IBM WebSphere Partner Gateway
Enterprise und Advanced Edition

Partnerhandbuch

Version 6.1.1

IBM WebSphere Partner Gateway
Enterprise und Advanced Edition

Partnerhandbuch

Version 6.1.1

Hinweis

Vor Verwendung dieser Informationen und des darin beschriebenen Produkts sollten die Informationen im Abschnitt „Bemerkungen" auf Seite 109 gelesen werden.

Kommentare zu dieser Dokumentation können an die folgende E-Mail-Adresse gerichtet werden: doc-comments@us.ibm.com.

Werden an IBM Informationen eingesandt, können diese beliebig verwendet werden, ohne dass eine Verpflichtung gegenüber dem Einsender entsteht.

Diese Veröffentlichung ist eine Übersetzung des Handbuchs
IBM WebSphere Partner Gateway Enterprise and Advanced Editions Partner Guide Version 6.1.1,
herausgegeben von International Business Machines Corporation, USA

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

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

Änderung des Textes bleibt vorbehalten.

Herausgegeben von:
SW TSC Germany
Kst. 2877
März 2008

Inhaltsverzeichnis

Zu diesem Handbuch

IBM WebSphere Partner Gateway ist ein elektronisches Dokumentverarbeitungssystem, das zur Verwaltung einer B2B-Handelsgemeinschaft (Business-to-Business Trading Community) eingesetzt werden kann. Der B2B-Bereich hat sich in den letzten Jahren kontinuierlich weiterentwickelt und unterstützt Unternehmen bei der schnellen, bequemen und wirtschaftlichen Durchführung einer Vielzahl automatisierter Transaktionen (z. B. zur Bestellungs- und Rechnungsverarbeitung).

Dieses Handbuch stellt den Community-Partnern alle erforderlichen Informationen zum Einrichten der Konsolkomponente (der sog. Community Console) und zum Ausführen täglicher Routineaufgaben zur Verfügung.

Zielgruppe

Die an einer IBM WebSphere Partner Gateway-Handelsgemeinschaft oder Hub-Community beteiligten Parteien sind der interne Partner, der Hubadministrator und die externen Partner. Zu jeder dieser Parteien gehören Benutzer mit Verwaltungsaufgaben, die über unterschiedliche Berechtigungsstufen verfügen. Außerdem können die Benutzer mit Verwaltungsaufgaben normale Benutzer mit speziellen Konsolzugriffsrechten zum System hinzufügen.

Typografische Konventionen

In diesem Dokument werden die folgenden typografischen Konventionen verwendet:

Konvention	Beschreibung
`Monospaceschrift`	In Monospaceschrift dargestellter Text kennzeichnet Elemente, die vom Benutzer eingegeben werden müssen, Werte für Argumente oder Befehlsoptionen, Beispiele und Codebeispiele sowie Informationen, die vom System am Bildschirm ausgegeben werden (Nachrichtentexte oder Systemanfragen).
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.
Kursivdruck	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.
`Monospaceschrift in Kursivdruck`	In kursiv gedruckter Monospaceschrift dargestellter Text kennzeichnet Variablennamen innerhalb von Textsegmenten, die in Monospaceschrift gedruckt sind.
Unterstrichener farbiger Text	Unterstrichener farbiger Text kennzeichnet Querverweise. Wenn Sie auf diesen Text klicken, dann springt das System zu dem Objekt, auf das verwiesen wird.

Text in einem blauen Rahmen	(Nur in PDF-Dateien) Ein blauer Rahmen um ein Textelement kennzeichnet einen Querverweis. Wenn Sie auf den umrandeten Text klicken, dann wird das Objekt aufgerufen, auf das sich der Verweis bezieht. Diese Konvention in PDF-Dateien entspricht der in der vorliegenden Tabelle bereits erläuterten Textkonvention mit dem unterstrichenen farbigen Text.
{INSTALL DIR}	Diese Angabe steht für das Verzeichnis, in dem das Produkt installiert wurde.
UNIX:/Windows:	Abschnitte, die mit einem dieser Hinweise beginnen, enthalten Angaben zu Unterschieden in den jeweiligen Betriebssystemen.
" " (Anführungszeichen)	(Nur in PDF-Dateien) Querverweise auf andere Abschnitte des Dokuments stehen in Anführungszeichen.
{ }	In einer Zeile mit Syntaxelementen wird in geschweiften Klammern eine Gruppe von Optionen dargestellt, von der eine Option ausgewählt werden muss.
`[ ]`	In einer Zeile mit Syntaxelementen wird in eckigen Klammern ein optionaler Parameter dargestellt.
`...`	In einer Zeile mit Syntaxelementen werden Auslassungen verwendet, um eine Wiederholung des vorherigen Parameters anzugeben. Die Angabe `option[,...]` bedeutet z. B., dass mehrere Optionen angegeben werden können, die durch Kommas getrennt werden müssen.
< >	In spitzen Klammern stehen variable Elemente eines Namens, um diese voneinander zu unterscheiden. Beispiel: *<server_name><connector_name>*tmp.log.
\, /	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

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

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

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

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 finden Sie auf der Unterstützungswebsite für WebSphere Partner Gateway unter der folgenden Adresse:

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 diesem Release

In diesem Abschnitt werden die neuen Funktionen von IBM WebSphere Partner Gateway beschrieben.

Neuerungen in Release 6.1.1

WebSphere Partner Gateway 6.1.1 unterstützt die folgenden neuen Funktionen:

- In früheren Releases war die Unterstützung der Basisauthentifizierung nur für Nachrichten des Typs ″Web-Services″ verfügbar. Diese Funktion wurde nun auf alle Protokolle erweitert. Für die Basisauthentifizierung wird empfohlen, eine gesicherte HTTP-Verbindung (d. h. HTTPS anstelle von HTTP) zu verwenden.
- Neben Unterzeichnung und Verschlüsselung wird nun auch die Unterstützung für die Komprimierung und Dekomprimierung von RNIF-Nachrichten bereitgestellt.
- Unterstützung für die Validierung des SOAP-Hauptteils (SOAP Body) und des SOAP-Umschlags (SOAP Envelope). Darüber hinaus können Sie den Umschlag eines SOAP-Umschlags entfernen.
- Das maximale Zeitlimit für synchrone Verbindungen und die maximale Anzahl synchroner Verbindungen können für jeden HTTP-Empfänger lokal gesteuert werden.
- Der FTP-Server ist in WebSphere Partner Gateway integriert und unterstützt das AS3-Protokoll, das FTP-Scripting-Ziel, den FTP-Scripting-Empfänger sowie den FTP/FTPS-Empfänger und das FTP/FTPS-Ziel.
- Ein Fehlerdokument kann an den einleitenden Partner, den empfangenden Partner oder beide Partner gesendet werden. Der Fehlerdokumentenfluss kann in WebSphere Partner Gateway Console konfiguriert werden und kann im WebSphere Partner Gateway-Format oder im Web-Services-Format vorliegen.
- Die Leistung der Archivierungsfunktion wurde verbessert.
- Mehrere interne Partner werden unterstützt.
- Sie können mehrere eingehende (inbound) und ausgehende (outbound) Dokumente gleichzeitig senden.
- Der FIPS-Modus wird unterstützt. Das Produkt kann für die Ausführung im FIPS-Modus oder im Standardmodus konfiguriert werden.
- Die Funktion für die Befehle ″Delete″ (Löschen) und ″Whereused″ (Verwendet von) wird für das Ziel, die Validierungszuordnungen, Dokumentdefinitionen, Interaktionen und Benutzer bereitgestellt.
- Für AS2- und AS3-Dokumente wird die Unterstützung für die Komprimierung großer Dateien bereitgestellt.
- Unterstützung für die Verschlüsselung und für Signaturen wird nun bereitgestellt.
- Die Konfigurationstypabhängigkeiten für die Migration umfassen auch Ereigniscodes und Alertbenachrichtigungen. Darüber hinaus wurde die Funktionalität der Partnermigration erweitert. Sie unterstützt nun den Import und Export von Definitionen alertfähiger Ereignisse.
- Das Hochladen mehrerer Zertifikate wird unterstützt. Die Konsole enthält nun einen neuen Assistenten für das Hochladen und Konfigurieren von Zertifikaten.
- Das Produkt unterstützt nun AIX 6.1, RHEL 5 (32- und 64-Bit), SLES 10 (64-Bit) und Windows Server 2003 (64-Bit).

Neuerungen in Release 6.1

WebSphere Partner Gateway V6.1 unterstützt die folgenden neuen Funktionen:

- Neue Geschäftsprotokolle: Unterstützung für AS3, SOAP with attachments, CIDX und ebXML Message Service (ebMS) 2.0.
- Verbesserte Unterstützung für angepasste XML-Dokumente, d. h. bessere Organisation, vollständige Unterstützung für XPath-Ausdrücke, Suchfelder, benutzerdefinierte Attribute und synchrone Unterstützung.
- Neue IPV6-Unterstützung (Internet Protocol Version 6) sowie erweitertes FTP-Scripting zur Unterstützung von AS3.
- Reorganisation von Dokumentdefinitionsattributen.
- Neue Dokumentdefinitionsattribute zur Verwendung mit Benutzerexits.
- Unbestreitbarkeit konfigurierbar nach Dokumenttyp und auf der Ebene der Handelspartner.
- Zusätzliche benutzerdefinierte Suchfelder in der Dokumentanzeige.
- Verbesserte Unterstützung für die AS-Anzeige auf der Basis des MDN-Rückgabestatus.
- EDI-Konfigurationsassistent und EIF-Importassistent (diese wurden zuvor im Support-Pack GA02 bereitgestellt).
- Neuer Alertbenachrichtigungsmodus zum Senden von Benachrichtigungen an alle beteiligten Parteien (Quellen- und Zielpartner) bzw. an alle subskribierten Kontakte. Dadurch reduziert sich der Aufwand für die Alertkonfiguration.
- Berechtigungen zum erneuten Senden und für das Gateway stehen nicht nur dem Administrator "Hubadmin", sondern auch anderen Benutzern zur Verfügung.
- Neue Benutzergruppe, damit mehrere Benutzer die Funktion des Hubadministrators übernehmen können.
- LDAP-Unterstützung für die Anmeldeauthentifizierung.
- Verwendung der Protokollierungs- und Tracefunktion von WebSphere Application Server für WebSphere Partner Gateway-Komponenten.
- Konfigurationsdaten der Merkmaldatei befinden sich jetzt an zentraler Position und werden über die WebSphere Partner Gateway-Konsole verwaltet.
- WebSphere MQ ist kein vorausgesetztes Produkt mehr; die interne Kommunikation erfolgt nun über die Unterstützung für WebSphere Platform Messaging.
- Auf der Basis des Partners und des Dokumenttyps auswählbares Archiv.
- Migration der WebSphere Partner Gateway-Konfiguration durch den Export und Import von Definitionen aus einer WebSphere Partner Gateway-Instanz in eine andere Instanz.
- Option für die vereinfachte Installation auf einer einzelnen Maschine (einfacher Modus).
- Verwendung von WebSphere Application Server Network Deployment zur Implementierung auf mehreren Maschinen, um Clustering und zentrales Infrastrukturmanagement zu ermöglichen.
- Unterstützung für die Verwendung von WebSphere Process Server Version 6.1 als Back-End-Integrationssystem.

Anmerkungen:

1. Die XML-basierte Administrator-API wird in Version 6.1 nicht weiter unterstützt.
2. WebSphere Partner Gateway Version 6.1 bietet keine Unterstützung für den RC5-Algorithmus.

Kapitel 1. Einführung

Hub-Community

Die Hub-Community von IBM WebSphere Partner Gateway besteht aus drei Einheiten, die für den Austausch von Geschäftsdokumenten in Echtzeit an einen zentralen Hub angeschlossen sind: Hubadministrator, interner Partner und externe Partner.

Hubadministrator

Der Hubadministrator ist ein Unternehmen, das für die Verwaltung des täglichen Betriebs der Hub-Community verantwortlich ist. Der Hubadministrator pflegt die Hardware- und Softwareinfrastruktur der Hub-Community rund um die Uhr. Zu den Zuständigkeiten gehören:

- Fehlerbehebung und Reparatur.
- Sicherstellung der korrekten Konfiguration der Hub-Community für alle externen Partner.
- Hilfe bei der Konfiguration neuer Partner der Hub-Community.
- Strategische Planung für zukünftiges Wachstum, um einen Betrieb der Hub-Community mit höchstmöglicher Effizienz sicherzustellen.

Die Rolle des Hubadministrators kann entweder einem Fremdanbieter innerhalb der Hub-Community übertragen werden, oder der interne Partner, der WebSphere Partner Gateway erworben hat, kann die Funktion des Hubadministrators ausführen.

Interner Partner

Der interne Partner ist das primäre Unternehmen und die treibende Kraft innerhalb der Hub-Community. Dieses Unternehmen ist für den Erwerb und den Aufbau der Hub-Community verantwortlich. Dazu gehört auch das Definieren der elektronischen Geschäftsprozesse, die zwischen dem Unternehmen und den externen Partnern abgewickelt werden.

Der interne Partner kann auch als Hubadministrator fungieren.

Externe Partner

Externe Partner sind die Unternehmen, die über die Hub-Community Geschäfte mit dem internen Partner abwickeln. Externe Partner müssen einen Konfigurationsprozess ausführen, um eine Verbindung zur Hub-Community herzustellen. Sobald die externen Partner verbunden sind, können sie elektronische Geschäftsdokumente mit dem internen Partner austauschen.

Symbole der Community Console

Die in der unten stehenden Tabelle aufgeführten Symbole gelten nur für die Community Console von WebSphere Partner Gateway.

Tabelle 1. Symbole der Community Console

Symbol	Symbolname
	Ausblenden
	Kopieren
	Rolle erstellen (Rolle ist nicht aktiv)
	Daten sind enthalten
	Aktivieren
	Löschen
	Unformatiertes Dokument anzeigen
	Dokument wird verarbeitet
	Dokumentverarbeitung fehlgeschlagen
	Dokumentverarbeitung erfolgreich
	Zuordnung herunterladen
	Bearbeiten
	Attributwerte bearbeiten
	Bearbeitung ausschalten
	RosettaNet-Attributwerte bearbeiten
	Erweitern
	Informationen exportieren
	Bericht exportieren
	Ziel inaktiviert
	Suchkriterien ausblenden
	Modifizieren
	Keine Daten enthalten
	Kalender öffnen
	Sortieren der Dokumente aktivieren/inaktivieren
	Anhalten

Tabelle 1. Symbole der Community Console (Forts.)

Symbol	Symbolname
	Drucken
	Eingabe erforderlich
	Starten
	Verarbeitung stoppen - Dokument wird momentan verarbeitet; aufgrund einer Benutzerangabe soll der Server die Verarbeitung des Dokuments stoppen
	Synchroner Datenfluss; für asynchrone Transaktionen wird kein Symbol angezeigt
	Zuordnung hochladen
	Details anzeigen
	Konfiguration der Attribute für die Dokumentenflussdefinition anzeigen
	Hilfefunktion anzeigen
	Mitglieder anzeigen
	Originaldokument anzeigen
	Berechtigungen anzeigen
	Gruppenzugehörigkeiten anzeigen
	Gültigkeitsfehler anzeigen
	Verwendet von

Verwendung der Community Console

Nachdem Sie WebSphere Partner Gateway konfiguriert haben, werden Sie zwei Konsoltools regelmäßig verwenden: die Ereignisanzeige und die Dokumentanalyse.

Verwenden Sie im Anzeigemodul die Ereignisanzeige zum Untersuchen von Ereignissen. Die meisten Dokumentarten werden mehrere Male versandt. Wenn der Versand eines Dokuments fehlschlägt und eine Warnung generiert wird, sollten Sie daher den Fehler suchen und beheben, um ähnliche Fehler in der Zukunft zu vermeiden.

Sie können ein bestimmtes Ereignis suchen und anschließend nachforschen, warum dieses Ereignis aufgetreten ist. Mit Hilfe der Ereignisanzeige können Sie nach Ereignissen anhand der Zeit, des Datums, des Ereignistyps, des Ereignisnamens und der Ereignisposition suchen. Der Hubadministrator kann außerdem anhand des Partners, der Quellen-IP und der Ereignis-ID suchen.

Anmerkung: Nicht alle Benutzer verfügen über den Zugriff auf Debugereignisse.

Mit Hilfe der von der Ereignisanzeige generierten Daten können Sie das Ereignis sowie das Dokument identifizieren, durch welches das Ereignis generiert wurde. Außerdem können Sie das unformatierte Dokument anzeigen, das das Feld, den Wert und die Ursache für den Fehler angibt.

Das am zweithäufigsten verwendete Tool ist die Dokumentanalyse, eine Funktion im Toolsmodul. Damit kann ermittelt werden, wie viele Dokumente empfangen wurden, wie viele Dokumente sich in Bearbeitung befinden und wie viele der fertig gestellten Dokumente fehlgeschlagen sind oder erfolgreich ausgeführt wurden. Verwenden Sie dieses Tool, um detailliertere Informationen über die fehlgeschlagenen Dokumente abzurufen und so zu ermitteln, warum sie fehlschlugen.

Das Modul **Kontenadmin** der Community Console wird primär zum Einrichten von WebSphere Partner Gateway und danach für die Pflege benutzt.

Kapitel 2. WebSphere Partner Gateway-Umgebung einrichten

In diesem Abschnitt werden die Tasks beschrieben, die der externe Partner ausführen muss, um WebSphere Partner Gateway für die Benutzer und die Umgebung des externen Partners vorzubereiten.

Zur Konfiguration von WebSphere Partner Gateway für Ihr Unternehmen müssen die folgenden Aktivitäten in der unten aufgeführten Reihenfolge von der Community Console aus durchgeführt werden:

1. „An der Community Console anmelden"
2. „Partnerprofil prüfen" auf Seite 6
3. „Ziel erstellen" auf Seite 7
4. „B2B-Funktionalitäten prüfen" auf Seite 7
5. „Digitale Zertifikate hochladen" auf Seite 9
6. „Konsolgruppen erstellen" auf Seite 30
7. „Benutzer erstellen" auf Seite 31
8. „FTP-Benutzer konfigurieren" auf Seite 32
9. „Kontaktinformationen erstellen" auf Seite 33
10. „Alerts erstellen und Kontakte hinzufügen" auf Seite 34
11. „Neue Adresse erstellen" auf Seite 41

An der Community Console anmelden

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*>.<*domain*>:58080/console (nicht gesichert)

   https://<*hostname*>.<*domain*>:58443/console (gesichert)

   Dabei gilt: <*hostname*> und <*domain*> sind der Name und die Position des Computers, der den Host für die Community Console-Komponente darstellt.

   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 mit Hilfe 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.

Partnerprofil prüfen

Verwenden Sie die Partnerfunktion in der Kontenadministration, um die Informationen, mit denen sich Ihr Unternehmen gegenüber dem System identifiziert, anzuzeigen und zu bearbeiten.

Partner können in ihrem Profil alle Attribute bis auf den Anmeldenamen des Unternehmens bearbeiten. Außerdem können Partner Geschäfts-IDs, E-Mail-IDs für alle Geschäfts IDs und IP-Adressen hinzufügen und entfernen. IP-Adressen oder Hostnamen können für folgende Betriebsmodi eingegeben werden: Produktion, Test, CPS-Manager und CPS-Partner.

Diese Funktion beinhaltet auch eine Option zum Zurücksetzen aller Benutzerkennwörter. Verwenden Sie diese Funktion ggf., wenn Sie der Meinung sind, dass ein Kennwort nicht ordnungsgemäß verwendet wurde.

Partnerprofil anzeigen und bearbeiten

1. Klicken Sie auf **Kontenadmin** > **Profile** > **Partner**.
2. Klicken Sie auf das Symbol **Mein Profil**, um das Profil zu bearbeiten. Das System ruft die Anzeige **Partnerdetails** auf.
3. Bearbeiten Sie Ihr Profil nach Bedarf (einige Werte können jedoch nicht geändert werden). In Tabelle 2 auf Seite 7 finden Sie eine Beschreibung der Werte.

Tabelle 2. Werte in den Partneranzeigen

Wert	Beschreibung
Anmeldename des Unternehmens	Identifiziert den Partner gegenüber dem System. Der Name kann maximal 15 Zeichen lang sein. Folgende Sonderzeichen dürfen nicht enthalten sein: ! # ; : \ / & ?. Dieser Wert kann nicht vom Partner geändert werden.
Anzeigename des Partners	Der Name des Partners, der für die Hub-Community angezeigt werden soll. Der Name kann maximal 30 Zeichen lang sein.
Partnertyp	Partnertyp - Externer Partner oder interner Partner. Partner können diesen Wert nur bearbeiten, wenn die Eigenschaft ″bcg.allow.partner.type.edit″ auf ″True″ gesetzt ist. Standardmäßig ist dieser Wert auf ″False″ gesetzt.
Status	**Aktiviert** oder **Inaktiviert**. Bei inaktiviertem Status ist der Partner in Suchkriterien und Dropdown-Listen nicht sichtbar.
Lieferantentyp	Gibt die Rolle des Partners an, z. B. Vertragshersteller oder Distributor.
Website	Gibt die Website des Partners an.
Geschäfts-ID	DUNS, DUNS+4 oder unformatierte Nummer, die das System zum Routing verwendet. Sie können weitere Geschäfts-ID-Nummern hinzufügen. • DUNS-Nummern müssen neun Ziffern haben. • DUNS+4-Nummern müssen dreizehn Ziffern haben. • Unformatierte ID-Nummern lassen bis zu 60 Alphazeichen, numerische Zeichen und Sonderzeichen zu. **Anmerkung:** EDI-Geschäfts-IDs müssen als Präfix Qualifikationsmerkmale aufweisen, die im EDI-Dokument verwendet werden. Das Format lautet: EDI-Qualifikationsmerkmal plus ″-″ und ID. Ein EDI-X12-Dokument unter Verwendung einer DUNS lautet beispielsweise 01-123456789.
E-Mail-ID	Eine gültige E-Mail-Adresse für jede Geschäfts-ID. Sie können für jede Geschäfts-ID weitere E-Mail-Adressen hinzufügen. Sind keine Geschäfts-IDs vorhanden, wird dieses Feld nicht angezeigt.
IP-Adresse oder Hostname	• Betriebsmodus z. B. CPS-Partner. • IP-Adresse oder Hostname des Partners.

4. Klicken Sie auf **Speichern**.

Ziel erstellen

Sie müssen ein Standardziel erstellen und verwalten. Andernfalls können Sie keine Verbindungen herstellen. Weitere Informationen zum Erstellen von Zielen finden Sie in Kapitel 3, „Ziele erstellen”, auf Seite 43.

B2B-Funktionalitäten prüfen

Anmerkung: Bei kleineren Installationen kann dieser Prozess vom Hubadministrator ausgeführt werden.

Verwenden Sie diese Funktion zum Anzeigen und Bearbeiten von vordefinierten, für den gesamten Hub geltenden B2B-Funktionalitäten und zum Aktivieren von zusätzlichen, lokalen B2B-Funktionalitäten, falls erforderlich.

Eine B2B-Funktionalität gibt einen bestimmten Typ von Geschäftsprozess an, der zwischen Ihnen und anderen Community-Teilnehmern ausgetauscht werden kann.

B2B- oder Dokumentverarbeitungsfunktionalitäten werden mit Hilfe von Dokumenttypdefinitionen festgelegt. Eine Dokumenttypdefinition stellt dem System alle notwendigen Informationen zum Empfangen, Verarbeiten und Weiterleiten von Dokumenten zwischen Community-Teilnehmern zur Verfügung.

Jede Funktionalität besteht aus bis zu fünf verschiedenen Dokumenttypdefinitionen:

Paket. Gibt Packformate für Dokumente an, die für die Übertragung der Dokumente über das Internet verwendet werden. Beispiele: RNIF, AS1, AS2 und AS3.

Protokoll. Gibt die Struktur und Position der Informationen in dem Dokument an. Das System benötigt diese Informationen zum Verarbeiten und Weiterleiten des Dokuments.

Dokumenttyp. Gibt den Geschäftsprozess an, der zwischen dem internen Partner und seinen externen Partnern verarbeitet wird.

Aktivität. Die Geschäftsfunktion, die der Prozess ausführt.

Aktion. Die einzelnen Dokumente, die einen vollständigen Geschäftsprozess bilden. Die Dokumente werden zwischen dem internen Partner und dem externen Partner verarbeitet.

Jede Dokumenttypdefinition beinhaltet Attribute (d. h. Informationen), die die Funktionalität der Definition festlegen. Ein Attribut besteht aus einer Einzelinformation, die einem bestimmten Dokumenttyp zugeordnet ist. Das System verwendet diese Informationen für verschiedene Funktionen, z. B. Prüfung der Dokumente oder Überprüfung auf Verschlüsselung.

B2B-Funktionalität prüfen und bearbeiten:

1. Klicken Sie auf **Kontenadmin** > **Profile** > **B2B-Funktionalität**. Das System ruft die Anzeige **B2B-Funktionalität** auf.
   - Wenn neben dem Paket ein Ordner dargestellt wird und in der Spalte **Aktiviert** die Nachricht "Aktiviert" angezeigt wird, wurde diese Funktionalität durch den Hubadministrator für Sie aktiviert.
   - Ein Haken unter **Quelle festlegen** bzw. **Ziel festlegen** gibt an, dass Sie diese Funktionalität mit der entsprechenden Rolle verwenden können (d. h. als Quelle oder Ziel oder beides).
   - Das Symbol zum Erstellen von Rollen unter **Quelle festlegen** oder **Ziel festlegen** gibt an, dass die Funktionalität für diese Rolle (d. h. für die Quelle und/oder das Ziel) nicht aktiviert ist.
   - Die Spalte **Aktiviert** zeigt den Status des Pakets an: **Aktiviert** oder **Inaktiviert**.

   Anmerkung: Die Funktionalität für Ziel, Quelle oder beides muss festgelegt sein, damit sie aktiviert werden kann.
2. Legen Sie für die Funktionalität das Einleiten (**Quelle festlegen**), Empfangen (**Ziel festlegen**) oder das Einleiten und Empfangen des Dokumenttypkontexts fest. In einem Zweiwege-PIP sind **Quelle festlegen** und **Ziel festlegen** für alle Aktionen gleich, unabhängig von der Tatsache, dass die Anforderung von einem Partner stammt und die entsprechende Bestätigung von einem anderen.

3. Legen Sie für die Funktionalität das Einleiten (**Quelle festlegen**), Empfangen (**Ziel festlegen**) oder das Einleiten und Empfangen für jede Dokumenttypdefinition einer niedrigeren Ebene fest.
4. Klicken Sie auf das Bearbeitungssymbol zum Anzeigen und (falls erforderlich) Ändern der Dokumenttypdefinitionen auf der unteren Ebene (z. B. Protokoll oder Dokumenttyp). Sie können auch die Attribute einer Dokumenttypdefinition ändern (z. B. **Ausführungszeit** oder **Wiederholungszahl**). Wenn Sie diese Anzeige zum ersten Mal verwenden, werden die Attribute auf die globale Ebene gesetzt. Sie können sie jedoch auf die lokale Ebene setzen, falls erforderlich. Wird ein Attribut auf die lokale Ebene gesetzt, wird dadurch die globale Einstellung in Ihrer Umgebung überschrieben, jedoch nicht geändert.
   - Wenn Sie eine Änderung auf einer beliebigen Ebene durchführen, wird diese Änderung an alle untergeordneten Ebenen weitergegeben.
   - Sie können einen einzelnen Ordner unterhalb eines Pakets auswählen und bearbeiten, falls Sie dies wünschen. Eine auf diese Weise ausgeführte Änderung wird nicht an niedrigere Ebenen weitergegeben.
   - Sie können die integrierte Option **Alles auswählen** durch Abwählen von unten nach oben überschreiben.
   - Signale, z. B. Empfangsbestätigungen, sind spezifisch für RosettaNet. Für jede Aktion gibt es drei Signale: Empfangsbestätigung, allgemeine Ausnahmebedingung und Ausnahmebedingung für Empfangsbestätigung. Sie können Attribute für Signale festlegen.
   - Fälschungssicherer Herkunftsnachweis erforderlich
   - AS-Geschäfts-ID

   Wenn Sie ein Attribut geändert haben, klicken Sie auf **Speichern**.

Digitale Zertifikate hochladen

Ein digitales Zertifikat ist ein Online-Identitätsnachweis, ähnlich einem Führerschein oder Ausweis. Mit einem digitalen Zertifikat können Sie eine Einzelperson oder eine Organisation identifizieren.

Digitale Signaturen sind Berechnungen auf der Basis eines elektronischen Dokuments, das für die Verschlüsselung einen öffentlichen Schlüssel verwendet. Durch diesen Prozess ist die digitale Signatur an das signierte (unterzeichnete) Dokument und an den Unterzeichner gebunden und kann nicht reproduziert werden. Mittlerweile haben digital signierte elektronische Transaktionen juristisch gesehen häufig dasselbe Gewicht wie unterzeichnete Papierdokumente.

WebSphere Partner Gateway verwendet digitale Zertifikate, um die Authentizität von Geschäftsdokumenttransaktionen zwischen dem internen Partner und den externen Partnern zu überprüfen. Außerdem werden sie für die Verschlüsselung und Entschlüsselung verwendet.

Sie können für abgehende Dokumente ein primäres und ein sekundäres Zertifikat angeben, um sicherzustellen, dass der Dokumentaustausch nicht unterbrochen wird. Das primäre Zertifikat wird für alle Transaktionen verwendet. Das sekundäre Zertifikat wird verwendet, wenn das primäre abgelaufen ist oder widerrufen wurde.

Digitale Zertifikate werden hochgeladen und während des Konfigurationsprozesses identifiziert.

Wenn festgestellt wird, dass ein Zertifikat abgelaufen ist oder widerrufen wurde, wird es inaktiviert und in der Community Console als inaktiviert ausgewiesen. Wenn das primäre Zertifikat abgelaufen ist oder widerrufen wurde, wird es inaktiviert. In diesem Fall wird dann das sekundäre Zertifikat als primäres Zertifikat verwendet. Wenn festgestellt wird, dass ein Zertifikat abgelaufen ist oder widerrufen wurde, wird ein Ereignis generiert.

Die Option **Zertifikatverwendung** ist je nach ausgewähltem Zertifikatstyp verfügbar. Im Hub-Operator-Profil kann die Zertifikatverwendung für **Digitale Signatur** oder **SSL-Clientzertifikat** festgelegt werden. Im Partnerprofil kann für das Verschlüsselungszertifikat die Zertifikatverwendung festgelegt werden. Wenn dasselbe Zertifikat für unterschiedliche Zwecke verwendet werden soll, z. B. im Hub-Operator-Profil für die digitale Signatur und die Verschlüsselung, muss es zweimal geladen werden. Hierbei wird ein Ladevorgang für die digitale Signatur und der andere für das Verschlüsselungszertifikat ausgeführt. Wird das Zertifikat allerdings für digitale Signaturen und für den SSL-Client verwendet, können die entsprechenden Kontrollkästchen im selben Zertifikatseintrag definiert werden.

Derartige Zertifikate können auch zweimal geladen werden, wobei ein Ladevorgang für die digitale Signatur und der andere für den SSL-Client ausgeführt wird. In diesem Fall muss beim sekundären Zertifikat dieselbe Vorgehensweise verwendet werden. Wenn die primären Zertifikate z. B. als separate Zertifikate für digitale Signaturen und für den SSL-Client geladen wurden, dann sollten auch die sekundären Zertifikate als separate Zertifikatseinträge geladen werden. (Dies gilt auch bei identischen Zertifikaten.)

Für die vollständige CertPath-Erstellung und -Validierung ist es erforderlich, dass Sie alle Zertifikate in der Zertifikatskette hochladen. Wenn zum Beispiel die Zertifikatskette die Zertifikate A -> B -> C -> D enthält, wobei A -> B bedeutet, dass A der Aussteller von B ist, dann sollten die Zertifikate A, B und C als Root-Zertifikate hochgeladen werden. Wenn eines der Zertifikate nicht verfügbar ist, wird der CertPath (Zertifikatspfad) nicht erstellt, und die Transaktion schlägt fehl. Die CA-Zertifikate können aus den von den Zertifizierungsstellen verwalteten Zertifikatrepositorys oder von dem Partner, der das Zertifikat zur Verfügung gestellt hat, angefordert werden. Root- und Intermediate-Zertifikate können nur im Hub-Operator-Profil hochgeladen werden.

Anmerkung: Bevor Sie die in den folgenden Abschnitten beschriebenen Prozeduren anwenden können, müssen die Zertifikate in das System geladen werden. Weitere Informationen zum Laden der Zertifikate finden Sie im Handbuch *Hubkonfiguration*.

