IBM WebSphere Partner Gateway Enterprise
und Advanced Edition

Teilnehmer-Handbuch

Version 6.0

IBM WebSphere Partner Gateway Enterprise
und Advanced Edition

Teilnehmer-Handbuch

Version 6.0

Hinweis

Vor Verwendung dieser Informationen und des darin beschriebenen Produkts sollten die Informationen unter „Bemerkungen" auf Seite 79 gelesen werden.

Ausgabe Juni 2005

Diese Veröffentlichung ist eine Übersetzung des Handbuchs

IBM WebSphere Partner Gateway Enterprise and Advanced Editions Participant Guide,

herausgegeben von International Business Machines Corporation, USA

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

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

Änderung des Textes bleibt vorbehalten.

Herausgegeben von:
SW TSC Germany
Kst. 2877
Juni 2005

Inhaltsverzeichnis

Zu diesem Handbuch

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-Teilnehmern 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 beteiligten Partner werden als Community Manager, Community Operator (Hubadministrator) und als Community-Teilnehmer (oder kurz Teilnehmer) bezeichnet. 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: *<servername><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.

Zugehörige Dokumentation

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

Sie können die Dokumentation herunterladen oder online unter der folgenden Adresse 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 können von der Unterstützungswebsite für WebSphere Business Integration heruntergeladen werden:

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

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

Neuerungen in diesem Release

Neuerungen in Release 6.0

Der vorliegende Abschnitt enthält Informationen zu den wichtigsten Änderungen, die in WebSphere Partner Gateway Version 6.0 vorgenommen wurden.

- Der Produktname wurde von WebSphere Business Integration Connect in WebSphere Partner Gateway geändert.
- Es wurde ein neues Kapitel zur Erstellung von Gateways zum Handbuch hinzugefügt. Weitere Informationen hierzu finden Sie in Kapitel 3, „Gateways erstellen", auf Seite 25.
- Dateinamen und Verzeichnisse wurden entsprechend der neuen Namenskonvention aktualisiert.
- Die Unterstützung für den FTP-Scripting-Transport wurde hinzugefügt. Weitere Informationen hierzu finden Sie in „FTP-Scripting-Gateway einrichten" auf Seite 34.
- Die Unterstützung mehrerer Zertifikate wurde hinzugefügt. Informationen dazu finden Sie im Abschnitt „Digitale Zertifikate hochladen" auf Seite 9.

Neuerungen in Release 4.2.2

In diesem Abschnitt werden die Änderungen beschrieben, die seit dem letzten Release (4.2.1) an diesem Handbuch vorgenommen wurden.

- Dieses Handbuch enthält nun ausschließlich Informationen zur Verwaltung und Pflege der Umgebung von WebSphere Partner Gateway.
- Der Community Console wurden neue Eingabehilfefunktionen zur Unterstützung von Sprachausgabeprogrammen hinzugefügt.

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: Community Operator, Community Manager und Teilnehmer.

Community Operator

Der Community Operator ist eine Firma, die für die Verwaltung des täglichen Betriebs der Hub-Community verantwortlich ist. Der Community Operator 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 Teilnehmer.
- Hilfe bei der Konfiguration neuer Teilnehmer der Hub-Community.
- Strategische Planung für zukünftiges Wachstum, um einen Betrieb der Hub-Community mit höchstmöglicher Effizienz sicherzustellen.

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

Community Manager

Der Community Manager ist die primäre Firma und treibende Kraft innerhalb der Hub-Community. Diese Firma ist verantwortlich für den Kauf und den Aufbau der Hub-Community, einschließlich der Definition von elektronischen Geschäftsprozessen zwischen ihr und den Teilnehmern der Community.

Der Community Manager kann auch als Community Operator fungieren.

Teilnehmer

Die Teilnehmer werden durch die Firmen dargestellt, die mit dem Community Manager über die Hub-Community im Geschäftsverkehr stehen. Die Teilnehmer müssen einen Konfigurationsprozess ausführen, um sich an die Hub-Community anzuschließen. Sobald die Teilnehmer verbunden sind, können sie mit dem Community Manager elektronische Geschäftsdokumente austauschen.

Symbole der Community Console

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

Tabelle 1. Symbole der Community Console

Symbol	Symbolname
	Es wurde ein TPA (Trade Participant Agreement) geschlossen
	Ausblenden
	Kopieren
	Rolle erstellen (Rolle ist nicht aktiv)
	Daten enthalten
	Inaktivieren
	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
	Gateway inaktiviert
	Suchkriterien ausblenden
	Modifizieren
	Keine Daten enthalten
	Kalender öffnen
	Anhalten

Tabelle 1. Symbole der Community Console (Forts.)

Symbol	Symbolname
	Drucken
	Eingabe erforderlich
	Starten
	Synchroner Datenfluss (es wird kein Symbol für asynchrone Transaktionen 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 Ereigniscodes und der Ereignisposition suchen. Der Hubadministrator kann außerdem anhand des Teilnehmers, 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, welches 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 Community-Teilnehmer ausführen muss, um WebSphere Partner Gateway für die Benutzer und die Umgebung des Teilnehmers 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. „Bei Community Console anmelden"
2. „Teilnehmerprofil prüfen" auf Seite 6
3. „Gateway erstellen" auf Seite 7
4. „B2B-Funktionalitäten prüfen" auf Seite 7
5. „Digitale Zertifikate hochladen" auf Seite 9
6. „Konsolgruppen erstellen" auf Seite 14
7. „Benutzer erstellen" auf Seite 14
8. „Kontaktinformationen erstellen" auf Seite 16
9. „Alerts erstellen und Kontakte hinzufügen" auf Seite 17
10. „Neue Adresse erstellen" auf Seite 24

Bei 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 eingeschaltet 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 den folgenden URL ein:

   http://<*hostname*>.<*domain*>:58080/console (unsecure)

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

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

   Anmerkung: Dieser 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 Community Operator den Benutzernamen, das Anfangskennwort und den Anmeldenamen des Unternehmens für die Anmeldung bei der Community Console. Sie benötigen diese Informationen für die folgende Prozedur. Sollten Sie diese Informationen nicht erhalten haben, wenden Sie sich an den zuständigen Community Operator.

Gehen Sie wie folgt vor, um sich bei der Community Console anzumelden (diese Anweisungen gelten sowohl für den Community Manager als auch für die Teilnehmer):

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.

Teilnehmerprofil prüfen

Verwenden Sie die Funktion **Kontenadmin-Teilnehmer** zum Anzeigen und Bearbeiten der Informationen, mit denen sich Ihr Unternehmen beim System identifiziert.

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

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.

Teilnehmerprofil anzeigen und bearbeiten

1. Klicken Sie auf **Kontenadmin** > **Profile** > **Community Teilnehmer**.
2. Klicken Sie auf das Symbol zum Bearbeiten. Das System ruft die Anzeige **Teilnehmerdetails** 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 Teilnehmeranzeigen

Wert	Beschreibung
Anmeldename des Unternehmens	Identifiziert den Teilnehmer beim System. Der Name kann maximal 15 Zeichen lang sein. Folgende Sonderzeichen dürfen nicht enthalten sein: ! # ; : \ / & ?. Dieser Wert kann nicht vom Teilnehmer geändert werden.
Anzeigename des Teilnehmers	Der Name des Teilnehmers, der für die Hub-Community angezeigt werden soll. Der Name kann maximal 30 Zeichen lang sein.
Teilnehmertyp	Teilnehmertyp - Community-Teilnehmer oder Community Manager. Dieser Wert kann vom Teilnehmer geändert werden.
Status	**Aktiviert** oder **Inaktiviert**. Bei inaktiviertem Status ist der Teilnehmer in Suchkriterien und Dropdown-Listen nicht sichtbar.
Lieferantentyp	Gibt die Rolle des Teilnehmers an, z. B. Vertragshersteller oder Distributor.
Website	Gibt die Website des Teilnehmers 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.
IP-Adresse oder Hostname	• Gatewaytyp, z. B. CPS-Teilnehmer. • IP-Adresse oder Hostname des Teilnehmers.

4. Klicken Sie auf **Speichern**.

Gateway erstellen

Sie müssen ein Standardgateway erstellen und pflegen. Andernfalls können Sie keine Verbindungen herstellen. Weitere Informationen zur Erstellung von Gateways finden Sie in Kapitel 3, „Gateways erstellen", auf Seite 25.

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 Dokumentenflussdefinitionen festgelegt. Eine Dokumentenflussdefinition 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 Dokumentenflussdefinitionen:

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

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

Dokumentenfluss. Gibt den Geschäftsprozess an, der zwischen dem Community Manager und seinen Teilnehmern verarbeitet wird.

Aktivität. Die Geschäftsfunktion, die der Prozess ausführt.

Aktion. Die einzelnen Dokumente, die einen vollständigen Geschäftsprozess bilden. Die Dokumente werden zwischen dem Community Manager und dem Teilnehmer verarbeitet.

Jede Dokumentenflussdefinition beinhaltet Attribute (d. h. Informationen), die die Funktionalität der Definition festlegen. Ein Attribut besteht aus einer Einzelinformation, die einem bestimmten Dokumentenfluss 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" erscheint, 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 Dokumentenflusskontextes fest. In einem Zweiwege-PIP sind **Quelle festlegen** und **Ziel festlegen** für alle Aktionen gleich, unabhängig von der Tatsache, dass die Anforderung von einem Teilnehmer 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 Dokumentenflussdefinition einer niedrigeren Ebene fest.
4. Klicken Sie auf das Bearbeitungssymbol zum Anzeigen und (falls erforderlich) Ändern der Dokumentenflussdefinitionen auf der unteren Ebene (z. B. Protokoll oder Dokumentenfluss). Sie können auch die Attribute einer Dokumenten-

flussdefinition 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.

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

WebSphere Partner Gateway verwendet digitale Zertifikate, um die Authentizität von Geschäftsdokumenttransaktionen zwischen dem Community Manager und den Teilnehmern 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 Unterschrift** oder **SSL-Clientzertifikat** festgelegt werden.

Im Teilnehmerprofil 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 Unterschrift und die Verschlüsselung, muss es zweimal geladen werden. Hierbei wird ein Ladevorgang für die digitale Unterschrift und der andere für das Verschlüsselungszertifikat ausgeführt. Wird das Zertifikat allerdings für digitale Unterschriften und für den SSL-Client verwendet, können die entsprechenden Markierungsfelder jedoch im selben Zertifikatseintrag definiert werden.

