des im Dokument aufgeführten Lizenzprogramms sowie des zugehörigen Lizenzmaterials erfolgt auf der Basis der IBM Rahmenvereinbarung bzw. der Allgemeinen Geschäftsbedingungen von IBM, der IBM Internationalen Nutzungsbedingungen für Programmpakete oder einer äquivalenten Vereinbarung.

Alle in diesem Dokument enthaltenen Leistungsdaten stammen aus einer kontrollierten 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 davon 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.

Die oben genannten Erklärungen bezüglich der Produktstrategien und Absichtserklärungen von IBM stellen die gegenwärtige Absicht von IBM dar, unterliegen Änderungen oder können zurückgenommen werden und repräsentieren nur die Ziele von IBM.

Alle von IBM angegebenen Preise sind empfohlene Richtpreise und können jederzeit ohne weitere Mitteilung geändert werden. Händlerpreise können u. U. von den hier genannten Preisen abweichen.

Diese Veröffentlichung dient nur zu Planungszwecken. Die in dieser Veröffentlichung enthaltenen Informationen können geändert werden, bevor die beschriebenen Produkte verfügbar sind.

Diese Veröffentlichung enthält Beispiele für Daten und Berichte des alltäglichen Geschäftsablaufes. Sie sollen nur die Funktionen des Lizenzprogramms 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.

COPYRIGHTLIZENZ

Diese Veröffentlichung enthält Musteranwendungsprogramme, die in Quellensprache geschrieben sind und Programmiertechniken in verschiedenen Betriebsumgebungen veranschaulichen. Sie dürfen diese Musterprogramme kostenlos kopieren, ändern und verteilen, wenn dies zu dem Zweck geschieht, Anwendungsprogramme zu entwickeln, zu verwenden, zu vermarkten oder zu verteilen, die mit der Anwendungsprogrammierschnittstelle konform sind, für die diese Musterprogramme geschrieben werden. Diese Beispiele wurden nicht unter allen denkbaren Bedingungen getestet. Daher kann IBM die Zuverlässigkeit, Wartungsfreundlichkeit oder Funktion dieser Programme weder zusagen noch gewährleisten.

Kopien oder Teile der Musterprogramme bzw. daraus abgeleiteter Code müssen folgenden Copyrightvermerk beinhalten:

Copyright (c) 1995-2008 International Business Machines Corporation und andere. Alle Rechte vorbehalten.

## Informationen zu Programmierschnittstellen

Die ggf. bereitgestellten Informationen zu Programmierschnittstellen sollen Ihnen bei der Erstellung von Anwendungssoftware unter Verwendung dieses Programms helfen. Mit allgemeinen Programmierschnittstellen können Sie Anwendungssoftware schreiben, die die Services aus den Tools dieses Programms abrufen. Diese Informationen können jedoch auch Angaben über Diagnose, Bearbeitung und Optimierung enthalten. Die Informationen zu Diagnose, Bearbeitung und Optimierung sollten Ihnen bei der Fehlerbehebung für die Anwendungssoftware helfen.

**Achtung:** Verwenden Sie diese Informationen zu Diagnose, Bearbeitung und Optimierung nicht als Programmierschnittstelle, da Änderungen vorbehalten sind.

## Marken und Servicemarken

Folgende Namen sind Marken oder eingetragene Marken der IBM Corporation in den USA und/oder anderen Ländern:

| | | | | |
|---|---|---|---|---|
| IBM | DB2 | IMS | MQIntegrator | Tivoli |
| Das IBM Logo | DB2 Universal Database | Informix | MVS | WebSphere |
| AIX | Domino | iSeries | OS/400 | z/OS |
| CICS | IBMLink | Lotus | Passport Advantage | |
| CrossWorlds | i5/OS | Lotus Notes | SupportPac | |

Microsoft, Windows, Windows NT und das Windows-Logo sind Marken der Microsoft Corporation in den USA und/oder anderen Ländern.

MMX, Pentium und ProShare sind Marken oder eingetragene Marken der Intel Corporation in den USA und/oder anderen Ländern.

Solaris, Java und alle auf Java basierenden Marken und Logos sind Marken von Sun Microsystems, Inc. in den USA und/oder anderen Ländern.

Linux ist eine Marke von Linus Torvalds in den USA und/oder anderen Ländern.

Weitere Unternehmens-, Produkt- oder Servicenamen können Marken anderer Hersteller sein.

WebSphere Partner Gateway Enterprise Edition und Advanced Edition enthalten Software, die vom Eclipse Project (www.eclipse.org) entwickelt wurde.

# Index

## Sonderzeichen



## Numerische Stichwörter



## A

## B



## C



## D

# E

## F



## G

# N



# O



# P

# Q



# R



# S

# T



# U



# V

# W



# X



# Z