Sie können Zertifikatablaufalerts erstellen; diese benachrichtigen Sie, wenn ein Zertifikat demnächst abläuft. Weitere Informationen finden Sie im Abschnitt „Alerts erstellen und Kontakte hinzufügen" auf Seite 34. Abgelaufene Zertifikate werden in der Datenbank von IBM WebSphere Partner Gateway gespeichert; sie können nicht vom System gelöscht werden.

Zertifikatbedingungen

Zertifizierungsstelle (Certificate Authority, CA). Eine Stelle, die Berechtigungsnachweise für die Sicherheit und öffentliche Schlüssel zur Nachrichtenverschlüsselung ausgibt. Fordert eine Einzelperson oder eine Firma ein digitales Zertifikat an, prüft die Zertifizierungsstelle die ihr überlassenen Informationen bei

einer Registrierungsstelle (Registration Authority, RA) nach. Wenn die Registrierungsstelle die Informationen bestätigt, stellt die Zertifizierungsstelle ein Zertifikat aus.

Beispiele für eine Zertifizierungsstelle sind VeriSign und Thawte.

Digitales Zertifikat. Ein digitales Zertifikat ist die elektronische Version einer ID-Karte. Es stellt Ihre Identität dar, wenn Sie B2B-Transaktionen über das Internet ausführen. Digitale Zertifikate werden von einer Zertifizierungsstelle abgerufen und bestehen aus drei Teilen:

- Der Abschnitt des öffentlichen Schlüssels Ihres Paars aus öffentlichen und privaten Schlüsseln.
- Informationen, die Sie identifizieren.
- Die digitale Signatur einer anerkannten juristischen Person (der Zertifizierungsstelle), mit der die Gültigkeit des Zertifikats bestätigt wird.

Digitale Signatur. Ein mit einem privaten Schlüssel erstellter digitaler Code. Mit Hilfe von digitalen Signaturen können Mitglieder der Hub-Community Übertragungen durch die Prüfung der Signatur authentifizieren. Wenn Sie eine Datei mit einer Signatur versehen, wird ein digitaler Code erstellt, der sowohl für den Inhalt der Datei als auch für Ihren privaten Schlüssel eindeutig ist. Mit Ihrem öffentlichen Schlüssel wird Ihre Signatur bestätigt.

Verschlüsselung. Eine Methode zum Verwürfeln von Informationen, damit diese unleserlich an alle Personen außer dem beabsichtigten Empfänger übergeben werden. Dieser muss die Informationen entschlüsseln, um sie lesen zu können.

Entschlüsselung. Eine Methode zum Entwürfeln von Informationen, um diese wieder lesbar zu machen. Der private Schlüssel des Empfängers wird zur Entschlüsselung verwendet.

Schlüssel. Ein digitaler Code zum Verschlüsseln, Signieren, Entschlüsseln und Prüfen von Dateien. Schlüssel können aus Schlüsselpaaren bestehen: einem privaten und einem öffentlichen Schlüssel.

Fälschungssicherer Herkunftsnachweis. Verhindert das Bestreiten vorangegangener Zusagen oder Aktionen. Bei elektronischen B2B-Transaktionen werden digitale Signaturen dazu verwendet, den Sender zu überprüfen und die Transaktion mit einer Zeitmarke zu versehen. Damit wird verhindert, dass die beteiligten Parteien den Anspruch stellen, die Transaktion sei nicht autorisiert oder nicht gültig gewesen.

Privater Schlüssel. Der geheime Abschnitt eines Schlüsselpaares. Mit Hilfe dieses Schlüssels werden die Informationen signiert und entschlüsselt. Nur Sie verfügen über den Zugriff auf Ihren privaten Schlüssel. Mit dem privaten Schlüssel wird außerdem eine eindeutige digitale Signatur generiert, die auf dem Inhalt des Dokuments basiert.

Öffentlicher Schlüssel. Der öffentliche Abschnitt eines Schlüsselpaares. Mit Hilfe dieses Schlüssels werden die Informationen verschlüsselt und die Signaturen geprüft. Ein öffentlicher Schlüssel kann an andere Mitglieder der Hub-Community verteilt werden. Ist der öffentliche Schlüssel einer Person bekannt, kann dadurch jedoch nicht der zugehörige private Schlüssel aufgedeckt werden.

Selbst signierter Schlüssel. Ein öffentlicher Schlüssel, der zum Beweis des Eigentumsrechts durch den zugehörigen privaten Schlüssel signiert wurde.

X.509-Zertifikat. Ein digitales Zertifikat, mit dem die Identität und das Eigentumsrecht an einem öffentlichen Schlüssel über ein Kommunikationsnetz hinweg bewiesen wird. Es enthält den Namen des Ausstellers (d. h. den Namen der Zertifizierungsstelle), die Identifizierungsinformationen des Benutzers und die digitale Signatur des Ausstellers.

Mit dem Zertifikat werden das Unternehmen und der Gültigkeitszeitraum des Zertifikats identifiziert.

Typen und unterstützte Formate von Zertifikaten

Alle Zertifikate müssen entweder das Format DER oder ASCII Privacy Enhanced Mail (PEM) haben. Die Zertifikate können von einem Format in das andere konvertiert werden.

Es gibt mehrere Typen von Zertifikaten:

- **SSL-Clientzertifikat (externe Partner und interner Partner)**. Ein Transportzertifikat. Wenn Sie für den ausgehenden Transport HTTPS verwenden, benötigen Sie ein SSL-Clientzertifikat. In den meisten Fällen muss das SSL-Clientzertifikat durch eine Zertifizierungsstelle signiert werden. Wenn das Zertifikat in einer Testumgebung verwendet wird, kann es selbst signiert werden.

  Sie müssen das Zertifikat über die Community Console in WebSphere Partner Gateway hochladen und eine Kopie an den Hub-Operator senden.
- **SSL-Serverzertifikat.** Aktiviert die SSL-Serverauthentifizierung. Die CA des SSL-Serverzertifikats muss unter den Partnern ausgetauscht werden.
- **Verschlüsselungszertifikat (externe Partner und interner Partner)**. Wenn Mitglieder der Hub-Community Dateien verschlüsseln, muss der Abschnitt des öffentlichen Schlüssels im Verschlüsselungszertifikat an die Mitglieder der Hub-Community gesendet werden. Der Teil mit dem zugehörigen privaten Schlüssel des Verschlüsselungszertifikats muss über die Community Console an den Hub-Operator hochgeladen werden. Sie müssen den öffentlichen Abschnitt des Partnerzertifikats über die Community Console in WebSphere Partner Gateway hochladen und eine Kopie des Zertifikats an den Hub-Operator senden.
- **Digitales Signaturzertifikat (externe Partner und interner Partner)**. Sofern Mitglieder der Hub-Community die Dokumente signieren, muss der öffentliche Abschnitt des Signaturzertifikats auf der Partnerebene als Signaturzertifikat in den Hub hochgeladen werden. Muss der Hub-Manager die Dokumente signieren, die er an Mitglieder der Hub-Community sendet, müssen Sie den öffentlichen Abschnitt des Zertifikats des Hub-Managers an die Mitglieder der Hub-Community senden. Das Signaturzertifikat des Hubs muss für den Hub-Operator über die Community Console hochgeladen werden.
- **VTP-Zertifikat (interner Partner)**. Dieses Zertifikat wird von der Dokumentverwaltung von WebSphere Partner Gateway für die Funktion **Simulator** des externen Partners verwendet. Das Zertifikat wird in das Dateisystem kopiert und nicht über die Community Console hochgeladen.

  In das Dateisystem kopierte VTP-Zertifikate sind für alle Partner aktiv, die über die Community Console erstellt werden. Diese Zertifikate prüfen signierte Dokumente, die vom Simulator des externen Partners empfangen werden. In das Dateisystem kopierte Zertifikate können über die Community Console nicht eingesehen werden.

SSL-Server- und Clientauthentifizierung

Ist eine Clientauthentifizierung nicht erforderlich, muss Folgendes zutreffen:

- Wenn es sich bei dem Zertifikat des Web-Servers der Hub-Community um ein selbst signiertes Zertifikat handelt, müssen die Partner über eine Kopie dieses Zertifikats verfügen.
- Stammt das Zertifikat des Web-Servers der Hub-Community von einer Zertifizierungsstelle, müssen die Partner über eine Kopie des CA-Root- und CA-Intermediate-Zertifikats verfügen.

Ist eine Clientauthentifizierung erforderlich, muss Folgendes zutreffen:

- Wenn es sich bei dem Zertifikat des Web-Servers der Hub-Community um ein selbst signiertes Zertifikat handelt, müssen die Partner über eine Kopie dieses Zertifikats verfügen.
- Stammt das Zertifikat des Web-Servers der Hub-Community von einer Zertifizierungsstelle, müssen die Partner über eine Kopie des CA-Root- und CA-Intermediate-Zertifikats verfügen.
- Der Zielserver muss über eine Kopie des Partnerzertifikats verfügen, falls dieses selbst signiert ist und in den gesicherten Schlüsselspeicher geladen wurde.
- Der Zielserver muss über eine Kopie des Zertifikats der Zertifizierungsstelle verfügen, falls dieses Zertifikat von einer Zertifizierungsstelle authentifiziert wurde und in den gesicherten Schlüsselspeicher geladen wurde.

Anmerkung: Vorherige Versionen von WebSphere Partner Gateway haben das Adressformat IPv6 nicht unterstützt. WebSphere Partner Gateway 6.1 unterstützt dieses Format nicht. Stellen Sie sicher, dass der letzte Ihrer Server für die Unterstützung des Adressformats IPv6 konfiguriert ist. Die Konfiguration des Formats IPv6 ist nur auf dem Server erforderlich.

Eingehende SSL-Zertifikate konfigurieren

In diesem Abschnitt wird beschrieben, 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 vorlegt, um den Hub gegenüber dem Partner zu identifizieren. Dieses Serverzertifikat kann selbst signiert oder von einer Zertifizierungsstelle (CA) signiert sein. In den meisten Fällen verwenden Sie ein CA-Zertifikat, um die Sicherheit zu erhöhen. Ein selbst signiertes Zertifikat kann beispielsweise in einer Testumgebung verwendet werden. 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 in 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, das sich im Verzeichnis `/<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. Verwenden Sie iKeyman, um das Zertifikat, das Ihren öffentlichen Schlüssel enthalten soll, in eine Datei zu extrahieren.

   Speichern Sie den Keystore in einer JKS-, PKCS12- oder JCEKS-Datei.
4. Verteilen Sie das Zertifikat an Ihre Partner. Die bevorzugte Verteilungsmethode ist das Versenden des Zertifikats in einer kennwortgeschützten komprimierten Datei (Zip) per E-Mail. Ihre Partner müssen sich an Sie wenden und das Kennwort für die komprimierte Datei anfordern.
5. Verwenden Sie die Administrationskonsole von WebSphere Application Server, um das neue Zertifikat in der SSL-Konfiguration und in den Einstellungen für den Empfänger und die Konsole zu definieren. 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: Gehen Sie wie folgt vor, wenn Sie ein von einer Zertifizierungsstelle (CA) signiertes Zertifikat verwenden:

1. Starten Sie das Dienstprogramm iKeyman, das sich im Verzeichnis `/<WAS_installationsverz>/bin` befindet.
2. Verwenden Sie iKeyman, um eine Zertifikatsanforderung und ein Schlüsselpaar für den Empfänger zu generieren.
3. Übergeben Sie eine Zertifikatssignaturanforderung (CSR - Certificate Signing Request) an eine Zertifizierungsstelle.
4. Wenn Sie das signierte Zertifikat von der Zertifizierungsstelle empfangen, stellen Sie das signierte Zertifikat mit iKeyman in den Keystore.
5. Verteilen Sie das CA-Zertifikat gegebenenfalls an alle Partner.
6. Verwenden Sie die Administrationskonsole von WebSphere Application Server, um das neue Zertifikat in der SSL-Konfiguration und in den Einstellungen für den Empfänger und die Konsole zu definieren. Sie können dazu den Aliasnamen des neuen Zertifikats im Keystore in der Konfiguration für den jeweiligen Knoten oder Server auswählen.

   Anmerkung: Zum Ausführen 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 wie folgt vor, um einen Client zu authentifizieren:

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 dieses 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, müssen Sie WebSphere Application Server für die Verwendung der Clientauthentifizierung konfigurieren, indem Sie das Dienstprogrammscript **bcgClientAuth.jacl** ausführen.

1. Navigieren Sie zum folgenden Verzeichnis: /<*Produktverz*>/bin
2. Rufen Sie das Script wie folgt auf, um die Clientauthentifizierung zu aktivieren:

```
./bcgwsadmin.sh -f /<Produktverz>/scripts/bcgClientAuth.jacl
   -conntype NONE set
```