Derartige Zertifikate können auch zweimal geladen werden, wobei ein Ladevorgang für die digitale Unterschrift 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 Unterschriften 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 Zertifikatkette hochladen. Wenn z. B. die Zertifikatkette die Zertifikate A -> B -> C -> D enthält, in der A -> B bedeutet, dass A der Aussteller von B ist, sollten die Zertifikate A, B, und C als Root-Zertifikate hochgeladen werden. Wenn eines der Zertifikate nicht verfügbar ist, wird der CertPath nicht erstellt und die Transaktion schlägt fehl. Die CA-Zertifikate können aus Zertifikatrepositories angefordert werden, die von den Zertifizierungsstellen oder von dem Partner verwaltet werden, die das Zertifikat zur Verfügung gestellt haben. 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 *Hub-Konfiguration*.

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 17. 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 Unterschrift einer anerkannten juristischen Person (der Zertifizierungsstelle), mit der die Gültigkeit des Zertifikats bestätigt wird.

Digitale Unterschrift. Ein mit einem privaten Schlüssel erstellter digitaler Code. Mit Hilfe von digitalen Unterschriften können Mitglieder der Hub-Community Übertragungen durch die Prüfung der Unterschrift authentifizieren. Wenn Sie eine Datei mit einer Unterschrift 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 Unterschrift 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 leserlich 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 Unterschriften 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 unterzeichnet und entschlüsselt. Nur Sie verfügen über den Zugriff auf Ihren privaten Schlüssel. Mit dem privaten Schlüssel wird außerdem eine eindeutige digitale Unterschrift 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 Unterschriften 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 unterzeichneter Schlüssel. Ein öffentlicher Schlüssel, der zum Beweis des Eigentumsrechts durch den zugehörigen privaten Schlüssel unterzeichnet 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 Unterschrift 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 (Teilnehmer und Community Manager)**. 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 unterzeichnet werden. Wenn das Zertifikat in einer Testumgebung verwendet wird, kann es selbst unterzeichnet 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 Teilnehmern ausgetauscht werden.
- **Verschlüsselungszertifikat (Teilnehmer und Community Manager)**. 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 Teilnehmerzertifikats über die Community Console in WebSphere Partner Gateway hochladen und eine Kopie des Zertifikats an den Hub-Operator senden.
- **Zertifikat für digitale Unterschrift (Teilnehmer und Community Manager)**. Sofern Mitglieder der Hub-Community die Dokumente unterzeichnen, muss der öffentliche Abschnitt des Signaturzertifikats auf der Teilnehmerebene als Signaturzertifikat in den Hub hochgeladen werden. Muss der Hub-Manager die Dokumente unterzeichnen, 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 (Community Manager)**. Dieses Zertifikat wird von der Dokumentverwaltung von WebSphere Partner Gateway für die Funktion **Community Participant Simulator** verwendet. Das Zertifikat wird in das Dateisystem kopiert und nicht über die Community Console hochgeladen.

  In das Dateisystem kopierte VTP-Zertifikate sind für alle Teilnehmer aktiv, die über die Community Console erstellt werden. Diese Zertifikate prüfen unterzeichnete Dokumente, die vom Community Participant Simulator 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 unterzeichnetes Zertifikat handelt, müssen die Teilnehmer über eine Kopie dieses Zertifikats verfügen.
- Stammt das Zertifikat des Web-Servers der Hub-Community von einer Zertifizierungsstelle, müssen die Teilnehmer 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 unterzeichnetes Zertifikat handelt, müssen die Teilnehmer über eine Kopie dieses Zertifikats verfügen.
- Stammt das Zertifikat des Web-Servers der Hub-Community von einer Zertifizierungsstelle, müssen die Teilnehmer über eine Kopie des CA-Root- und CA-Intermediate-Zertifikats verfügen.
- Der Zielserver muss über eine Kopie des Teilnehmerzertifikats verfügen, falls dieses selbst unterzeichnet 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.

Digitales Zertifikat laden und definieren

1. Klicken Sie auf **Kontenadmin** > **Profile** > **Zertifikate**. Das System ruft die Anzeige **Zertifikatliste** auf.
2. Klicken Sie in der oberen rechten Ecke der Anzeige auf **Zertifikat laden**. Das System ruft die Anzeige **Neues Zertifikat erstellen** auf.
3. Wählen Sie den **Zertifikatstyp** aus: Prüfung der digitalen Unterschrift, Verschlüsselung oder SSL-Client. Sie können mehrere digitale Unterschriften und SSL-Zertifikate hochladen. Es kann jedoch nur ein Verschlüsselungszertifikat hochgeladen werden.
   - **Zertifikat für digitale Unterschriften**. Wenn Sie digital unterzeichnen oder digital unterzeichnete Dokumente prüfen, benötigen Sie ein Zertifikat für digitale Unterschriften.
   - **Verschlüsselungszertifikat**. Wenn Mitglieder der Hub-Community Dateien verschlüsseln, benötigen Sie ein Zertifikat für die Verschlüsselung und Entschlüsselung.
   - **SSL-Clientzertifikat**. Ein Transportzertifikat. Wenn Sie für den ausgehenden Transport HTTPS verwenden, benötigen Sie ein SSL-Clientzertifikat.
4. Geben Sie im Feld **Beschreibung** einen eindeutigen Namen für das Zertifikat im Textfeld **Zertifikat** ein.
5. Wählen Sie **Aktiviert** oder **Inaktiviert** aus.
6. Klicken Sie auf **Durchsuchen**, und navigieren Sie zu dem digitalen Zertifikat.
7. Wählen Sie den **Gateway-Typ** aus, z. B. CPS-Teilnehmer (nur für SSL-Zertifikate). Mit dieser Funktion können Sie ein Zertifikat basierend auf der Zieladresse auswählen.
8. Wählen Sie den Typ der **Zertifikatverwendung** aus:
   - Primär — wird für alle Transaktionen verwendet.
   - Sekundär — wird verwendet, wenn das primäre Zertifikat abgelaufen ist oder widerrufen wurde.
9. Klicken Sie auf **Hochladen**.

Konsolgruppen erstellen

Verwenden Sie die Funktion **Gruppe**, um eine Gruppe für einen bestimmten Benutzertyp mit spezifischen 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, für die die Benutzer aus der Gruppe während des Testlaufs Zugriff haben müssen.

Das System erstellt automatisch die Gruppen **Administrator** und **Standard** mit standardmäßigen Berechtigungseinstellungen. Die Standardeinstellungen für Berechtigungen können vom Hubadministrator oder vom Community-Teilnehmer überschrieben werden.

Achtung: Administrator- und Standardgruppen werden vom System generiert und können nicht bearbeitet oder gelöscht werden. Der Community Operator 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 zum Erstellen von Benutzerprofilen. Das System verwendet Benutzerprofile 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**).

- Ist der Anmeldestatus eines Benutzers **Aktiviert**, kann er sich bei der Community Console anmelden. Ist der Anmeldestatus eines Benutzers **Inaktiviert**, ist eine Anmeldung bei 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 den Benutzernamen (Anmeldenamen für den Benutzer) ein.
4. Wählen Sie aus, ob Sie den Konsolzugriff für diesen Benutzer aktivieren oder inaktivieren möchten.
5. Geben Sie den Namen des Benutzers ein (Vorname und Nachname).
6. Geben Sie die E-Mail-Adresse ein, die das System zum Senden von Alertbenachrichtigungen an den Benutzer verwenden soll.
7. Geben Sie die Telefonnummer und Faxnummer des Benutzers ein.
8. Wählen Sie 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.
9. Wählen Sie aus, ob der Benutzer nur für Ihr Unternehmen sichtbar sein soll (**Lokal**) oder für die gesamte Hub-Community (**Global**).
10. 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.
11. Klicken Sie auf **Speichern**. Wiederholen Sie diese Schritte, um zusätzliche Benutzer hinzuzufügen.

Benutzer zu 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 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 Community Manager die üblichen Grenzen, sollte der Netzwerkadministrator benachrichtigt werden, um sicherzustellen, dass das System die erhöhte Übertragungsrate effizient bearbeitet.

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 Namen des Kontakts im Namensfeld ein.
4. Geben Sie die Adresse des Kontakts im Adressfeld ein.
5. Wählen Sie den Kontakttyp aus der Dropdown-Liste aus (z. B. B2B-Leiter oder Geschäftsleiter).
6. Geben Sie die E-Mail-Adresse des Kontakts ein.
7. Geben Sie die Telefonnummer und Faxnummer des Kontakts ein.
8. Wählen Sie den Alertstatus des Kontakts aus. Bei Aktivierung empfängt dieser Kontakt alle subskribierten Alerts.
9. Der Wert für die Subskribierung wird vom System ausgefüllt.
10. Wählen Sie die Sichtbarkeitsstufe für den Kontakt aus. Wenn Sie **Lokal** auswählen, ist der Kontakt nur für Ihr Unternehmen sichtbar. Wenn Sie **Global** auswählen, ist der Kontakt für den Community Operator und den Community Manager sichtbar. Sowohl der Community Operator als auch der Community Manager 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 23.

    Informationen zur Erstellung eines volumenbasierten Alerts und zum Hinzufügen von Kontakten zu dem Alert finden Sie im Abschnitt „Volumenbasierten Alert erstellen" auf Seite 18.

    Informationen zur Erstellung eines ereignisbasierten Alerts und zum Hinzufügen von Kontakten zu dem Alert finden Sie im Abschnitt „Ereignisbasierten Alert erstellen" auf Seite 21.

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 (ereignisbasierter Alert) oder auf dem erwarteten Dokumentenflussvolumen (volumenbasierter Alert).

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

  Wenn Sie z. B. ein Teilnehmer sind, können Sie einen volumenbasierten Alert erstellen, der Sie benachrichtigt, wenn Sie keine Übertragungen vom Community Manager an einem beliebigen Werktag 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 Community Managers hervorgehoben werden.

  Wenn Sie Teilnehmer sind, können Sie auch einen volumenbasierten Alert erstellen, der Sie warnt, wenn die Anzahl der Übertragungen vom Community Manager die normale Rate überschreitet. Wenn Sie z. B. normalerweise ungefähr 1000 Übertragungen pro Tag empfangen, können Sie das erwartete Volumen auf 1000 und die 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 Community Managers ermittelt werden, sodass Sie langfristig unter Umständen mehr Server zu Ihrer Umgebung hinzufügen müssen.

  Beachten Sie, dass die Überwachung des Volumens durch volumenbasierte Alerts auf der Grundlage des Dokumentenflusses erfolgt, den Sie beim Erstellen des Alerts auswählen. WebSphere Partner Gateway beachtet nur Dokumente, die den in Ihrem Alert ausgewählten Dokumentenfluss beinhalten und generiert nur dann Alerts, wenn alle Kriterien für einen Alert erfüllt sind.
- Verwenden Sie einen ereignisbasierten 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 ereignisbasierten 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 Community-Teilnehmer kann lediglich einen volumenbasierten Alert erstellen, der auf dem an den Community Manager gesendeten Dokumentvolumen basiert. Will der Teilnehmer einen volumenbasierten Alert auf der Grundlage des vom Community Manager an den Teilnehmer gesendeten Dokumentvolumens erstellen, muss der Teilnehmer beim Community Operator das Einrichten eines volumenbasierten Alerts anfordern, wobei der Teilnehmer als Alerteigner angegeben wird.

Tipp:

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

Volumenbasierten 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 als Alerttyp **Volumenalert** aus (dies ist die Standardeinstellung). Das System zeigt die entsprechenden Textfenster für einen Volumenalert an.
4. Geben Sie in dem Textfenster einen Namen für den Alert ein.
5. Wählen Sie einen Teilnehmer mit der Berechtigung zum Erstellen eines volumenbasierten Alerts aus (Community Manager oder Community Operator).
6. Wählen Sie aus den Dropdown-Listen **Paket**, **Protokoll** und **Dokumentenfluss** aus.

   Die Auswahl für Paket, Protokoll und Dokumentenfluss muss mit der Auswahl für Paket, Protokoll und Dokumentenfluss des Teilnehmers 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 19 fort:
   - **Erwartet** - Wählen Sie diese Option aus, wenn die Generierung eines Alerts beim Abweichen des Dokumentenflussvolumens von einer exakten Menge erfolgen soll. Führen Sie folgende Schritte aus, um einen Alert für das erwartete Dokumentenflussvolumen zu erstellen:

a. Geben Sie im Textfenster **Volumen** die Anzahl der erwarteten, innerhalb eines in 8 ausgewählten Zeitrahmens zu empfangenden Dokumentenflüsse ein. Geben Sie eine positive Zahl ein. Der Alert funktioniert nicht, wenn hier eine negative Zahl eingegeben wird.

b. Geben Sie im Textfenster **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 durch ein Dokumentenflussvolumen kleiner als 18 oder größer als 22 ausgelöst.

   – Ist das Volumen = 20 und die Abweichung (%) = 0, wird ein Alert durch ein beliebiges Dokumentenflussvolumen ungleich 20 ausgelöst.

- **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 Textfenster **Min** die Mindestanzahl der erwarteten, innerhalb eines in 8 ausgewählten Zeitrahmens zu empfangenden Dokumentenflüsse ein. Ein Alert wird nur dann ausgelöst, wenn das Dokumentenflussvolumen unter diesen Wert sinkt.

  b. Geben Sie im Textfenster **Max** die maximale Anzahl der erwarteten, innerhalb eines in 8 ausgewählten Zeitrahmens zu empfangenden Dokumentenflüsse ein.

  Anmerkung: In beide Textfenster, **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 Dokumentenflüsse innerhalb eines in 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 den Status des 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 Teilnehmer aus (nur Community Manager oder Community Operator).
16. Wenn der hinzuzufügende Kontakt im Textfenster der Kontakte aufgelistet ist, wählen Sie ihn aus, und klicken Sie auf **Subskribieren**. Gehen Sie zu 21.

    Wenn der hinzuzufügende Kontakt nicht im Textfenster 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 Alertteilnehmer 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 Community Operator und Community Manager sichtbar zu machen. Sowohl der Community Operator als auch der Community Manager 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 volumenbasierten 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.

Ereignisbasierten 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 als Alerttyp **Ereignisalert** aus. Das System zeigt die entsprechenden Textfenster für einen ereignisbasierten Alert an.
4. Geben Sie in dem Textfenster einen Namen für den Alert ein.
5. Wählen Sie einen Teilnehmer aus, der den Alert auslösen soll (diese Option ist nur für den Community Manager und den Community Operator verfügbar).

   Wählen Sie die Option **Alle Teilnehmer** aus, um den Alert allen Teilnehmern im System zuzuordnen. Wenn Sie eine Alertsuche ausführen und als Alertteilnehmer **Alle Teilnehmer** auswählen, zeigt das System alle Alerts an, die keinem spezifischen Teilnehmer zugeordnet sind.
6. Wählen Sie den Ereignistyp aus: **Debugging**, **Information**, **Warnung**, **Fehler**, **Kritisch** oder **Alle**.
7. 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
8. Wählen Sie den Status des Alerts aus: **Aktiviert** oder **Inaktiviert**.
9. Klicken Sie auf **Speichern**.
10. Klicken Sie auf die Registerkarte **Benachrichtigen**.
11. Klicken Sie auf das Symbol zum Bearbeiten.
12. Wählen Sie einen Teilnehmer aus (nur Community Manager oder Community Operator).
13. Wenn der hinzuzufügende Kontakt im Textfenster der Kontakte aufgelistet ist, wählen Sie ihn aus, und klicken Sie auf **Subskribieren**. Gehen Sie zu 18.

    Wenn der hinzuzufügende Kontakt nicht im Textfenster 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 Alertteilnehmer durch den Alerteigner hinzugefügt werden.
14. Geben Sie die E-Mail-Adresse, Telefonnummer und Faxnummer des Kontakts ein.
15. 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.
16. 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 Community Operator und Community Manager sichtbar zu machen. Sowohl der Community Operator als auch der Community Manager kann den Kontakt für Alerts subskribieren.

17. 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.
18. 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.
19. 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 Teilnehmer aus (nur Community Manager oder Community Operator).
8. Wenn der hinzuzufügende Kontakt im Textfenster der Kontakte aufgelistet ist, wählen Sie ihn aus, und klicken Sie auf **Subskribieren**. Gehen Sie zu 13.

   Wenn der hinzuzufügende Kontakt nicht im Textfenster 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 Alertteilnehmer durch den Alerteigner 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 Community Operator und Community Manager sichtbar zu machen. Sowohl der Community Operator als auch der Community Manager 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 Teilnehmerprofil 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 Textfenster ein.
5. Klicken Sie auf **Speichern**.

Kapitel 3. Gateways erstellen

Gateways dienen zur Definition von Eingangspunkten in das System. Im vorliegenden Kapitel werden die Arbeitsschritte zum Erstellen von Gateways erläutert und die folgenden Themen behandelt:

Übersicht

WebSphere Partner Gateway verwendet Gateways zum Weiterleiten (Routing) von Dokumenten an die jeweilige Zieladresse. Der Empfänger kann hierbei ein Community-Teilnehmer oder der Community Manager sein. Das Transportprotokoll für abgehende Dokumente legt fest, welche Informationen während der Gatewaykonfiguration verwendet werden.

Bei Teilnehmergateways werden standardmäßig die folgenden Transportprotokolle unterstützt:

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

  Anmerkung: Für Teilnehmer (nicht jedoch für den Community Manager) kann ein SMTP-Gateway definiert werden.
- Dateiverzeichnis
- FTP-Scripting

Sie können auch ein benutzerdefiniertes Transportprotokoll angeben, das im Rahmen der Gatewayerstellung hochgeladen wird.

HTTP-Gateway einrichten

Sie können ein HTTP-Gateway einrichten, um Dokumente vom Hub an die IP-Adresse Ihres Teilnehmers zu senden. Beim Einrichten eines HTTP-Gateways können Sie außerdem angeben, dass die zu verarbeitenden Dokumente über einen konfigurierten Proxy-Server gesendet werden sollen.

Gehen Sie wie folgt vor, um die Erstellung eines HTTP-Gateways zu starten:

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

Gateway-Details

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

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

Gatewaykonfiguration

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

1. Wählen Sie in der Liste **Transport** den Eintrag für **HTTP/1.1** 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: http://*<server name>*:*<optional port>*/*<path>*

   Beispiel:

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

   Wenn Sie ein Gateway für einen Web-Service einrichten, müssen Sie den privaten URL angeben, der vom Web-Service-Provider bereitgestellt wurde. Dieser 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.
3. Geben Sie optional einen Benutzernamen und ein Kennwort ein, wenn diese Angaben für den Zugriff auf den HTTP-Server erforderlich sind.
4. Geben Sie im Feld **Wiederholungszähler** ein, wie oft das Gateway 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 Gateway 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 Gateway (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 Gateway manuell wieder in den Onlinemodus versetzt wird.
9. Geben Sie im Feld **Verbindungszeitlimit** die Zeitdauer in Sekunden ein, die ein Socket ohne Datenverkehr geöffnet bleiben soll. Der Standardwert ist 120 Sekunden.
10. Wenn Sie den Vorbereitungs- oder Nachbereitungsschritt für das Gateway konfigurieren wollen, sollten Sie die Informationen im Abschnitt „Handler konfigurieren" auf Seite 38 lesen. Klicken Sie andernfalls auf **Speichern**.

HTTPS-Gateway einrichten

Sie können ein HTTPS-Gateway einrichten, um Dokumente vom Hub an die IP-Adresse Ihres Teilnehmers zu senden. Beim Einrichten eines HTTPS-Gateways 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-Gateway zu erstellen:

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

Gateway-Details

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

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

Gatewaykonfiguration

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

1. Wählen Sie in der Liste **Transport** den Eintrag für **HTTPS/1.0** oder **HTTPS/1.1** 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: 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 Gateway 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 Gateway 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 Gateway (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 Gateway 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 Gateway konfigurieren wollen, sollten Sie die Informationen im Abschnitt „Handler konfigurieren” auf Seite 38 lesen. Klicken Sie andernfalls auf **Speichern**.

FTP-Gateway einrichten

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

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

Gateway-Details

Führen Sie auf der Seite **Gateway-Details** die folgenden Arbeitsschritte aus:

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

Gatewaykonfiguration

Führen Sie im Abschnitt **Gatewaykonfiguration** 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 Gateway 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 Gateway 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 Gateway (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 Gateway 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 Markierungsfeldes unter **Eindeutigen Dateinamen verwenden** bei, wenn dies sinnvoll ist. Andernfalls können Sie die Auswahl zurücknehmen, indem Sie auf das Markierungsfeld 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 Gateway konfigurieren wollen, sollten Sie die Informationen im Abschnitt „Handler konfigurieren” auf Seite 38 lesen. Klicken Sie andernfalls auf **Speichern**.