Anmerkung: Rufen Sie das Script wie folgt auf, um die Clientauthentifizierung zu inaktivieren:

```
./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. Andernfalls 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 die Community Console aktiviert. Für HTTPS überprüft WebSphere Partner Gateway Zertifikate anhand der Geschäfts-IDs in den eingehenden Dokumenten. Um diese Funktion zu verwenden, müssen Sie das Partnerprofil erstellen, das Clientzertifikat importieren und es als SSL markieren.

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 das Zertifikat gespeichert ist.
e. Wählen Sie **SSL-Client** als Zertifikatstyp aus.
f. Geben Sie eine Beschreibung des Zertifikats ein. Diese Angabe ist erforderlich.
g. Ändern Sie den Status in **Aktiviert**.
h. Wenn Sie einen anderen Betriebsmodus als **Produktion** (die Standardeinstellung) auswählen wollen, wählen Sie ihn in der Liste aus.
i. Klicken Sie auf **Fertig stellen**.

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, finden Sie weitere Informationen im Abschnitt „HTTPS-Ziel einrichten" auf Seite 45.
   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 Version 6.1 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 "bcgconsole-Cluster" 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 ″bcgreceiver-Cluster″ 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** 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 ″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.

Anmerkung:

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 X.509-DER-Format vorliegen.

Anmerkung: Sie können das Format mit dem Dienstprogramm iKeyman konvertieren. Führen Sie die folgenden Schritte aus, 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 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 im Profil des Hubbetreibers.

1. Klicken Sie auf **Kontenadmin > Profile > Zertifikate**, um die Seite **Zertifikatliste** anzuzeigen.

   Stellen Sie sicher, dass Sie an der 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 Zertifikatstyp aus.
4. Geben Sie eine Beschreibung des Zertifikats ein. Diese Angabe ist erforderlich.
5. Ändern Sie den Status in **Aktiviert**.
6. Klicken Sie auf **Durchsuchen**, und navigieren Sie zu dem Verzeichnis, in dem das Zertifikat gespeichert ist.
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** (die 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 der 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, so dass diese es ihren vertrauenswürdigen Zertifikaten hinzufügen können.

Sie können über mehr als ein SSL-Zertifikat verfügen. Eines ist das primäre Zertifikat, das standardmäßig verwendet wird. Das andere Zertifikat ist das sekundäre Zertifikat, das verwendet wird, wenn das primäre Zertifikat abgelaufen ist.

Selbst signiertes Zertifikat verwenden: Gehen Sie wie folgt vor, wenn Sie ein selbst signiertes Zertifikat verwenden wollen:

1. Starten Sie das Dienstprogramm iKeyman.
2. Verwenden Sie iKeyman, um ein selbst signiertes Zertifikat und ein Schlüsselpaar zu generieren.
3. Verwenden Sie iKeyman, um das Zertifikat, das Ihren öffentlichen Schlüssel enthalten soll, in eine Datei zu extrahieren.

4. Verteilen Sie das Zertifikat an Ihre Partner. Die bevorzugte Verteilungsmethode ist das Versenden des Zertifikats in einer kennwortgeschützten komprimierten Datei (Zip) 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 signierte Zertifikat und den Schlüssel über die Community Console.
   a. Klicken Sie auf **Kontenadmin > Profile > Zertifikate**, um die Seite **Zertifikatliste** anzuzeigen.

      Stellen Sie sicher, dass Sie an der 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 Zertifikatstyp aus.
   d. Geben Sie eine Beschreibung des Zertifikats ein. Diese Angabe ist erforderlich.
   e. Ändern Sie den Status in **Aktiviert**.
   f. Klicken Sie auf **Durchsuchen**, und navigieren Sie zu dem Verzeichnis, in dem das Zertifikat gespeichert ist.
   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** (die Standardeinstellung) auswählen wollen, wählen Sie ihn in der Liste aus.
   j. Wenn Sie über zwei SSL-Zertifikate verfügen, geben Sie an, welches von ihnen das primäre bzw. das sekundäre Zertifikat ist, indem Sie **Primär** oder **Sekundär** in der Liste **Zertifikatverwendung** auswählen.
   k. Klicken Sie auf **Hochladen** und dann auf **Speichern**.

Wenn Sie primäre und sekundäre Zertifikate für die SSL-Clientauthentifizierung und die digitale Signatur hochladen und Sie die primären Zertifikate als zwei separate Einträge hochladen, müssen Sie sicherstellen, dass die entsprechenden sekundären Zertifikate als zwei unterschiedliche Einträge hochgeladen werden.

Von der Zertifizierungsstelle signiertes Zertifikat verwenden: Gehen Sie wie folgt vor, wenn Sie ein von einer Zertifizierungsstelle (CA) signiertes Zertifikat verwenden:

1. Verwenden Sie iKeyman, um eine Zertifikatsanforderung und ein Schlüsselpaar für den Empfänger zu generieren.
2. Übergeben Sie eine Zertifikatssignaturanforderung (CSR - Certificate Signing Request) an eine Zertifizierungsstelle.
3. Wenn Sie das signierte Zertifikat von der Zertifizierungsstelle empfangen, stellen Sie das signierte Zertifikat mit iKeyman in den Keystore.
4. Verteilen Sie das signierte CA-Zertifikat an alle Partner.

Zertifikate zum Aktivieren der Verschlüsselung verwenden

In diesem Abschnitt werden Verschlüsselungszertifikate beschrieben.

Eingehende Verschlüsselungszertifikate 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 außer 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 empfangen kann, müssen Sie eine Verbindung zu diesem Partner mit der folgenden Dokumentdefinition erstellen:

- 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 abrufen:

Selbst signiertes Zertifikat generieren: Gehen Sie wie folgt vor, wenn Sie ein selbst signiertes Zertifikat verwenden wollen:

1. Starten Sie das Dienstprogramm iKeyman.
2. Verwenden Sie iKeyman, um ein selbst signiertes Zertifikat und ein Schlüsselpaar zu generieren.
3. Verwenden Sie iKeyman, um das Zertifikat, das Ihren öffentlichen Schlüssel enthalten soll, in eine Datei zu extrahieren.
4. Verteilen Sie das Zertifikat an Ihre Partner. Die Partner müssen die Datei in ihr B2B-Produkt importieren, um sie als Verschlüsselungszertifikat verwenden zu können. Weisen Sie Ihre Partner an, das Zertifikat zu verwenden, wenn sie verschlüsselte Dateien an den internen Partner senden wollen. Wenn Ihr Zertifikat von einer CA signiert ist, stellen Sie auch das CA-Zertifikat 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** > **Neues Zertifikat erstellen**.
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 im 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 **Verschlüsselung** 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 **Fertig stellen**, um die Änderungen zu speichern und den Assistenten zu schließen.

Von der Zertifizierungsstelle signiertes Zertifikat verwenden: Gehen Sie wie folgt vor, wenn Sie ein von einer Zertifizierungsstelle (CA) signiertes Zertifikat verwenden:

1. Starten Sie das Dienstprogramm iKeyman.
2. Verwenden Sie iKeyman, um eine Zertifikatsanforderung und ein Schlüsselpaar für den Empfänger zu generieren.
3. Übergeben Sie eine Zertifikatssignaturanforderung (CSR - Certificate Signing Request) an eine Zertifizierungsstelle.
4. Wenn Sie das signierte Zertifikat von der Zertifizierungsstelle empfangen, stellen Sie das signierte 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 verschlüsselt 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, das standardmäßig verwendet wird. Das andere Zertifikat ist das sekundäre Zertifikat, das 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 X.509-DER-Format 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 die 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 **Fertig stellen** 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 **Fertig stellen** 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 **Fertig stellen**, 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 der 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** > **Zertifikate** > **Neues Zertifikat erstellen**.
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 mit Hilfe eines Truststore laden, in dem sich mehrere Zertifikate befinden, wird die Liste zur Auswahl der hochzuladenden Root CA- und Intermediate CA-Zertifikate mit allen Zertifikaten gefüllt. Sie können auch mehrere Zertifikate hochladen.
8. Klicken Sie auf **Fertig stellen**.

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**, 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 möglicherweise 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 gewünschten 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, das standardmäßig verwendet wird. Das andere Zertifikat ist das sekundäre Zertifikat, das verwendet wird, wenn das primäre Zertifikat abgelaufen ist.

Selbst signiertes Zertifikat generieren: Gehen Sie wie folgt vor, wenn Sie ein selbst signiertes Zertifikat verwenden wollen:

1. Starten Sie das Dienstprogramm iKeyman.
2. Verwenden Sie iKeyman, um ein selbst signiertes Zertifikat und ein Schlüsselpaar zu generieren.
3. Verwenden Sie iKeyman, um das Zertifikat, das Ihren öffentlichen Schlüssel enthalten soll, in eine Datei zu extrahieren.
4. Verteilen Sie das Zertifikat an Ihre Partner. Die bevorzugte Verteilungsmethode ist das Versenden des Zertifikats in einer kennwortgeschützten komprimierten Datei (Zip) 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**} > **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.
   - **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.

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 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 **Fertig stellen** 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 **Fertig stellen** 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 **Fertig stellen**, 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, müssen Sie sicherstellen, dass die entsprechenden sekundären Zertifikate als zwei unterschiedliche Einträge hochgeladen werden.

Von Zertifizierungsstelle signiertes Zertifikat abrufen: Gehen Sie wie folgt vor, wenn Sie ein von einer Zertifizierungsstelle (CA) signiertes Zertifikat verwenden:

1. Starten Sie das Dienstprogramm iKeyman.
2. Verwenden Sie iKeyman, um eine Zertifikatsanforderung und ein Schlüsselpaar für den Empfänger zu generieren.
3. Übergeben Sie eine Zertifikatssignaturanforderung (CSR - Certificate Signing Request) an eine Zertifizierungsstelle.
4. Wenn Sie das signierte Zertifikat von der Zertifizierungsstelle empfangen, stellen Sie das signierte Zertifikat mit iKeyman in den Keystore.
5. Verteilen Sie das signierte CA-Zertifikat an alle Partner.

Eingehendes Signaturzertifikat 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 die 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 einer **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 **Fertig stellen**, 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 **Kontenadmin > Profile > Zertifikate**, um die Seite **Zertifikatliste** anzuzeigen.

       Stellen Sie sicher, dass Sie an der 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. Diese Angabe ist erforderlich.
    e. Ändern Sie den Status in **Aktiviert**.
    f. Klicken Sie auf **Durchsuchen**, und navigieren Sie zu dem Verzeichnis, in dem das Zertifikat gespeichert ist.
    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 signiert**.

Konsolgruppen erstellen

Verwenden Sie die Funktion **Gruppe**, um eine Gruppe für einen bestimmten Benutzertyp mit bestimmten Konsolberechtigungen zu erstellen. Erstellen Sie z. B. eine Gruppe "Tester" für Benutzer, die während des Testlaufs einer Testverbindung zugeordnet sind. Nachdem Sie die Gruppe "Tester" erstellt haben, ordnen Sie der Gruppe Berechtigungen zu. Diese basieren auf den Konsolfunktionen, auf die die Benutzer aus der Gruppe während des Testlaufs Zugriff haben müssen.

Das System erstellt automatisch die Gruppen **Administrator** und **Standard** mit standardmäßigen Berechtigungseinstellungen. Standardeinstellungen für Berechtigungen können von einem beliebigen Benutzer der Hubadministratorgruppen oder der Administratorgruppe des Partners geändert werden.

Achtung: Administrator- und Standardgruppen werden vom System generiert und können nicht bearbeitet oder gelöscht werden. Die Hubadministratorgruppe verfügt über die zusätzliche Gruppe ″Hubadmin″.

Erstellen Sie Gruppen wie folgt:

1. Klicken Sie auf **Kontenadmin** > **Profile** > **Gruppen**. Das System ruft die Anzeige **Gruppenliste** auf.
2. Klicken Sie in der oberen rechten Ecke der Anzeige auf **Erstellen**. Das System ruft die Anzeige **Gruppendetails** auf.
3. Geben Sie **Name** und **Beschreibung** der neuen Gruppe ein.
4. Klicken Sie auf **Speichern**. Wiederholen Sie diese Schritte, um zusätzliche Gruppen hinzuzufügen.

Benutzer erstellen

Verwenden Sie diese Funktion, um Benutzerprofile zu erstellen. Das System verwendet Partnerprofile zum Steuern des Konsolzugriffs, der Alertzustellung und der Benutzersichtbarkeit.

Ein Benutzerprofil beinhaltet den Namen des Benutzers und seine Kontaktinformationen (E-Mail-Adresse und Telefonnummer), den Anmeldestatus (**Aktiviert** oder **Inaktiviert**) sowie den Alertstatus (**Aktiviert** oder **Inaktiviert**) und die Sichtbarkeit (**Lokal** oder **Global**). Der Benutzername ist eindeutig.

- Ist der Anmeldestatus eines Benutzers **Aktiviert**, kann er sich an der Community Console anmelden. Ist der Anmeldestatus eines Benutzers **Inaktiviert**, ist eine Anmeldung an der Community Console nicht möglich.
- Ist der Alertstatus eines Benutzers **Aktiviert**, kann er Alertbenachrichtigungen empfangen. Ist der Alertstatus eines Benutzers **Inaktiviert**, kann er keine Alertbenachrichtigungen empfangen.
- Ist die Sichtbarkeit eines Benutzers **Lokal**, ist er nur für Ihr Unternehmen sichtbar. Ist die Sichtbarkeit eines Benutzers **Global**, ist er für die gesamte Hub-Community sichtbar.

Außerdem können Sie automatisch ein Kennwort für einen Benutzer generieren.

Neuen Benutzer erstellen

Mit dieser Funktion können Sie einen neuen Benutzer hinzufügen. Nachdem Sie Ihre Benutzer und Gruppen definiert haben, können Sie den Gruppen Benutzer hinzufügen.

1. Klicken Sie auf **Kontenadmin** > **Profile** > **Benutzer**. Das System ruft die Anzeige **Benutzerliste** auf.
2. Klicken Sie in der oberen rechten Ecke der Anzeige auf **Erstellen**. Das System ruft die Anzeige **Benutzerdetails** auf.
3. Geben Sie bei **Benutzername** den Benutzernamen (Anmeldenamen für den Benutzer) ein.
4. Wählen Sie bei **Status** aus, ob der Konsolzugriff für diesen Benutzer aktiviert oder inaktiviert werden soll.
5. Geben Sie den Vor- und Nachnamen des Benutzer ein (bei **Vorname** und **Nachname**.)
6. Geben Sie bei **E-Mail** die E-Mail-Adresse ein, die das System zum Senden von Alertbenachrichtigungen an den Benutzer verwenden soll.

7. Geben Sie bei **Telefon** und **Faxnummer** die Telefon- und Faxnummer des Benutzers ein.
8. Wählen Sie die Einstellungen für **Sprachlocale**, **Formatlocale** und **Zeitzone** aus.
9. Wählen Sie bei **Alertstatus** aus, ob Sie die Alertbenachrichtigung für diesen Benutzer aktivieren oder inaktivieren möchten. Bei Aktivierung empfängt der Benutzer alle subskribierten Alerts. Bei Inaktivierung empfängt der Benutzer keine Alerts.

   Anmerkung: Der Wert für die Subskribierung wird vom System ausgefüllt.
10. Wählen Sie bei der Option für die subskribierte Sichtbarkeit des Benutzers aus, ob der Benutzer nur für Ihr Unternehmen sichtbar sein soll (**Lokal**) oder für die gesamte Hub-Community (**Global**).
11. Klicken Sie auf **Kennwort autom. generieren**, um ein Kennwort automatisch zu generieren. Wenn Sie für diesen Benutzer ein Kennwort auswählen möchten, geben Sie in den Textfeldern **Kennwort** und **Kennwort bestätigen** das Kennwort ein.
12. Klicken Sie auf **Speichern**. Wiederholen Sie diese Schritte, um zusätzliche Benutzer hinzuzufügen.

FTP-Benutzer konfigurieren

Gehen Sie wie folgt vor, um den aktuellen Benutzer als FTP-Benutzer zu aktivieren:

1. Klicken Sie auf **Kontenadmin** > **Profile** > **Benutzer**. Das System ruft die Anzeige **Benutzerliste** auf.
2. Wählen Sie den gewünschten Benutzer aus, und klicken Sie auf das Symbol **Bearbeiten**.
3. Klicken Sie auf **FTP-Konfiguration**.
4. Geben Sie das **Ausgangsverzeichnis** ein. Hierbei handelt es sich um den relativen Pfad von dem für ″bcg.ftp.config.rootdirectory″ angegebenen Wert. Dieses Feld muss ausgefüllt werden.
5. Aktivieren oder inaktivieren Sie die **Schreibberechtigung** für das Ausgangsverzeichnis.
6. Aktivieren oder inaktivieren Sie die Berechtigung **Verzeichnis erstellen/ entfernen**.
7. Wählen Sie einen Wert für **Maximale Anzahl Anmeldungen** aus. Dies ist die maximal zulässige Anzahl der gleichzeitigen Anmeldungen. Wenn Sie **Angepasste Begrenzung** auswählen, müssen Sie den angepassten Wert im Textfeld eingeben.
8. Wählen Sie einen Wert für **Maximale Anzahl Anmeldungen von derselben IP** aus. Dies ist die maximal zulässige Anzahl der gleichzeitigen Anmeldungen von derselben IP-Adresse. Wenn Sie in der Liste die Option **Angepasste Begrenzung** auswählen, müssen Sie den angepassten Wert im Textfeld eingeben.
9. Wählen Sie einen Wert für **Maximale Leerlaufzeit** aus. Dies ist die maximale Leerlaufzeit der Verbindung in Sekunden, nach der die Benutzerverbindung gelöscht wird. Wenn Sie in der Liste die Option **Angepasste Begrenzung** auswählen, müssen Sie den angepassten Wert im Textfeld eingeben.
10. Wählen Sie einen Wert für **Maximaler Upload** aus. Dies ist die maximale Geschwindigkeit für den Upload in Byte pro Sekunde. Wenn Sie in der Liste die Option **Angepasste Begrenzung** auswählen, müssen Sie den angepassten Wert im Textfeld eingeben.

11. Wählen Sie einen Wert für **Maximaler Download** aus. Dies ist die maximale Geschwindigkeit für den Download in Byte pro Sekunde. Wenn Sie in der Liste die Option **Angepasste Begrenzung** auswählen, müssen Sie den angepassten Wert im Textfeld eingeben.
12. Klicken Sie auf **Speichern**.

Benutzer Gruppen zuordnen

1. Klicken Sie auf **Kontenadmin** > **Profile** > **Benutzer**. Das System ruft die Anzeige **Benutzerliste** auf.
2. Klicken Sie auf das Symbol zum Anzeigen von Details, um die Details der Gruppenzugehörigkeit des Zielbenutzers anzuzeigen.
3. Klicken Sie auf das Symbol zum Bearbeiten, um die Gruppenzugehörigkeiten des Benutzers zu bearbeiten.
4. Wählen Sie eine Gruppe aus, und klicken Sie zum Hinzufügen oder Entfernen eines Benutzers zu der oder aus der Gruppe auf die Schaltflächen **Der Gruppe hinzufügen** bzw. **Aus Gruppe entfernen**.
5. Klicken Sie auf das Symbol zum Ausschalten der Bearbeitung, wenn Sie mit dem Bearbeiten fertig sind.

Kontaktinformationen erstellen

Verwenden Sie die Funktion **Kontakte** zum Erstellen von Kontaktinformationen für wichtige Kontakte. Diese Informationen werden zum Identifizieren der Empfänger von Benachrichtigungen verwendet, wenn Ereignisse auftreten und das System Alertbenachrichtigungen generiert.

In Abhängigkeit von der Größe Ihres Unternehmens möchten Sie wahrscheinlich beim Auftreten verschiedener Typen von Ereignissen verschiedene Kontakte benachrichtigen. Wenn für ein Dokument z. B. die Gültigkeitsprüfung nicht erfolgreich ausgeführt wird, sollten die Ansprechpartner für Sicherheit zur Auswertung des Problems benachrichtigt werden. Überschreiten die Übertragungen des internen Partners die üblichen Grenzen, sollte der Netzwerkadministrator benachrichtigt werden, um sicherzustellen, dass das System die erhöhte Übertragungsrate effizient verarbeitet.

Nachdem Sie die Kontaktinformationen erstellt haben, kehren Sie zur Alertfunktion zurück, um die entsprechenden Kontakte mit den jeweiligen erstellten Alerts zu verbinden.

Erstellen Sie neue Kontakte wie folgt:

1. Klicken Sie auf **Kontenadmin** > **Profile** > **Kontakte**. Das System zeigt eine Liste der aktuellen Kontakte an.
2. Klicken Sie in der oberen rechten Ecke der Anzeige auf **Erstellen**. Das System ruft die Anzeige **Kontaktdetails** auf.
3. Geben Sie den Vor- und Nachnamen der Kontaktperson bei **Vorname** und **Nachname** ein.
4. Geben Sie die Adresse der Kontaktperson bei **Adresse** ein.
5. Wählen Sie den **Kontakttyp** aus der Dropdown-Liste (zum Beispiel: B2B-Leiter oder Geschäftsleiter).
6. Geben Sie die E-Mail-Adresse der Kontaktperson bei **E-Mail** ein.
7. Geben Sie die Telefon- und Faxnummer der Kontaktperson unter **Telefon** und **Faxnummer** ein.

8. Wählen Sie die Einstellungen für **Sprachlocale**, **Locale für das Format** und **Zeitzone** aus.
9. Wählen Sie bei **Alertstatus** aus, ob Sie die Alertbenachrichtigung für diese Kontaktperson aktivieren oder inaktivieren möchten. Bei Aktivierung empfängt die Kontaktperson alle subskribierten Alerts. Bei Inaktivierung empfängt die Kontaktperson keine Alerts.

   Anmerkung: Der Wert für die Subskribierung wird vom System ausgefüllt.
10. Wählen Sie die Einstellung für die subskribierte Sichtbarkeit der Kontaktperson aus. Wenn Sie **Lokal** auswählen, ist der Kontakt nur für Ihr Unternehmen sichtbar. Wenn Sie **Global** auswählen, ist der Kontakt für den Hubadministrator und den internen Partner sichtbar. Sowohl der Hubadministrator als auch der interne Partner kann den Kontakt für Alerts subskribieren.
11. Klicken Sie auf **Speichern**. Es gibt verschiedene Möglichkeiten, um den Kontakt einem Alert hinzuzufügen:

    Informationen zum Hinzufügen eines Kontakts zu einem vorhandenen Alert finden Sie im Abschnitt „Neuen Kontakt zu vorhandenem Alert hinzufügen" auf Seite 40.

    Informationen zur Erstellung eines volumenabhängigen Alerts und zum Hinzufügen von Kontakten zu dem Alert finden Sie im Abschnitt „Volumenabhängigen Alert erstellen" auf Seite 36.

    Informationen zur Erstellung eines ereignisgesteuerten Alerts und zum Hinzufügen von Kontakten zu dem Alert finden Sie im Abschnitt „Ereignisgesteuerten Alert erstellen" auf Seite 38.

Alerts erstellen und Kontakte hinzufügen

Die Zustellung von Informationen zu Systemfehlern an die richtigen Empfänger zur richtigen Zeit ist der Schlüssel zu einer schnellen Fehlerbehebung.

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, Ermittlung und Behebung von Verarbeitungsfehlern.

Ein Alert besteht aus einer textbasierten E-Mail-Nachricht, die an die subskribierten Kontakt oder an eine Verteilerliste von wichtigen Kontakten gesendet wird. Alerts basieren auf dem Auftreten eines Systemereignisses (ereignisgesteuerter Alert) oder auf dem erwarteten Dokumentenflussvolumen (volumenabhängiger Alert).

- Verwenden Sie einen volumenabhängigen Alert zum Empfangen einer Nachricht über steigendes oder abnehmendes Übertragungsvolumen.

  Wenn Sie z. B. ein externer Partner sind, können Sie einen volumenabhängigen Alert erstellen, der Sie benachrichtigt, wenn Sie an einem beliebigen Werktag keine Übertragungen vom internen Partner erhalten (setzen Sie das Volumen auf **Nullvolumen**, die Häufigkeit auf **Täglich** und die Option **Wochentage** auf die Auswahl für Montag bis Freitag). Durch diesen Alert können Netzübertragungsprobleme des internen Partners hervorgehoben werden.

Wenn Sie ein externer Partner sind, können Sie auch einen volumenabhängigen Alert erstellen, der Sie warnt, wenn die Anzahl der Übertragungen vom internen Partner die normale Rate überschreitet. Wenn Sie z. B. normalerweise ungefähr 1000 Übertragungen pro Tag empfangen, können Sie das erwartete Volumen auf 1000 und die prozentuale Abweichung auf 25 % setzen. Sie werden dann durch den Alert benachrichtigt, wenn Sie mehr als 1250 Übertragungen pro Tag empfangen (Sie werden ebenfalls benachrichtigt, wenn das Übertragungsvolumen unter 750 sinkt). Mit Hilfe dieses Alerts kann eine erhöhte Nachfrage auf der Seite des internen Partners ermittelt werden. Diese Nachfrage kann unter Umständen dazu führen, dass Sie langfristig mehr Server zu Ihrer Umgebung hinzufügen müssen.

Beachten Sie, dass die Überwachung des Volumens durch volumenabhängige Alerts auf der Grundlage des Dokumenttyps erfolgt, den Sie beim Erstellen des Alerts auswählen. WebSphere Partner Gateway beachtet nur Dokumente, die den in Ihrem Alert ausgewählten Dokumenttyp beinhalten und generiert nur dann Alerts, wenn alle Kriterien für einen Alert erfüllt sind.

- Verwenden Sie einen ereignisgesteuerten Alert zum Empfangen von Benachrichtigungen, wenn Fehler in der Dokumentverarbeitung auftreten. Möglicherweise möchten Sie z. B. einen Alert erstellen, der Sie benachrichtigt, wenn Ihre Dokumente auf Grund von Gültigkeitsfehlern nicht verarbeitet werden können oder weil Dokumente doppelt empfangen wurden. Sie können auch Alerts erstellen, die Sie benachrichtigen, wenn ein Zertifikat demnächst abläuft.

  Verwenden Sie vordefinierte Ereigniscodes von WebSphere Partner Gateway zum Erstellen von ereignisgesteuerten Alerts. Es gibt fünf Ereignistypen: Debugging, Information, Warnung, Fehler, Kritisch. Innerhalb jedes Ereignistyps gibt es zahlreiche Ereignisse. Sie können vordefinierte Ereignisse in der Anzeige **Alert: Ereignisse** auflisten. Beispiele: **240601 AS-Wiederholungsfehler** oder **108001 Kein Zertifikat**.

Anmerkung: Der externe Partner kann lediglich einen volumenabhängigen Alert erstellen, der auf dem an den internen Partner gesendeten Dokumentvolumen basiert. Will der externe Partner einen volumenabhängigen Alert auf der Grundlage des vom internen Partner an den externen Partner gesendeten Dokumentvolumens erstellen, muss der externe Partner beim Hubadministrator das Einrichten eines volumenabhängigen Alerts anfordern, wobei der externe Partner als Alerteigner angegeben wird.

Tipp:

- Verwenden Sie einen volumenabhängigen Alert zum Empfangen einer Benachrichtigung, wenn das erwartete Übertragungsvolumen des externen Partners oder des internen Partners unter den Betriebsgrenzwert sinkt.
- Durch diesen Alert können Netzübertragungsprobleme des externen Partners oder des internen Partners hervorgehoben werden.
- Verwenden Sie einen ereignisgesteuerten Alert zum Empfangen von Benachrichtigungen, wenn Fehler in der Dokumentverarbeitung auftreten. Sie können z. B. einen ereignisgesteuerten Alert erstellen, der Sie benachrichtigt, wenn die Verarbeitung von Dokumenten auf Grund von Gültigkeitsfehlern fehlgeschlagen ist.

Volumenabhängigen Alert erstellen

1. Klicken Sie auf **Kontenadmin** > **Alerts**. Das System ruft die Anzeige **Alertsuche** auf.
2. Klicken Sie in der oberen rechten Ecke der Anzeige auf **Erstellen**. Das System zeigt die Registerkarte zum Definieren von Alerts an.
3. Wählen Sie **Volumenalert** als **Alerttyp** aus (dies ist die Standardeinstellung). Das System zeigt die entsprechenden Textfelder für einen Volumenalert an.
4. Geben Sie einen **Alertnamen** für den Alert ein.
5. Wählen Sie einen **Partner** mit der Berechtigung zum Erstellen eines volumenabhängigen Alerts aus (nur interner Partner oder Hubadministrator).
6. Wählen Sie das **Paket**, das **Protokoll** und den **Dokumenttyp** in den Dropdown-Listen aus.

   Die Auswahl für das Paket, das Protokoll und den Dokumenttyp muss mit der Auswahl für das Paket, das Protokoll und den Dokumenttyp des externen Partners der Quellen-Community übereinstimmen.
7. Wählen Sie eine der drei Optionen für das Volumen (**Erwartet**, **Bereich** oder **Nullvolumen**) aus, und fahren Sie dann mit Schritt 8 auf Seite 37 fort.
   - **Erwartet** - Wählen Sie diese Option aus, wenn die Generierung eines Alerts beim Abweichen des Dokumenttypvolumens von einer exakten Menge erfolgen soll. Führen Sie folgende Schritte aus, um einen Alert für das erwartete Dokumenttypvolumen zu erstellen:
     a. Geben Sie im Textfeld **Volumen** die Anzahl der erwarteten, innerhalb eines in Schritt 8 ausgewählten Zeitrahmens zu empfangenden Dokumenttypen ein. Geben Sie eine positive Zahl ein. Der Alert funktioniert nicht, wenn hier eine negative Zahl eingegeben wird.
     b. Geben Sie im Textfeld **Abweichung (%)** eine Zahl zur Festlegung des Grenzwerts ein, um den das Dokumentenflussvolumen abweichen kann, bevor es zu einer Aktivierung des Alerts kommt. Beispiel:
        – Ist das Volumen = 20 und die Abweichung (%) = 10, wird ein Alert ausgelöst, wenn das Dokumentenflussvolumen kleiner als 18 oder größer als 22 ist.
        – Ist das Volumen = 20 und die Abweichung (%) = 0, wird ein Alert ausgelöst, wenn das Dokumentenflussvolumen einen beliebigen Wert ungleich 20 aufweist.
   - **Bereich**. Wählen Sie die Option **Bereich** zum Generieren eines Alerts aus, wenn das Dokumentenflussvolumen außerhalb eines Minimum/Maximum-Bereichs liegen soll. Führen Sie folgende Schritte aus, um auf der Basis eines Wertebereichs einen Alert zu erstellen:
     a. Geben Sie im Textfeld **Min** die Mindestanzahl der erwarteten, innerhalb eines in Schritt 8 ausgewählten Zeitrahmens zu empfangenden Dokumenttypen ein. Ein Alert wird nur dann ausgelöst, wenn das Dokumentenflussvolumen unter diesen Wert sinkt.
     b. Geben Sie im Textfeld **Max** die maximale Anzahl der erwarteten, innerhalb eines in Schritt 8 ausgewählten Zeitrahmens zu empfangenden Dokumenttypen ein.

     Anmerkung: In beiden Textfeldern, **Min** und **Max**, muss ein Wert eingegeben werden, wenn ein Alert basierend auf einem Volumenbereich erstellt wird.

- **Nullvolumen**. Wählen Sie **Nullvolumen** aus, um einen Alert auszulösen, wenn keine Dokumenttypen innerhalb eines in Schritt 8 ausgewählten Zeitrahmens auftreten.

8. Geben Sie als Zeitrahmen (Häufigkeit), innerhalb dessen das System das Dokumentenflussvolumen zur Alertgenerierung überwacht, entweder **Täglich** oder **Bereich** aus.
   - **Täglich**. Wählen Sie **Täglich** aus, um das Dokumentenflussvolumen an einem oder mehreren Tagen in der Woche oder im Monat zu überwachen. Wählen Sie z. B. die Option **Täglich** aus, wenn Sie 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.) überwachen möchten.
   - **Bereich**. Wählen Sie **Bereich** aus, wenn Sie das Dokumentenflussvolumen zwischen zwei bestimmten Tagen in der Woche oder im Monat überwachen möchten. Wählen Sie z. B. die Option **Bereich** aus, um das Dokumentenflussvolumen an allen Tagen zwischen Montag und Freitag oder an allen Tagen zwischen dem 5. und 20. jedes Monats zu überwachen.
9. Wählen Sie die Start- und Endzeit im 24-Stundenformat aus, zu der das System das Dokumentenflussvolumen für die im nächsten Schritt ausgewählten Tage überwachen soll. Beachten Sie, dass bei Auswahl einer Bereichshäufigkeit das Dokumentenflussvolumen von der Startzeit des ersten Tages bis zur Endzeit des letzten Tages in dem Bereich überwacht wird.
10. Wählen Sie die entsprechenden Tage der Woche oder des Monats aus, an denen eine Alertüberwachung ausgeführt werden soll. Wenn Sie **Täglich** als Häufigkeit ausgewählt haben, wählen Sie entweder die Wochentage oder die entsprechenden Tage im Monat für die Alertüberwachung aus. Wenn Sie **Bereich** als Häufigkeit ausgewählt haben, wählen Sie zwei Tage in der Woche oder zwei Tage im Monat aus, zwischen denen die Alertüberwachung ausgeführt werden soll.
11. Wählen Sie bei **Alertstatus** den Status dieses Alerts aus: **Aktiviert** oder **Inaktiviert**.
12. Klicken Sie auf **Speichern**.
13. Klicken Sie auf die Registerkarte **Benachrichtigen**.
14. Klicken Sie auf das Symbol zum Bearbeiten.
15. Wählen Sie einen Partner (nur interner Partner und Hubadministrator) aus.
16. Wenn der hinzuzufügende Kontakt im Textfeld der Kontakte aufgelistet ist, wählen Sie ihn aus, und klicken Sie auf **Subskribieren**. Fahren Sie mit Schritt 21 fort.

    Wenn der hinzuzufügende Kontakt nicht im Textfeld der Kontakte aufgelistet ist, klicken Sie auf **Neuen Kontakt hinzufügen**. Das System zeigt das Dialogfeld **Neuen Kontakt erstellen** an.

    Beachten Sie, dass die Option **Neuen Kontakt hinzufügen** nur für den Alerteigner dargestellt wird, um dem Alerteigner zugeordnete Kontakte zu erstellen. Mit dieser Funktion können keine Kontakte für Alertpartner durch den Alerteigner hinzugefügt werden.
17. Geben Sie die E-Mail-Adresse, Telefonnummer und Faxnummer des Kontakts ein.
18. 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 diesen Alert generiert.
    - Wählen Sie **Inaktiviert** aus, falls Sie keine E-Mail-Nachrichten an diesen Kontakt senden möchten, wenn das System diesen Alert generiert.

19. 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. Sowohl der Hubadministrator als auch der interne Partner kann den Kontakt für Alerts subskribieren.
20. Klicken Sie auf **Speichern**, um den Kontakt zu speichern. Klicken Sie auf **Speichern & Subskribieren**, um den Kontakt zur Liste der Kontakte für diesen Alert hinzuzufügen.
21. Klicken Sie auf **Speichern**.

Anmerkung: Die nach der ursprünglichen Überwachungsperiode an volumenabhängigen Alerts ausgeführten Änderungen werden am nächsten Tag der Überwachungsperiode wirksam. Beispielsweise erfolgt eine Überwachung durch einen Alert mittwochs und donnerstags von 13:00 bis 15:00 Uhr. Am Mittwoch um 16:00 Uhr wird die Überwachung durch den Alert auf 17:00 bis 19:00 Uhr geändert. Der Alert überwacht nicht zwei Mal am Mittwoch, sondern die Änderung wird am Donnerstag wirksam.

Ereignisgesteuerten Alert erstellen

Anmerkung: Der E-Mail-Server für Alerts muss konfiguriert werden. Informationen zum Konfigurieren des E-Mail-Servers für Alerts finden Sie im Handbuch *IBM WebSphere Partner Gateway Verwaltung*.

1. Klicken Sie auf **Kontenadmin** > **Alerts**. Das System ruft die Anzeige **Alertsuche** auf.
2. Klicken Sie in der oberen rechten Ecke der Anzeige auf **Erstellen**. Das System zeigt die Registerkarte zum Definieren von Alerts an.
3. Wählen Sie als **Alerttyp** die Einstellung **Ereignisalert** aus. Das System zeigt die entsprechenden Textfelder für einen ereignisgesteuerten Alert an.
4. Geben Sie einen **Alertnamen** für den Alert ein. Dies ist jetzt Ihre Kennung für diesen Alert.
5. Wählen Sie einen **Partner** aus, der den Alert auslösen soll (diese Option ist nur für den internen Partner und den Hubadministrator verfügbar).

   Wählen Sie die Option **Alle Partner** aus, um den Alert allen Partnern im System zuzuordnen. Wenn Sie eine Alertsuche ausführen und als Alertpartner **Alle Partner** auswählen, zeigt das System alle Alerts an, die keinem bestimmten Partner zugeordnet sind.
6. Wählen Sie das **Paket**, das **Protokoll** und den **Dokumenttyp** in den Dropdown-Listen aus.