SMTP-Gateway einrichten

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

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

Gateway-Details

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

1. Geben Sie den Namen des Gateways ein. Dieses Feld muss ausgefüllt werden.

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

Gatewaykonfiguration

Führen Sie im Abschnitt **Gatewaykonfiguration** 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 Gateway 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 Gateway 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 Gateway (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 Gateway 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 Gateway konfigurieren wollen, sollten Sie die Informationen im Abschnitt „Handler konfigurieren” auf Seite 38 lesen. Klicken Sie andernfalls auf **Speichern**.

JMS-Gateway einrichten

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

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

Gateway-Details

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

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

Gatewaykonfiguration

Führen Sie im Abschnitt **Gatewaykonfiguration** 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 die angegebene Zieladresse weitergeleitet werden soll. Dieses Feld muss ausgefüllt werden.
3. Geben Sie optional einen 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 Gateway 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 Gateway 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 Gateway (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 Gateway 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 des 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 Gateway konfigurieren wollen, sollten Sie die Informationen im Abschnitt „Handler konfigurieren" auf Seite 38 lesen. Klicken Sie andernfalls auf **Speichern**.

Dateiverzeichnis-Gateway einrichten

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

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

Gateway-Details

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

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

Gatewaykonfiguration

Führen Sie im Abschnitt **Gatewaykonfiguration** 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 Gateway 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 Gateway 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 Gateway (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 Gateway manuell wieder in den Onlinemodus versetzt wird.
8. Behalten Sie die Auswahl des Markierungsfeldes unter **Eindeutigen Dateinamen verwenden** bei, wenn dies sinnvoll ist. Andernfalls können Sie die Auswahl zurücknehmen, indem Sie auf das Markierungsfeld 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 Gateway konfigurieren wollen, sollten Sie die Informationen im Abschnitt „Handler konfigurieren″ auf Seite 38 lesen. Klicken Sie andernfalls auf **Speichern**.

FTPS-Gateway einrichten

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

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

Gateway-Details

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

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

Gatewaykonfiguration

Führen Sie im Abschnitt **Gatewaykonfiguration** 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 Gateway 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 Gateway 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 Gateway (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 Gateway 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 Markierungsfeldes unter **Eindeutigen Dateinamen verwenden** bei, wenn dies sinnvoll ist. Andernfalls können Sie die Auswahl zurücknehmen, indem Sie auf das Markierungsfeld 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 Gateway konfigurieren wollen, sollten Sie die Informationen im Abschnitt „Handler konfigurieren” auf Seite 38 lesen. Klicken Sie andernfalls auf **Speichern**.

FTP-Scripting-Gateway einrichten

Ein FTP-Scripting-Gateway wird nach einem von Ihnen definierten Zeitplan ausgeführt. Die Funktionsweise eines FTP-Scripting-Gateways wird über ein FTP-Befehlsscript gesteuert.

FTP-Script erstellen

Zur Verwendung eines FTP-Scripting-Gateways müssen Sie eine Datei erstellen, die alle erforderlichen FTP-Befehle enthält, die vom FTP-Server akzeptiert werden.

1. Erstellen Sie ein Script für die Gateways, 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 %BCGOPTIONNx%
   mput *
   quit
   ```

   Beim Aktivieren des Gateways werden die Platzhalterzeichen (z. B. %BCGSERVERIP%) durch die Werte ersetzt, die Sie beim Erstellen einer bestimmten Instanz eines FTP-Scripting-Gateways eingeben. Die entsprechenden Angaben sind in der folgenden Tabelle aufgeführt:

Tabelle 3. Zuordnung zwischen Scriptparametern und Feldeinträgen des FTP-Scripting-Gateways

Scriptparameter	Feldeintrag des FTP-Scripting-Gateways
%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-Gateways

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

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

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

Gateway-Details

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

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

Gatewaykonfiguration

Führen Sie im Abschnitt **Gatewaykonfiguration** 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 Gateway 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 Gateway 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 Gateway eine Sperre anfordern soll, so dass keine andere Instanz eines FTP-Scripting-Gateways 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 Gateways 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 Gateway 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 Gateway konfigurieren wollen, sollten Sie die Informationen im Abschnitt „Handler konfigurieren" lesen. Klicken Sie andernfalls auf **Speichern**.

Handler konfigurieren

Für ein Gateway 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 *Hub-Konfiguration*. 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**.

Standardgateway angeben

Nach der Erstellung der erforderlichen Gateways für den Community Manager oder Teilnehmer müssen Sie einen der Gateways als Standardgateway festlegen.

1. Klicken Sie auf **Kontenadmin > Profile > Gateways**.
2. Klicken Sie auf **Erstellen**.
3. Klicken Sie auf **Standardgateways anzeigen**.

   Daraufhin wird eine Liste mit den für den Teilnehmer definierten Gateways angezeigt.
4. Wählen Sie in der Liste **Produktion** das Gateway aus, das als Standardeinheit für den aktuellen Teilnehmer definiert werden soll. Sie können auch Standardgateways für andere Gatewaytypen (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 ″Teilnehmerverbindung nicht gefunden″, ″RosettaNet-Gültigkeitsfehler″ und ″Dokumentzustellung fehlgeschlagen″.

Sie verwenden dieses Modul außerdem zum Pflegen Ihres Teilnehmerprofils sowie zum Verwalten von Zertifikaten, Gateways, 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

Welche Funktion möchten Sie verwenden?
„Gateways verwalten″
„Zertifikate verwalten″ auf Seite 42
„Gruppen verwalten″ auf Seite 43
„Benutzer verwalten″ auf Seite 44
„Kontakte verwalten″ auf Seite 46
„Alerts verwalten″ auf Seite 47
„Adressen verwalten″ auf Seite 49

Gateways verwalten

Verwenden Sie die Funktion **Gateways** zum Anzeigen von Gateway-Informationen, mit denen Dokumente an ihre ordnungsgemäße Zieladresse weitergeleitet werden. Mit dieser Funktion können Sie den Ziel-URI, das Transportprotokoll und den Gatewaystatus anzeigen.

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

Liste der Gateways anzeigen

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

Details zu Gateways anzeigen oder bearbeiten

Wichtig: Wenn Sie ein Gateway inaktivieren, wird damit auch die Teilnehmerverbindung inaktiviert, die dem Gateway zugeordnet ist. Das Gateway

funktioniert dann nicht. Wenn Sie das Gateway offline setzen, werden die Dokumente in einer Warteschlange gehalten, bis das Gateway wieder online gesetzt wird.

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

Tabelle 5. Werte in der Gateway-Anzeige

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

5. Klicken Sie auf **Speichern**.

Standardgateways anzeigen, auswählen oder bearbeiten

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

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.

Gruppenzugehörigkeiten anzeigen und Benutzer zu 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 die Schaltfläche **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

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 Community Operator 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 Benutzerprofile anzeigen und bearbeiten.

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 verwendete E-Mail-Adresse für Alertbenachrichtigungen.
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 verwendete E-Mail-Adresse für Alertbenachrichtigungen.
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 (Univer- 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**.

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 Kontakte für Sicherheit zur Auswertung des Problems benachrichtigt werden. Überschreiten die Übertragungen des Community Managers die üblichen Grenzen, sollte der Netzwerkadministrator benachrichtigt werden, um sicherzustellen, dass das System die erhöhte Übertragungsrate effizient bearbeitet.

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 verwendete E-Mail-Adresse für Alertbenachrichtigungen.
Sichtbarkeit	• Lokal - Der Kontakt ist nur für Ihr Unternehmen sichtbar. • Global - Der Kontakt ist für den Community Operator und den Community Manager sichtbar. Sowohl der Community Operator als auch der Community Manager 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 Community Operator und den Community Manager sichtbar. Sowohl der Community Operator als auch der Community Manager 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 über 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 Community Manager kann alle Alerts anzeigen, unabhängig vom Alerteigner (dem Ersteller des Alerts).

1. Klicken Sie auf **Kontenadmin** > **Alerts**. Das System ruft die Anzeige **Alertsuche** auf.
2. Wählen Sie die Suchkriterien aus 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 Teilnehmer aus (nur Community Manager oder Community Operator). Der Community Manager kann alle Alerts anzeigen, unabhängig vom Alerteigner.
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 aus 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 Teilnehmer

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 Community Manager und Community Operator

Wert	Beschreibung
Alerteigner	Der Ersteller des Alerts.
Alertteilnehmer	Der Teilnehmer, 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 aus 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 Community Operator 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 aus 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 Community Operator und der Alerteigner (der Ersteller des Alerts) können den Alert entfernen.

Adressen verwalten

Mit dieser Funktion können Sie die Adressen in Ihrem Teilnehmerprofil 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"
- „AS1/AS2-Anzeige" auf Seite 54
- „RosettaNet-Anzeige" auf Seite 56
- „Dokumentanzeige" auf Seite 58
- „Gateway-Warteschlange" auf Seite 62

Die RosettaNet- und die AS1/AS2-Anzeige umfassen zusätzliche Suchkriterien für den Hubadministrator. Weitere Informationen hierzu finden Sie im Handbuch *Verwaltung*.

Anmerkung: Der Terminus "Teilnehmer" wird in den Anzeigen verwendet, um Mitglieder der Hub-Community einschließlich des Community Managers zu identifizieren.

Ereignisanzeige

Mit Hilfe der Ereignisanzeige können Sie Ereignisse anhand der Zeit, des Datums, des Ereignistyps, des Ereigniscodes und der Ereignisposition suchen. Der Hubadministrator kann außerdem anhand des Teilnehmers, der Quellen-IP und der Ereignis-ID suchen.

Die von der Ereignisanzeige generierten Daten identifizieren u. a. den Ereigniscode, 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 Teilnehmer erfolgreich zum System hinzugefügt wurde oder eine Teilnehmerverbindung erfolgreich zwischen dem Community Manager und einem Teilnehmer 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 Business Integration Connect beinhaltet vordefinierte Ereignisse. Verwenden Sie die Alertfunktion des Produkts (Modul **Kontenadmin**) zum Erstellen von ereignisbasierten 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 spezifischen 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 Ereigniscodes (z. B. 210031) und der Ereignisposition suchen.

Die über die Ereignisanzeige verfügbaren Daten umfassen den Ereignisnamen, die Zeitmarke, den Benutzer und die Teilnehmerinformationen. 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 Business Integration Connect 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 52
Ereignisdetails anzeigen	Seite 53

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 unkritischste 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 aus 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.
Teilnehmer	Wählen Sie alle Teilnehmer oder einen bestimmten Teilnehmer aus (nur Community Manager).
Ereignistyp	Ereignistyp: **Debugging**, **Information**, **Warnung**, **Fehler** oder **Kritisch**.
Ereigniscode	Suchen Sie basierend auf dem ausgewählten Ereignistyp nach verfügbaren Ereigniscodes.
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 die Häufigkeit der Suchergebnisaktualisierung (nur Community Manager).

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 aus 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.

AS1/AS2-Anzeige

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

Die AS1/AS2-Anzeige kann außerdem zum Anzeigen von gepackten B2B-Transaktionen und B2B-Prozessdetails verwendet werden, die das Übertragungsprotokoll AS1 oder AS2 (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. Ein weiterer Vorteil von AS2 ist die Bereitstellung eines Maßes an Sicherheit, das FTP nicht zur Verfügung stellt. AS2 bietet eine Verschlüsselungsbasis mit garantierter Zustellung.

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 AS1/AS2-Anzeige die Nachrichten-ID, die Zeitmarken, den Dokumentenfluss, den Gatewaytyp, den Synchronstatus und die Dokumentdetails anzeigen. Beim Anzeigen der Dokumentdetails werden zusätzliche Dokumentverarbeitungsinformationen dargestellt.

Tasks der AS1/AS2-Anzeige ausführen

Tabelle 17. Tasks der AS1/AS2-Anzeige

Was möchten Sie tun?	Siehe
Nachrichten suchen	Seite 57
Unformatierte Dokumente anzeigen	Seite 58

Nachrichten suchen

1. Klicken Sie auf **Anzeigen** > **AS1/AS2-Anzeige**. Das System zeigt die AS1/AS2-Anzeige an.
2. Wählen Sie die Suchkriterien aus den Dropdown-Listen aus.

Tabelle 18. Suchkriterien der AS1/AS2-Anzeige

Wert	Beschreibung
Startdatum und -zeit	Datum und Uhrzeit der Prozesseinleitung.
Enddatum und -zeit	Datum und Uhrzeit der Fertigstellung des Prozesses.
Teilnehmer	Gibt den Teilnehmer an (nur Community Manager).
Meine Rolle ist der	Gibt an, ob der Teilnehmer die Quelle (einleitender Teilnehmer) oder das Ziel (empfangender Teilnehmer) ist.