7. Wählen Sie den Ereignistyp aus: **Debugging**, **Information**, **Warnung**, **Fehler**, **Kritisch** oder **Alle**. Diese Auswahl wirkt als Filter, um die Ereignisse zu begrenzen, die in der Liste **Ereignisname** angezeigt werden.
8. Wählen Sie das Ereignis aus, das 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 benachrichtigt, wenn ein Zertifikat demnächst abläuft.
   - 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

9. Wählen Sie den Status des Alerts aus: **Aktiviert** oder **Inaktiviert**.
10. Klicken Sie auf **Speichern**.
11. Klicken Sie auf die Registerkarte **Benachrichtigen**.
12. Klicken Sie auf das Symbol zum Bearbeiten.
13. Wählen Sie einen Partner (nur interner Partner und Hubadministrator) aus.
14. Wenn der hinzuzufügende Kontakt im Textfeld der Kontakte aufgelistet ist, wählen Sie ihn aus, und klicken Sie auf **Subskribieren**. Fahren Sie mit Schritt 19 fort.

    Wenn der hinzuzufügende Kontakt nicht im Textfeld der Kontakte aufgelistet ist, klicken Sie auf **Neuen Kontakt hinzufügen**. Das System zeigt das Dialogfeld **Neuen Kontakt erstellen** an.

    Beachten Sie, dass die Option **Neuen Kontakt hinzufügen** nur für den Alerteigner dargestellt wird, um dem Alerteigner zugeordnete Kontakte zu erstellen. Mit dieser Funktion können durch den Alerteigner keine Kontakte für Alertpartner hinzugefügt werden.
15. Geben Sie die E-Mail-Adresse, Telefonnummer und Faxnummer des Kontakts ein. Nur die E-Mail-Adresse wird zum Senden von Alerts verwendet. Die übrigen Einträge dienen als zusätzliche Informationsquelle.
16. 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 diesen Alert generiert.
    - Wählen Sie **Inaktiviert** aus, falls Sie keine E-Mail-Nachrichten an diesen Kontakt senden möchten, wenn das System diesen Alert generiert.
17. 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. Sowohl der Hubadministrator als auch der interne Partner kann den Kontakt für Alerts subskribieren.
18. Klicken Sie zum Speichern des Kontakts auf **Speichern**. Klicken Sie auf **Speichern und subskribieren**, um den Kontakt zu speichern und der Liste der Kontakte für diesen Alert hinzuzufügen.
19. Wählen Sie den Zustellmodus aus:
    - **Alerts unverzüglich senden**. Wenn Sie diese Option auswählen, sendet das System beim Auftreten des Alerts Alertbenachrichtigungen an den Kontakt. Verwenden Sie diese Option für kritische Alerts.
    - **Alerts stapeln nach**. Bei Auswahl dieser Option können Sie angeben, wann der Kontakt Alertbenachrichtigungen empfangen soll. Verwenden Sie diese Option für nicht kritische Alerts.

      Die Optionen **Anzahl** und **Zeit** schließen sich nicht gegenseitig aus.

      Bei Auswahl der Option **Anzahl** muss immer auch die Option **Zeit** ausgewählt werden.

      – Wird die Anzahl der Alerts (**Anzahl**) während des Zeitlimits erreicht, den Sie angegeben haben (**Zeit**), generiert das System eine Alertbenachrichtigung.

      – Tritt ein Alert auf, ohne dass die Anzahl der Alerts (**Anzahl**) während des ausgewählten Zeitlimits (**Zeit**) erreicht wurde, generiert das System bei Ablauf des Zeitlimits eine Alertbenachrichtigung.

Die Option **Zeit** kann ohne die Option **Anzahl** verwendet werden; der Option **Anzahl** muss jedoch immer ein Zeitlimit (**Zeit**) zugeordnet werden.

– **Anzahl**. Bei Auswahl dieser Option muss ebenfalls die Option **Zeit** verwendet werden. Geben Sie eine Zahl (n) ein. Dies ist die Anzahl der Alerts, die innerhalb des ausgewählten Zeitraums (**Zeit**) auftreten müssen, damit das System eine Alertbenachrichtigung an den Kontakt für diesen Alert sendet.

  Nachfolgend finden Sie ein Beispiel für die Zusammenarbeit dieser beiden Optionen:

  In unserem Beispiel sind die Optionen für **Alerts stapeln nach** für die Anzahl auf 10 (10 Alerts) und für die Zeit auf 2 (2 Stunden) gesetzt. Das System hält alle Benachrichtigungen für diesen Alert zurück, bis 10 Alerts in einem Zeitraum von zwei Stunden auftreten oder bis das Ende des Zeitraums erreicht wird.

  Erreicht die Alertanzahl 10 in einem Zeitraum von zwei Stunden, sendet das System alle Alertbenachrichtigungen für diesen Alert an den Kontakt.

  Tritt ein Alert auf, ohne dass 10 Alerts während des Zeitraums (zwei Stunden) eingetreten sind, sendet das System am Ende des Zeitraums eine Alertbenachrichtigung für den Alert an den Kontakt.

– **Zeit**. Wählen Sie die Anzahl der Stunden (n) aus. Das System hält Alertbenachrichtigungen n Stunden lang zurück. Alle n Stunden sendet das System alle zurückgehaltenen Alertbenachrichtigungen an den Kontakt.

  Wenn Sie beispielsweise 2 eingeben, hält das System alle Benachrichtigungen für diesen Alert zurück, die in einem Intervall von zwei Stunden auftreten. Ist der Intervall von zwei Stunden zu Ende, sendet das System alle Alertbenachrichtigungen.

20. Klicken Sie auf **Speichern**.

Neuen Kontakt zu vorhandenem Alert hinzufügen

1. Klicken Sie auf **Kontenadmin** > **Alerts**. Das System ruft die Anzeige **Alertsuche** auf.
2. Geben Sie die Suchkriterien mit Hilfe der Dropdown-Listen ein. Geben Sie den Namen des Alerts ein.
3. Klicken Sie auf **Suchen**. Das System zeigt eine Liste der Alerts an, auf die Ihre Suchkriterien zutreffen, falls vorhanden.
4. Klicken Sie auf das Symbol zum Anzeigen von Details, um Details zu den Alerts anzuzeigen.
5. Klicken Sie auf das Symbol zum Bearbeiten, um die Alertdetails zu bearbeiten.
6. Klicken Sie auf die Registerkarte **Benachrichtigen**.
7. Wählen Sie einen Partner (nur interner Partner und Hubadministrator) aus.
8. Wenn der hinzuzufügende Kontakt im Textfeld der Kontakte aufgelistet ist, wählen Sie ihn aus, und klicken Sie auf **Subskribieren**. Fahren Sie mit Schritt 13 fort.

   Wenn der hinzuzufügende Kontakt nicht im Textfeld der Kontakte aufgelistet ist, klicken Sie auf **Neuen Kontakt hinzufügen**. Das System zeigt das Dialogfeld **Neuen Kontakt erstellen** an.

   Beachten Sie, dass die Option **Neuen Kontakt hinzufügen** nur für den Alerteigner dargestellt wird, um dem Alerteigner zugeordnete Kontakte zu erstellen. Mit dieser Funktion können durch den Alerteigner keine Kontakte für Alertpartner hinzugefügt werden.

9. Geben Sie die E-Mail-Adresse, Telefonnummer 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 diesen Alert generiert.
    - Wählen Sie **Inaktiviert** aus, falls Sie keine E-Mail-Nachrichten an diesen Kontakt senden möchten, wenn das System diesen 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. Sowohl der Hubadministrator als auch der interne Partner kann den Kontakt für Alerts subskribieren.
12. Klicken Sie zum Speichern des Kontakts auf **Speichern**. Klicken Sie auf **Speichern und subskribieren**, um den Kontakt zu speichern und der Liste der Kontakte für diesen Alert hinzuzufügen.
13. Klicken Sie auf **Speichern**.

Neue Adresse erstellen

Mit dieser Funktion können Sie Adressen in Ihrem Partnerprofil erstellen. Das System ist für die Unterstützung verschiedener Adresstypen für die Positionen **Unternehmen**, **Rechnungsstellung** und **Technik** konfiguriert.

Erstellen Sie eine neue Adresse wie folgt:

1. Klicken Sie auf **Kontenadmin** > **Profile** > **Adressen**. Das System ruft die Anzeige **Adressen** auf.
2. Klicken Sie in der oberen rechten Ecke der Anzeige auf **Erstellen** > **Neu** > **Adresse**. Das System ruft die Anzeige **Adressen** auf.
3. Wählen Sie den Adresstyp aus der Dropdown-Liste aus (**Rechnungsstellung**, **Unternehmen** oder **Technik**).
4. Geben Sie die Adresse im entsprechenden Textfeld ein.
5. Klicken Sie auf **Speichern**.

Kapitel 3. Ziele erstellen

Ziele definieren Eingangspunkte in das System. Im vorliegenden Kapitel werden die Arbeitsschritte zum Erstellen von Zielen erläutert und die folgenden Themen behandelt:

Übersicht

WebSphere Partner Gateway verwendet Ziele, um Dokumente an die richtigen Bestimmungsorte weiterzuleiten. Der Empfänger kann ein externer Partner oder der interne Partner sein. Das Transportprotokoll für abgehende Dokumente legt fest, welche Informationen während der Zielkonfiguration verwendet werden.

Die folgenden Transportprotokolle werden für die Partnerziele (standardmäßig) unterstützt:

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

  Anmerkung: Sie können ein SMTP-Ziel nur für externe Partner (nicht für den internen Partner) definieren.
- Dateiverzeichnis
- FTP-Scripting

Sie können ferner ein benutzerdefiniertes Transportprotokoll angeben, das Sie während der Erstellung des Ziels hochladen.

HTTP-Ziel einrichten

Sie können ein HTTP-Ziel so einrichten, dass Dokumente vom Hub an die IP-Adresse Ihres Partners gesendet werden. Beim Einrichten eine 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 der Erstellung eines HTTP-Ziels zu beginnen:

1. Klicken Sie auf **Kontenadmin > Profile > Ziele**.
2. Klicken Sie auf **Erstellen**.

Zieldetails

Führen Sie auf der Seite **Liste der Ziele** die folgenden Arbeitsschritte aus:

1. Geben Sie den Namen ein, um das Ziel zu identifizieren. Dieses Feld muss ausgefüllt werden. Der hier eingegebene Name wird später in der Liste der Ziele aufgeführt.
2. Geben Sie optional den Status des Ziels an. Die Standardeinstellung lautet **Aktiviert**. Ein Ziel, das aktiviert wurde, kann zum Senden von Dokumenten verwendet werden. Ein inaktiviertes Ziel kann hingegen nicht für den Dokumentenversand eingesetzt werden.
3. Geben Sie optional an, ob sich das Ziel im Online- oder Offlinemodus befindet. Die Standardeinstellung ist **Online**.
4. Geben Sie optional eine Beschreibung für das Ziel ein.

Zielkonfiguration

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

1. Wählen Sie optional einen zu verwendenden Proxy-Server aus. Die **Forward Proxy-Liste** enthält alle von Ihnen erstellten Proxy-Server sowie den Standard-Proxy-Server. Der Standardwert für dieses Feld ist **Standardmäßigen Forward Proxy verwenden**. Wenn der ausgewählte Partner einen anderen Proxy-Server verwenden soll, wählen Sie diesen Server in der Liste aus. Wenn diese Funktion nicht für den ausgewählten Partner verwendet werden soll, wählen Sie die Option **Keinen Forward Proxy verwenden** aus.
2. Wählen Sie in der Liste **Transport** den Eintrag für **HTTP/1.1** aus.
3. Geben Sie im Feld **Adresse** die URI ein, an die das Dokument zugestellt werden soll. Dieses Feld muss ausgefüllt werden.

   Das Format lautet: http://*<server name>:<optional port>/<path>*

   Beispiel:

   ```
   http://anotherserver.ibm.com:57080/bcgreceiver/Receiver
   ```

   Wenn Sie ein Ziel für einen Web-Service einrichten, müssen Sie die private URL angeben, die vom Web-Service-Provider bereitgestellt wurde. Diese URL gibt die Adresse an, unter der WebSphere Partner Gateway den Web-Service aufruft, wenn dieser als Proxy für den Web-Service-Provider eingesetzt wird.
4. Geben Sie optional einen Benutzernamen und ein Kennwort ein, wenn diese Angaben für den Zugriff auf den HTTP-Server erforderlich sind.
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 im Feld **Anzahl Threads** die Anzahl der Dokumente ein, die gleichzeitig verarbeitet werden können. Der Standardwert ist ″3″.
8. Wählen Sie im Feld **Client-IP prüfen** den Wert **Ja** aus, wenn die IP-Adresse des Absenders geprüft werden soll, bevor das Dokument verarbeitet wird. Wählen Sie andernfalls **Nein** aus. Der Standardwert ist **Nein**.

9. Wählen Sie im Feld **Autom. Warteschlange** den Wert **Ja** aus, wenn das Ziel (automatisch) in den Offlinemodus versetzt werden soll, wenn voraussichtlich ein Zustellungsfehler auf Grund einer zu erwartenden Überschreitung der zulässigen Wiederholungsanzahl auftritt. Wählen Sie andernfalls **Nein** aus. Der Standardwert 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 Vorbereitungs- oder Nachbereitungsschritt für das Ziel konfigurieren wollen, sollten Sie die Informationen im Abschnitt „Handler konfigurieren" auf Seite 56 lesen. Klicken Sie andernfalls auf **Speichern**.

HTTPS-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 ein HTTPS-Ziel zu erstellen:

1. Klicken Sie auf **Kontenadmin > Profile > Ziele**.
2. Klicken Sie auf **Erstellen**.

Zieldetails

Führen Sie auf der Seite **Liste der Ziele** die folgenden Arbeitsschritte aus:

1. Geben Sie den Namen ein, um das Ziel zu identifizieren. Dieses Feld muss ausgefüllt werden.
2. Geben Sie optional den Status des Ziels an. Die Standardeinstellung lautet **Aktiviert**. Ein Ziel, das aktiviert wurde, kann zum Senden von Dokumenten verwendet werden. Ein inaktiviertes Ziel kann hingegen nicht für den Dokumentenversand eingesetzt werden.
3. Geben Sie optional an, ob sich das Ziel im Online- oder Offlinemodus befindet. Die Standardeinstellung ist **Online**.
4. Geben Sie optional eine Beschreibung für das Ziel ein.

Zielkonfiguration

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

1. Wählen Sie in der Liste **Transport** den Eintrag für **HTTPS/1.0** oder **HTTPS/1.1** aus. Die Konfiguration des HTTP/S-Ziels umfasst nicht die Konfiguration des Forward Proxy.
2. Geben Sie im Feld **Adresse** die URI ein, an die das Dokument zugestellt werden soll. Dieses Feld muss ausgefüllt werden.

   Das Format lautet: https://*<server name>:<optional port>/<path>*

   Beispiel:

   ```
   https://anotherserver.ibm.com:57443/bcgreceiver/Receiver
   ```
3. Geben Sie optional einen Benutzernamen und ein Kennwort ein, wenn diese Angaben für den Zugriff auf den gesicherten 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** den Wert **Ja** aus, wenn die IP-Adresse des Absenders geprüft werden soll, bevor das Dokument verarbeitet wird. Wählen Sie andernfalls **Nein** aus. Der Standardwert ist **Nein**.
8. Wählen Sie im Feld **Client-SSL-Zertifikat prüfen** die Option **Ja** aus, wenn das digitale Zertifikat des sendenden Partners in Bezug auf die dem Dokument zugeordnete Geschäfts-ID geprüft werden soll. Der Standardwert ist **Nein**.
9. Wählen Sie im Feld **Autom. Warteschlange** den Wert **Ja** aus, wenn das Ziel (automatisch) in den Offlinemodus versetzt werden soll, wenn voraussichtlich ein Zustellungsfehler auf Grund einer zu erwartenden Überschreitung der zulässigen Wiederholungsanzahl auftritt. Wählen Sie andernfalls **Nein** aus. Der Standardwert 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 Vorbereitungs- oder Nachbereitungsschritt für das Ziel konfigurieren wollen, sollten Sie die Informationen im Abschnitt „Handler konfigurieren” auf Seite 56 lesen. Klicken Sie andernfalls auf **Speichern**.

FTP-Ziel einrichten

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

1. Klicken Sie auf **Kontenadmin > Profile > Ziele**.
2. Klicken Sie auf **Erstellen**.

Zieldetails

Führen Sie auf der Seite **Zieldetails** die folgenden Arbeitsschritte aus:

1. Geben Sie den Namen ein, um das Ziel zu identifizieren. Dieses Feld muss ausgefüllt werden.
2. Geben Sie optional den Status des Ziels an. Die Standardeinstellung lautet **Aktiviert**. Ein Ziel, das aktiviert wurde, kann zum Senden von Dokumenten verwendet werden. Ein inaktiviertes Ziel kann hingegen nicht für den Dokumentenversand eingesetzt werden.
3. Geben Sie optional an, ob sich das Ziel im Online- oder Offlinemodus befindet. Die Standardeinstellung ist **Online**.
4. Geben Sie optional eine Beschreibung für das Ziel ein.

Zielkonfiguration

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

1. Wählen Sie in der Liste **Transport** den Eintrag für **FTP** aus.

2. Geben Sie im Feld **Adresse** die URI ein, an die das Dokument zugestellt werden soll. Dieses Feld muss ausgefüllt werden.

   Das Format lautet: ftp://<*ftp server name*>: <*portno*>

   Beispiel:

   ```
   ftp://ftpserver1.ibm.com:2115
   ```

   Wenn Sie keine Portnummer eingeben, verwendet das System den FTP-Standardport.
3. Geben Sie optional einen Benutzernamen und ein Kennwort ein, wenn diese Angaben für den Zugriff auf den FTP-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** den Wert **Ja** aus, wenn die IP-Adresse des Absenders geprüft werden soll, bevor das Dokument verarbeitet wird. Wählen Sie andernfalls **Nein** aus. Der Standardwert ist **Nein**.
8. Wählen Sie im Feld **Autom. Warteschlange** den Wert **Ja** aus, wenn das Ziel (automatisch) in den Offlinemodus versetzt werden soll, wenn voraussichtlich ein Zustellungsfehler auf Grund einer zu erwartenden Überschreitung der zulässigen Wiederholungsanzahl auftritt. Wählen Sie andernfalls **Nein** aus. Der Standardwert 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. Behalten Sie die Auswahl des Kontrollkästchens unter **Eindeutigen Dateinamen verwenden** bei, wenn dies sinnvoll ist. Andernfalls können Sie die Auswahl zurücknehmen, indem Sie auf das Kontrollkästchen klicken, um den Haken zu entfernen. Wenn Sie die Option **Eindeutigen Dateinamen verwenden** auswählen, wird der ursprüngliche Dateiname in der Datenbank gespeichert.
11. Wenn Sie den Vorbereitungs- oder Nachbereitungsschritt für das Ziel konfigurieren wollen, sollten Sie die Informationen im Abschnitt „Handler konfigurieren” auf Seite 56 lesen. Klicken Sie andernfalls auf **Speichern**.

SMTP-Ziel einrichten

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

1. Klicken Sie auf **Kontenadmin > Profile > Ziele**.
2. Klicken Sie auf **Erstellen**.

Zieldetails

Führen Sie auf der Seite **Liste der Ziele** die folgenden Arbeitsschritte aus:

1. Geben Sie den Namen ein, um das Ziel zu identifizieren. Dieses Feld muss ausgefüllt werden.

2. Geben Sie optional den Status des Ziels an. Die Standardeinstellung lautet **Aktiviert**. Ein Ziel, das aktiviert wurde, kann zum Senden von Dokumenten verwendet werden. Ein inaktiviertes Ziel kann hingegen nicht für den Dokumentenversand eingesetzt werden.
3. Geben Sie optional an, ob sich das Ziel im Online- oder Offlinemodus befindet. Die Standardeinstellung ist **Online**.
4. Geben Sie optional eine Beschreibung für das Ziel ein.

Zielkonfiguration

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

1. Wählen Sie in der Liste **Transport** den Eintrag für **SMTP** aus.
2. Geben Sie im Feld **Adresse** die URI ein, an die das Dokument zugestellt werden soll. Dieses Feld muss ausgefüllt werden.

   Das Format lautet: mailto:*<user@server name>*

   Beispiel:

   ```
   mailto:admin@anotherserver.ibm.com
   ```
3. Geben Sie optional einen Benutzernamen und ein Kennwort ein, wenn diese Angaben für den Zugriff auf den SMTP-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** den Wert **Ja** aus, wenn die IP-Adresse des Absenders geprüft werden soll, bevor das Dokument verarbeitet wird. Wählen Sie andernfalls **Nein** aus. Der Standardwert ist **Nein**.
8. Wählen Sie im Feld **Autom. Warteschlange** den Wert **Ja** aus, wenn das Ziel (automatisch) in den Offlinemodus versetzt werden soll, wenn voraussichtlich ein Zustellungsfehler auf Grund einer zu erwartenden Überschreitung der zulässigen Wiederholungsanzahl auftritt. Wählen Sie andernfalls **Nein** aus. Der Standardwert 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 **Authentifizierung erforderlich** an, ob für das Dokument ein Benutzername und ein Kennwort angegeben werden. Der Standardwert ist **Nein**.
10. Wenn Sie den Vorbereitungs- oder Nachbereitungsschritt für das Ziel konfigurieren wollen, sollten Sie die Informationen im Abschnitt „Handler konfigurieren” auf Seite 56 lesen. Klicken Sie andernfalls auf **Speichern**.

JMS-Ziel einrichten

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

1. Klicken Sie auf **Kontenadmin > Profile > Ziele**.
2. Klicken Sie auf **Erstellen**.

Zieldetails

Führen Sie auf der Seite **Liste der Ziele** die folgenden Arbeitsschritte aus:

1. Geben Sie den Namen ein, um das Ziel zu identifizieren. Dieses Feld muss ausgefüllt werden.
2. Geben Sie optional den Status des Ziels an. Die Standardeinstellung lautet **Aktiviert**. Ein Ziel, das aktiviert wurde, kann zum Senden von Dokumenten verwendet werden. Ein inaktiviertes Ziel kann hingegen nicht für den Dokumentenversand eingesetzt werden.
3. Geben Sie optional an, ob sich das Ziel im Online- oder Offlinemodus befindet. Die Standardeinstellung ist **Online**.
4. Geben Sie optional eine Beschreibung für das Ziel ein.

Zielkonfiguration

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

1. Wählen Sie in der Liste **Transport** den Eintrag für **JMS** aus.
2. Geben Sie im Feld **Adresse** die URI ein, an die das Dokument zugestellt werden soll. Dieses Feld muss ausgefüllt werden.

   Für WebSphere MQ JMS lautet das Format der URI-Zieladresse wie folgt:

   ```
   file:///<user_defined_MQ_JNDI_bindings_path>
   ```

   Beispiel:

   ```
   file:///opt/JNDI-Directory
   ```

   Das Verzeichnis enthält die Bindungsdatei (".bindings") für die dateibasierte JNDI-Komponente. Diese Datei gibt für WebSphere Partner Gateway an, wie das Dokument an das angegebene Ziel weitergeleitet werden soll. Dieses Feld muss ausgefüllt werden.
3. Geben Sie optional einen JMS-Benutzernamen und ein Kennwort ein, wenn diese Angaben für den Zugriff auf die JMS-Warteschlange 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** den Wert **Ja** aus, wenn die IP-Adresse des Absenders geprüft werden soll, bevor das Dokument verarbeitet wird. Wählen Sie andernfalls **Nein** aus. Der Standardwert ist **Nein**.
8. Wählen Sie im Feld **Autom. Warteschlange** den Wert **Ja** aus, wenn das Ziel (automatisch) in den Offlinemodus versetzt werden soll, wenn voraussichtlich ein Zustellungsfehler auf Grund einer zu erwartenden Überschreitung der zulässigen Wiederholungsanzahl auftritt. Wählen Sie andernfalls **Nein** aus. Der Standardwert 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 **Authentifizierung erforderlich** an, ob für das Dokument ein Benutzername und ein Kennwort angegeben werden. Der Standardwert ist **Nein**.

10. Geben Sie im Feld **JMS-Factory-Name** den Namen der Java-Klasse ein, die der JMS-Provider für die Verbindung zur JMS-Warteschlange verwendet. Dieses Feld muss ausgefüllt werden.
11. Geben Sie im Feld **JMS-Nachrichtenklasse** die Nachrichtenklasse ein. Hierbei können Sie alle zulässigen JMS-Nachrichtenklassen wie z. B. TextMessage oder BytesMessage auswählen. Dieses Feld muss ausgefüllt werden.
12. Geben Sie im Feld **JMS-Nachrichtentyp** den gewünschten Nachrichtentyp ein. Dieses Feld muss nicht zwingend ausgefüllt werden.
13. Geben Sie im Feld **Provider-URL-Pakete** den Namen der Klassen (oder der JAR-Datei) ein, die Java zum Erkennen der JMS-Kontext-URL verwendet. Dieses Feld kann optional ausgefüllt werden. Wird hier kein Wert angegeben, verwendet das System den Dateisystempfad zur Bindungsdatei.
14. Geben Sie im Feld **JMS-Warteschlangenname** den Namen der JMS-Warteschlange ein, an die die zu verarbeitenden Dokumente gesendet werden sollen. Dieses Feld muss ausgefüllt werden.
15. Geben Sie im Feld **JMS-JNDI-Factory-Name** den Factory-Namen ein, der zum Herstellen der Verbindung zum Namensservice verwendet wird. Dieses Feld muss ausgefüllt werden.
16. Wenn Sie den Vorbereitungs- oder Nachbereitungsschritt für das Ziel konfigurieren wollen, sollten Sie die Informationen im Abschnitt „Handler konfigurieren" auf Seite 56 lesen. Klicken Sie andernfalls auf **Speichern**.

Dateiverzeichnisziel einrichten

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

1. Klicken Sie auf **Kontenadmin > Profile > Ziele**.
2. Klicken Sie auf **Erstellen**.

Zieldetails

Führen Sie auf der Seite **Liste der Ziele** die folgenden Arbeitsschritte aus:

1. Geben Sie den Namen ein, um das Ziel zu identifizieren. Dieses Feld muss ausgefüllt werden.
2. Geben Sie optional den Status des Ziels an. Die Standardeinstellung lautet **Aktiviert**. Ein Ziel, das aktiviert wurde, kann zum Senden von Dokumenten verwendet werden. Ein inaktiviertes Ziel kann hingegen nicht für den Dokumentenversand eingesetzt werden.
3. Geben Sie optional an, ob sich das Ziel im Online- oder Offlinemodus befindet. Die Standardeinstellung ist **Online**.
4. Geben Sie optional eine Beschreibung für das Ziel ein.

Zielkonfiguration

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

1. Wählen Sie in der Liste **Transport** den Eintrag für **Dateiverzeichnis** aus.
2. Geben Sie im Feld **Adresse** die URI ein, an die das Dokument zugestellt werden soll. Dieses Feld muss ausgefüllt werden.

   Das Format für UNIX-Systeme und Windows-Systeme, bei denen sich das Dateiverzeichnis auf demselben Laufwerk wie WebSphere Partner Gateway befindet, lautet wie folgt: file:///<path to target directory>

   Beispiel:

   ```
   file:///localfiledir
   ```

Hierbei steht *localfiledir* für ein Verzeichnis unterhalb des Stammverzeichnisses.

Auf Windows-Systemen, bei denen sich das Dateiverzeichnis auf einem anderen Laufwerk als WebSphere Partner Gateway befindet, lautet das Format wie folgt: file:///<drive letter>:/<path>

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** den Wert **Ja** aus, wenn die IP-Adresse des Absenders geprüft werden soll, bevor das Dokument verarbeitet wird. Wählen Sie andernfalls **Nein** aus. Der Standardwert ist **Nein**.
7. Wählen Sie im Feld **Autom. Warteschlange** den Wert **Ja** aus, wenn das Ziel (automatisch) in den Offlinemodus versetzt werden soll, wenn voraussichtlich ein Zustellungsfehler auf Grund einer zu erwartenden Überschreitung der zulässigen Wiederholungsanzahl auftritt. Wählen Sie andernfalls **Nein** aus. Der Standardwert 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. Behalten Sie die Auswahl des Kontrollkästchens unter **Eindeutigen Dateinamen verwenden** bei, wenn dies sinnvoll ist. Andernfalls können Sie die Auswahl zurücknehmen, indem Sie auf das Kontrollkästchen klicken, um den Haken zu entfernen. Wenn Sie die Option **Eindeutigen Dateinamen verwenden** auswählen, wird der ursprüngliche Dateiname in der Datenbank gespeichert.
9. Wenn Sie den Vorbereitungs- oder Nachbereitungsschritt für das Ziel konfigurieren wollen, sollten Sie die Informationen im Abschnitt „Handler konfigurieren″ auf Seite 56 lesen. Klicken Sie andernfalls auf **Speichern**.

FTPS-Ziel einrichten

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

1. Klicken Sie auf **Kontenadmin > Profile > Ziele**.
2. Klicken Sie auf **Erstellen**.

Zieldetails

Führen Sie auf der Seite **Liste der Ziele** die folgenden Arbeitsschritte aus:

1. Geben Sie den Namen ein, um das Ziel zu identifizieren. Dieses Feld muss ausgefüllt werden.
2. Geben Sie optional den Status des Ziels an. Die Standardeinstellung lautet **Aktiviert**. Ein Ziel, das aktiviert wurde, kann zum Senden von Dokumenten verwendet werden. Ein inaktiviertes Ziel kann hingegen nicht für den Dokumentenversand eingesetzt werden.
3. Geben Sie optional an, ob sich das Ziel im Online- oder Offlinemodus befindet. Die Standardeinstellung ist **Online**.
4. Geben Sie optional eine Beschreibung für das Ziel ein.

Zielkonfiguration

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

1. Wählen Sie in der Liste **Transport** den Eintrag für **FTPS** aus.
2. Geben Sie im Feld **Adresse** die URI ein, an die das Dokument zugestellt werden soll. Dieses Feld muss ausgefüllt werden.

   Das Format lautet: ftp://<*ftp server name*>: <*portno*>

   Beispiel:

   ```
   ftp://ftpserver1.ibm.com:2115
   ```

   Wenn Sie keine Portnummer eingeben, verwendet das System den FTP-Standardport.
3. Geben Sie optional einen Benutzernamen und ein Kennwort ein, wenn diese Angaben für den Zugriff auf den gesicherten FTP-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 sollen. Der Standardwert ist ″3″.
7. Wählen Sie im Feld **Client-IP prüfen** den Wert **Ja** aus, wenn die IP-Adresse des Absenders geprüft werden soll, bevor das Dokument verarbeitet wird. Wählen Sie andernfalls **Nein** aus. Der Standardwert ist **Nein**.
8. Wählen Sie im Feld **Autom. Warteschlange** den Wert **Ja** aus, wenn das Ziel (automatisch) in den Offlinemodus versetzt werden soll, wenn voraussichtlich ein Zustellungsfehler auf Grund einer zu erwartenden Überschreitung der zulässigen Wiederholungsanzahl auftritt. Wählen Sie andernfalls **Nein** aus. Der Standardwert 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. Behalten Sie die Auswahl des Kontrollkästchens unter **Eindeutigen Dateinamen verwenden** bei, wenn dies sinnvoll ist. Andernfalls können Sie die Auswahl zurücknehmen, indem Sie auf das Kontrollkästchen klicken, um den Haken zu entfernen. Wenn Sie die Option **Eindeutigen Dateinamen verwenden** auswählen, wird der ursprüngliche Dateiname in der Datenbank gespeichert.
11. Wenn Sie den Vorbereitungs- oder Nachbereitungsschritt für das Ziel konfigurieren wollen, sollten Sie die Informationen im Abschnitt „Handler konfigurieren” auf Seite 56 lesen. Klicken Sie andernfalls auf **Speichern**.

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.

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 stellt ein Beispiel dafür dar, wie eine Verbindung zum angegebenen FTP-Server hergestellt werden kann (für den Name und Kennwort angegeben wurden), wie in das angegebene Verzeichnis des FTP-Servers gewechselt und wie alle Dateien in das angegebene Verzeichnis des Servers hochgeladen werden können.

   ```
   open %BCGSERVERIP% %BCGUSERID% %BCGPASSWORD% %BCGOPTIONx%
   cd %BCGOPTIONx%
   mput *
   quit
   ```

   Beim Aktivieren des Ziels 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 3. 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 bis zu 10 benutzerdefinierte Optionen angeben.
2. Speichern Sie die Datei.

FTP-Scriptbefehle

Zur Erstellung des Scripts können Sie die folgenden Befehle verwenden:

- ascii, binary, passive

  Diese Befehle werden nicht an den FTP-Server gesendet. Sie dienen zur Änderung des Übertragungsmodus (ascii, binary oder passive), der bei der Datenübertragung an den FTP-Server benutzt wird.
- cd

  Mit diesem Befehl kann in das angegebene Verzeichnis gewechselt werden.
- delete

  Mit diesem Befehl kann eine Datei vom FTP-Server gelöscht werden.
- mkdir

  Mit diesem Befehl wird ein Verzeichnis auf dem FTP-Server erstellt.
- mput

  Bei diesem Befehl wird ein einziges Argument angegeben, in dem mindestens eine Datei definiert ist, die an ein fernes System übertragen werden soll. Dieses Argument kann die Standard-Platzhalterzeichen enthalten, um mehrere Dateien anzugeben (z. B. "*" und "?").
- open

  Dieser Befehl akzeptiert die drei Parameter ftp server ip address, username und password. Diese sind den Variablen %BCGSERVERIP%, %BCGUSERID% und %BCGPASSWORD% zugeordnet. Die erste Zeile im FTP-Scripting-Zielscript lautet wie folgt: `open %BCGSERVERIP% %BCGUSERID% %BCGPASSWORD%` .

- quit, bye

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

  Dieser Befehl gibt an, dass alle Eingaben nach QUOTE als Befehl an das ferne System gesendet werden sollen. Auf diese Weise können Befehle an einen fernen FTP-Server gesendet werden, der im FTP-Standardprotokoll möglicherweise nicht definiert ist.
- rmdir

  Dieser Befehl dient zum Entfernen eines Verzeichnisses vom FTP-Server.
- site

  Mit diesem Befehl können Sie sitespezifische Befehle für das ferne System eingeben. Das ferne System stellt dann fest, ob der Befehlsinhalt zulässig ist.

FTP-Scripting-Ziele

Wenn Sie mit FTP-Scripting-Zielen arbeiten, müssen Sie die folgenden Arbeitsschritte ausführen:

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

1. Klicken Sie auf **Kontenadmin > Profile > Ziele**.
2. Klicken Sie auf **Erstellen**.

Zieldetails

Führen Sie auf der Seite **Liste der Ziele** die folgenden Arbeitsschritte aus:

1. Geben Sie den Namen ein, um das Ziel zu identifizieren. Dieses Feld muss ausgefüllt werden.
2. Geben Sie optional den Status des Ziels an. Die Standardeinstellung lautet **Aktiviert**. Ein Ziel, das aktiviert wurde, kann zum Senden von Dokumenten verwendet werden. Ein inaktiviertes Ziel kann hingegen nicht für den Dokumentenversand eingesetzt werden.
3. Geben Sie optional an, ob sich das Ziel im Online- oder Offlinemodus befindet. Die Standardeinstellung ist **Online**.
4. Geben Sie optional eine Beschreibung für das Ziel ein.

Zielkonfiguration

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

1. Wählen Sie in der Liste **Transport** den Eintrag für **FTP-Scripting** aus.
2. Geben Sie die IP-Adresse des FTP-Servers ein, an den die Dokumente gesendet werden sollen. Der hier eingegebene Wert ersetzt bei der Ausführung des FTP-Scripts den Wert %BCGSERVERIP%.
3. Geben Sie die Benutzer-ID und das Kennwort ein, die für den Zugriff auf den FTP-Server erforderlich sind. Die hier eingegebenen Werte ersetzen bei der Ausführung des FTP-Scripts die Werte %BCGUSERID% und %BCGPASSWORD%.
4. Wenn die Zieleinheit im sicheren Modus arbeitet, verwenden Sie für den **FTPS-Modus** die Standardeinstellung **Ja**. Klicken Sie andernfalls auf **Nein**.
5. Führen Sie die folgenden Schritte aus, um die Scriptdatei hochzuladen:
   a. Klicken Sie auf **Scriptdatei hochladen**.

b. Geben Sie den Namen der Datei ein, die das Script für die Dokumentverarbeitung enthält, oder klicken Sie auf **Durchsuchen**, um zu der gewünschten Datei zu navigieren.
c. Klicken Sie auf **Datei laden**, um die Scriptdatei ins Dateitextfeld **Momentan geladene Scriptdatei** zu laden.
d. Wenn Sie die gewünschte Scriptdatei geladen haben, klicken Sie auf **Speichern**.
e. Klicken Sie auf **Fenster schließen**.

6. Geben Sie im Feld **Wiederholungszähler** ein, wie oft das Ziel versuchen soll, ein Dokument zu senden, bevor der Vorgang fehlschlägt. Der Standardwert ist ″3″.
7. Geben Sie im Feld **Wiederholungsintervall** die Zeitdauer ein, die das Ziel zwischen den einzelnen Wiederholungsversuchen warten soll. Der Standardwert ist 300 Sekunden.
8. Geben Sie unter **Verbindungszeitlimit** die Zeitdauer in Sekunden ein, die ein Socket ohne Datenverkehr geöffnet bleiben soll. Der Standardwert ist 120 Sekunden.
9. Geben Sie im Feld **Benutzer sperren** an, ob das Ziel eine Sperre anfordern soll, so dass keine andere Instanz eines FTP-Scripting-Ziels gleichzeitig auf das gewünschte Verzeichnis des FTP-Servers zugreifen kann.

Benutzerdefinierte Attribute

Wenn Sie zusätzliche Attribute angeben wollen, müssen Sie die im Folgenden aufgeführten Arbeitsschritte ausführen. Der Wert, den Sie für die Option eingeben, wird bei Ausführung des FTP-Scripts an Stelle von %BCGOPTION*x*% eingesetzt. Hierbei steht *x* für die Nummer der Option.

1. Klicken Sie auf **Neu**.
2. Geben Sie neben **Option 1** einen Wert ein.
3. Wenn weitere Attribute angegeben werden sollen, müssen Sie nochmals auf **Neu** klicken und dann einen Wert eingeben.
4. Wiederholen Sie Schritt 3 für jedes Attribut, das definiert werden soll.

Beispiel: Sie verwenden das FTP-Script