Einleitende Geschäfts-ID	Geschäftsidentifikationsnummer des Quellenteilnehmers, z. B. DUNS.
Gatewaytyp	**Produktion** oder **Test**. Die Option **Test** ist nur auf Systemen verfügbar, die den Testgatewaytyp unterstützen.
Paket	Beschreibt das Format, die Packung, die Verschlüsselung und die Identifizierung des Inhaltstyps für das Dokument.
Protokoll	Für die Teilnehmer verfügbares Dokumentformat, z. B. RosettaNet von XML.
Dokumentenfluss	Der spezifische Geschäftsprozess.
Nachrichten-ID	Zu dem gepackten AS1- oder AS2-Dokument zugeordnete ID-Nummer. Die Suchkriterien können einen Stern (*) als Platzhalterzeichen beinhalten. Die maximale Länge beträgt 255 Zeichen.
Synchroner 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 MDN).
Sortieren nach	Sortieren der Ergebnisse nach diesem Wert.
Absteigend oder Aufsteigend	Aufsteigend - Zeigt die älteste Zeitmarke zuerst oder das Ende des Alphabets an. Absteigend - Zeigt die jüngste Zeitmarke zuerst oder den Beginn 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** > **AS1/AS2-Anzeige**. Das System zeigt die AS1/AS2-Anzeige an.
2. Wählen Sie die Suchkriterien aus 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. AS1/AS2-Anzeige: Paketdetails

Wert	Beschreibung
Nachrichten-ID	Zu dem gepackten AS1- oder AS2-Dokument zugeordnete ID-Nummer. 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.
Quellenteilnehmer	Der Teilnehmer, der einen Geschäftsprozess einleitet.
Zielteilnehmer	Der Teilnehmer, der den Geschäftsprozess empfängt.
Zeitmarke der Einleitung	Datum und Uhrzeit des Verarbeitungsbeginns des Dokuments.
Gatewaytyp	Test oder Produktion. Die Option **Test** ist nur auf Systemen verfügbar, die den Testgatewaytyp 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.

RosettaNet-Anzeige

Verwenden Sie die RosettaNet-Anzeige, um einen spezifischen 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 (Participant Interface Processes) definiert. Jeder PIP identifiziert ein bestimmtes Geschäftsdokument sowie die Art und Weise, wie dieses zwischen dem Community Manager und den Teilnehmern 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 20. Tasks der RosettaNet-Anzeige

Was möchten Sie tun?	Siehe
RosettaNet-Prozesse suchen	Seite 57
RosettaNet-Prozessdetails anzeigen	Seite 57
Unformatierte Dokumente anzeigen	Seite 58

RosettaNet-Prozesse suchen

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

Tabelle 21. RosettaNet-Suchkriterien

Wert	Beschreibung
Startdatum und -zeit	Datum und Uhrzeit der Prozesseinleitung.
Enddatum und -zeit	Datum und Uhrzeit der Fertigstellung des Prozesses.
Teilnehmer	Gibt den Teilnehmer an (nur Community Manager).
Meine Rolle ist der	Gibt an, ob der Teilnehmer die Quelle (einleitender Teilnehmer) oder das Ziel (empfangender Teilnehmer) ist.
Einleitende Geschäfts-ID	Geschäftsidentifikationsnummer des einleitenden Teilnehmers, z. B. DUNS.
Gatewaytyp	**Produktion** oder **Test**. Die Option **Test** ist nur auf Systemen verfügbar, die den Testgatewaytyp unterstützen.
Protokoll	Für die Teilnehmer verfügbare Protokolle.
Dokumentenfluss	Der spezifische Geschäftsprozess.
Prozessinstanz-ID	Die eindeutige Identifikationsnummer, die dem Prozess zugeordnet ist. Die Kriterien können einen Stern (*) als Platzhalterzeichen beinhalten.
Sortieren nach	Sortieren Sie Ergebnisse z. B. nach der Zeitmarke der Empfangszeit.
Absteigend oder Aufsteigend	Aufsteigend - Zeigt die älteste Zeitmarke zuerst oder das Ende des Alphabets an. Absteigend - Zeigt die jüngste Zeitmarke zuerst oder den Beginn 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.

RosettaNet-Prozessdetails anzeigen

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

Tabelle 22. Dokumentverarbeitungsdetails

Wert	Beschreibung
Teilnehmer	Die in den Geschäftsprozess einbezogenen Teilnehmer.
Zeitmarken	Datum und Uhrzeit des Verarbeitungsbeginns des ersten Dokuments.
Dokumentenfluss	Der spezifische Geschäftsprozess, z. B. RosettaNet (1.1): 3A7.
Gatewaytyp	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 Teilnehmer zugeordnet wird. Dieses Feld befindet sich nicht in einer festgelegten Position und variiert je nach Dokumenttyp.
Quellenteilnehmer	Der einleitende Teilnehmer.
Zielteilnehmer	Der empfangende Teilnehmer.

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 aus 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 Dokumentenfluss, 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 „Datenprüffehler anzeigen" auf Seite 61.
- 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), Teilnehmerverbindung, Gatewaytyp, Dokumentstatus, Protokoll, Dokumentenfluss und Prozessversion. Die Suchergebnisse zeigen alle Dokumente an, die Ihre Suchkriterien erfüllen, und geben die Zeitmarken, den Prozess, die Teilnehmerverbindung und die Gatewaytypen 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 aus den Dropdown-Listen aus.

Tabelle 23. Suchkriterien der Dokumentanzeige

Wert	Beschreibung
Startdatum und -zeit	Datum und Uhrzeit der Prozesseinleitung.
Enddatum und -zeit	Datum und Uhrzeit der Fertigstellung des Prozesses.
Teilnehmer	Gibt den Teilnehmer an (nur Community Manager).
Meine Rolle ist der	Gibt an, ob der Teilnehmer die Quelle (einleitender Teilnehmer) oder das Ziel (empfangender Teilnehmer) ist.
Suchen in	Suchen im sendenden oder empfangenden Dokumentenfluss.
Gatewaytyp	**Produktion** oder **Test**. Die Option **Test** ist nur auf Systemen verfügbar, die den Testgatewaytyp unterstützen.
Dokumentstatus	Aktueller Dokumentstatus im System. Sie können **Im Vorgang**, **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 Teilnehmer verfügbar ist.
Dokumentenfluss	Der spezifische Geschäftsprozess.
Dokument-ID	Erstellt durch den Quellenteilnehmer. Die Kriterien können einen Stern (*) als Platzhalterzeichen beinhalten.
Referenz-ID	Die vom System erstellte ID-Nummer zum Überwachen des Dokumentstatus.
Quellen-IP-Adresse	Die IP-Adresse des Quellenteilnehmers.
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.

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 24. Mit Hilfe der Dokumentanzeige verfügbare Dokumentinformationen

Wert	Beschreibung
Teilnehmer	Die in den Geschäftsprozess einbezogenen Quellenteilnehmer (Sender) und Zielteilnehmer (Empfänger).
Zeitmarken	Das Datum und die Uhrzeit des Verarbeitungsbeginns und -endes des Dokuments.
Dokumentenfluss	Der Geschäftsprozess, der gerade ausgeführt wird.
Gatewaytyp	Test oder Produktion. Die Option **Test** ist nur auf Systemen verfügbar, die den Testgatewaytyp unterstützen.
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 aus 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 25. 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 Quellenteilnehmer zugeordnet wird.
Dokumentzeitmarke	Datum und Uhrzeit der Erstellung durch den Teilnehmer.
Gateway	Das Gateway, durch das das Dokument geleitet wird.
Verbindungsdokumentenfluss	Vom System für ein Dokument ausgeführte Aktionen, um die Kompatibilität des Dokuments mit Geschäftsanforderungen der Teilnehmer untereinander sicherzustellen.
Quelle und Ziel	Die in den Geschäftsprozess einbezogenen Quellen- und Zielteilnehmer.
Eingangszeitmarke	Das Datum und die Uhrzeit, zu der das System das Dokument vom Teilnehmer empfangen hat.
Zeitmarke Endstatus	Das Datum und die Uhrzeit, zu der das Dokument vom System erfolgreich zum Zielteilnehmer weitergeleitet wurde.
Quellen- und Zielgeschäfts-ID	Die Geschäftsidentifikationsnummer des Quellen- und des Zielteilnehmers, z. B. DUNS.
Quellen- und Zieldokumentenfluss	Der spezifische Geschäftsprozess, der zwischen dem Quellen- und dem Zielteilnehmer 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 „Datenprüffehler anzeigen" auf Seite 61.

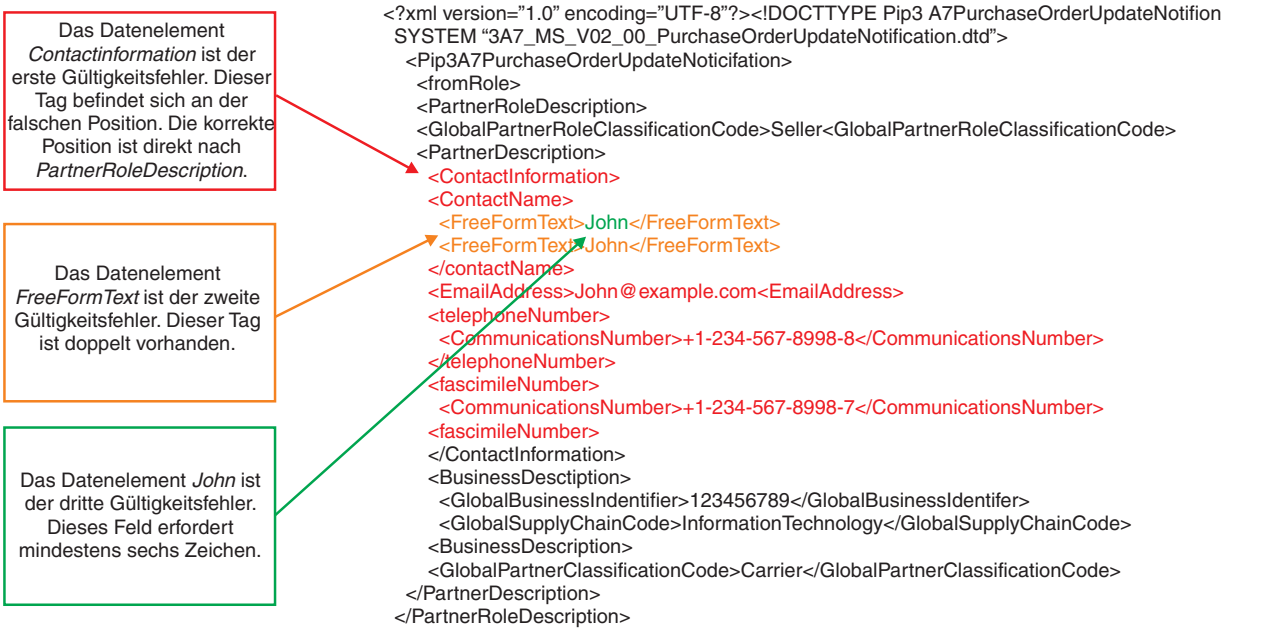
Datenprüffehler anzeigen

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 in rot angezeigt. Treten bis zu drei separate Gültigkeitsfehler innerhalb von verschachtelten XML-Feldern auf, werden folgende Farben zur Unterscheidung zwischen den Fehlerfeldern verwendet:

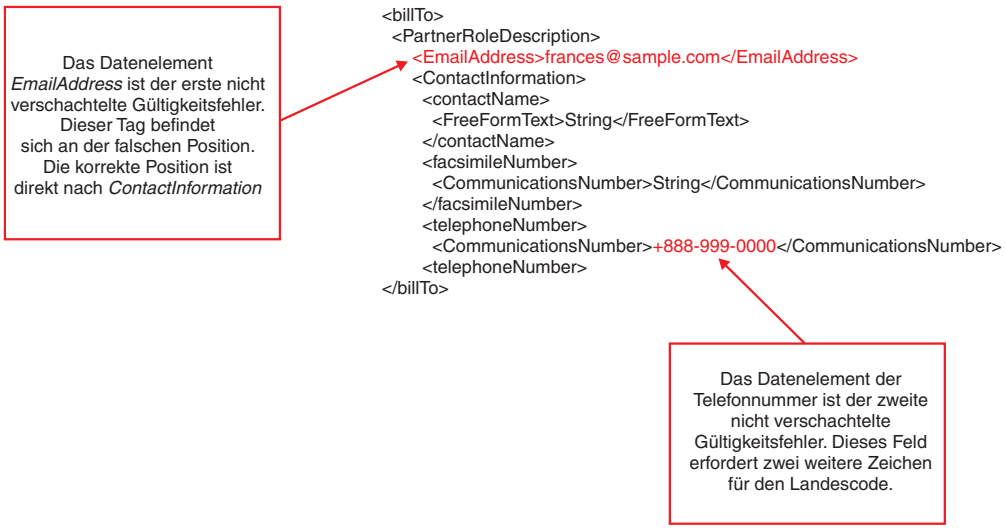
Tabelle 26. Farbig markierte Dokumentprüffehler

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 58.

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 nur für Hubadmin-Benutzer verfügbar.

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

Gateway-Warteschlange

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

Mit der Funktion der **Gateway-Warteschlange** 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 **Gateway-Warteschlange** können Sie folgende Operationen ausführen:

- Eine Liste aller Gateways 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 Gateway-Warteschlange befindet. Dies kann auf ein Problem beim Dokument selbst hindeuten. Darüber hinaus können Sie Dokumentdetails anzeigen, um eine Fehlerdiagnose bei Dokumenten auszuführen oder Dokumente aus der Warteschlange zu löschen.

- Gateway-Details anzeigen, um den einwandfreien Betrieb sicherzustellen. Dokumente, die sich in einer Gateway-Warteschlange stauen, sind möglicherweise ein Hinweis auf einen Fehler beim Zustellmanager oder im Gateway.
- Den Gateway-Status überprüfen. Bei einem Gateway, das offline gesetzt ist, werden Dokumente so lange in der Warteschlange gesammelt, bis das Gateway online gesetzt wird. Der Gateway-Status hat keinen Einfluss auf die Verbindungsfunktionalität. Die Dokumente werden weiterhin verarbeitet und für die Zustellung in die Warteschlange gestellt.

Gateway-Liste anzeigen

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

1. Klicken Sie auf **Anzeigen** > **Gateway-Warteschlange**. In der Community Console wird das Fenster **Gateway-Warteschlange** angezeigt.
2. Geben Sie die in Tabelle 27 aufgelisteten Parameter ein.

Tabelle 27. Fenster "Gateway-Warteschlange"

Kriterien	Beschreibung
In Warteschlange mindestens	Mindestanzahl von Minuten, die ein Dokument bereits in der Gateway-Warteschlange gewartet hat. Wenn beispielsweise "6 Minuten" ausgewählt ist, werden alle Gateways mit Dokumenten angezeigt, die bereits 6 Minuten oder länger auf die Zustellung warten. Der Standardwert ist 0.
Minimum in Warteschlange	Mindestanzahl von Dokumenten in einer Gateway-Warteschlange. Der Standardwert ist 1.
Sortieren nach	Sortiert Suchergebnisse nach **Teilnehmer** (Standard), **Gateway-Name** oder **Zeitmarke letztes Senden**.
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.
Aktualisieren	Schalten Sie die Aktualisierung ein oder aus (Standard).
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 Gateway, die Ihren Suchkriterien entsprechen. In **Tabelle 28** sind die von der Suche zurückgegebenen Informationen dargestellt.

Tabelle 28. Ergebnisse der Suche in der Gateway-Warteschlange

Kriterien	Beschreibung
Teilnehmer	Dem Gateway zugeordneter Handelspartner.
Gateway	Name des Gateways.
In Warteschlange	Anzahl der Dokumente in der Gateway-Warteschlange, die für die Zustellung anstehen. Link zu Gateway-Details.
Status	Gibt an, ob das Gateway online oder offline ist.