```
Open %BCGSERVERIP% %BCGUSERID% %BCGPASSWORD%
          cd %BCGOPTION1%
          mput *
          quit
```

In diesem Fall gibt %BCGOPTION% einen Verzeichnisnamen an.

Zeitplan

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

1. Geben Sie an, ob Sie mit der intervall- oder der kalenderbasierten Zeitplanung arbeiten möchten.
   - Wenn Sie **Intervallbasierte Zeitplanung** auswählen, müssen Sie die Anzahl der Sekunden bis zum Sendeaufruf des Ziels angeben (oder den Standardwert übernehmen).
   - Wenn Sie sich für die **Kalenderbasierte Zeitplanung** entscheiden, müssen Sie den Zeitplanungstyp (**Täglicher Zeitplan**, **Wöchentlicher Zeitplan** oder **Angepasster Zeitplan**) auswählen.
     – Wenn Sie **Täglicher Zeitplan** auswählen, müssen Sie die Uhrzeit eingeben, zu der der Sendeaufruf an das Ziel erfolgen soll.

– Wenn Sie **Wöchentlicher Zeitplan** auswählen, müssen Sie zusätzlich zur Uhrzeit mindestens einen Wochentag auswählen.
– Wenn Sie **Angepasster Zeitplan** verwenden wollen, müssen Sie die Uhrzeit und dann die Option **Bereich** oder **Ausgewählte Tage** für die gewünschte Woche bzw. den gewünschten Monat auswählen. Mit Hilfe der Option **Bereich** können Sie das Start- und das Enddatum angeben. (Klicken Sie z. B. auf den Eintrag für **Montag** und **Freitag**, wenn der Sendeaufruf an den Server zu einer bestimmten Uhrzeit und nur an Wochentagen ausgeführt werden soll.) Mit der Option **Ausgewählte Tage** können Sie bestimmte Wochentage oder Tage innerhalb eines Monats auswählen.

2. Wenn Sie den Vorbereitungs- oder Nachbereitungsschritt für das Ziel konfigurieren wollen, sollten Sie die Informationen im Abschnitt „Handler konfigurieren" lesen. Klicken Sie andernfalls auf **Speichern**.

Handler konfigurieren

Für ein Ziel können die beiden Verarbeitungspunkte für die Vorbereitung und die Nachbereitung geändert werden.

Das System bietet keine Standardhandler für den Vorbereitungs- und den Nachbereitungsschritt an. Aus diesem Grund enthält die **Verfügbarkeitsliste** standardmäßig auch keine Handlereinträge. Wenn Sie einen Handler hochgeladen haben, können Sie diesen auswählen und in die **Konfigurationsliste** verschieben.

Um einen benutzerdefinierten Handler für diese Konfigurationspunkte anzuwenden, müssen Sie diesen zuerst hochladen. Weitere Informationen zu den Arbeitsschritten, die zum Hochladen eines Handlers ausgeführt werden müssen, finden Sie im Handbuch *Hubkonfiguration*. Führen Sie anschließend die folgenden Schritte aus:

1. Wählen Sie in der Liste **Konfigurationspunkt-Handler** entweder **preprocess** oder **postprocess** aus.
2. Wählen Sie in der **Verfügbarkeitsliste** den gewünschten Handler aus, und klicken Sie dann auf **Hinzufügen**.
3. Wenn Sie die Attribute des Handlers ändern wollen, müssen Sie diesen in der **Konfigurationsliste** auswählen und dann auf **Konfigurieren** klicken. Daraufhin wird eine Liste der Attribute angezeigt, die geändert werden können. Führen Sie die erforderlichen Änderungen durch, und klicken Sie dann auf die Option für **Werte festlegen**.
4. Klicken Sie auf **Speichern**.

Die **Konfigurationsliste** kann wie folgt weiter bearbeitet werden:

- Entfernen eines Handlers. Wählen Sie hierzu in der **Konfigurationsliste** den gewünschten Handler aus, und klicken Sie dann auf **Entfernen**. Der Handler wird daraufhin in die **Verfügbarkeitsliste** verschoben.
- Ändern der Reihenfolge, in der die Handlerverarbeitung erfolgen soll. Wählen Sie hierzu den gewünschten Handler aus, und klicken Sie dann auf **Nach oben** oder **Nach unten**.

Standardziel angeben

Nachdem Sie Ziele für den internen Partner oder externen Partner erstellt haben, wählen Sie eines der Ziele als Standardziel aus.

1. Klicken Sie auf **Kontenadmin > Profile > Ziele**.
2. Klicken Sie auf **Erstellen**.
3. Klicken Sie auf **Standardziele anzeigen**.

   Daraufhin wird eine Liste mit den für den Partner definierten Zielen angezeigt.
4. 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.
5. Klicken Sie auf **Speichern**.

Kapitel 4. Verbindungen und Benutzer der Community verwalten: Kontenadministrator

Die Funktionen im Modul **Kontenadmin** steuern, wie und von wem WebSphere Partner Gateway verwendet wird.

Beispielsweise kann der Zugriff auf die Community Console und ihre jeweiligen Funktionen gesteuert werden. Außerdem kann beeinflusst werden, wer beim Auftreten von wichtigen Ereignissen Warnungen erhalten soll. Beispiele für diese Ereignisse sind ″Partnerverbindung nicht gefunden″, ″RosettaNet-Gültigkeitsfehler″ und ″Dokumentzustellung fehlgeschlagen″.

Sie verwenden dieses Modul außerdem zum Pflegen Ihres Partnerprofils sowie zum Verwalten von Zertifikaten, Zielen, Benutzern, Gruppen, Kontakten, Adressen, Warnungen und B2B-Funktionalitäten. (B2B-Funktionalitäten definieren die Typen von Geschäftsprozessen, die Ihr System senden und empfangen kann.) Wenn Sie sich mit dem Konfigurationsprozess beschäftigt haben, sind Sie mit diesen Funktionen bereits vertraut.

Tabelle 4. Funktionen des Kontenadministrators

Zu verwendende Funktion
„Ziele verwalten″
„Zertifikate verwalten″ auf Seite 61
„Gruppen verwalten″ auf Seite 61
„Benutzer verwalten″ auf Seite 63
„Kontakte verwalten″ auf Seite 65
„Alerts verwalten″ auf Seite 66
„Adressen verwalten″ auf Seite 68

Ziele verwalten

Verwenden Sie die Funktion **Ziele**, um die Zielinformationen anzuzeigen, die verwendet werden, um Dokumente an ihre ordnungsgemäße Zieladresse weiterzuleiten. Mit dieser Funktion können Sie die Ziel-URI, das Transportprotokoll und den Zielstatus anzeigen.

Achtung: Einige Werte für Ziele sind abhängig vom ausgewählten Transportprotokoll. Einschränkungen sind in der Wertetabelle und in der Vorgehensweise angegeben.

Liste der Ziele anzeigen

Klicken Sie auf **Kontenadmin** > **Profile** > **Ziele**, um eine Liste der Ziele im System anzuzeigen.

Zieldetails anzeigen oder bearbeiten

Wichtig: Wenn Sie ein Ziel inaktivieren, wird damit auch die Partnerverbindung inaktiviert, die dem Ziel zugeordnet ist. Das Ziel funktioniert dann nicht. Wenn Sie das Ziel offline setzen, werden die Dokumente in einer Warteschlange gehalten, bis das Ziel wieder online gesetzt wird.

1. Klicken Sie auf **Kontenadmin** > **Profile** > **Ziele**. Das System ruft die Anzeige **Liste der Ziele** auf.
2. Klicken Sie auf das Symbol zum Anzeigen von Details, um die Zieldetails anzuzeigen.
3. Klicken Sie auf das Symbol zum Bearbeiten, um Zieldetails zu bearbeiten.
4. Bearbeiten Sie die Informationen wie erforderlich. In der folgenden Tabelle werden Werte für Ziele beschrieben.

Tabelle 5. Werte in der Zielanzeige

Wert	Beschreibung
Zielname	Der Name des Ziels. Anmerkung: "Zielname" ist ein Feld mit benutzerdefiniertem, freiem Format. Benutzer sollten für die einzelnen Ziele unterschiedliche Namen verwenden, um potenzielle Verwechslungen zu vermeiden.
Transport	Für die Weiterleitung von Dokumenten verwendetes Protokoll.
Ziel-URI	Die URI des Ziels.
Online oder Offline	Im Offlinemodus werden die Dokumente in einer Warteschlange gehalten, bis das Ziel wieder online gesetzt wird.
Status	**Aktiviert** oder **Inaktiviert**. Dokumente, die durch ein Ziel mit inaktivem Status geleitet werden, können nicht erfolgreich verarbeitet werden.
Standard	Gibt das Standardziel an.

5. Klicken Sie auf **Speichern**.

Standardziele anzeigen, auswählen oder bearbeiten

1. Klicken Sie auf **Kontenadmin** > **Profile** > **Ziele**. Das System ruft die Anzeige **Liste der Ziele** auf.
2. Klicken Sie in der oberen rechten Ecke der Anzeige auf **Standardziele anzeigen**. Das System ruft die Anzeige **Liste der Standardziele** auf.
3. Verwenden Sie die Dropdown-Liste zum Auswählen oder Ändern eines oder mehrerer Standardziele.
4. Klicken Sie auf **Speichern**.

Verwendungsposition eines Ziels anzeigen

Gehen Sie wie folgt vor, um Details dazu anzuzeigen, wo ein bestimmtes Ziel eingesetzt wird:

1. Klicken Sie auf **Kontenadmin** > **Profile** > **Ziele**.
2. Klicken Sie in der Liste der Ziele auf das Symbol **Verwendet von** für das gewünschte Ziel. Eine Liste wird angezeigt, in der aufgeführt wird, wo das ausgewählte Ziel verwendet wird.

   Anmerkung: Diese Anzeige enthält die Informationen auf verschiedenen Seiten, da das Ziel von vielen Kanälen verwendet werden kann. Auf jeder Seite werden maximal 10 Verbindungen angezeigt.

Ziel löschen

Die Funktion zum Löschen eines Ziels ist für alle Ziele mit Ausnahme des Standardziels verfügbar. Gehen Sie wie folgt vor, um ein Ziel zu löschen:

1. Klicken Sie auf **Kontenadmin** > **Profile** > **Ziele**.

2. Klicken Sie in der Liste der Ziele auf das Symbol **Löschen** für das Ziel, das gelöscht werden soll.

   Anmerkung: Das Symbol **Löschen** steht für das Standardziel nicht zur Verfügung. Darüber hinaus ist die Löschoperation nur zulässig, wenn das ausgewählte Ziel nicht für eine Verbindung verwendet wird. Weitere Informationen zur Verwendung von Zielen finden Sie im Abschnitt „Verwendungsposition eines Ziels anzeigen" auf Seite 60.

3. Klicken Sie im Warnfenster auf **OK**, um das Löschen zu bestätigen.

Zertifikate verwalten

Dieser Abschnitt erklärt die Schritte zum Anzeigen, Bearbeiten und Löschen von digitalen Zertifikaten unter Verwendung der Community Console.

Details zu digitalen Zertifikaten anzeigen und bearbeiten

1. Klicken Sie auf **Kontenadmin** > **Profile** > **Zertifikate**. Das System zeigt eine Liste der vorhandenen digitalen Zertifikate an.
2. Klicken Sie auf das Symbol zum Anzeigen von Details, um Details zu den Zertifikaten anzuzeigen. Das System ruft die Anzeige **Zertifikatdetails** auf.
3. Klicken Sie auf das Symbol zum Bearbeiten, um das Zertifikat zu bearbeiten.
4. Bearbeiten Sie die Daten wie erforderlich.
5. Klicken Sie auf **Speichern**.

Digitales Zertifikat inaktivieren

1. Klicken Sie auf **Kontenadmin** > **Profile** > **Zertifikate**. Das System ruft die Anzeige **Zertifikatliste** auf.
2. Klicken Sie auf das Symbol zum Anzeigen von Details, um Details zu den Zertifikaten anzuzeigen. Das System ruft die Anzeige **Zertifikatdetails** auf.
3. Klicken Sie auf das Symbol zum Bearbeiten, um das Zertifikat zu bearbeiten.
4. Klicken Sie auf **Inaktiviert**.
5. Klicken Sie auf **Speichern**.

Gruppen verwalten

Sie können Gruppen unter Verwendung der Community Console anzeigen, bearbeiten und löschen. Diese Funktion ist nur für Benutzer der Administratorgruppe von internen bzw. externen Partnern verfügbar.

Gruppenzugehörigkeiten anzeigen und Benutzer Gruppen zuordnen

1. Klicken Sie auf **Kontenadmin** > **Profile** > **Gruppen**. Das System ruft die Anzeige **Gruppenliste** auf.

Tabelle 6. Werte in der Gruppenlistenanzeige

Wert	Beschreibung
Name	Der Name der Gruppe.
Beschreibung	Die Beschreibung der Gruppe.
Gruppentyp	Der Typ, z. B. ″System″.

2. Klicken Sie auf das Symbol zum Anzeigen von Mitgliedern, um eine Liste der Mitglieder einer Gruppe anzuzeigen. Wird dieses Symbol nicht angezeigt, hat die Gruppe keine Mitglieder. Klicken Sie im Untermenü auf **Zugehörigkeiten**.
3. Klicken Sie auf das Symbol zum Bearbeiten, um die Benutzer einer Gruppe zu bearbeiten.
4. Klicken Sie auf **Der Gruppe hinzufügen**, um Benutzer der Gruppe zuzuordnen.
5. Klicken Sie zum Speichern und Beenden auf das Symbol zum Ausschalten der Bearbeitung.

Gruppenberechtigungen anzeigen, bearbeiten und zuordnen

Die Gruppenberechtigung für Benutzer und Gruppen kann nicht Benutzern der Administratorgruppe festgelegt werden. Die Berechtigungen anderer Gruppen können immer identisch zu oder niedriger als die Administratorberechtigungen sein. Verfügt der Administrator beispielsweise über den Lesezugriff auf die Adresse, kann die Berechtigung anderer Gruppen auf ″Kein Zugriff″ oder ″Lesezugriff″ festgelegt werden.

1. Klicken Sie auf **Kontenadmin** > **Profile** > **Gruppen**. Das System ruft die Anzeige **Gruppenliste** auf.
2. Klicken Sie auf das Symbol zum Anzeigen von Berechtigungen, um die Berechtigungen einer Gruppe anzuzeigen. Das System zeigt eine Liste der ausgewählten Gruppenberechtigungen an.
3. Wählen Sie für jede Komponente **Kein Zugriff**, **Lesezugriff** oder **Lese-/Schreibzugriff** aus.
4. Klicken Sie auf **Speichern**.

Gruppendetails anzeigen oder bearbeiten

1. Klicken Sie auf **Kontenadmin** > **Profile** > **Gruppen**. Das System ruft die Anzeige **Gruppenliste** auf.
2. Klicken Sie auf das Symbol zum Anzeigen von Details, um Details zur Gruppe (Name und Beschreibung) anzuzeigen. Das System ruft die Anzeige **Gruppendetails** auf.
3. Klicken Sie auf das Symbol zum Bearbeiten, um die Gruppendetails zu bearbeiten. (Vom System generierte Gruppen können nicht bearbeitet werden.)
4. Bearbeiten Sie die Daten wie erforderlich.
5. Klicken Sie auf **Speichern**.

Einschränkungen: Administrator- und Standardgruppen werden vom System generiert und können nicht bearbeitet oder gelöscht werden. Der Hubadministrator verfügt über die zusätzliche Gruppe ″Hubadmin″.

Gruppe löschen

1. Klicken Sie auf **Kontenadmin** > **Profile** > **Gruppen**. Das System ruft die Anzeige **Gruppenliste** auf.
2. Klicken Sie auf das Symbol zum Anzeigen von Details, um die Gruppendetails anzuzeigen. Das System ruft die Anzeige **Gruppendetails** auf.
3. Klicken Sie auf das Symbol zum Bearbeiten, um Gruppendetails zu bearbeiten.
4. Klicken Sie auf **Löschen**. Bestätigen Sie, dass Sie die Löschung ausführen möchten.

Achtung: Administrator- und Standardgruppen werden vom System generiert und können nicht bearbeitet oder gelöscht werden.

Benutzer verwalten

Mit dieser Funktion können Sie Partnerprofile anzeigen und bearbeiten. Diese Funktion ist nur für Benutzer der Administratorgruppe von internen bzw. externen Partnern verfügbar.

Anmerkung: Sie können diese Funktion dazu verwenden, einem Benutzer ein neues Kennwort zuzuordnen oder automatisch zu generieren.

1. Klicken Sie auf **Kontenadmin** > **Profile** > **Benutzer**. Das System ruft die Anzeige **Benutzerliste** auf.

   Die folgende Tabelle beschreibt die Werte in der Anzeige **Benutzerliste**.

Tabelle 7. Werte in der Benutzerlistenanzeige

Wert	Beschreibung
Benutzername	Der Anmeldename für die Community Console.
Vollständiger Name	Der vollständige Name des Benutzers.
E-Mail	Die für Alertbenachrichtigungen verwendete E-Mail-Adresse.
Subskribiert	Wenn diese Option ausgewählt ist, werden dem Benutzer ein oder mehrere Alerts zugeordnet. Wird dieser Benutzer aus dem System entfernt, werden alle Alertsubskriptionen für diesen Benutzer ebenfalls entfernt.
Anmeldestatus	Bei aktiviertem Status kann sich der Benutzer bei der Community Console anmelden.

2. Klicken Sie auf das Symbol zum Anzeigen von Details, um die Details zu einem Benutzer anzuzeigen.
3. Klicken Sie auf das Symbol zum Bearbeiten, um die Benutzerdetails zu bearbeiten.
4. Bearbeiten Sie die Informationen wie erforderlich. Die folgende Tabelle beschreibt die Werte in der Anzeige **Benutzerdetails**.

Tabelle 8. Benutzerdetails

Wert	Beschreibung
Benutzername	Der Anmeldename für den Konsolbenutzer.
Aktiviert	Aktivieren oder Inaktivieren des Konsolzugriffs.
Vorname	Der Vorname des Benutzers.
Nachname	Der Nachname des Benutzers.
E-Mail	Die für Alertbenachrichtigungen verwendete E-Mail-Adresse.
Telefon	Die Telefonnummer des Benutzers.
Faxnummer	Die Faxnummer des Benutzers.
Sprachlocale	Auswahl des geografischen Bereichs des Benutzers. Der Standardwert ist die vom Hubadministrator festgelegte Locale.
Formatlocale	Auswahl des Landes des Benutzers. Der Standardwert ist die vom Hubadministrator festgelegte Locale.
Zeitzone	Auswahl der Zeitzone des Benutzers. Der Standardwert ist die vom Hubadministrator festgelegte Zeitzone.
Alertstatus	Bei aktiviertem Status empfängt der Benutzer alle subskribierten Alerts. Wählen Sie **Inaktivieren** aus, wenn dieser Benutzer nicht mehr alle Alerts erhalten soll.
Subskribiert	Dieser Wert wird vom System ausgefüllt.
Sichtbarkeit	Wählen Sie **Lokal** aus, damit der Benutzer nur innerhalb Ihres Unternehmens sichtbar ist. Wählen Sie **Global** aus, damit der Benutzer für Ihr Unternehmen und für den Manager sichtbar ist.

Anmerkung: Die Standardlocale und -zeitzone des Systems nach Installation und Initialisierung ist Englisch (United States) bei UTC (Universal Time Coordinated). Das System verwendet UTC für seine Zeitzonenberechnungen. Der UTC-Standardwert kann auf Systemebene nicht geändert werden. Der Benutzer kann jedoch die Zeitzone ändern, die in der Community Console angezeigt wird.

Wenn sich der Benutzer *Hubadmin* zum ersten Mal im System anmeldet, nimmt er die Locale und Zeitzone des Systems an (Englisch, UTC). Da der Hubadmin-Benutzer als Superuser für die Systemkonfiguration verantwortlich ist, werden die von ihm ausgewählten Einstellungen für Locale und Zeitzone der Community Console als neue Standardwerte für alle Benutzer der Community Console festgelegt. Die einzelnen Benutzer haben auch die Möglichkeit, ihre Locale und Zeitzone nach Bedarf zu ändern.

5. Klicken Sie auf **Speichern**.

Benutzer löschen

Zum Löschen von Benutzern sind die entsprechenden Berechtigungen erforderlich. Mit dieser Funktionalität können alle Benutzer mit Ausnahme des Hubadministrators (HUBADMIN) gelöscht werden.

Verwenden Sie diese Funktion wie folgt, um einen Benutzer zu löschen:

1. Klicken Sie auf **Kontenadmin** > **Profile** > **Benutzer**.
2. Klicken Sie auf das Symbol **Löschen** für den Benutzer, der gelöscht werden soll.
3. Klicken Sie im Warnfenster auf **OK**, um die Löschoperation zu bestätigen. Wenn Sie auf **Abbrechen** klicken, wird die Löschoperation abgebrochen.

Kontakte verwalten

Verwenden Sie die Funktion **Kontakte** zum Anzeigen und Bearbeiten von Kontaktinformationen für wichtige Kontakte.

In Abhängigkeit von der Größe Ihres Unternehmens möchten Sie wahrscheinlich beim Auftreten verschiedener Typen von Ereignissen verschiedene Kontakte benachrichtigen. Wenn für ein Dokument z. B. die Gültigkeitsprüfung nicht erfolgreich ausgeführt wird, sollten die Ansprechpartner für Sicherheit zur Auswertung des Problems benachrichtigt werden. Überschreiten die Übertragungen des internen Partners die üblichen Grenzen, sollte der Netzwerkadministrator benachrichtigt werden, um sicherzustellen, dass das System die erhöhte Übertragungsrate effizient verarbeitet.

Kontaktdetails anzeigen oder bearbeiten

1. Klicken Sie auf **Kontenadmin** > **Profile** > **Kontakte**. Das System zeigt eine Liste der aktuellen Kontakte an.

   Die folgende Tabelle gibt die Werte an, die in der Anzeige **Kontakte** dargestellt werden.

Tabelle 9. Werte in der Kontaktlistenanzeige

Wert	Beschreibung
Vollständiger Name	Der vollständige Name des Kontakts.
Kontakttyp	Beschreibt die Rolle des Kontakts, z. B. B2B-Leiter oder Geschäftsleiter.
E-Mail	Die für Alertbenachrichtigungen verwendete E-Mail-Adresse.
Sichtbarkeit	• Lokal - Der Kontakt ist nur für Ihr Unternehmen sichtbar. • Global - Der Kontakt ist für den Hubadministrator und den internen Partner sichtbar. Sowohl der Hubadministrator als auch der interne Partner kann den Kontakt für Alerts subskribieren.
Subskribiert	Ist diese Option ausgewählt, werden diesem Kontakt einer oder mehrere Alerts zugeordnet. Wird der Kontakt aus dem System entfernt, werden damit auch alle Alertsubskriptionen aus dem System entfernt.
Alertstatus	Wenn der Alertstatus aktiviert ist, empfängt dieser Kontakt alle subskribierten Alerts.

2. Klicken Sie auf das Symbol zum Anzeigen von Details, um Details zu Kontakten anzuzeigen. Das System ruft die Anzeige **Kontaktdetails** auf.
3. Klicken Sie auf das Symbol zum Bearbeiten, um die Kontaktdetails zu bearbeiten.
4. Bearbeiten Sie die Informationen wie erforderlich. In der folgenden Tabelle werden Werte für Kontakte beschrieben.

Tabelle 10. Kontaktdetails

Wert	Beschreibung
Vorname	Der Vorname des Kontakts.
Nachname	Der Nachname des Kontakts.
Adresse	Adresse des Kontakts, einschließlich Straße, Stadt, Staat und Postleitzahl.
Kontakttyp	Beschreibt die Rolle des Kontakts, z. B. B2B-Leiter oder Geschäftsleiter.
E-Mail	E-Mail-Adresse des Kontakts für Alertbenachrichtigung.
Telefon	Die Telefonnummer des Kontakts.
Faxnummer	Die Faxnummer des Kontakts.
Alertstatus	Wenn diese Option aktiviert ist, empfängt der Kontakt alle subskribierten Alerts. Wählen Sie **Inaktivieren** aus, wenn dieser Kontakt nicht mehr alle Alerts erhalten soll.
Subskribiert	Dieser Wert wird vom System ausgefüllt.
Sichtbarkeit	• Lokal - Der Kontakt ist nur für Ihr Unternehmen sichtbar. • Global - Der Kontakt ist für den Hubadministrator und den internen Partner sichtbar. Sowohl der Hubadministrator als auch der interne Partner kann den Kontakt für Alerts subskribieren.

5. Klicken Sie auf **Speichern**.

Kontakt entfernen

1. Klicken Sie auf **Kontenadmin** > **Profile** > **Kontakte**. Das System zeigt eine Liste der aktuellen Kontakte an.
2. Klicken Sie auf das Symbol zum Löschen, um den entsprechenden Kontakt zu löschen.

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.

Alertdetails und Kontakte anzeigen oder bearbeiten

Der interne Partner kann alle Alerts unabhängig vom Alerteigner (dem Ersteller des Alerts) anzeigen.

1. Klicken Sie auf **Kontenadmin** > **Alerts**. Das System ruft die Anzeige **Alertsuche** auf.
2. Wählen Sie die Suchkriterien in den Dropdown-Listen aus, und geben Sie den Alertnamen ein. Sie können auch auf **Suchen** klicken, ohne Suchkriterien auszuwählen (das System zeigt alle Alerts an).
3. Klicken Sie auf **Suchen**. Das System ruft die Anzeige **Alertsuche - Ergebnisse** auf.
4. Klicken Sie auf das Symbol zum Anzeigen von Details, um die Details zu einem Alert anzuzeigen.
5. Klicken Sie auf das Symbol zum Bearbeiten, um die Alertdetails zu bearbeiten.

6. Bearbeiten Sie die Informationen wie erforderlich.
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 die Kontakte für diesen Alert, falls erforderlich.
10. Klicken Sie auf **Speichern**.

Alerts suchen

1. Klicken Sie auf **Kontenadmin** > **Alerts**. Das System ruft die Anzeige **Alertsuche** auf.
2. Wählen Sie die Suchkriterien in den Dropdown-Listen aus, und geben Sie den Alertnamen ein. Sie können auch auf **Suchen** klicken, ohne Suchkriterien auszuwählen (das System zeigt alle Alerts an).

Tabelle 11. Alertsuchkriterien für Partner

Wert	Beschreibung
Alerttyp	Alert für Umfang oder Ereignis bzw. alle Alerttypen.
Alertname	Der Name des Alerts.
Alertstatus	Aktivierte oder inaktivierte Alerts bzw. alle Alerts.
Subskribierte Kontakte	Dem Alert zugeordnete Kontakte. Die Auswahlmöglichkeiten sind **Hat Subskribenten**, **Keine Subskribenten** oder **Alle**.
Ergebnisse pro Seite	Steuert die Art der Anzeige von Suchergebnissen.

Tabelle 12. Alertsuchkriterien für den internen Partner und dne Hubadministrator

Wert	Beschreibung
Alerteigner	Der Ersteller des Alerts.
Alertpartner	Der Partner, für den der Alert zutrifft.
Alerttyp	Alert für Umfang oder Ereignis bzw. alle Alerttypen.
Alertname	Der Name des Alerts.
Alertstatus	Aktivierte oder inaktivierte Alerts bzw. alle Alerts.
Subskribierte Kontakte	Dem Alert zugeordnete Kontakte. Die Auswahlmöglichkeiten sind **Hat Subskribenten**, **Keine Subskribenten** oder **Alle**.
Ergebnisse pro Seite	Steuert die Art der Anzeige von Suchergebnissen.

3. Klicken Sie auf **Suchen**. Das System zeigt eine Liste der Alerts an, auf die Ihre Suchkriterien zutreffen, falls vorhanden.

Alert inaktivieren oder aktivieren

1. Klicken Sie auf **Kontenadmin** > **Alerts**. Das System ruft die Anzeige **Alertsuche** auf.
2. Wählen Sie die Suchkriterien in den Dropdown-Listen aus, und geben Sie den Alertnamen ein.
3. Klicken Sie auf **Suchen**. Das System zeigt eine Liste der Alerts an, auf die Ihre Suchkriterien zutreffen, falls vorhanden.
4. Suchen Sie den Alert und klicken Sie bei ″Status″ auf **Inaktiviert** oder **Aktiviert**. Nur der Hubadministrator und der Alerteigner (der Ersteller des Alerts) sind dazu berechtigt, den Alertstatus zu bearbeiten.

Alert entfernen

1. Klicken Sie auf **Kontenadmin** > **Alerts**. Das System ruft die Anzeige **Alertsuche** auf.
2. Wählen Sie die Suchkriterien in den Dropdown-Listen aus, und geben Sie den Alertnamen ein.
3. Klicken Sie auf **Suchen**. Das System zeigt eine Liste der Alerts an, auf die Ihre Suchkriterien zutreffen, falls vorhanden.
4. Suchen Sie den Alert und klicken Sie auf das Symbol zum Löschen. Nur der Hubadministrator und der Alerteigner (der Ersteller des Alerts) können den Alert entfernen.

Ereignisbenachrichtigung

WebSphere Partner Gateway ermöglicht Ihnen, einen Ereignisalert zu konfigurieren, so dass beim Auftreten eines Ereignisses sowohl der Quellenpartner als auch der Zielpartner des Ereignisses benachrichtigt werden. Es stehen jetzt zwei Optionen für die Alertbenachrichtigung zur Verfügung:

- Alle betroffenen Beteiligten benachrichtigen
- Nur subskribierte Ansprechpartner benachrichtigen

Wenn Sie die Option zur Benachrichtigung aller betroffenen Beteiligten auswählen, benachrichtigt der Alert automatisch die Kontakte des Quellenpartners und des Zielpartners des Ereignisses, sowie die Kontakte des Alerteigners. Der Benutzer muss bei der Auswahl dieses Modus keine subskribierten Ansprechpartner angeben (und ist auch nicht dazu berechtigt). Wenn der Modus zur Benachrichtigung der subskribierten Ansprechpartner ausgewählt ist, benachrichtigt der Alert nur die subskribierten Ansprechpartner.

Nach der Angabe der zu benachrichtigenden Partner, können Sie Folgendes auswählen:

- Alerts unverzüglich senden
- Alerts stapeln nach (Anzahl oder Zeit)

Anmerkung: Der E-Mail-Server für die Alerts muss so konfiguriert sein, dass er diese zusätzliche Funktion verwenden kann. Weitere Anweisung zur Konfiguration dieses Servers finden Sie im *System Administrator Guide* .

Adressen verwalten

Mit dieser Funktion können Sie die Adressen in Ihrem Partnerprofil verwalten.

Adresse bearbeiten

1. Klicken Sie auf **Kontenadmin** > **Profile** > **Adressen**. Das System ruft die Anzeige **Adressen** auf.
2. Suchen Sie die zu bearbeitende Adresse, und klicken Sie auf das Symbol zum Bearbeiten.
3. Führen Sie die erforderlichen Änderungen aus. In der folgenden Tabelle werden Werte für Adressen beschrieben.

Tabelle 13. Adresswerte

Wert	Beschreibung
Adresstyp	Unternehmen, Rechnungsstellung und Technik
Adresse	Adresse, einschließlich Straße, Stadt, Staat und Postleitzahl

4. Klicken Sie auf **Speichern**.

Adresse löschen

1. Klicken Sie auf **Kontenadmin** > **Profile** > **Adressen**. Das System ruft die Anzeige **Adressen** auf.
2. Suchen Sie die zu löschende Adresse, und klicken Sie auf das Symbol zum Löschen.
3. Bestätigen Sie, dass Sie die Adresse löschen möchten.

Kapitel 5. Ereignisse und Dokumente anzeigen: Anzeigefunktionen

Mit den Anzeigefunktionen können Sie den allgemeinen Systemzustand anzeigen. Außerdem werden sie für die Fehlerbehebung bei Problemen mit Ereignissen verwendet.

Das Anzeigemodul umfasst folgende Funktionen:

- „Ereignisanzeige"
- „AS-Anzeige" auf Seite 74
- „ebMS-Anzeige" auf Seite 76
- „RosettaNet-Anzeige" auf Seite 78
- „Dokumentanzeige" auf Seite 81
- „Zielwarteschlange" auf Seite 86

Die RosettaNet- und die AS-Anzeigen umfassen zusätzliche Suchkriterien für den Hubadministrator. Weitere Informationen hierzu finden Sie im Handbuch *Verwaltung*.

Anmerkung: Der Terminus ″Partner″ wird in den Anzeigen verwendet, um Mitglieder der Hub-Community einschließlich des internen Partners zu identifizieren.

Ereignisanzeige

Mit Hilfe der Ereignisanzeige können Sie nach Ereignissen anhand der Zeit, des Datums, des Ereignistyps, des Ereignisnamens und der Ereignisposition suchen. Der Hubadministrator kann außerdem anhand des Partners, der Quellen-IP und der Ereignis-ID suchen.

Die von der Ereignisanzeige generierten Daten identifizieren u. a. den Ereignisnamen, die Zeitmarke und die Quellen-IP. Mit Hilfe dieser Daten können Sie die Ereignis- und Dokumentdetails zur Ermittlung des Problems anzeigen. Außerdem können Sie das unformatierte Dokument anzeigen, welches das Feld, den Wert und die Ursache für den Fehler angibt.

Ein Ereignis informiert Sie darüber, dass im System eine besondere Bedingung eingetreten ist. Ein Ereignis kann Ihnen mitteilen, dass eine Systemoperation oder -funktion erfolgreich ausgeführt wurde (z. B. dass ein Partner erfolgreich zum System hinzugefügt wurde oder eine Partnerverbindung erfolgreich zwischen dem internen Partner und einem externen Partner erstellt wurde). Ein Ereignis kann außerdem ein Problem identifizieren (z. B. dass das System ein Dokument nicht verarbeiten konnte oder einen nicht kritischen Fehler in einem Dokument erkannt hat). Die meisten Dokumentarten werden mehrere Male versandt. Wenn der Versand eines Dokuments fehlschlägt und eine Warnung generiert wird, sollten Sie daher den Fehler suchen und beheben, um ähnliche Fehler in der Zukunft zu vermeiden.

WebSphere Partner Gateway beinhaltet vordefinierte Ereignisse. Verwenden Sie die Alertfunktion des Produkts (Modul **Kontenadmin**) zum Erstellen von ereignisgesteuerten Alerts. Dieser Prozess identifiziert die Ereignisse, die für Sie von

Bedeutung sind. Verwenden Sie anschließend die Funktion **Kontakte** (ebenfalls im Modul **Kontenadmin**), um die Mitarbeiter zu identifizieren, die das System im Falle eines solchen Ereignisses benachrichtigt.

Die Ereignisanzeige stellt Ereignisse basierend auf bestimmten Suchkriterien dar. Sie können ein bestimmtes Ereignis suchen und anschließend nachforschen, warum dieses Ereignis aufgetreten ist. Mit Hilfe der Ereignisanzeige können Sie Ereignisse anhand der Zeit, des Datums, des Ereignistyps (Debugging, Information, Warnung, Fehler und Kritisch), des Ereignisnamens (z. B. 210031) und der Ereignisposition suchen.

Die über die Ereignisanzeige verfügbaren Daten umfassen den Ereignisnamen, die Zeitmarke, den Benutzer und die Partnerinformationen. Mit Hilfe dieser Daten können Sie das Dokument oder den Prozess identifizieren, mit dem das Ereignis erstellt wurde. Bezieht sich das Ereignis auf ein Dokument, können Sie außerdem das unformatierte Dokument anzeigen, welches das Feld, den Wert und die Ursache für den Fehler angibt.

Ereignistypen

WebSphere Partner Gateway umfasst folgende Ereignistypen.

Tabelle 14. Ereignistypen

Ereignistyp	Beschreibung
Debugging	Debugereignisse werden für Operationen und Unterstützung auf niedriger Systemebene verwendet. Ihre Sichtbarkeit und Verwendung unterliegt der Berechtigungsstufe des Benutzers. Nicht alle Benutzer verfügen über den Zugriff auf Debugereignisse.
Informationen	Informationsereignisse werden bei erfolgreicher Fertigstellung einer Systemoperation generiert. Diese Ereignisse stellen auch den Status der aktuell verarbeiteten Dokumente zur Verfügung. Informationsereignisse erfordern keine Benutzeraktion.
Warnung	Warnungsereignisse treten auf Grund von nicht kritischen Abweichungen bei der Dokumentverarbeitung auf oder bei Systemfunktionen, mit deren Hilfe die Operation fortgesetzt werden kann.
Fehler	Fehlerereignisse treten auf Grund von Abweichungen in der Dokumentverarbeitung auf, die das Beenden des Prozesses verursachen.
Kritisch	Kritische Ereignisse werden generiert, wenn Dienste auf Grund eines Systemausfalls beendet werden. Kritische Ereignisse erfordern Maßnahmen durch die Benutzerunterstützung.

Tasks der Ereignisanzeige ausführen

Tabelle 15. Tasks der Ereignisanzeige

Was möchten Sie tun?	Siehe
Ereignisse suchen	Seite 72
Ereignisdetails anzeigen	Seite 73

Ereignisse suchen

1. Klicken Sie auf **Anzeigen** > **Ereignisanzeige**.

   Ereignisse werden in der Anzeige **Ereignisanzeige - Suche** von links nach rechts nach Wertigkeit zusammengefasst. Die Information links ist der unkri-

tischste Ereignistyp, und die Information rechts ist der kritischste Ereignistyp. (Debugereignisse können nicht von allen Benutzern angezeigt werden.) Für jedes ausgewählte Ereignis wird dieses Ereignis sowie alle Ereignisse mit einer höheren Wertigkeit in der Ereignisanzeige angezeigt. Wird z. B. der Warnungsereignistyp in den Suchkriterien ausgewählt, werden die Ereignisse **Warnung**, **Fehler** und **Kritisch** angezeigt. Werden Informationsereignisse ausgewählt, werden alle Ereignistypen angezeigt.

2. Wählen Sie die Suchkriterien in den Dropdown-Listen aus.

Tabelle 16. Suchkriterien für Ereignisse

Wert	Beschreibung
Startdatum und -zeit	Datum und Uhrzeit des Auftretens des ersten Ereignisses. Der Standardwert ist zehn Minuten vorher.
Enddatum und -zeit	Datum und Uhrzeit des Auftretens des letzten Ereignisses.
Partner	Wählen Sie alle Partner oder einen bestimmten Partner (nur interner Partner) aus.
Ereignistyp	Ereignistyp: **Debugging**, **Information**, **Warnung**, **Fehler** oder **Kritisch**.
Ereignisname	Suchen Sie basierend auf dem ausgewählten Ereignistyp nach verfügbaren Ereignisnamen.
Ereignisposition	Position, in der das Ereignis erstellt wurde: alle, unbekannt, Quelle (Sender), Ziel (Empfänger).
Sortieren nach	Wert zum Sortieren von Ergebnissen.
Aufsteigend oder Absteigend	Sortieren in aufsteigender oder absteigender Reihenfolge.
Ergebnisse pro Seite	Anzahl der angezeigten Einträge pro Seite.
Aktualisieren	Die Standardeinstellung ist **Aus**. Wenn die Option **Aktualisieren** auf **Ein** gesetzt ist, führt die Ereignisanzeige erst eine neue Abfrage aus und verbleibt anschließend im Aktualisierungsmodus.
Aktualisierungsrate	Steuert, wie häufig die Suchergebnisse aktualisiert werden sollen (nur interner Partner).

3. Klicken Sie auf **Suchen**. Das System zeigt eine Liste der Ereignisse an.

Tipp: Die Ereignisliste kann basierend auf dem oben in der Ereignisanzeige ausgewählten Ereignistyp erneut gefiltert werden. Mit der nächsten Aktualisierung der Anzeige wird der neu ausgewählte Ereignistyp angezeigt.

Ereignisdetails anzeigen

1. Klicken Sie auf **Anzeigen** > **Ereignisanzeige**.
2. Wählen Sie die Suchkriterien in den Dropdown-Listen aus.
3. Klicken Sie auf **Suchen**. Das System zeigt eine Liste der Ereignisse an.
4. Klicken Sie auf das Symbol zum Anzeigen von Details neben dem Ereignis, das angezeigt werden soll. Das System zeigt die Ereignisdetails und zugeordneten Dokumente an.
5. Klicken Sie auf das Symbol zum Anzeigen von Details neben dem Dokument, das ggf. angezeigt werden soll.
6. Klicken Sie auf das Symbol zum Anzeigen des unformatierten Dokuments, um das unformatierte Dokument ggf. anzuzeigen.
7. Klicken Sie auf das Symbol zum Anzeigen von Gültigkeitsfehlern, um Gültigkeitsfehler anzuzeigen.

Wird die Fehlernachricht ausgegeben, dass kein gültiges Verschlüsselungszertifikat gefunden wurde, ist weder das primäre noch das sekundäre Zertifikat gültig. Die Zertifikate sind möglicherweise abgelaufen oder sie wurden widerrufen. Sind die Zertifikate abgelaufen oder wurden sie widerrufen, wird das entsprechende Ereignis (Kein gültiges Verschlüsselungszertifikat gefunden) in der Ereignisanzeige ausgegeben.

Tipp: Ist in der Detailansicht der Ereignisanzeige die Kopie eines Dokumentereignisses zu sehen, zeigen Sie das zuvor gesendete Originaldokument an, indem Sie unter **Dokumentdetails** auf das Symbol zum Anzeigen des Originaldokuments klicken.

AS-Anzeige

Verwenden Sie die AS-Anzeigen, um Transportinformationen zu Dokumenten zu suchen, die das AS1-, AS2 oder AS3-Übertragungsprotokoll verwenden, und diese anzuzeigen. Sie können Nachrichten-IDs, die Ziel-URI und Status der MDN (Message Disposition Notification) und die Dokumentdetails (das Dokument und den Wrapper) anzeigen.

Die AS-Anzeigen können außerdem zum Anzeigen von gepackten B2B-Transaktionen und B2B-Prozessdetails verwendet werden, die das Übertragungsprotokoll AS1, AS2 oder AS3 (Applicability Statement 1 oder 2) verwenden. Sie können den Ablauf des B2B-Prozesses und der zugeordneten Geschäftsdokumente, Bestätigungssignale, Prozessstatus, HTTP-Header und Inhalte der übertragenen Dokumente anzeigen.

AS2 definiert einen Standard für Datenübertragungen unter Verwendung von HTTP, genauso wie sein Vorläufer AS1 einen Standard für Datenübertragungen unter Verwendung von SMTP definiert.

AS2 gibt an, wie Daten verbunden, zugestellt, geprüft und beantwortet werden können. Dabei wird der Inhalt eines Dokuments nicht beachtet, sondern nur sein Transport. AS2 erstellt eine Oberfläche für das Dokument, sodass es mit Hilfe von HTTP oder HTTPS über das Internet transportiert werden kann. Das Dokument und die Oberfläche zusammen stellen eine Nachricht dar. AS2 bietet Sicherheit und Verschlüsselung der HTTP-Pakete. AS2 bietet eine Verschlüsselungsbasis mit garantierter Zustellung. AS3 stellt einen neuen Standard zur gesicherten Übertragung von Dokumenten über FTP oder FTPS zur Verfügung.

Eine wichtige Komponente von AS2 bildet der Empfangsmechanismus, der als MDN (Message Disposition Notification) bezeichnet wird. Somit kann der Sender des Dokuments sicher sein, dass der Empfänger das Dokument erfolgreich erhalten hat. Dabei gibt der Sender an, wie die MDN zurückgesendet werden soll (synchron oder asynchron; unterzeichnet oder nicht unterzeichnet).

Sie können mit Hilfe der AS-Anzeige die Nachrichten-ID, die Zeitmarken, den Dokumenttyp, den Zieltyp, den Synchronstatus und die Dokumentdetails anzeigen. Beim Anzeigen der Dokumentdetails werden zusätzliche Dokumentverarbeitungsinformationen dargestellt.

Tasks der AS-Anzeige ausführen

Tabelle 17. Tasks der AS1/AS2-Anzeige

Was möchten Sie tun?	Siehe
AS-Nachrichten suchen	Seite „Nachrichten suchen"
Unformatierte Dokumente anzeigen	Seite „Nachrichtendetails anzeigen" auf Seite 76

Nachrichten suchen

1. Klicken Sie auf **Anzeigen** > **AS-Anzeige**. Das System zeigt die AS-Anzeige an.
2. Wählen Sie die Suchkriterien in den Dropdown-Listen aus.

Tabelle 18. AS-Anzeige, Suchkriterien

Wert	Beschreibung
Startdatum und -zeit	Datum und Uhrzeit der Prozesseinleitung.
Enddatum und -zeit	Datum und Uhrzeit der Fertigstellung des Prozesses.
Quellenpartner	Gibt den übertragenden Partner an (nur interner Partner).
Zielpartner	Gibt den empfangenden Partner an.
Suchen in	Gibt an, ob das zu durchsuchende Dokument der Quellen- oder Zieldokumenttyp ist.
AS-Quellengeschäfts-ID	Geschäftsidentifikationsnummer des Quellenpartners, z. B. DUNS.
Quellengeschäfts-ID der Nutzdaten	Identifikationsnummer der Nutzdaten der Quelle.
Betriebsmodus	Produktion, Test, Externer Partner für RN-Simulator oder Interner Partner für RN-Simulator. Die Option **Test** ist nur auf Systemen verfügbar, die den Zieltyp **Test** unterstützen.
Paket	Beschreibt das Format, die Packung, die Verschlüsselung und die Identifizierung des Inhaltstyps für das Dokument.
Protokoll	Für die Partner verfügbares Dokumentformat, z. B. RosettaNet von XML.
Dokumenttyp	Der genaue Geschäftsprozess.
Nachrichten-ID	Die ID-Nummer, die dem gepackten AS1-, AS2- oder AS3-Dokument zugeordnet ist. Die Suchkriterien können einen Stern (*) als Platzhalterzeichen beinhalten. Die maximale Länge beträgt 255 Zeichen.
Dokument-ID	Die eindeutige Identifikationsnummer, die dem Dokument zugeordnet ist.
Synchron/Asynchron	Suche nach Dokumenten, die im synchronen oder asynchronen Modus empfangen wurden. Synchroner Modus bedeutet, dass die Verbindung zwischen dem Initiator und dem Document Manager geöffnet bleibt, bis die Transaktion vollständig ausgeführt wurde (einschließlich Anforderung und MDN).
MDN-Status	Hier können Sie den Status von MDN für diese Nachricht auswählen.
Sortieren nach	Sortieren der Ergebnisse nach diesem Wert.
Absteigend oder Aufsteigend	Aufsteigend - Zeigt die Ergebnisse beginnend mit der ältesten Zeitmarke oder dem Ende des Alphabets an. Absteigend - Zeigt die Ergebnisse beginnend mit der jüngsten Zeitmarke oder dem Anfang des Alphabets an.
Ergebnisse pro Seite	Auswahl der Anzahl angezeigter Einträge pro Seite.

3. Klicken Sie auf **Suchen**. Das System zeigt eine Liste der Nachrichten an.

Nachrichtendetails anzeigen

1. Klicken Sie auf **Anzeigen** > **AS-Anzeige**. Das System zeigt die AS-Anzeige an.
2. Wählen Sie die Suchkriterien in den Dropdown-Listen aus.
3. Klicken Sie auf **Suchen**. Das System zeigt eine Liste der Nachrichten an.
4. Klicken Sie auf das Symbol zum Anzeigen von Details neben der Nachricht, die angezeigt werden soll. Das System zeigt die Nachricht und die zugeordneten Dokumentdetails an.

Tabelle 19. AS-Anzeigen: Paketdetails

Wert	Beschreibung
Nachrichten-ID	Die ID-Nummer, die dem gepackten AS1-, AS2- oder AS3-Dokument zugeordnet ist. Diese Nummer identifiziert lediglich das Paket. Das Dokument selbst hat eine separate Dokument-ID-Nummer, die beim Anzeigen der Dokumentdetails dargestellt wird. Die maximale Länge beträgt 255 Zeichen.
Quellenpartner	Der Partner, der einen Geschäftsprozess einleitet.
Zielpartner	Der Partner, der den Geschäftsprozess empfängt.
Zeitmarke der Einleitung	Datum und Uhrzeit des Verarbeitungsbeginns des Dokuments.
Zieltyp	Test oder Produktion. Die Option **Test** ist nur auf Systemen verfügbar, die den Zieltyp **Test** unterstützen.
MDN-URI	Die Zieladresse für die MDN. Diese Adresse kann als HTTP-URI oder E-Mail-Adresse angegeben werden.
MDN-Dispositionstext	Dieser Text stellt den Status der ursprünglich empfangenen Nachricht bereit (erfolgreich oder fehlgeschlagen). Beispiele: • Automatic-=action/MDN-sent-automatically; processed. • Automatic-action/MDN-sent-automatically;processed/Warning;duplicate-document. • Automatic-action/MDN-sent-automatically;processed/Error;description-failed. • Automatic-action/MDN-sent-automatically;failed:unsupported MIC-algorithms.

5. (Optional) Klicken Sie auf das Symbol zum Anzeigen des unformatierten Dokuments, um das unformatierte Dokument anzuzeigen.

ebMS-Anzeige

Der Mechanismus ″ebXML Message Service″ (ebMS) bietet ein standardisiertes Verfahren zum Austauschen von Geschäftsnachrichten zwischen ebXML-Handelspartnern. Mit ebMS können Geschäftsnachrichten zuverlässig ausgetauscht werden, ohne auf proprietäre Technologien und Lösungen zurückgreifen zu müssen. Eine ebXML-Nachricht enthält Strukturen für einen Nachrichtenheader (erforderlich für Routing und Zustellung) sowie einen Abschnitt mit Nutzdaten. ebMS bietet ein standardisiertes Verfahren zum Austauschen von Geschäftsnachrichten zwischen ebXML-Handelspartnern. Eine ebXML-Nachricht ist ein vom Kommunikationsprotokoll unabhängiger MIME/Multipart-Nachrichtenumschlag.

Tasks der ebMS-Anzeige ausführen

Tabelle 20. Tasks der ebMS-Anzeige

Was möchten Sie tun?	Siehe
ebMS-Prozesse suchen	„ebMS-Prozesse suchen"
ebMS-Prozesse anzeigen	„ebMS-Prozessdetails anzeigen"
Unformatierte Dokumente anzeigen	„Unformatierte Dokumente anzeigen" auf Seite 78
Dokumentstatus anzeigen	„Dokumentstatus anzeigen" auf Seite 78

ebMS-Prozesse suchen

1. Klicken Sie auf **Anzeigen** > **ebMS-Anzeige**. Das System ruft die Anzeige **ebMS-Anzeige - Suche** auf.
2. Wählen Sie die Suchkriterien in den Dropdown-Listen aus.

Wert	Beschreibung
Startdatum und -zeit	Datum und Uhrzeit der Prozesseinleitung.
Enddatum und -zeit	Datum und Uhrzeit der Fertigstellung des Prozesses.
Quellenpartner	Gibt den sendenden Partner an.
Zielpartner	Gibt den empfangenden Partner an.
Quellengeschäfts-ID	Geschäftsidentifikationsnummer des einleitenden Partners, z. B. DUNS.
Betriebsmodus	Produktion, Test, Externer Partner für RN-Simulator oder Interner Partner für RN-Simulator. Die Option **Test** ist nur auf Systemen verfügbar, die den Zieltyp **Test** unterstützen.
Protokoll	Für die Partner verfügbare Protokolle.
Dokumenttyp	Der Typ des zu verarbeitenden Dokuments.
Dialog-ID	Die eindeutigen Identifikationsinformationen, die dem Prozess zugeordnet sind. Die Kriterien können einen Stern (*) als Platzhalterzeichen beinhalten.
Sortieren nach	Sortiert die Ergebnisse z. B. nach der Zeitmarke der Empfangszeit.
Absteigend oder Aufsteigend	Aufsteigend - Zeigt die Ergebnisse beginnend mit der ältesten Zeitmarke oder dem Ende des Alphabets an. Absteigend - Zeigt die Ergebnisse beginnend mit der jüngsten Zeitmarke oder dem Anfang des Alphabets an.
Ergebnisse pro Seite	Anzeige von n Ergebnissen pro Seite.

3. Klicken Sie auf **Suchen**. Das System zeigt ebMS-Prozesse an, die mit Ihren Suchkriterien übereinstimmen.

ebMS-Prozessdetails anzeigen

1. Klicken Sie auf **Anzeigen** > **ebMS-Anzeige**. Das System ruft die Anzeige **ebMS-Anzeige - Suche** auf.
2. Wählen Sie die Suchkriterien in den Dropdown-Listen aus.
3. Klicken Sie auf **Suchen**. Das System zeigt die Ergebnisse Ihrer Suche an.

Tabelle 21. Werte für die Suchkriterien der ebMS-Anzeige

Wert	Beschreibung
Partner	In den Geschäftsprozess einbezogene Partner.

Tabelle 21. Werte für die Suchkriterien der ebMS-Anzeige (Forts.)

Wert	Beschreibung
Quellenzeitmarke	Datum und Uhrzeit des Verarbeitungsbeginns des ersten Dokuments.
Dokumenttyp	Der genaue Geschäftsprozess, z. B. ebMS 2.0 : ALMService Production.
Betriebsmodus	Der Betriebsmodus, z. B. Produktion.
Dialog-ID	Die eindeutige Identifikationsnummer, die diesem Ereignis zugeordnet ist.

Unformatierte Dokumente anzeigen

Gehen Sie wie folgt vor, um das unformatierte Dokument anzuzeigen:

1. Klicken Sie auf **Anzeigen** > **ebMS-Anzeige**.
2. Wählen Sie die Suchkriterien in den Dropdown-Listen aus. Weitere Informationen hierzu finden Sie im Abschnitt „ebMS-Prozesse suchen" auf Seite 77.
3. Klicken Sie auf **Suchen**.
4. Klicken Sie auf das Symbol **Zum Anzeigen des unformatierten Dokuments anklicken** unterhalb des Abschnitts **Legende**.

- Informationen zur Fehlerbehebung bei nicht verarbeiteten Dokumenten finden Sie im Abschnitt „Datenvalidierungsfehler anzeigen" auf Seite 84.
- Die Anzeige des unformatierten Dokuments stellt den HTTP-Header mit dem unformatierten Dokument dar.

Dokumentstatus anzeigen

1. Klicken Sie auf **Anzeigen** > **ebMS-Anzeige**.
2. Wählen Sie die Suchkriterien in den Dropdown-Listen aus. Weitere Informationen hierzu finden Sie im Abschnitt „ebMS-Prozesse suchen" auf Seite 77.
3. Klicken Sie auf **Suchen**.
4. Klicken Sie auf **Status anfordern**.
5. Klicken Sie auf **Status anzeigen**.

RosettaNet-Anzeige

Verwenden Sie die RosettaNet-Anzeige, um einen bestimmten Prozess zu suchen, der ein Ereignis generiert hat. Wenn Sie den Zielprozess angeben, können Sie die Prozessdetails und das unformatierte Dokument anzeigen.

RosettaNet ist eine Unternehmensgruppe, die einen Industriestandard für e-business Transaktionen geschaffen hat. Geschäftsprozesse zwischen Mitgliedern der Hub-Community werden durch PIPs (Partner Interface Processes) definiert. Jeder PIP identifiziert ein bestimmtes Geschäftsdokument sowie die Art und Weise, wie dieses zwischen dem internen Partner und den externen Partnern verarbeitet wird.

In der RosettaNet-Anzeige wird der Ablauf der Dokumente dargestellt, aus denen ein Geschäftsprozess besteht. Werte, die mit der RosettaNet-Anzeige dargestellt werden können, umfassen den Prozessstatus, Details, unformatierte Dokumente sowie zugeordnete Prozessereignisse.

Die RosettaNet-Anzeige stellt Prozesse auf der Basis spezieller Suchkriterien dar.

Tasks der RosettaNet-Anzeige ausführen

Tabelle 22. Tasks der RosettaNet-Anzeige

Was möchten Sie tun?	Siehe
RosettaNet-Prozesse suchen	Seite 79
RosettaNet-Prozessdetails anzeigen	Seite 80
Unformatierte Dokumente anzeigen	Seite 80

RosettaNet-Prozesse suchen

1. Klicken Sie auf **Anzeigen** > **RosettaNet-Anzeige**. Das System ruft die Anzeige **RosettaNet-Anzeige - Suche** auf.
2. Wählen Sie die Suchkriterien in den Dropdown-Listen aus. BEGINNEN SIE HIER

Tabelle 23. RosettaNet-Suchkriterien

Wert	Beschreibung
Startdatum und -zeit	Datum und Uhrzeit der Prozesseinleitung.
Enddatum und -zeit	Datum und Uhrzeit der Fertigstellung des Prozesses.
Quellenpartner	Gibt den sendenden Partner an.
Zielpartner	Gibt den empfangenden Partner an.
Quellengeschäfts-ID	Geschäftsidentifikationsnummer des einleitenden Partners, z. B. DUNS.
Betriebsmodus	Produktion, Test, Externer Partner für RN-Simulator oder Interner Partner für RN-Simulator. Die Option **Test** ist nur auf Systemen verfügbar, die den Zieltyp **Test** unterstützen.
Protokoll	Für die Partner verfügbare Protokolle.
Dokumenttyp	Der Typ des zu verarbeitenden Dokuments.
Prozessinstanz-ID	Die eindeutige Identifikationsnummer, die dem Prozess zugeordnet ist. Die Kriterien können einen Stern (*) als Platzhalterzeichen beinhalten.
Sortieren nach	Sortiert die Ergebnisse z. B. nach der Zeitmarke der Empfangszeit.
Absteigend oder Aufsteigend	Aufsteigend - Zeigt die Ergebnisse beginnend mit der ältesten Zeitmarke oder dem Ende des Alphabets an. Absteigend - Zeigt die Ergebnisse beginnend mit der jüngsten Zeitmarke oder dem Anfang des Alphabets an.
Ergebnisse pro Seite	Anzeige von n Ergebnissen pro Seite.

3. Klicken Sie auf **Suchen**. Das System zeigt RosettaNet-Prozesse an, die mit Ihren Suchkriterien übereinstimmen.
4. Klicken Sie auf das Symbol zum Anzeigen von Details neben dem ebMS-Prozess, der angezeigt werden soll. Das System zeigt Details und zugeordnete Dokumente zu dem ausgewählten Prozess an.
5. Klicken Sie auf das Symbol zum Anzeigen von Details neben dem Dokument, das angezeigt werden soll. Das System zeigt das Dokument und die zugeordneten Ereignisdetails an.

RosettaNet-Prozessdetails anzeigen

1. Klicken Sie auf **Anzeigen** > **RosettaNet-Anzeige**. Das System ruft die Anzeige **RosettaNet-Anzeige - Suche** auf.
2. Wählen Sie die Suchkriterien in den Dropdown-Listen aus.
3. Klicken Sie auf **Suchen**. Das System zeigt die Ergebnisse Ihrer Suche an.

Tabelle 24. Dokumentverarbeitungsdetails

Wert	Beschreibung
Partner	In den Geschäftsprozess einbezogene Partner.
Zeitmarken	Datum und Uhrzeit des Verarbeitungsbeginns des ersten Dokuments.
Dokumenttyp	Der genaue Geschäftsprozess, z. B. RosettaNet (1.1): 3A7.
Zieltyp	Beispiel: Produktion.
Prozessinstanz-ID	Die eindeutige Nummer, die dem Prozess durch das einleitende Mitglied der Community zugeordnet wird.
Dokument-ID	Die proprietäre Dokumentkennung, die durch den sendenden Partner zugeordnet wird. Dieses Feld befindet sich nicht in einer festgelegten Position und variiert je nach Dokumenttyp.
Quellenpartner	Der einleitende Partner.
Zielpartner	Der empfangende Partner.

4. Klicken Sie auf das Symbol zum Anzeigen von Details neben dem RosettaNet-Prozess, der angezeigt werden soll. Das System zeigt Details und zugeordnete Dokumente zu dem ausgewählten Prozess an.
5. Klicken Sie auf das Symbol zum Anzeigen von Details neben dem Dokument, das angezeigt werden soll. Das System zeigt das Dokument und die zugeordneten Ereignisdetails an.

Unformatierte Dokumente anzeigen

1. Klicken Sie auf **Anzeigen** > **RosettaNet-Anzeige**. Das System ruft die Anzeige **RosettaNet-Anzeige - Suche** auf.
2. Wählen Sie die Suchkriterien in den Dropdown-Listen aus.
3. Klicken Sie auf **Suchen**. Das System zeigt eine Liste der Prozesse an.
4. Klicken Sie auf das Symbol zum Anzeigen von Details neben dem Prozess, der angezeigt werden soll. Das System zeigt Prozessdetails und zugeordnete Dokumente für den ausgewählten Prozess an.
5. Klicken Sie auf das Symbol zum Anzeigen des unformatierten Dokuments neben dem Dokumenttyps, um das unformatierte Dokument anzuzeigen.

Einschränkungen: Unformatierte Dokumente, die größer als 100 KB sind, werden abgeschnitten.

Tipp:

- Informationen zur Fehlerbehebung bei nicht verarbeiteten Dokumenten finden Sie im Abschnitt „Datenvalidierungsfehler anzeigen" auf Seite 84.
- Die Anzeige des unformatierten Dokuments stellt den HTTP-Header mit dem unformatierten Dokument dar.

Dokumentanzeige

Mit Hilfe der Dokumentanzeige können Sie ein bestimmtes, zu untersuchendes Dokument suchen und anzeigen. Sie können anhand folgender Angaben nach Dokumenten suchen: Datum, Zeit, Prozesstyp (sendender Prozess oder empfangender Prozess), Partnerverbindung, Zieltyp, Dokumentstatus, Protokoll, Dokumenttyp und Prozessversion.

Einige Protokolle wie zum Beispiel das angepasste XML-Protokoll (XML, Extensible Markup Language) verwenden XML-Formate und können Informationen aus Dokumenten extrahieren und speichern, so dass Sie danach mit Hilfe der Dokumentanzeige suchen können. Diesem Zweck dienen die Feldattribute für die Benutzersuche in einer XML-Formatdefinition. Wird das Dokument unter Verwendung eines XML-Formats weitergeleitet, das Suchfelder enthält, können die mit Hilfe der Suchfelder erhaltenen Dokumentinformationen Ziel einer Suche sein. Beispiel ist ein angepasstes XML-Dokument, das eine Bestellung darstellt. Mit Ihrem Wissen über die Struktur des Dokuments können Sie ein XML-Format mit einem Suchfeld definieren, das die Bestellnummern extrahiert. Werden Dokumente unter Verwendung dieses XML-Formats weitergeleitet, können Sie mit Hilfe der Bestellnummer danach suchen, indem Sie die Nummer in die entsprechenden benutzerdefinierten Suchfelder in der Suchanzeige der Dokumentanzeige eingeben.

Die Weiterleitung kann auch für EDI-Dokumente (EDI, Electronic Data Interchange) definiert werden, wobei ebenfalls Informationen aus dem Dokument extrahiert werden. In diesem Fall wird dies durch die Codierung einer DIS-Map erreicht, wodurch die benutzerdefinierten Suchfelder mit Werten gefüllt werden.

Sie können ferner einen Benutzerexit schreiben, der Informationen aus dem Dokument extrahiert, so dass es Ziel einer Suche sein kann. Verwenden Sie die Methode BusinessDocumentInterface.setAttribute() für den Benutzerexit, um die benutzerdefinierten Suchfelder mit Werten zu füllen.

Die Suchergebnisse zeigen alle Dokumente an, die Ihre Suchkriterien erfüllen, und geben die Zeitmarken, den Prozess, die Partnerverbindung und die Zieltypen an. Suchen Sie das Zieldokument und verwenden Sie die Funktionen der Anzeige, um das unformatierte Dokument anzuzeigen. Die Dokumentanzeige kann darüber hinaus verwendet werden, um fehlgeschlagene oder erfolgreiche Dokumente erneut zu senden.

Dokumente suchen

1. Klicken Sie auf **Anzeigen** > **Dokumentanzeige**. Das System ruft die Anzeige **Dokumentanzeige - Suche** auf.

2. Wählen Sie die Suchkriterien in den Dropdown-Listen aus.

Tabelle 25. Suchkriterien der Dokumentanzeige

Wert	Beschreibung
Startdatum und -zeit	Datum und Uhrzeit der Prozesseinleitung.
Enddatum und -zeit	Datum und Uhrzeit der Fertigstellung des Prozesses.
Quellenpartner	Gibt den sendenden Partner an.
Zielpartner	Gibt den empfangenden Partner an..
Suchen in	Suchen im sendenden oder empfangenden Dokumenttyp.
Betriebsmodus	Produktion, Test, Externer Partner für RN-Simulator oder Interner Partner für RN-Simulator. Die Option **Test** ist nur auf Systemen verfügbar, die den Zieltyp **Test** unterstützen.
Dokumentstatus	Aktueller Dokumentstatus im System. Sie können **Wird ausgeführt**, **Erfolgreich** oder **Fehlgeschlagen** auswählen. Der Standardwert ist **Alle**.
Paket	Beschreibt das Format, die Packung, die Verschlüsselung und die Identifizierung des Inhaltstyps für das Dokument.
Protokoll	Der Typ des Prozessprotokolls, das für die Partner verfügbar ist.
Dokumenttyp	Der genaue Geschäftsprozess.
Dokument-ID	Erstellt durch den Quellenpartner. Die Kriterien können einen Stern (*) als Platzhalterzeichen beinhalten.
Referenz-ID	Die vom System erstellte ID-Nummer zum Überwachen des Dokumentstatus.
Quellen-IP-Adresse	IP-Adresse des Quellenpartners.
Filter	Suche nach Dokumenten, die im synchronen Modus empfangen wurden. Dies bedeutet, dass die Verbindung zwischen dem Initiator und dem Document Manager geöffnet bleibt, bis die Transaktion vollständig ausgeführt wurde (einschließlich Anforderung und Empfangsbestätigung oder Anforderung und Antwort).
Sortieren nach	Wert zum Sortieren von Ergebnissen.
Ergebnisse pro Seite	Anzahl der angezeigten Einträge pro Seite.
Absteigend	Sortieren der Ergebnisse in absteigender Reihenfolge.
Benutzerdefinierte Suchfelder	Führt die Suche auf der Basis von benutzerdefinierten Kriterien aus.

Anmerkung: Warnungsereignisse werden standardmäßig angezeigt. Um alle Ereignisse anzuzeigen, wählen Sie **Debugging** aus.

3. Klicken Sie auf **Suchen**. Das System zeigt eine Liste der Dokumente an, die Ihren Suchkriterien entsprechen.

Tabelle 26. Mit Hilfe der Dokumentanzeige verfügbare Dokumentinformationen

Wert	Beschreibung
Partner	Die in den Geschäftsprozess einbezogenen Quellenpartner (Sender) und Zielpartner (Empfänger).
Zeitmarken	Das Datum und die Uhrzeit des Verarbeitungsbeginns und -endes des Dokuments.
Dokumenttyp	Der Geschäftsprozess, der gerade ausgeführt wird.
Zieltyp	Test oder Produktion. Die Option **Test** ist nur auf Systemen verfügbar, die den Zieltyp **Test** unterstützen.

Tabelle 26. Mit Hilfe der Dokumentanzeige verfügbare Dokumentinformationen (Forts.)

Wert	Beschreibung
Synchron	Gibt an, dass das Dokument im synchronen Modus empfangen wurde. Dies bedeutet, dass die Verbindung zwischen dem Initiator und dem Document Manager geöffnet bleibt, bis die Transaktion vollständig ausgeführt wurde (einschließlich Anforderung und Empfangsbestätigung oder Anforderung und Antwort).

Dokumentdetails, Ereignisse und unformatierte Dokumente anzeigen

1. Klicken Sie auf **Anzeigen** > **Dokumentanzeige**. Das System ruft die Anzeige **Dokumentanzeige - Suche** auf.
2. Wählen Sie die Suchkriterien in den Dropdown-Listen aus.
3. Klicken Sie auf **Suchen**. Das System zeigt eine Liste der Dokumente an.
   - Klicken Sie auf das Symbol des geöffneten Ordners, das sich neben dem unter **Zugeordnete Dokumente** angezeigten Dokument befindet, um die zugehörigen Details und Ereignisse anzuzeigen. Das System zeigt Prozessdetails und Ereignisse für das ausgewählte Dokument an. Verfügen EDI-Austauschdokumente über untergeordnete EDI-Transaktionen, die beim Entfernen des Umschlags bzw. beim Einfügen in den Umschlag generiert wurden, können Sie diese anzeigen. Wählen Sie hierzu das Optionsfeld **Untergeordnete Elemente des Dokuments** für die Quelle oder das Ziel aus. Weitere Informationen zur Anzeige von EDI-Dokumenten finden Sie im Handbuch *Verwaltung*.