Zuletzt gesendet	Datum und Uhrzeit, zu dem bzw. der ein Dokument zuletzt erfolgreich an das Gateway gesendet wurde.

Anmerkung: In der Community Console wird ein Gateway 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 nach Dokumenten in der Warteschlange zu suchen, die bestimmte Suchkriterien erfüllen:

1. Klicken Sie auf **Anzeigen** > **Gateway-Warteschlange**.
2. Klicken Sie im Fenster **Gateway-Warteschlange** auf **Suchen**.
3. Geben Sie die folgenden Parameter an:

Tabelle 29. Suchkriterien für die Gateway-Warteschlange

Parameter	Beschreibung
Teilnehmer	Name des Handelspartners, der das Dokument empfängt.
Gateway	Name des Gateways.
Referenz-ID	Eindeutige Identifikationsnummer, die dem Dokument durch das System zugeordnet wird.
Dokument-ID	Eindeutige Identifikationsnummer, die dem Dokument durch den Quellenteilnehmer zugeordnet wird.
Sortieren nach	Sortiert Suchergebnisse nach Teilnehmer (Standard), Referenz-ID, Dokument-ID oder nach der Zeit, zu der das Dokument in die Gateway-Warteschlange eingegangen ist.
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.

4. Klicken Sie zum Anzeigen umfangreicher Dokumentdetails auf **Referenz-ID**. Der Abschnitt "Informationen zur Dokumentanzeige" in der Onlinehilfe enthält eine Beschreibung der detaillierten Informationen, die in den Dokumentdetails angezeigt werden.

Dokumente aus der Zustellungswarteschlange löschen

Nachfolgend ist 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** > **Gateway-Warteschlange**.
2. Klicken Sie im Fenster **Gateway-Warteschlange** auf **Suchen**.
3. Geben Sie die Parameter im Fenster ein (siehe Tabelle 29 auf Seite 64).
4. Klicken Sie auf das Symbol zum Löschen, um das entsprechende Dokument zu löschen.

Gateway-Details anzeigen

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

1. Klicken Sie auf **Anzeigen** > **Gateway-Warteschlange**.
2. Geben Sie im Fenster **Gateway-Warteschlange** die Suchkriterien ein (siehe Tabelle 27 auf Seite 63).
3. Klicken Sie auf **Suchen**.
4. Klicken Sie in der Liste der Gateways auf den Link für die Dokumentenzahl in der Spalte **In Warteschlange**. Daraufhin werden die Gateway-Details und eine Liste von Dokumenten in der Warteschlange angezeigt.

Gateway-Status ändern

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

1. Klicken Sie auf **Anzeigen** > **Gateway-Warteschlange**.
2. Geben Sie im Fenster **Gateway-Warteschlange** die Suchkriterien ein (siehe Tabelle 27 auf Seite 63).
3. Klicken Sie auf **Suchen**.
4. Klicken Sie in der Liste der Gateways auf den Link für die Dokumentenzahl in der Spalte **In Warteschlange**. Daraufhin werden die Gateway-Details und eine Liste von Dokumenten in der Warteschlange angezeigt.
5. Klicken Sie auf **Online** in den **Gateway-Informationen**, um ein Gateway offline zu setzen oder klicken Sie auf **Offline**, um ein Gateway online zu setzen. (Sie müssen als Hubadministrator angemeldet sein, um den Gateway-Status ändern zu können.)

Kapitel 6. Dokumentenfluss analysieren: Tools

Verwenden Sie das Dokumentanalysetool, um einen detaillierten Überblick über die Anzahl der Dokumente im System, geordnet nach Status (**Empfangen**, **Im Vorgang**, **Fehlgeschlagen** und **Erfolgreich**), zu erhalten. Die Suchkriterien umfassen Datum, Uhrzeit, Prozesstyp (sendender Prozess oder empfangender Prozess), Gatewaytyp, Protokoll, Dokumentenfluss 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 **Teilnehmerverbindung testen** wird zum Testen des Gateways oder Web-Servers verwendet.

Tabelle 30. Tools

Welche Funktion möchten Sie verwenden?	Siehe
Dokumentanalyse	Seite 67
Dokumentvolumenbericht	Seite 69
Teilnehmerverbindung testen	Seite 71

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 31. Dokumentstatus

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

Dokumente im System anzeigen

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

Tabelle 32. Dokumentsuchkriterien

Wert	Beschreibung
Startdatum und -zeit	Datum und Uhrzeit der Prozesseinleitung.
Enddatum und -zeit	Datum und Uhrzeit der Fertigstellung des Prozesses.
Quellenteilnehmer	Der Teilnehmer, der den Geschäftsprozess eingeleitet hat (nur Community Manager).
Zielteilnehmer	Der Teilnehmer, der den Geschäftsprozess empfangen hat (nur Community Manager).
Suchen in	Suchen im sendenden oder empfangenden Dokumentenfluss.
Gatewaytyp	Beispiel: **Produktion** oder **Test**. **Test** ist nur auf Systemen verfügbar, die den Testgatewaytyp unterstützen.
Paket	Beschreibt das Format, die Packung, die Verschlüsselung und die Inhaltstypidentifikation des Dokuments.
Protokoll	Das für die Teilnehmer verfügbare Dokumentprotokoll.
Dokumentenfluss	Ein spezifischer Geschäftsprozess.
Sortieren nach	Sortieren der Ergebnisse nach dem Namen des Quellenteilnehmers oder Zielteilnehmers.
Aktualisieren	Steuert die Häufigkeit der periodischen Suchergebnisaktualisierung (nur Community Manager).
Aktualisierungsrate	Steuert die Häufigkeit der Suchergebnisaktualisierung (nur Community Manager).

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 aus 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 Zielteilnehmern. Das System zeigt eine Liste aller Dokumente für die ausgewählten Teilnehmer an. Die Anzahl der Dokumente wird in Spalten nach Verarbeitungsstatus angezeigt.
5. Wählen Sie den Link für Menge in der Spalte **Empfangen**, **Im Vorgang**, **Fehlgeschlagen** oder **Erfolgreich** aus. Das System stellt Dokumentverarbeitungsdetails im Dokumentanalysebericht dar. Wenn Sie **Fehlgeschlagen** ausgewählt haben, umfasst der Bericht auch eine Dokumentereigniszusammenfassung.

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 33. Dokumentstatus

Wert	Beschreibung
Insgesamt empfangen	Die Gesamtzahl der vom System empfangenen Dokumente.
Im Vorgang	Die im Vorgang befindlichen Dokumente werden aktuell 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 schließliche Nachricht, durch die die Dokumentverarbeitung fertig gestellt wird, wurde vom System an den Zielteilnehmer 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 Community Manager sind, unterstützen Sie die Teilnehmer 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 aus den Dropdown-Listen aus.

Tabelle 34. Dokumentvolumenbericht, Suchkriterien

Wert	Beschreibung
Startdatum und -zeit	Datum und Uhrzeit der Prozesseinleitung.
Enddatum und -zeit	Datum und Uhrzeit der Fertigstellung des Prozesses.
Quellenteilnehmer	Der Teilnehmer, der den Geschäftsprozess eingeleitet hat (nur Community Manager).
Zielteilnehmer	Der Teilnehmer, der den Geschäftsprozess empfangen hat (nur Community Manager).
Suchen in	Suchen im sendenden oder empfangenden Dokumentenfluss.
Gatewaytyp	**Produktion** oder **Test**. **Test** ist nur auf Systemen verfügbar, die den Testgatewaytyp unterstützen.
Paket	Beschreibt das Format, die Packung, die Verschlüsselung und die Inhaltstypidentifikation des Dokuments.
Protokoll	Typ des Prozessprotokolls, z. B. XML, EDI, Flachdatei.
Dokumentenfluss	Ein spezifischer Geschäftsprozess.
Sortieren nach	Sortieren der Ergebnisse nach diesen Kriterien (Dokumentenfluss oder Zieldokumentenfluss).
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 aus 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 ausdrucken

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

Teilnehmerverbindung testen

Mit der Funktion **Teilnehmerverbindung testen** können Sie das Gateway oder den Web-Server testen. Wenn Sie Community Manager sind, können Sie auch einen bestimmten Teilnehmer auswählen. Bei diesem Test wird eine leere Anforderung POST an ein Gateway oder einen URL gesendet. Die Anforderung ähnelt dem Eingeben des 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 Gateway oder Web-Server empfangene Antwort gibt deren Status an:

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

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

Testen einer Teilnehmerverbindung:

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

Tabelle 35. Teilnehmerverbindung testen, Werte

Wert	Beschreibung
Teilnehmer	Zu testender Teilnehmer (nur Community Manager).
Gateway	Zeigt die verfügbaren Gateways basierend auf dem oben ausgewählten Teilnehmer an.
URL	Wird dynamisch ausgefüllt, basierend auf dem oben ausgewählten Gateway.
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.

Web-Server-Ergebniscodes

200-299:

- 200 - OK - Successful transmission. Dies ist kein Fehler. Hier ist die angeforderte Datei.
- 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 der 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 ein neuer, permanenter URL zugeordnet; alle zukünftigen Verweise auf diese Ressource sollten mit Hilfe eines der zurückgegebenen URLs erfolgen.
- 302 - Moved Temporarily. Die angeforderte Ressource befindet sich temporär unter einem neuen URL. Umleitung zu einem 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 dem angeforderten URL finden. Diese Datei ist nicht vorhanden. Sie erhalten diese Nachricht, wenn Sie in Ihrem Browser einen fehlerhaften 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: Ein URL wurde nicht korrekt eingegeben, ein Lesezeichen zeigt auf eine nicht mehr unter dieser Adresse vorhandene Datei, eine Suchmaschine sucht nach einem 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 den angeforderten URL identifiziert wird.
- 406 - None Acceptable. Der Server hat eine mit dem 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 Authorisierung 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 Gateway. Der Server empfing beim Zugriff auf das Gateway oder den übergeordneten Server zum Erfüllen der Anforderung eine ungültige Antwort.
- 503 - Service Temporarily Unavailable. Der Server ist wegen einer temporären Überlastung bzw. Wartung aktuell nicht in der Lage, die Anforderung zu bearbeiten. Der Server verfügt über keine Ressourcen.
- 504 - Gateway Time out. Der Server empfing beim Zugriff auf das Gateway oder den übergeordneten Server zum Erfüllen der Anforderung keine rechtzeitige Antwort.
- 505 - HTTP Version Not Supported

Glossar

A

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

Aktion. Vom System für ein Dokument ausgeführte Aktionen, um die Kompatibilität des Dokuments mit Geschäftsanforderungen der Teilnehmer untereinander sicherzustellen.

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

Aktivierung. Die Verbindung eines Teilnehmers 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.

C

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

Community Manager, untergeordnetes Element. Ein untergeordnetes Element des Community Managers ist ein spezieller Teilnehmertyp, der in der Community Console die Funktion eines Teilnehmers hat, sich beim Routing jedoch wie ein Community Manager verhält.

Community-Teilnehmer. Ein Mitglied der Hub-Community, das Geschäftstransaktionen mit dem Community Manager austauscht.

D

Digitale Unterschrift. Eine digitale Unterschrift ist eine elektronische Unterschrift, die zur Authentifizierung der Teilnehmer 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.

Dokumentenflussdefinition. Stellt dem System alle notwendigen Informationen zum Empfangen, Verarbeiten und Weiterleiten von Dokumenten zwischen Community-Teilnehmern zur Verfügung. Typen von Dokumentenflussdefinitionen sind Paket, Protokoll, Dokumentenfluss, Aktivität und Aktion.

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.

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

Gateway. Eine B2B-Netzposition, die als Eingang zu einem anderen Netzwerk fungiert. Ein Gateway kann Datenumsetzung und Kompatibilitätsanforderungen zur Sicherstellung des Datentransfers ermitteln.

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

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 Teilnehmern.

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 Teilnehmer und Community Manager 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 Teilnehmers 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 Teilnehmer erfolgreich das Testen von Geschäftsregeln beendet hat und der Community Manager 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.

PIP (Partner Interface Process). Definiert Geschäftsprozesse zwischen Community Managern und Partnern (in WebSphere Partner Gateway sind Partner Teilnehmer). 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 spezifische 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 einer Kontaktperson ein Alert durch einen Teilnehmer (lokal) oder auch durch den Community Manager (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, Im Vorgang, Fehlgeschlagen oder Erfolgreich.

Subskribierter Kontakt. 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

Teilnehmerverbindung. Eine Teilnehmerverbindung definiert die Verbindung zwischen den Umgebungen von zwei spezifischen Teilnehmern der Community. Über diese Verbindung wird ein eindeutiger Prozess ausgeführt.

Test. Der Status, in dem ein Teilnehmer 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 Datenaustauschfolge sowie zugehörige Arbeit, die zu Zwecken der Geschäftsausführung zwischen den Teilnehmern 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.

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

URL. Ein URL (Uniform Resource Locator) ist die Adresse eines Dokuments oder 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.

Bemerkungen

Möglicherweise bietet IBM die in dieser Dokumentation beschriebenen Produkte, Services oder Funktionen nicht in allen Ländern oder Regionen an. Informationen über die gegenwärtig im jeweiligen Land verfügbaren Produkte und Services sind beim IBM Ansprechpartner erhältlich. Hinweise auf IBM Lizenzprogramme oder andere IBM Produkte bedeuten nicht, dass nur Programme, Produkte oder 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 anderen Schutzrechte der IBM verletzen. Die Verantwortung für den Betrieb von Fremdprodukten, Fremdprogrammen und Fremdservices liegt beim Kunden.

Für in diesem Handbuch beschriebene Erzeugnisse und Verfahren kann es IBM Patente oder Patentanmeldungen geben. Mit der Auslieferung dieses Handbuchs ist keine Lizenzierung dieser Patente verbunden. Lizenzanforderungen sind schriftlich an folgende Adresse zu richten (Anfragen an diese Adresse müssen auf Englisch formuliert werden):

IBM Europe
Director of Licensing
92066 Paris La Defense Cedex
France

Trotz sorgfältiger Bearbeitung können technische Ungenauigkeiten oder Druckfehler in dieser Veröffentlichung nicht ausgeschlossen werden. Die Angaben in diesem Handbuch werden in regelmäßigen Zeitabständen aktualisiert. Die Änderungen werden in Überarbeitungen oder in Technical News Letters (TNLs) bekannt gegeben. IBM kann ohne weitere Mitteilung jederzeit Verbesserungen und/oder Änderungen an den in dieser Veröffentlichung beschriebenen Produkten und/oder Programmen vornehmen.

Verweise in diesen Informationen auf Websites anderer Anbieter dienen lediglich als Benutzerinformationen und stellen keinerlei Billigung des Inhalts dieser Websites dar. Das über diese Websites verfügbare Material ist nicht Bestandteil des Materials für dieses IBM Produkt. Die Verwendung dieser Websites geschieht auf eigene Verantwortung.

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

Lizenznehmer des Programms, die Informationen zu diesem Produkt wünschen mit der Zielsetzung: (i) den Austausch von Informationen zwischen unabhängigen, erstellten Programmen und anderen Programmen (einschließlich des vorliegenden Programms) sowie (ii) die gemeinsame Nutzung der ausgetauschten Informationen zu ermöglichen, wenden sich an folgende Adresse:

IBM Burlingame Laboratory Director
IBM Burlingame Laboratory
577 Airport Blvd., Suite 800
Burlingame, CA 94010
U.S.A

Die Bereitstellung dieser Informationen kann unter Umständen von bestimmten Bedingungen - in einigen Fällen auch von der Zahlung einer Gebühr - abhängig sein.

Die Lieferung des im Handbuch aufgeführten Lizenzprogramms sowie des zugehörigen Lizenzmaterials erfolgt im Rahmen der Allgemeinen Geschäftsbedingungen der IBM, der Internationalen Nutzungsbedingungen der IBM für Programmpakete oder einer äquivalenten Vereinbarung.

Alle in diesem Dokument enthaltenen Leistungsdaten stammen aus einer gesteuerten Umgebung. Die Ergebnisse, die in anderen Betriebsumgebungen erzielt werden, können daher erheblich von den hier erzielten Ergebnissen abweichen. Einige Daten stammen möglicherweise von Systemen, deren Entwicklung noch nicht abgeschlossen ist. Eine Gewährleistung, dass diese Daten auch in allgemein verfügbaren Systemen erzielt werden, kann nicht gegeben werden. Darüber hinaus wurden einige Daten unter Umständen durch Extrapolation berechnet. Die tatsächlichen Ergebnisse können abweichen. Benutzer dieses Dokuments sollten die entsprechenden Daten in ihrer spezifischen Umgebung prüfen.

Alle Informationen zu Produkten anderer Anbieter stammen von den Anbietern der aufgeführten Produkte, deren veröffentlichten Ankündigungen oder anderen allgemein verfügbaren Quellen. IBM hat diese Produkte nicht getestet und kann daher keine Aussagen zu Leistung, Kompatibilität oder anderen Merkmalen machen. Fragen zu den Leistungsmerkmalen von Produkten anderer Anbieter sind an den jeweiligen Anbieter zu richten.

Diese Veröffentlichung enthält möglicherweise Beispiele für Daten und Berichte des alltäglichen Geschäftsablaufes. Sie sollen nur die Funktionen des Lizenzprogrammes illustrieren; sie können Namen von Personen, Firmen, Marken oder Produkten enthalten. Alle diese Namen sind frei erfunden; Ähnlichkeiten mit tatsächlichen Namen und Adressen sind rein zufällig.

Die oben genannten Erklärungen bezüglich der Produktstrategien und Absichtserklärungen von IBM stellen die gegenwärtige Absicht der IBM dar, unterliegen Änderungen oder können zurückgenommen werden, und repräsentieren nur die Ziele der IBM.

COPYRIGHTLIZENZ

Diese Veröffentlichung enthält möglicherweise Beispielanwendungsprogramme, die in Quellensprache geschrieben sind. Sie dürfen diese Beispielprogramme kostenlos kopieren, ändern und verteilen, wenn dies zu dem Zweck geschieht, Anwendungsprogramme zu entwickeln, verwenden, vermarkten oder zu verteilen, die mit der Anwendungsprogrammierschnittstelle konform sind, für die diese Beispielprogramme geschrieben werden. Die Beispiele wurden eventuell nicht unter allen denkbaren Bedingungen getestet. IBM kann deshalb nicht garantieren, dass die Zuverlässigkeit, Wartungsfreundlichkeit und Funktion dieser Programme gegeben ist.

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

COPYRIGHT- UND BERECHTIGUNGSHINWEIS

Copyright (c) 1995-2003 International Business Machines Corporation und andere

Alle Rechte vorbehalten.

Hiermit wird jeder Person, die eine Kopie dieser Software und der zugehörigen Dokumentationsdateien (die "Software") erhält, die kostenlose Genehmigung erteilt, uneingeschränkt mit der Software zu handeln. Dazu gehört ohne Einschränkung das Recht, Kopien der Software zu nutzen, zu kopieren, zu ändern, zusammenzufügen, zu veröffentlichen, zu verteilen und/oder zu verkaufen und den #Personen, denen die Software zur Verfügung gestellt wird, das gleiche Recht einzuräumen, vorausgesetzt, dass der obige Copyrightvermerk und dieser Berechtigungshinweis auf allen Kopien der Software sowie der zugehörigen Dokumentation erscheinen.

DIE SOFTWARE WIRD OHNE WARTUNG (AUF "AS-IS"-BASIS) UND OHNE GEWÄHRLEISTUNG (VERÖFFENTLICHT ODER STILLSCHWEIGEND), EINSCHLIESSLICH, ABER NICHT BEGRENZT AUF DIE IMPLIZIERTE GEWÄHRLEISTUNG FÜR DIE HANDELSÜBLICHKEIT, DIE VERWENDUNGSFÄHIGKEIT FÜR EINEN BESTIMMTEN ZWECK UND DIE FREIHEIT DER RECHTE DRITTER ZUR VERFÜGUNG GESTELLT. UNTER KEINEN UMSTÄNDEN IST DER ODER SIND DIE COPYRIGHTINHABER HAFTBAR FÜR SPEZIELLE, UNMITTELBARE, MITTELBARE ODER FOLGESCHÄDEN ODER SCHÄDEN DURCH NUTZUNGSAUSFALL, DATENVERLUST, GEWINNEINBUSSEN. DIES GILT UNABHÄNGIG VON DER HAFTUNGSGRUNDLAGE, SEI SIE VERSCHULDENSABHÄNGIG ODER VERSCHULDENSUNABHÄNGIG, SOFERN SIE IN IRGENDEINER FORM AUF DIE NUTZUNG DER SOFTWARE ZURÜCKZUFÜHREN WÄRE.

Mit Ausnahme der Verwendung in diesem Hinweis darf der Name eines Copyrightinhabers ohne seine vorherige schriftliche Genehmigung nicht zu Werbezwecken, anderen Arten der Verkaufsförderung oder zur Nutzung in dieser Software verwendet werden.

Informationen zur Programmierschnittstelle

Werden Informationen zur Programmierschnittstelle bereitgestellt, ermöglichen Ihnen diese das Erstellen von Anwendungssoftwareprogrammen mit Hilfe dieses Programms. Allgemeine Programmierschnittstellen ermöglichen Ihnen das Schreiben von Anwendungssoftwareprogrammen, die die Services der Tools des vorliegenden Programms nutzen. Diese Informationen enthalten möglicherweise auch Diagnose-, Änderungs- und Optimierungsinformationen. Diese Informationen werden bereitgestellt, um Ihnen die Behebung von Fehlern in Ihren Anwendungssoftwareprogrammen zu erleichtern.

Achtung: Diese Diagnose-, Änderungs- und Optimierungsinformationen dürfen nicht als Programmierschnittstelle verwendet werden, da sie jederzeit geändert werden können.

Marken und Servicemarken

Folgende Namen sind in gewissen Ländern Marken oder eingetragene Marken der International Business Machines Corporation:

i5/OS
IBM
IBM Logo
AIX
CICS
CrossWorlds
DB2
DB2 Universal Database
Domino
IMS
Informix
iSeries
Lotus
Lotus Notes
MQIntegrator
MQSeries
MVS
OS/400
Passport Advantage
SupportPac
WebSphere
z/OS

Microsoft, Windows, Windows NT und das Windows-Logo sind in gewissen Ländern Marken der Microsoft Corporation.

MMX, Pentium und ProShare sind in gewissen Ländern Marken oder eingetragene Marken der Intel Corporation.

Java und alle Java-basierten Marken sind in gewissen Ländern Marken von Sun Microsystems, Inc.

Linux ist in gewissen Ländern eine Marke von Linus Torvalds.

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

WebSphere Partner Gateway Enterprise und Advanced Edition, Version 6.0.

Index

E

F

G

H

I

J

K

L