   - Klicken Sie zum Anzeigen des unformatierten Dokuments mit HTTP-Header auf das Symbol zum Anzeigen unformatierter Dokumente neben dem Dokument. Das System zeigt dann den Inhalt des unformatierten Dokuments an.

Beim Anzeigen von Dokumentdetails werden folgende Dokumentverarbeitungsinformationen angezeigt:

Tabelle 27. Dokumentverarbeitungswerte, mit der Dokumentanzeige verfügbar

Wert	Beschreibung
Referenz-ID	Die eindeutige Identifikationsnummer, die dem Dokument durch das System zugeordnet wird.
Dokument-ID	Die eindeutige Identifikationsnummer, die dem Dokument durch den Quellenpartner zugeordnet wird.
Dokumentzeitmarke	Datum und Uhrzeit der Erstellung durch den Partner.
Ziel	Das Ziel, durch das das Dokument geleitet wird.
Verbindungsdokumenttyp	Vom System für ein Dokument ausgeführte Aktionen, um die Kompatibilität des Dokuments mit Geschäftsanforderungen der Partner untereinander sicherzustellen.
Quelle und Ziel	Die in den Geschäftsprozess einbezogenen Quellen- und Zielpartner.
Eingangszeitmarke	Das Datum und die Uhrzeit, zu der das System das Dokument vom Partner empfangen hat.
Zeitmarke Endstatus	Das Datum und die Uhrzeit, zu der das Dokument vom System erfolgreich zum Zielpartner weitergeleitet wurde.
Quellen- und Zielgeschäfts-ID	Die Geschäftsidentifikationsnummer des Quellen- und des Zielpartners, z. B. DUNS.
Quellen- und Zieldokumenttyp	Der genaue Geschäftsprozess, der zwischen dem Quellen- und dem Zielpartner ausgeführt wird.

Einschränkungen: Unformatierte Dokumente, die größer als 100 KB sind, werden abgeschnitten.

Tipp: Zeigt das System ein Ereignis **Doppeltes Dokument** an, dann sehen Sie sich das zuvor gesendete Originaldokument an, indem Sie das Symbol des blauen Pfeils neben dem Ereignis **Doppeltes Dokument** auswählen und anschließend auf das Symbol zum Anzeigen des Originaldokuments klicken.

Tipp: Informationen zur Fehlerbehebung bei nicht verarbeiteten Dokumenten finden Sie im Abschnitt „Datenvalidierungsfehler anzeigen" auf Seite 84.

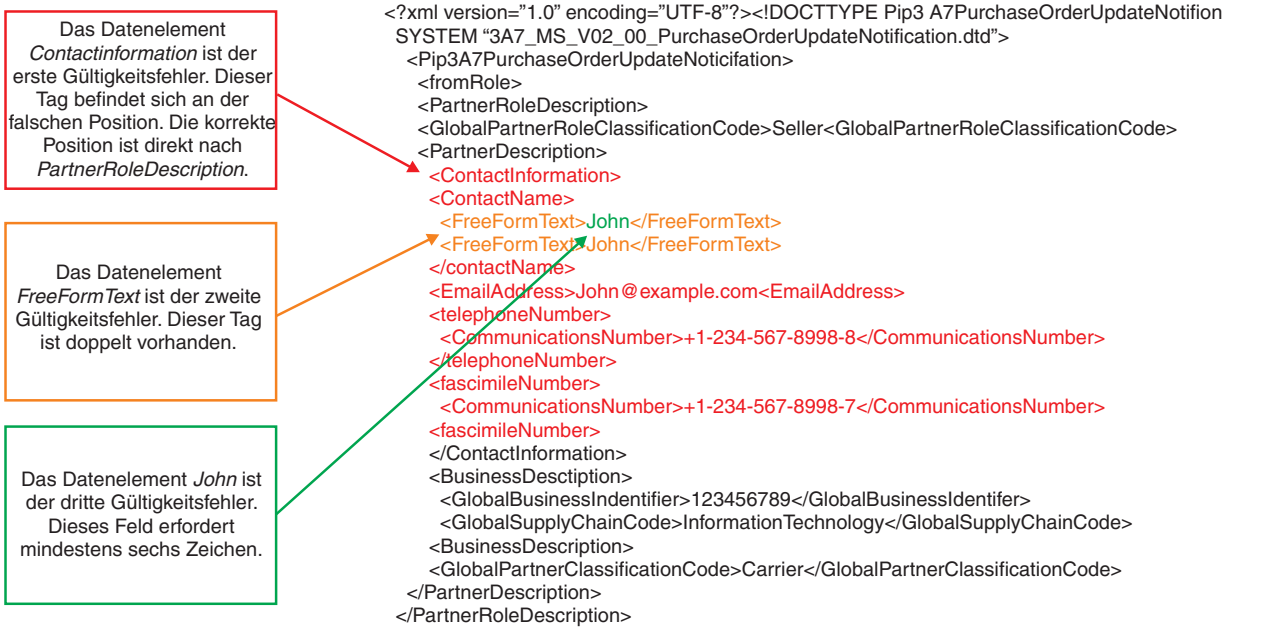
Datenvalidierungsfehler anzeigen

Sie können mit Hilfe des farbig markierten Textes in den XML-Feldern mit Gültigkeitsfehlern schnell nach Dokumenten suchen, deren Verarbeitung fehlgeschlagen ist. Felder mit Gültigkeitsfehlern werden rot angezeigt. Treten bis zu drei separate Gültigkeitsfehler innerhalb von verschachtelten XML-Feldern auf, werden folgende Farben zur Unterscheidung zwischen den Fehlerfeldern verwendet:

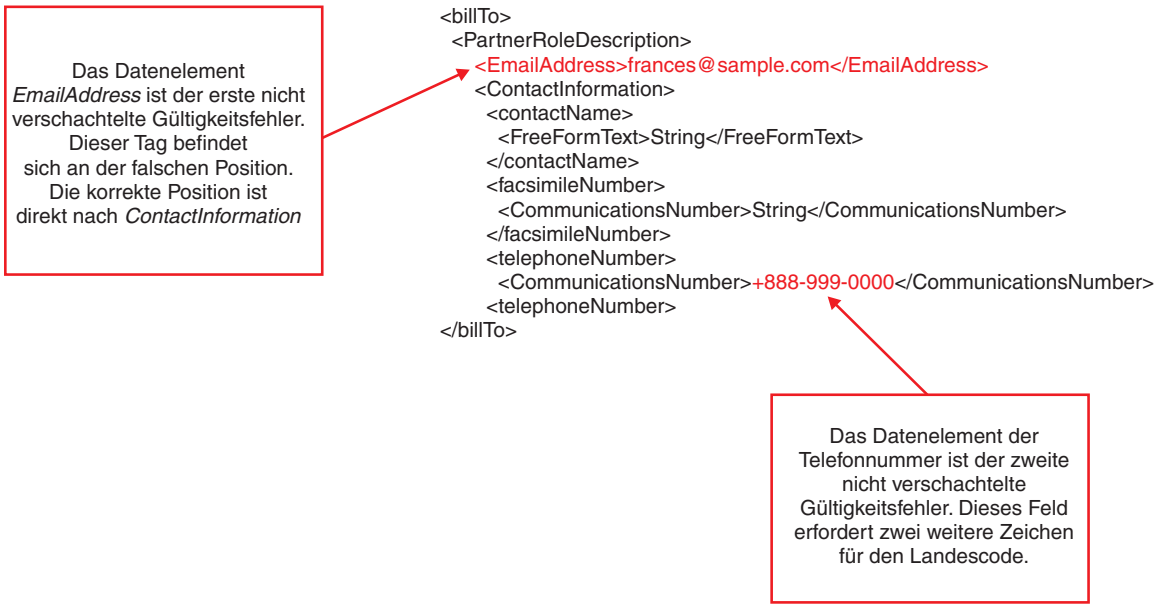
Tabelle 28. Farbig markierte Dokumentprüffehler

Wert	Beschreibung
Rot	Erster Gültigkeitsfehler
Orange	Zweiter Gültigkeitsfehler
Grün	Dritter Gültigkeitsfehler

Nachfolgend ist ein Beispiel für verschachtelte XML-Gültigkeitsfehler aufgeführt:



Beispiel für nicht verschachtelte XML-Gültigkeitsfehler:



Zum Anzeigen von Gültigkeitsfehlern in einem unformatierten Dokument siehe „Unformatierte Dokumente anzeigen" auf Seite 80.

Einschränkungen: Die Community Console zeigt nur die ersten 100 KB eines unformatierten Dokuments an. Gültigkeitsfehler, die mehr als 100 KB umfassen, können nicht angezeigt werden.

Funktion "Prozess stoppen" verwenden

Klicken Sie auf **Prozess stoppen**, um ein Dokument zu stoppen, das gerade bearbeitet wird. Diese Funktion ist nicht auf den Hubadmin-Benutzer beschränkt. Um dieses Funktion nutzen zu können, müssen die Berechtigungen der Gruppe konfiguriert werden.

Anmerkung: Das System benötigt unter Umständen bis zu einer Stunde, um das Dokument zu stoppen. Während dieser Zeit zeigt die Dokumentanzeige das Dokument weiterhin mit dem Status **Wird ausgeführt** an.

Zielwarteschlange

In der **Zielwarteschlange** können Dokumente angezeigt werden, die in der Warteschlange stehen, um von einem beliebigen Ziel im System übermittelt zu werden. Sie können sämtliche Ziele anzeigen, in deren Warteschlangen sich zu übermittelnde Dokumente befinden, die Dokumente in einer Warteschlange anzeigen und löschen sowie Ziele aktivieren oder inaktivieren.

Mit der Funktion der **Zielwarteschlange** kann sichergestellt werden, dass eilige Dokumente nicht unnötig in der Warteschlange stehen. Darüber hinaus kann mit dieser Funktion sichergestellt werden, dass die maximale Anzahl von Dokumenten in der Warteschlange nicht überschritten wird. Mit Hilfe der **Zielwarteschlange** können Sie folgende Operationen ausführen:

- Eine Liste aller Ziele mit Dokumenten anzeigen, die für die Zustellung in der Warteschlange stehen.
- Ein Dokument anzeigen, dass sich bereits über einen längeren Zeitraum (30 Sekunden oder länger) in einer Zielwarteschlange befindet. Dies kann auf ein Problem beim Dokument selbst hindeuten. Darüber hinaus können Sie Dokumentdetails anzeigen, um eine Fehlerdiagnose für Dokumente in der Warteschlange auszuführen.

  Anmerkung: Wenn Sie ein FTP-Scripting-Ziel mit einem Intervall- oder Kalenderzeitplan implementieren, verbleiben Dokumente über einen längeren Zeitraum in dieser Warteschlange und werden erst dann entfernt, wenn das für sie definierte Intervall abgelaufen ist bzw. das definierte Datum und die entsprechende Uhrzeit erreicht sind. Diese Funktionsweise ist beabsichtigt und die Dokumente sollten nicht vorzeitig aus der Warteschlange entfernt werden.
- Zieldetails anzeigen, um den einwandfreien Betrieb sicherzustellen. Dokumente, die sich in einer Zielwarteschlange stauen, sind möglicherweise ein Hinweis auf einen Fehler beim Zustellmanager oder im Ziel.
- Den Zielstatus überprüfen. Bei einem Ziel, das offline gesetzt ist, werden Dokumente so lange in der Warteschlange gesammelt, bis das Ziel wieder online gesetzt wird. Der Zielstatus wirkt sich nicht auf die Verbindungsfunktionalität aus, und die Dokumente werden weiter verarbeitet und für die Zustellung in die Warteschlange gestellt.
- Über die Felder **Partnername** und **Ziel** können Sie die Größe der Zielwarteschlangenliste begrenzen.

Anzeigen der Liste der Ziele

Gehen Sie wie folgt vor, um eine Liste der Dokumente anzuzeigen, die sich im Ziel befinden.

1. Wählen Sie **Anzeigen** > **Zielwarteschlange** aus. In der Community Console wird das Fenster **Zielwarteschlange** angezeigt.

2. Geben Sie die in Tabelle 29 aufgelisteten Parameter ein.

Tabelle 29. Fenster "Zielwarteschlange"

Kriterien	Beschreibung
Partnername	Um dieses Feld auszufüllen, können Sie eine der folgenden Vorgehensweisen verwenden: 1. Sie können den Namen des Partners angeben. 2. Sie können in diesem Feld einen Teil des Partnernamens angeben und auf **Partner anzeigen** klicken. Wählen Sie den Partner anschließend in der Liste der Partner aus. 3. Sie können das Platzhalterzeichen * angeben und auf **Partner anzeigen** klicken. Wählen Sie den Partner anschließend in der Liste der Partner aus. Wenn Sie auf **Partner anzeigen** klicken, wird das Feld **Partner** auf der Seite angezeigt. Im Feld **Partner** werden alle verfügbaren Partner in alphabetischer Reihenfolge aufgelistet.
Ziel	Der erste Eintrag in der Liste ist `Alle`. Dieser Eintrag ist standardmäßig ausgewählt. Der verbleibende Teil der Liste ist eine sortierte Liste der Zieltransporte. In dieser Liste können Sie nur ein einzelnes Ziel auswählen. Der Standardwert ist `Alle`. **Anmerkung:** Die Liste der Ziele wird automatisch mit den ausgewählten Partnerzielen gefüllt, und die Liste wird in alphabetischer Reihenfolge dargestellt.
In Warteschlange mindestens	Mindestanzahl von Minuten, die ein Dokument bereits in der Zielwarteschlange gewartet hat. Wenn beispielsweise "6 Minuten" ausgewählt ist, werden alle Ziele mit Dokumenten angezeigt, die bereits 6 Minuten oder länger auf die Zustellung warten. Der Standardwert ist `0`.
Sortieren nach	Sortiert Suchergebnisse nach **Partner** (Standard) oder **Zielname**.
Aktualisieren	Schaltet die Aktualisierung ein oder aus (Standard).
Minimum in Warteschlange	Mindestanzahl von Dokumenten in einer Zielwarteschlange. Der Standardwert ist `1`.
Richtung	Klicken Sie auf **Aufsteigend**, um die Dokumente beginnend bei der ältesten Zeitmarke oder beim Ende des Alphabets anzuzeigen. Klicken Sie auf **Absteigend**, um die Dokumente beginnend mit der neuesten Zeitmarke oder beim Anfang des Alphabets anzuzeigen.
Aktualisierungsrate	Anzahl der Sekunden, die die Community Console vor dem Aktualisieren der angezeigten Daten wartet.

3. Klicken Sie auf **Suchen**. Das System sucht alle Dokumente im Ziel, die Ihren Suchkriterien entsprechen. In **Tabelle 30** werden die Informationen angezeigt, die von der Suche zurückgegeben werden.

Tabelle 30. Ergebnisse nach der Suche in der Zielwarteschlange

Kriterien	Beschreibung
Partner	Dem Ziel zugeordneter Handelspartner.
Ziel	Der Name des Ziels.
In Warteschlange	Die Anzahl der Dokumente in der Zielwarteschlange, die für die Zustellung anstehen. Link zu Zieldetails.
Status	Gibt an, ob das Ziel online oder offline ist.
Zuletzt gesendet	Datum und Uhrzeit, zu dem bzw. der ein Dokument zuletzt erfolgreich an das Ziel gesendet wurde.

Anmerkung: In der Community Console wird ein Ziel nur dann angezeigt, wenn es unter Verwendung der UND-Logik alle Anforderungen der Suchkriterien erfüllt.

Dokumente in der Warteschlange anzeigen

Gehen Sie wie folgt vor, um für einen bestimmten Partner die Dokumente in der Warteschlange anzuzeigen:

1. Klicken Sie auf **Anzeigen** > **Zielwarteschlange**.
2. Klicken Sie im Fenster **Zielwarteschlange - Suche** auf **Dokumentensuche**.
3. Geben Sie im Fenster **Dokumente in Warteschlange - Suche** die Suchkriterien an (siehe Tabelle 31 auf Seite 88).

Tabelle 31. Fenster "Dokumente in Warteschlange - Suche"

Kriterien	Beschreibung
Partnername	Um dieses Feld auszufüllen, können Sie eine der folgenden Vorgehensweisen verwenden: 1. Sie können den Namen des Partners in dem Feld angeben. 2. Sie können in diesem Feld einen Teil des Partnernamens angeben und auf **Partner anzeigen** klicken. Wählen Sie den Partner anschließend in der Liste aus. 3. Sie können das Platzhalterzeichen * angeben und auf **Partner anzeigen** klicken. Wählen Sie den Partner anschließend in der Liste der Partner aus. **Anmerkung:** Wenn Sie auf **Partner anzeigen** klicken, wird das Feld **Partner** auf der Seite angezeigt. Im Feld **Partner** werden alle verfügbaren Partner in alphabetischer Reihenfolge aufgelistet.
Ziel	Der erste Eintrag in der Liste ist `Alle`. Dieser Eintrag ist standardmäßig ausgewählt. Der verbleibende Teil der Liste ist eine sortierte Liste der Zieltransporte. In dieser Liste können Sie nur ein einzelnes Ziel auswählen. Der Standardwert ist `Alle`. **Anmerkung:** Die Liste der Ziele wird automatisch mit den ausgewählten Partnerzielen gefüllt, und die Liste wird in alphabetischer Reihenfolge dargestellt.
Sortieren nach	Wählen Sie aus, ob die Liste nach Partnern (die Standardeinstellung), nach Ziel, Referenz-ID oder nach der Zeitmarke für das Einreihen in die Warteschlange (d. h. dem Zeitpunkt, zu dem das Dokument das letzte Mal gesendet wurde) sortiert werden soll.
Referenz-ID	Geben Sie die eindeutige Identifikationsnummer an, die dem Dokument vom System zugeordnet wird.
Richtung	Klicken Sie auf **Aufsteigend**, um die Dokumente beginnend bei der ältesten Zeitmarke oder beim Ende des Alphabets anzuzeigen. Klicken Sie auf **Absteigend**, um die Dokumente beginnend mit der neuesten Zeitmarke oder beim Anfang des Alphabets anzuzeigen.
Dokument-ID	Geben Sie die eindeutige Identifikationsnummer an, die dem Dokument vom Quellenpartner zugeordnet wird.
Ergebnisse pro Seite	Gibt die Anzahl der auf einer Seite angezeigten Dokumente an.
Maximal zulässige Anzahl an Dokumenten	Gibt die Anzahl der anzuzeigenden Datensätze an.

4. Klicken Sie auf **Suchen**. Die Ergebnisse der Warteschlangensuche werden angezeigt.

Dokumente aus der Zustellungswarteschlange löschen

Im Folgenden wird die Vorgehensweise zum Löschen von Dokumenten aus der Zustellungswarteschlange beschrieben. Sie müssen als Hubadministrator angemeldet sein, um Dokumente aus der Warteschlange löschen zu können.

1. Klicken Sie auf **Anzeigen** > **Zielwarteschlange**.
2. Klicken Sie im Fenster **Zielwarteschlange** auf **Suchen**.
3. Geben Sie die Parameter im Fenster ein (siehe Tabelle 30 auf Seite 87).
4. Klicken Sie auf das Symbol zum Löschen, um das entsprechende Dokument zu löschen.

Zieldetails anzeigen

Gehen Sie wie folgt vor, um Informationen zu einem bestimmten Ziel sowie eine Liste von Dokumenten in der Warteschlange anzuzeigen:

1. Klicken Sie auf **Anzeigen** > **Zielwarteschlange**.
2. Geben Sie im Fenster **Zielwarteschlange** die Suchkriterien ein (siehe Tabelle 29 auf Seite 87).
3. Klicken Sie auf **Suchen**.
4. Klicken Sie in der Liste der Ziele auf den Link für die Dokumentenzahl in der Spalte **In Warteschlange**. Daraufhin werden die Zieldetails und eine Liste von Dokumenten in der Warteschlange angezeigt.

Zielstatus ändern

Gehen Sie wie folgt vor, um ein Ziel online oder offline zu setzen:

1. Klicken Sie auf **Anzeigen** > **Zielwarteschlange**.
2. Geben Sie im Fenster **Zielwarteschlange** die Suchkriterien ein (siehe Tabelle 29 auf Seite 87).
3. Klicken Sie auf **Suchen**.
4. Klicken Sie in der Liste der Ziele auf den Link für die Dokumentenzahl in der Spalte **In Warteschlange**. Daraufhin werden die Zieldetails und eine Liste von Dokumenten in der Warteschlange angezeigt.
5. Klicken Sie in den **Zielinformationen** auf **Online**, um ein Ziel offline zu setzen oder klicken Sie auf **Offline**, um ein Ziel online zu setzen. (Sie müssen als Hubadministrator angemeldet sein, um den Zielstatus ändern zu können.)

Kapitel 6. Dokumenttyp analysieren: Tools

Verwenden Sie das Dokumentanalysetool, um einen detaillierten Überblick über die Anzahl der Dokumente im System, geordnet nach Status (**Empfangen**, **Wird ausgeführt**, **Fehlgeschlagen** und **Erfolgreich**), zu erhalten. Die Suchkriterien umfassen Datum, Uhrzeit, Prozesstyp (sendender Prozess oder empfangender Prozess), Zieltyp, Protokoll, Dokumententyp und Prozessversion. Verwenden Sie die Suchergebnisse zum Lokalisieren und Anzeigen der fehlgeschlagenen Dokumente und zum Untersuchen der Gründe für das Fehlschlagen.

Der Dokumentvolumenbericht ist ein nützliches Tool zum Verwalten, Überwachen und zur Fehlerbehebung beim Verarbeitungsablauf Ihrer Geschäftsdokumente. Der Bericht zeigt das Dokumentvolumen an, das vom System innerhalb eines bestimmten Zeitraums verarbeitet wird. Dieser Bericht kann angezeigt, ausgedruckt und gesichert (exportiert) und an andere Mitarbeiter gesendet werden. Sie können diesen Bericht anpassen, um Informationen basierend auf bestimmten Suchkriterien anzuzeigen.

Das Tool **Partnerverbindung testen** wird zum Testen des Ziels oder des Web-Servers verwendet.

Tabelle 32. Tools

Zu verwendende Funktion	Siehe
Dokumentanalyse	Seite 91
Dokumentvolumenbericht	Seite 94
Partnerverbindung testen	Seite 96
EDI-Berichte	Seite 99
FTP-Berichte	Seite 102

Dokumentanalyse

Verwenden Sie das Dokumentanalysetool, um einen detaillierten Überblick über die Anzahl der Dokumente im System, sortiert nach Status innerhalb eines bestimmten Zeitraums, zu erhalten.

Verwenden Sie die Suchkriterien zum Lokalisieren fehlgeschlagener Dokumente und zum Untersuchen der Gründe für das Fehlschlagen.

Die Anzeige **Dokumentanalyse** beinhaltet ein Alarmsignal. Ist ein Prozess fehlgeschlagen, blinkt die Zeile mit dem fehlgeschlagenen Prozess rot auf.

Dokumentstatus

In der folgenden Tabelle werden die verschiedenen Dokumentstatus beschrieben.

Tabelle 33. Dokumentstatus

Status	Beschreibung
Empfangen	Das Dokument wurde vom System empfangen und wartet nun auf die Verarbeitung.
Wird ausgeführt	Das Dokument befindet sich gerade in einem der folgenden Verarbeitungsschritte: • **Unvollständig**. Das System wartet z. B. auf andere Dokumente. • **Datenvalidierung**. Das System prüft z. B. gerade den Inhalt des Dokuments. • **Umsetzung**. Das System konvertiert z. B. gerade das Dokument in ein anderes Protokoll. • **Warteschlange**. Das Dokument wartet z. B. gerade darauf, an den externen Partner oder den Partner weitergeleitet zu werden.
Fehlgeschlagen	Die Dokumentverarbeitung wurde wegen Fehlern im System, auf Grund der Datenprüfung oder wegen Kopien von Dokumenten unterbrochen.
Erfolgreich	Die abschließende Nachricht, durch die die Dokumentverarbeitung fertig gestellt wird, wurde vom System an den Zielpartner übertragen.

Dokumente im System anzeigen

1. Klicken Sie auf **Tools** > **Dokumentanalyse**. Das System ruft die Anzeige **Dokumentanalyse - Suche** auf.
2. Wählen Sie die Suchkriterien in den Dropdown-Listen aus.

Tabelle 34. Dokumentsuchkriterien

Wert	Beschreibung
Startdatum und -zeit	Datum und Uhrzeit der Prozesseinleitung.
Enddatum und -zeit	Datum und Uhrzeit der Fertigstellung des Prozesses.
Quellenpartner	Der Partner, der den Geschäftsprozess eingeleitet hat (nur interner Partner).
Zielpartner	Der Partner, der den Geschäftsprozess empfangen hat (nur interner Partner).
Suchen in	Suchen im sendenden oder empfangenden Dokumententyp.
Zieltyp	Beispiel: **Produktion** oder **Test**. Die Option **Test** ist nur auf Systemen verfügbar, die den Zieltyp **Test** unterstützen.
Paket	Beschreibt das Format, die Verpackung, die Verschlüsselung und die Inhaltstypidentifikation des Dokuments.
Protokoll	Das für die Partner verfügbare Dokumentprotokoll.
Dokumenttyp	Ein bestimmter Geschäftsprozess.
Sortieren nach	Sortieren der Ergebnisse nach dem Namen des Quellenpartners oder Zielpartners.
Aktualisieren	Steuert, ob die Suchergebnisse in bestimmten Zeitabständen aktualisiert werden sollen (nur interner Partner).
Aktualisierungsrate	Steuert, wie häufig die Suchergebnisse aktualisiert werden sollen (nur interner Partner).

3. Klicken Sie auf **Suchen**. Das System zeigt die Zusammenfassung der Dokumentanalyse an.

Prozess- und Ereignisdetails anzeigen

1. Klicken Sie auf **Tools** > **Dokumentanalyse**. Das System ruft die Anzeige **Dokumentanalyse - Suche** auf.
2. Wählen Sie die Suchkriterien in den Dropdown-Listen aus.
3. Klicken Sie auf **Suchen**. Das System zeigt die Zusammenfassung der Dokumentanalyse an.
4. Klicken Sie auf das Symbol zum Anzeigen von Details neben den gewünschten Quellen- und Zielpartnern. Das System zeigt eine Liste aller Dokumente für die ausgewählten Partner an. Die Anzahl der Dokumente wird in Spalten nach Verarbeitungsstatus angezeigt.
5. Wählen Sie den Link für Menge in der Spalte **Empfangen**, **Wird ausgeführt**, **Fehlgeschlagen** oder **Erfolgreich** aus. Das System stellt Dokumentverarbeitungsdetails im Dokumentanalysebericht dar. Wenn Sie **Fehlgeschlagen** ausgewählt haben, umfasst der Bericht auch eine Dokumentereigniszusammenfassung.

Verarbeitung angepasster XML-Dateien

WebSphere Partner Gateway V6.0 und frühere Versionen stellten die Unterstützung für die Verarbeitung von angepasstem XML (XML - Extensible Markup Language) bereit, indem sie XML-Formate verwendeten. Mit XML-Formaten in WebSphere Partner Gateway V6.0 und früheren Versionen kann nicht die volle Funktionalität der XPath-Ausdruckssprache zum Extrahieren von Verarbeitungsinformationen aus Dokumenten genutzt werden. Daher wurde in WebSphere Partner Gateway V6.1 die Art, in der XML-Formate verwendet werden, überarbeitet. In WebSphere Partner Gateway V6.1 können in den Formaten Ausdrücke entsprechend XPath Version 1.0 verwendet werden. Durch die zusätzliche Verarbeitungsleistung der vollständigen XPath-Unterstützung wird die Größe der Dateien, die mit den XML-Formaten für vollständiges XPath verwendet werden können, begrenzt. Damit große Dateien verarbeitet werden können, wird eine Option bereitgestellt, die beim Definieren einer Dokumentfamilie festgelegt wird. Formate in einer Familie, in der die Option für die Verarbeitung großer Dateien aktiviert ist, verwenden die eingeschränkte XPath-Verarbeitungsleistung, die in WebSphere Partner Gateway V6.0 und früheren Versionen bereitgestellt wurde. Große Dateien können jedoch verarbeitet werden. Wird die Option für die Verarbeitung großer Dateien in einer Dokumentfamilie verwendet, gelten die folgenden Einschränkungen für Ausdrücke, die in den in der Familie gespeicherten XML-Formaten verwendet werden:

1. Es können nur einfache Elementpfade verwendet werden, die im Stammelement des Dokuments beginnen.
2. Elementpfade dürfen keine Namensbereichspräfixe enthalten, selbst wenn diese im Dokument angezeigt werden können.

Das Fenster **XML-Formate verwalten** enthält eine Dropdown-Liste mit dem Namen **Option für große Datei**. Die Liste enthält die Auswahlmöglichkeiten *Keine*, *Prozessor für große Dateien verwenden* und *Namespace-abhängigen Prozessor für große Dateien verwenden*. Der Benutzer kann eine Option für große Dateien verwenden, wenn er XML-Formate schreibt, die mit großen Dokumenten übereinstimmen sollen, die nicht mit dem vollständigen XPath-Prozessor verarbeitet werden können. Die Option für namespace-abhängige Prozessoren legt fest, dass die Elementpfade Namespacepräfixe enthalten sollen, wenn sie in einem Dokument angezeigt werden.

Anmerkung: Sobald die Familie erstellt ist, kann diese Option nicht mehr geändert werden. Grund hierfür ist, dass die Dokumentfamilie möglicherweise bereits XML-Formate enthält, die ungültig werden, wenn der Typ der Familie geändert wird. Die Verarbeitung angepasster XML-Dateien ist für Partner nicht verfügbar.

Dokumentvolumenbericht

Der Dokumentvolumenbericht ist ein nützliches Tool zum Verwalten, Überwachen und zur Fehlerbehebung beim Verarbeitungsablauf Ihrer Geschäftsdokumente. Der Bericht zeigt das Dokumentvolumen an, das vom System innerhalb eines bestimmten Zeitraums verarbeitet wird. Dieser Bericht kann angezeigt, ausgedruckt und gesichert (exportiert) und an andere Mitarbeiter gesendet werden.

Sie können diesen Bericht anpassen, um Informationen basierend auf bestimmten Suchkriterien anzuzeigen.

Der Dokumentvolumenbericht zeigt die Anzahl der Dokumente, die sich gerade in der Verarbeitung befinden, mit ihrem Status an:

Tabelle 35. Dokumentstatus

Wert	Beschreibung
Insgesamt empfangen	Die Gesamtzahl der vom System empfangenen Dokumente.
Wird ausgeführt	Die momentan ausgeführten Dokumente werden zur Zeit getestet und geprüft. Es wurde kein Fehler erkannt, aber der Vorgang ist noch nicht abgeschlossen.
Fehlgeschlagen	Die Dokumentverarbeitung wurde wegen eines Fehlers unterbrochen.
Erfolgreich	Die abschließende Nachricht, durch die die Dokumentverarbeitung fertig gestellt wird, wurde vom System an den Zielpartner übertragen.

Verwenden Sie diesen Bericht zum Ausführen folgender Tasks:

- Ermitteln, ob wichtige Geschäftsprozesse fertig gestellt wurden.
- Trends im Prozessvolumen zur Kostenkontrolle protokollieren.
- Prozessqualität verwalten (Erfolg und Fehler).
- Wenn Sie interner Partner sind, unterstützen Sie die Partner beim Protokollieren der Prozesseffektivität.

Dokumentvolumenbericht erstellen

1. Klicken Sie auf **Tools** > **Dokumentvolumenbericht**. Das System ruft die Anzeige **Dokumentvolumenbericht - Suche** auf.
2. Wählen Sie die Suchkriterien in den Dropdown-Listen aus.

Tabelle 36. Dokumentvolumenbericht, Suchkriterien

Wert	Beschreibung
Startdatum und -zeit	Datum und Uhrzeit der Prozesseinleitung.
Enddatum und -zeit	Datum und Uhrzeit der Fertigstellung des Prozesses.
Quellenpartner	Der Partner, der den Geschäftsprozess eingeleitet hat (nur interner Partner).
Zielpartner	Der Partner, der den Geschäftsprozess empfangen hat (nur interner Partner).
Suchen in	Suchen im sendenden oder empfangenden Dokumententyp.
Zieltyp	**Produktion** oder **Test**. Die Option **Test** ist nur auf Systemen verfügbar, die den Zieltyp **Test** unterstützen.
Paket	Beschreibt das Format, die Verpackung, die Verschlüsselung und die Inhaltstypidentifikation des Dokuments.
Protokoll	Typ des Prozessprotokolls, z. B. XML, EDI, Flachdatei.
Dokumenttyp	Ein bestimmter Geschäftsprozess.
Sortieren nach	Sortieren der Ergebnisse nach diesen Kriterien (Dokumenttyp oder Zieldokumenttyp).
Ergebnisse pro Seite	Anzahl der angezeigten Einträge pro Seite.

3. Klicken Sie auf **Suchen**. Das System zeigt den Bericht an.

Dokumentvolumenbericht exportieren

1. Klicken Sie auf **Tools** > **Dokumentvolumenbericht**. Das System ruft die Anzeige **Dokumentvolumenbericht - Suche** auf.
2. Wählen Sie die Suchkriterien in den Dropdown-Listen aus.
3. Klicken Sie auf **Suchen**. Das System zeigt den Bericht an.
4. Klicken Sie auf das Symbol zum Exportieren des Berichts, um den Bericht zu exportieren. Navigieren Sie zum Speichern der Datei zur gewünschten Position.

Anmerkung: Berichte werden als CSV-Dateien (CSV = Comma-Separated Values; durch Kommas getrennte Werte) gespeichert. Die entsprechenden Dateinamen haben das Suffix ".csv".

Berichte drucken

1. Klicken Sie auf **Tools** > **Dokumentvolumenbericht**. Das System ruft die Anzeige **Dokumentvolumenbericht - Suche** auf.
2. Wählen Sie die Suchkriterien in den Dropdown-Listen aus.
3. Klicken Sie auf **Suchen**. Das System zeigt den Bericht an.
4. Klicken Sie auf das Symbol zum Drucken, um den Bericht zu drucken.

Partnerverbindung testen

Mit der Funktion **Partnerverbindung testen** können Sie das Ziel oder den Web-Server testen. Wenn Sie interner Partner sind, können Sie auch einen bestimmten Partner auswählen. Bei diesem Test wird eine leere POST-Anforderung an ein Ziel oder eine URL gesendet. Die Anforderung ähnelt dem Eingeben der URL von Yahoo (www.yahoo.com) in das Adressfeld Ihres Browsers. Es wird nichts versandt, sondern es handelt sich um eine leere Anforderung. Die vom Ziel oder dem Web-Server empfangene Antwort gibt deren Status an:

- Wird eine Antwort zurückgegeben, ist der Server aktiv.
- Wird keine Antwort zurückgegeben, ist der Server nicht aktiv.

Wichtig: Die Funktion **Partnerverbindung testen** kann mit HTTP ausgeführt werden, das keinerlei Verbindungsparameter erfordert.

Gehen Sie wie folgt vor, um eine Partnerverbindung zu testen:

1. Klicken Sie auf **Tools > Partnerverbindung testen**. Das System ruft die Anzeige **Partnerverbindung testen** auf.
2. Wählen Sie die Testkriterien aus den Dropdown-Listen aus.

Tabelle 37. Partnerverbindung testen, Werte

Wert	Beschreibung
Partner	Zu testender Partner (nur interner Partner).
Ziel	Zeigt die verfügbaren Ziele basierend auf dem oben ausgewählten Partner an.
URL	Wird dynamisch ausgefüllt, basierend auf dem oben ausgewählten Ziel.
Befehl	POST oder GET.

3. Klicken Sie auf **URL testen**. Das System zeigt die Testergebnisse an. Informationen zum zurückgegebenen Statuscode finden Sie in den folgenden Abschnitten.

Ergebniscodes des Web-Servers

200-299:

- 200 - OK - Successful transmission. Es liegen keine Fehler vor. Die angeforderte Datei wurde zugestellt.
- 201 - Created. Die Anforderung wurde erfüllt und führte zur Erstellung einer neuen Ressource. Auf die neu erstellte Ressource kann durch die URLs verwiesen werden, die im URL-Headerfeld der Antwort zurückgegeben werden, wobei die genaueste URL für die Ressource durch ein Headerfeld ″Location″ bereitgestellt wird.
- 202 - Accepted. Die Anforderung wurde zur Verarbeitung angenommen, aber die Verarbeitung wurde noch nicht fertig gestellt.
- 203 - Non-Authoritative Information. Die zurückgegebenen META-Informationen im Header ″Entity″ stellen nicht den endgültigen Satz dar, der vom Quellenserver bereitgestellt wurde, sondern werden von einer lokalen Kopie oder der Kopie eines Fremdanbieters erfasst.
- 204 - No Content. Der Server hat die Anforderung erfüllt, aber es müssen keine neuen Informationen zurückgesendet werden.
- 206 - Partial Content. Sie haben einen Bytebereich der Datei angefordert; diesen erhalten Sie hiermit. Dies ist neu in HTTP 1.1.

300-399:

- 301 - Moved Permanently. Der angeforderten Ressource wurde eine neue, permanente URL zugeordnet; alle zukünftigen Verweise auf diese Ressource sollten mit Hilfe einer der zurückgegebenen URLs erfolgen.
- 302 - Moved Temporarily. Die angeforderte Ressource befindet sich temporär unter einer neuen URL. Umleitung zu einer neuen URL. Die ursprüngliche Seite ist umgezogen. Dies ist kein Fehler; die meisten Browser rufen die neue Seite ohne Verzögerung ab, wenn sie dieses Ergebnis sehen.

400-499:

- 400 - Bad Request. Die Anforderung konnte vom Server nicht verstanden werden, da ihre Syntax nicht ordnungsgemäß formatiert ist. Der Client hat eine fehlerhafte Anforderung ausgeführt.
- 401 - Unauthorized. Für die Anforderung ist eine Benutzerauthentifizierung erforderlich. Die Antwort muss ein Headerfeld "WWW-Authenticate" mit einer auf die angefragte Quelle anwendbaren Anforderung enthalten. Der Benutzer forderte ein Dokument an, stellte jedoch keinen gültigen Benutzernamen bzw. kein gültiges Kennwort zur Verfügung.
- 402 - Payment Required. Dieser Code wird aktuell nicht unterstützt, aber für die zukünftige Verwendung reserviert.
- 403 - Forbidden. Der Server hat die Anforderung verstanden, führt sie jedoch auf Grund einer unspezifizierten Ursache nicht aus. Der Zugriff auf dieses Dokument wird explizit verweigert. (Dies passiert unter Umständen deshalb, weil der Web-Server über keine Leseberechtigung für die angeforderte Datei verfügt.) Der Server sendet Ihnen die Datei nicht. Möglicherweise wurde die Berechtigung explizit inaktiviert.
- 404 - Not Found. Der Server konnte keine Übereinstimmung mit der angeforderten URL finden. Diese Datei ist nicht vorhanden. Sie erhalten diese Nachricht, wenn Sie in Ihrem Browser eine fehlerhafte URL eingeben. Sie wird unter Umständen auch versandt, wenn der Server dazu aufgefordert wurde, das Dokument zu schützen und deshalb nicht berechtigten Personen mitzuteilen, es existiere nicht. 404-Fehler treten bei Anforderungen von Seiten auf, die nicht existieren, und können folgende Ursachen haben: Eine URL wurde nicht korrekt eingegeben, ein Lesezeichen verweist auf eine nicht mehr unter dieser Adresse vorhandene Datei, eine Suchmaschine sucht nach einer Datei "robots.txt" (damit werden Seiten gekennzeichnet, die nicht durch Suchmaschinen indexiert werden sollen), ein Benutzer rät einen Dateinamen, Links von Ihrer Site oder anderen Sites sind fehlerhaft, etc.
- 405 - Method Not Allowed. Die in der Anforderungszeile angegebene Methode ist für die Ressource nicht zulässig, die durch die angeforderte URL identifiziert wird.
- 406 - None Acceptable. Der Server hat eine mit der angeforderten URL übereinstimmende Ressource gefunden; diese erfüllt jedoch nicht die durch die Anforderungsheader "Accept" und "Accept-Encoding" angegebenen Bedingungen.
- 407 - Proxy Authentication Required. Dieser Code ist für eine zukünftige Verwendung reserviert. Er ähnelt dem Code 401 (Unauthorized), gibt jedoch an, dass der Client sich zunächst mit einem Proxy authentifizieren muss. HTTP 1.0 stellt keine Möglichkeit zur Proxyauthentifizierung zur Verfügung.
- 408 - Request Time out. Der Client hat keine Anforderung innerhalb der Zeitspanne erstellt, die der Server bereit ist, zu warten.
- 409 - Conflict. Die Anforderung konnte auf Grund eines Konflikts mit dem aktuellen Status der Ressource nicht fertig gestellt werden.

- 410 - Gone. Die angeforderte Ressource ist beim Server nicht mehr verfügbar, und es ist keine Weiterleitungsadresse bekannt.
- 411 - Authorization Refused. Der vom Client bereitgestellte Berechtigungsnachweis der Anforderung wurde vom Server zurückgewiesen und ist unzureichend, um die Autorisierung für den Zugriff auf die Ressource zu gewähren.
- 412 - Precondition Failed
- 413 - Request Entity Too Large
- 414 - Request URI Too Large
- 415 - Unsupported Media Type

500-599:

- 500 - Internal Server Error. Beim Server ist eine unerwartete Bedingung aufgetreten, sodass er die Anforderung nicht erfüllen konnte. Beim Web-Server ist ein Fehler aufgetreten, sodass er keine korrekte Antwort ausgeben konnte. Normalerweise kann dieser Fehler von der Seite des Browsers aus nicht behoben werden; der Serveradministrator muss wahrscheinlich das Fehlerprotokoll des Servers überprüfen, um die Ursache des Fehlers zu finden. Oftmals ist dies die Fehlernachricht für ein CGI-Script, das nicht ordnungsgemäß codiert ist.
- 501 - Method Not Implemented. Der Server unterstützt nicht die notwendige Funktionalität zum Erfüllen der Anforderung. Die Anwendungsmethode (GET oder POST) ist nicht implementiert.
- 502 - Bad Destination. Der Server empfing beim Zugriff auf das Ziel oder den übergeordneten Server zum Erfüllen der Anforderung eine ungültige Antwort.
- 503 - Service Temporarily Unavailable. Der Server ist wegen einer temporären Überlastung bzw. Wartung momentan nicht in der Lage, die Anforderung zu bearbeiten. Der Server verfügt über keine Ressourcen.
- 504 - Destination Time out. Der Server empfing beim Zugriff auf das Ziel oder den übergeordneten Server zum Erfüllen der Anforderung keine rechtzeitige Antwort.
- 505 - HTTP Version Not Supported

EDI-Berichte

Verwenden Sie EDI-Berichte, um überfällige funktionale Bestätigungen (Functional Acknowledgement - FA) für Electronic Data Interchange (EDI) zu suchen. Darüber hinaus können Sie auch zurückgewiesene EDI-Transaktionen suchen. In den folgenden Abschnitten wird die Vorgehensweise für die Verwendung der EDI-Berichte beschrieben.

Suche nach überfälligen EDI-FAs

Auf der Seite **Suche nach überfälligen EDI-FAs** werden Suchkriterien für die Suche nach überfälligen funktionalen EDI-Bestätigungen (EDI-FAs) bereitgestellt.

Anmerkung: Alle Sätze, die aus vorherigen Suchoperationen nach überfälligen funktionalen EDI-Bestätigungen entfernt wurden, werden auch von späteren Suchoperationen ignoriert. Daher werden entfernte Sätze in späteren Berichten nicht angezeigt. Sätze können aus einem Bericht entfernt werden, indem auf der Seite **Bericht für überfällige funktionale EDI-Bestätigungen** die Option **Ausgewählte Sätze ignorieren** ausgewählt wird. Nur der Hubadministrator kann Sätze aus einem Bericht löschen.

Gehen Sie wie folgt vor, um nach überfälligen EDI-FA-Sätzen zu suchen:

1. Klicken Sie auf **Tools > EDI-Berichte**. Die Seite **Suche nach überfälligen EDI-FAs** wird angezeigt.
2. Wählen Sie in der Dropdown-Liste eines oder mehrere der folgenden Suchkriterien aus:

Tabelle 38. Suchkriterien für überfällige EDI-FAs

Wert	Beschreibung
Startdatum und -zeit	Das Datum und die Zeit für den Beginn der Transaktion.
Enddatum und -zeit	Das Datum und die Zeit für das Ende der Transaktion.
Quellenpartner	Der Partner, der die Transaktion eingeleitet hat.
Zielpartner	Der Partner, der die Transaktion empfangen hat.
Suchen in	Gibt an, ob im Quellendokumenttyp oder im Zieldokumenttyp gesucht werden soll.
Paket	Beschreibt das Format, die Verpackung, die Verschlüsselung und die Inhaltstypidentifikation des Dokuments.
Protokoll	Typ des Prozessprotokolls, z. B. XML, EDI, Flachdatei. Die angezeigten Protokolle variieren abhängig von dem im Feld **Paket** ausgewählten Wert.
Dokumenttyp	Der jeweilige Dokumenttyp. Die angezeigten Typen variieren abhängig von der Auswahl im Feld **Protokoll**.
Referenz-ID	Gibt eine Transaktions-ID an.
Sortieren nach	Gibt die Kriterien zum Sortieren der Suchergebnisse an. Die Standardwerte sind **Überfällig seit** und **Absteigend**. Verwenden Sie **Absteigend**, um die FAs zuerst anzuzeigen, die am längsten überfällig sind. Wählen Sie **Aufsteigend** aus, um die FAs zuerst anzuzeigen, die am wenigsten überfällig sind.
Ergebnisse pro Seite	Gibt an, wie viele Ergebnisse einer Transaktionssuche auf jeder einzelnen Seite angezeigt werden sollen.

3. Klicken Sie auf **Suchen**, um den Bericht über die Suche nach überfälligen EDI-FAs anzuzeigen.

Berichte zu überfälligen EDI-FAs anzeigen

Das Suchergebnis wird abhängig von den auf der Seite **Suche nach überfälligen EDI-FAs** ausgewählten Suchkriterien auf der Seite **Bericht für überfällige EDI-FAs** angezeigt.

Der Bericht für überfällige EDI-FAs (funktionale EDI-Bestätigungen) enthält die folgenden Daten (falls anwendbar):

Tabelle 39. Bericht zu überfälligen EDI-FAs

Wert	Beschreibung
Datum	Das Datum, an dem die EDI-Transaktion vom Quellenpartner an den Zielpartner gesendet wurde.
Zeit	Die Uhrzeit (Greenwich Mean Time), zu der die EDI-Transaktion vom Quellenpartner an den Zielpartner gesendet wurde.
Aktivitäts-ID	Die virtuell eindeutige ID (VUID) der Transaktion.
Quellenhandelspartner	Der Partner, der die Transaktion gesendet hat.
Quellenpaket	Das Quellenpaket der Transaktion.
Quellenprotokoll	Das Quellenprotokoll der Transaktion.
Quellendokumenttyp	Der Quellendokumenttyp der Transaktion.
Zielhandelspartner	Der Partner, der die Transaktion gesendet hat.
Zielpaket	Das Zielpaket der Transaktion.
Zielprotokoll	Das Zielprotokoll der Transaktion.
Zieldokumenttyp	Der Zieldokumenttyp der Transaktion.
Austauschnummer	Die Austauschnummer der Transaktion.
Gruppennummer	Die Gruppennummer der Transaktion.
Transaktionsnummer	Die Kenn-Nummer der Transaktion.
FA fällig am	Das Datum, an dem die FA für die Transaktion fällig war.
Überfällig seit	Die Zeitdauer, seit der die FA bereits überfällig ist.
Ausgewählte Sätze ignorieren	Wenn Sie diese Option für einen Satz auswählen, wird dieser Satz aus dem Bericht entfernt. Wenn ein Satz aus einem Bericht entfernt wird, wird dieser Satz auch von späteren Suchen nach überfälligen funktionalen EDI-Bestätigungen ignoriert und wird daher auch in diesen Berichten nicht angezeigt. Nur der Hubadministrator kann Sätze aus einem Bericht löschen.

Suche nach zurückgewiesenen EDI-Transaktionen

Auf der Seite **Suche nach zurückgewiesenen EDI-Transaktionen** werden Kriterien angezeigt, mit deren Hilfe Sie EDI-Transaktionen (EDI, Electronic Data Interchange - elektronischer Datenaustausch) suchen können, deren funktionale Bestätigung (FA) einen Fehlercode enthält. Transaktionsdatensätze ohne FAs werden von der Suche nach zurückgewiesenen EDI-Transaktionen nicht zurückgegeben.

Gehen Sie wie folgt vor, um nach zurückgewiesenen EDI-Sätzen zu suchen:

1. Klicken Sie auf **Tools > EDI-Berichte > Bericht zu zurückgewiesenen EDI-Transaktionen**.
2. Wählen Sie in der Dropdown-Liste eines oder mehrere der folgenden Suchkriterien aus:

Tabelle 40. Suchkriterien für zurückgewiesene EDI-Transaktionen

Wert	Beschreibung
Startdatum und -zeit	Das Datum und die Zeit für den Beginn der Transaktion.
Enddatum und -zeit	Das Datum und die Zeit für das Ende der Transaktion.
Quellenpartner	Der Partner, der die Transaktion eingeleitet hat.
Zielpartner	Der Partner, der die Transaktion empfangen hat.
Suchen in	Gibt an, ob im Quellendokumenttyp oder im Zieldokumenttyp gesucht werden soll.
Paket	Beschreibt das Format, die Verpackung, die Verschlüsselung und die Inhaltstypidentifikation des Dokuments.
Protokoll	Typ des Prozessprotokolls, z. B. XML, EDI, Flachdatei.Die angezeigten Protokolle variieren abhängig von dem im Feld **Paket** ausgewählten Wert.
Dokumenttyp	Der jeweilige Dokumenttyp. Die angezeigten Typen variieren abhängig von der Auswahl im Feld **Protokoll**.
Referenz-ID	Gibt eine Transaktions-ID an.
Sortieren nach	Gibt die Kriterien zum Sortieren der Suchergebnisse an. Die Standardwerte sind **Überfällig seit** und **Absteigend**. Verwenden Sie **Absteigend**, um die FAs zuerst anzuzeigen, die am längsten überfällig sind. Wählen Sie **Aufsteigend** aus, um die FAs zuerst anzuzeigen, die am wenigsten überfällig sind.
Ergebnisse pro Seite	Gibt an, wie viele Ergebnisse einer Transaktionssuche auf jeder einzelnen Seite angezeigt werden sollen.

3. Klicken Sie auf **Suchen**, um die zurückgewiesenen EDI-Transaktionen anzuzeigen.

Berichte zu zurückgewiesenen EDI-Transaktionen anzeigen

Das Suchergebnis wird abhängig von den auf der Seite **Suche nach zurückgewiesenen EDI-Transaktionen** ausgewählten Suchkriterien auf der Seite **Bericht für zurückgewiesene EDI-Transaktionen** angezeigt.

Der Bericht für zurückgewiesene EDI-Transaktionen enthält die folgenden Daten (falls anwendbar):

Tabelle 41. Bericht für zurückgewiesene EDI-Transaktionen

Wert	Beschreibung
Datum	Das Datum, an dem die EDI-Transaktion empfangen wurde.
Zeit	Die Uhrzeit (Greenwich Mean Time), zu der die EDI-Transaktion vom Quellenpartner an den Zielpartner gesendet wurde.
Aktivitäts-ID	Die virtuell eindeutige ID (VUID) der Transaktion.
Quellenhandelspartner	Der Partner, der die Transaktion gesendet hat.
Quellenpaket	Das Quellenpaket der Transaktion.
Quellenprotokoll	Das Quellenprotokoll der Transaktion.
Quellendokumenttyp	Der Quellendokumenttyp der Transaktion.
Zielhandelspartner	Der Partner, der die Transaktion empfangen hat.
Zielpaket	Das Zielpaket der Transaktion.
Zielprotokoll	Das Zielprotokoll der Transaktion.
Zieldokumenttyp	Der Zieldokumenttyp der Transaktion.
Austauschnummer	Die Austauschnummer der Transaktion.
Gruppennummer	Die Gruppennummer der Transaktion.
Transaktionsnummer	Die Kenn-Nummer der Transaktion.
Statuscode	Der Statuscode der funktionalen Bestätigung (FA).
Statustext	Der Statustext der funktionalen Bestätigung (FA).

FTP-Berichte

FTP-Berichte stellen Details zu FTP-Statistiken und FTP-Verbindungen bereit.

FTP-Statistiken

Auf der Seite **FTP-Statistiken** wird der Status des FTP-Servers im schreibgeschützten Modus angezeigt.

Anmerkung: Die Statistik wird nicht angezeigt, wenn der FTP-Server oder der FTP-Management-Server nicht verfügbar ist.

Gehen Sie wie folgt vor, um den Status des FTP-Servers anzuzeigen:

1. Klicken Sie auf **Tools > FTP-Berichte**. Die Seite **FTP-Statistiken** wird angezeigt.
2. Die folgenden Informationen zum Serverstatus werden angezeigt:

Tabelle 42. FTP-Statistik

Wert	Beschreibung
Startzeit des Servers	Die Zeit, zu der der FTP-Server gestartet wurde.
Anzahl erstellter Verzeichnisse	Die Anzahl der Verzeichnisse, die von Benutzern mit Hilfe des Befehls ″mkdir″ erstellt wurden.
Anzahl entfernter Verzeichnisse	Die Anzahl der Verzeichnisse, die von Benutzern mit Hilfe des Befehls ″rmdir″ entfernt wurden.
Anzahl hochgeladener Dateien	Die Anzahl der von allen Benutzern hochgeladenen Dateien.
Anzahl heruntergeladener Dateien	Die Anzahl der von allen Benutzern heruntergeladenen Dateien.
Anzahl gelöschter Dateien	Die Anzahl der von allen Benutzern mit Hilfe des Befehls ″delete″ gelöschten Dateien.
Hochgeladene Byte	Die Summe der hochgeladenen Byte.
Heruntergeladene Byte	Die Summe der heruntergeladenen Byte.
Aktuelle Anmeldungen	Die Anzahl der momentan angemeldeten Benutzer.
Gesamtzahl Anmeldungen	Die Summe der Anmeldungen seit dem letzten Zurücksetzen.
Gesamtzahl fehlgeschlagene Anmeldungen	Die Summe der fehlgeschlagenen Anmeldungen.
Aktuelle Verbindungen	Die Anzahl der momentan aktiven Verbindungen.
Gesamtzahl Verbindungen	Die Summe der Verbindungen seit dem letzten Zurücksetzen.

3. Klicken Sie auf **Neu laden**, um die Anzahl der momentan angemeldeten Benutzer zu aktualisieren.
4. Klicken Sie auf **Zurücksetzen**, um die Werte zurückzusetzen.

FTP-Verbindungen

Zeigen Sie die FTP-Verbindungen an, indem Sie die folgenden Schritte ausführen:

1. Klicken Sie auf **Tools > FTP-Berichte > FTP-Verbindungen**.
2. Im Bericht werden die folgenden Verbindungsinformationen angezeigt:

Tabelle 43. FTP-Verbindungen

Wert	Beschreibung
Anmeldename	Die Anmeldebenutzer-ID für diese Verbindung. Ist dieses Feld leer, bedeutet dies, dass der Benutzer nur eine Verbindung hergestellt, sich aber noch nicht angemeldet hat.
Zeit der Anmeldung	Der Zeitpunkt, zu dem sich der Benutzer angemeldet hat. Ist dieses Feld leer, bedeutet dies, dass der Benutzer nur eine Verbindung hergestellt hat.
Zeit des letzten Zugriffs	Der Zeitpunkt, zu dem der Benutzer das letzte Mal zuvor auf diese Verbindung zugegriffen hat. Ist dieses Feld leer, bedeutet dies, dass der Benutzer sich zwar angemeldet hat, aber noch keinen Befehl ausgegeben hat.
Clientadresse	Die IP-Adresse des Clients, von der aus der Benutzer sich angemeldet hat.

Glossar

A

Ablauf. Die erforderliche Reihenfolge der Dokumente, die zur erfolgreichen Ausführung eines Geschäftsprozesses benötigt werden.

Aktion. (1) Vom System für ein Dokument ausgeführte Aktionen, um die Kompatibilität des Dokuments mit Geschäftsanforderungen der Partner untereinander sicherzustellen. (2) Eine Reihe von Verarbeitungsschritten, wie beispielsweise die Dokumentprüfung und -transformation.

Aktionsinstanz-ID. Identifiziert Dokumente mit Geschäftsinhalt, z. B. Bestellungen oder Angebotsanfragen.

Aktivierung. Die Verbindung eines Partners mit dem System.

Alert. Alerts stellen schnelle Benachrichtigungen und Problemlösungen bereit, wenn voreingestellte Betriebsgrenzwerte überschritten werden. Ein Alert besteht aus einer textbasierten E-Mail-Nachricht, die an Einzelpersonen oder an eine Verteilerliste von wichtigen Kontakten innerhalb oder außerhalb des Netzes gesendet wird. Alerts können auf dem Auftreten eines Systemereignisses oder dem erwarteten Prozessvolumen basieren.

Antwortgeschäftsaktion. Identifiziert den Typ des Geschäftsdokuments, das als Antwort auf eine Aktion in demselben Prozess gesendet wurde.

B

Berichte. Mit dem Berichtsmodul können Benutzer detaillierte Berichte über das Volumen der in der Verarbeitung befindlichen Prozesse erstellen sowie über vom System generierte Ereignisse.

Betriebsmodus. Identifiziert Dokumente, die während des Testlaufs oder der tatsächlichen Produktion an ein bestimmtes Gateway geleitet werden.

C

Community Console. Die Community Console ist ein webbasiertes Tool für die Überwachung des Verarbeitungsablaufs der Geschäftsdokumente in Ihrem Unternehmen zum und vom internen Partner bzw. zu und von den externen Partnern.

D

Digitale Signatur. Eine digitale Signatur ist eine elektronische Unterschrift, die zur Authentifizierung der Partner verwendet wird sowie zur Sicherstellung, dass der ursprüngliche Inhalt eines versandten Dokuments nicht geändert wurde.

Dokument. Eine Sammlung von Informationen, die einer Unternehmenskonvention unterliegen. Informationen können aus Text, Bildern und Tönen bestehen.

Dokumentdefinition. Stellt dem System alle notwendigen Informationen zum Empfangen, Verarbeiten und Weiterleiten von Dokumenten zwischen Community-Teilnehmern zur Verfügung. Dokumentdefinitionstypen umfassen Pakete, Protokolle, Dokumenttypen, Aktivitäten und Aktionen.

Dokumentprotokoll. Ein Satz von Regeln und Anweisungen (Protokoll) zum Formatieren und Übertragen von Informationen über ein Computernetz hinweg. Beispiele umfassen RosettaNet, XML, Flachdatei und EDI.

DUNS. Die D-U-N-S-Nummer von D&B ist eine eindeutige Identifikationsfolge mit neun Ziffern, die eindeutige Kennungen für einzelne Geschäftsobjekte zur Verfügung stellt und gleichzeitig Unternehmensstrukturen miteinander verbindet. D&B verbindet die D-U-N-S-Nummern von Mutterfirmen, Tochterunternehmen, Hauptniederlassungen und Filialen von über 64 Millionen Mitgliedern einer Unternehmensfamilie auf der ganzen Welt miteinander. Sie werden von einflussreichen und Standards setzenden Unternehmen verwendet und von über 50 weltweiten Industrie- und Handelsverbänden erkannt, empfohlen und häufig benötigt. Dazu gehören die Vereinten Nationen, die US-Regierung, die australische Regierung und die Europäische Kommission. In der heutigen globalen Wirtschaft ist die D-U-N-S-Nummer von D&B zum Standard für die Überwachung von Unternehmen weltweit geworden.

E

EDI. Die Datenübertragung von Computer zu Computer in einem strukturierten, vorbestimmten Format. Der Fokus der EDI-Aktivität liegt traditionell auf dem Ersatz von vordefinierten Geschäftsformularen, z. B. Bestellungen und Rechnungen, durch ähnlich definierte elektronische Formulare.

Eingehender Manager. Ruft Dokumente vom NAS ab und bereitet sie für die entsprechende Aktionstask der Steuerkomponente des Geschäftsprozesses vor.

Einrichtung. Bei der Einrichtung (oder Aufnahme, engl. on-boarding) wird eine Folge von erforderlichen Schritten ausgeführt, um das B2B-Gateway eines Benutzers mit der Infrastruktur des Systems zu verbinden.

Ereignis. Eine vom System generierte Nachricht, die der Verarbeitung von Dokumenten zugeordnet ist.

Externer Partner. Ein Mitglied der Hub-Community, das Geschäftstransaktionen mit dem internen Partner austauscht.

F

Filter. Zum Entfernen von Daten innerhalb einer Subtransaktion auf der Basis von vordefinierten Parametern.

FTP. File Transfer Protocol (FTP), ein standardmäßiges Internetprotokoll, stellt die einfachste Möglichkeit dar, Dateien zwischen Computern über das Internet auszutauschen.

G

Geschäftsprozess. Ein vordefinierter Satz von Transaktionen, die die Methode darstellen, mit der die erforderliche Arbeit zum Erreichen eines Geschäftsziels ausgeführt wird.

Geschäftsregeltests. Der Prozess des Testens und Behebens von Dokumentinhaltsfehlern zwischen Partnern.

Geschäftssignalcode. Gibt den Typ des Signals (Dokument) an, das als Reaktion auf eine Aktion gesendet wird. Beispiele hierfür sind eine Empfangsbestätigung oder eine allgemeine Ausnahmebedingung.

Geschlossen. Das Datum und die Uhrzeit, zu der die Transaktion des letzten Dokuments in einem Prozess ausgeführt wurde bzw. ein Prozess abgebrochen wurde.

Global. Eine Kontaktperson, der vom externen Partner und dem internen Partner Alerts zugeordnet werden können.

Gruppe. Ein Benutzerverbund, der über Zugriffsrechte für die Community Console verfügt, die diese Gruppe zur Ausführung verschiedener Funktionen berechtigen.

Gültigkeitsprüfung. Bei der Gültigkeitsprüfung wird die Subtransaktion eines Prozesses mit den angegebenen Anforderungen verglichen, um seine Gültigkeit bzw. Ungültigkeit zu ermitteln. Der Inhalt und die Transaktionssequenz sind typische Parameter.

H

HTTP. Hypertext Transfer Protocol (HTTP) ist eine Menge von Regeln (Protokoll) zum Austauschen von Dateien (Text, Grafiken, Töne, Videos und andere Multimediadateien) über das Internet.

HTTPS. HTTPS (Hypertext Transfer Protocol über Secure Socket Layer) ist ein Webprotokoll, das Seitenanforderungen von Benutzern sowie die durch den Web-Server zurückgegebenen Seiten verschlüsselt und entschlüsselt.

I

ID für Antwort. Die ID-Nummer der Antwortgeschäftsaktion.

K

Klassifizierung. Gibt die Rolle des Partners in einem Geschäftsprozess an.

Kontenadmin. Mit Hilfe des Moduls **Kontenadmin** können Sie die Informationen anzeigen und bearbeiten, die Ihr Unternehmen im Netz identifizieren. Diese Anzeige wird auch dazu verwendet, Konsolzugriffsberechtigungen für andere Mitarbeiter in Ihrem Unternehmen zu verwalten.

L

Live. Der Status, bei dem ein Partner erfolgreich das Testen von Geschäftsregeln beendet hat und der interne Partner eine Leistungsanforderung ausgegeben hat, um sie in einen Livestatus zu versetzen.

P

Pakete. Identifizieren Dokumentpackformate, die vom Systemserver empfangen werden können. Beispiele: AS1 und AS2.

Partnerverbindung. Eine Partnerverbindung definiert die Verbindung zwischen den Umgebungen von zwei bestimmten Mitgliedern der Community. Über diese Verbindung wird ein eindeutiger Prozess ausgeführt.

PIP (Partner Interface Process). Definiert Geschäftsprozesse zwischen internen Partnern und externen Partnern (in WebSphere Partner Gateway werden Partner auch als Teilnehmer bezeichnet). Jeder PIP identifiziert ein bestimmtes Geschäftsdokument sowie die Art und Weise, wie dieses verarbeitet wird.

Platzhalterzeichen. Die Kriterien für Suchen mit Platzhalterzeichen beinhalten den Stern (*).

Produktion. Zum Routing von Livedokumenten verwendetes Zielgateway.

Profil. Mit Hilfe des Moduls **Profil** können Sie die Informationen anzeigen und bearbeiten, die Ihr Unternehmen im System identifizieren.

Protokolle. Identifizieren bestimmte Typen von Dokumentformaten für verschiedene Geschäftsprozesse. Beispiele: RosettaNet und XML.

Prozessinstanz-ID. Die eindeutige Identifikationsnummer für einen bestimmten Geschäftsprozess.

R

RNIF. Das RNIF (RosettaNet Implementation Framework) stellt eine Richtlinie zum Erstellen eines standardmäßigen Umhüllungsbehälters für alle PIPs (Partner Interface Processes) dar.

RTF. Rich Text Format (RTF) ist ein Dateiformat, mit dem Sie Textdateien zwischen unterschiedlichen Textverarbeitungsprogrammen auf unterschiedlichen Betriebssystemen austauschen können. Beispielsweise können Sie eine Datei mit Microsoft Word unter Windows 98 erstellen, als RTF-Datei speichern (diese hat dann das Suffix .rtf) und an jemanden senden, der WordPerfect 6.0 unter Windows 3.1 verwendet.

S

Service. Gibt an, ob eine Nachricht RosettaNet-basiert ist.

Servlet. Ein kleines Programm, das auf dem Web-Server ausgeführt wird und eingehende Dokumente in den NAS schreibt.

Sichtbarkeit. Die Sichtbarkeit definiert, ob einem Alert eine Kontaktperson durch einen Partner (lokal) oder auch durch den internen Partner (global) zugeordnet werden kann.

Signal. Das Dokument, das als Antwort auf eine Aktion gesendet wird.

Signalinstanz-ID. Identifiziert Dokumente, die als Antwort auf Aktionen versandte positive oder negative Rückmeldungen darstellen.

Signalversion. Die Version des Geschäftsprozesses, der als Signal versandt wird.

SMTP. Simple Mail Transfer Protocol (SMTP) ist ein Protokoll, das zum Versenden und Empfangen von E-Mails verwendet wird.

SR. Serviceanforderung

SSL. Secure Sockets Layer (SSL) stellt eine sichere Methode zum Versenden von Daten mit Hilfe des Protokolls HTTP dar.

Status. (1) Dokumente, die sich in der Verarbeitung durch das System befinden, haben einen der folgenden vier Status: (2) Empfangen, Wird ausgeführt, Fehlgeschlagen oder Erfolgreich.

Subskribierte Kontakte. Ein subskribierter Kontakt stellt eine Einzelperson dar, die zum Empfangen von E-Mail-Alerts bestimmt ist.

Substitution. Das Ersetzen von Daten innerhalb einer Subtransaktion durch andere Daten basierend auf vordefinierten Parametern.

T

Test. Der Status, in dem ein Partner während des Einrichtungsprozesses die vorbeugende Datenbereinigung oder das Testen von Geschäftsregeln ausführt.

Tools. Mit Hilfe des Moduls **Tools** können Sie Verarbeitungsfehler beheben, indem fehlerhafte Dokumente, Datenfelder und deren zugeordnete Ereignisse angezeigt werden.

Transaktion. Eine Folge des Datenaustauschs und der zugehörigen Arbeitsschritte, die zu Zwecken der Geschäftsausführung zwischen den Partnern als eine Einheit behandelt werden.

Transaktions-ID. Die ID-Nummer des Geschäftsprozesses.

Transportprotokoll. Eine Menge von Regeln (Protokoll), die zum Senden von Daten in Form von Nachrichteneinheiten zwischen Computern über das Internet verwendet wird. Beispiele hierfür sind HTTP, HTTPS, SMTP und FTP.

U

Übersetzung. Die Konvertierung eines Dokuments von einem Protokoll in ein anderes Protokoll.

Umschlag entfernen. Das Extrahieren eines Dokuments aus einem EDI-Umschlag.

Umsetzung. Ersetzt den Inhalt eines Dokuments durch Daten aus einer Querverweistabelle.

Untergeordnetes Element des internen Partners. Das untergeordnete Element des internen Partners ist ein spezieller Partnertyp, der in der Console die Funktion eines externen Partners hat, sich beim Routing jedoch wie ein interner Partner verhält.

URL. Eine URL (Uniform Resource Locator) ist die Adresse eines Dokuments oder eines Prozesses (Ressource), auf das/den über das Internet zugegriffen werden kann.

V

Version. Das bestimmte Release eines Dokumentprotokolls.

Versuchsanzahl. Gibt an, ob eine Transaktion den ersten Versuch oder eine Wiederholung darstellt. 1 ist der erste Versuch. 2 oder eine höhere Zahl ist die Anzahl der Wiederholungen.

Vorbeugende Datenbereinigung. Der Prozess des Testens und Behebens von Fehlern in der Dokumentstruktur und im Dokumentformat auf der Basis von Geschäftsprozessstandards.

Z

Ziel. Eine B2B-Netzposition, die als Eingang zu einem anderen Netzwerk fungiert. Ein Ziel kann Probleme bei der Datenumsetzung und Kompatibilität beheben und so die Datenübertragung sicherstellen.

Bemerkungen

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. An Stelle 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 Angaben in diesem Handbuch werden in regelmäßigen Zeitabständen aktualisiert. Die Änderungen werden in Überarbeitungen oder in Technical News Letters (TNLs) bekannt gegeben. IBM kann ohne weitere Mitteilung jederzeit Verbesserungen und/oder Änderungen an den in dieser Veröffentlichung beschriebenen Produkten und/oder Programmen vornehmen.

Verweise in diesen Informationen auf Websites anderer Anbieter 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
USA

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.

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.

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.

COPYRIGHTLIZENZ

Diese Veröffentlichung enthält Musteranwendungsprogramme, die in Quellensprache geschrieben sind. 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.

WebSphere Partner Gateway enthält den Code ICU4J, für den Sie unter den Bedingungen der Internationalen Nutzungsbedingungen für Programmpakete, unter Vorbehalt der Bedingungen für ausgeschlossene Komponenten, eine Lizenz von IBM erhalten. Die Bereitstellung des folgenden Hinweises durch IBM ist jedoch erforderlich:

COPYRIGHT UND GENEHMIGUNGSNACHWEIS

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, das IBM Logo, AIX, CICS, DB2, DB2 Universal Database, IBMLink, IMS, MQSeries, MVS, OS/390, WebSphere und z/OS.

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.

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 Version 6.1.1

Index

E

F

G

H

I

J

K

L

O

P

R

S

T

U

V

W

X

Z