

IBM WebSphere Business Integration Connect Enterprise
und Advanced Edition



Teilnehmer-Handbuch

IBM WebSphere Business Integration Connect Enterprise
und Advanced Edition



Teilnehmer-Handbuch

Bemerkungen

Vor Verwendung dieser Informationen und des darin beschriebenen Produkts sollten die allgemeinen Informationen unter „Bemerkungen“ auf Seite 65 unbedingt gelesen werden.

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

Diese Veröffentlichung ist eine Übersetzung des Handbuchs
IBM WebSphere Business Integration Connect Enterprise and Advanced Editions Participant Guide,

herausgegeben von International Business Machines Corporation, USA

© Copyright International Business Machines Corporation 2003, 2004

© Copyright IBM Deutschland Informationssysteme GmbH 2004

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

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

Änderung des Textes bleibt vorbehalten.

Herausgegeben von:

SW TSC Germany

Kst. 2877

Juli 2004

Inhaltsverzeichnis

Zu diesem Handbuch	v
Neuerungen in diesem Release	v
Zugehörige Dokumente	v
In diesem Handbuch verwendete Konventionen und Terminologie	vi
Typografische Konventionen	vi
Begriffe	vi
Hilfe anfordern	viii
Onlinehilfe	viii
Kundendienst	viii
Produktdokumentation	viii
Kapitel 1. Einführung	1
Was ist eine Hub-Community?	1
Community Operator	1
Community Manager	1
Teilnehmer	1
Symbole der Community Console	2
Verwendung der Community Console	4
Kapitel 2. Umgebung für Business Integration Connect einrichten	5
Bei der Community Console anmelden	5
Ein Teilnehmerprofil prüfen	6
Ein Teilnehmerprofil anzeigen und bearbeiten	7
Einen Gateway erstellen	7
B2B-Funktionalitäten prüfen	9
Digitale Zertifikate hochladen	11
Zertifikatbedingungen	11
Beschreibung	12
Typen und unterstützte Formate von Zertifikaten	13
SSL-Server- und Clientauthentifizierung	14
Ein digitales Zertifikat laden und definieren	14
Konsolengruppen erstellen	15
Benutzer erstellen	15
Einen neuen Benutzer erstellen	16
Benutzer zu Gruppen zuordnen	16
Kontaktinformationen erstellen	16
Alerts erstellen und Kontakte hinzufügen	17
Einen volumenbasierten Alert erstellen	19
Einen ereignisbasierten Alert erstellen	21
Einen neuen Kontakt zu einem vorhandenen Alert hinzufügen	23
Eine neue Adresse erstellen	24
Kapitel 3. Verbindungen und Benutzer der Community verwalten: Kontenadmin	25
Gateways verwalten	25
Liste der Gateways anzeigen	25
Details zu Gateways anzeigen oder bearbeiten	25
Standardgateways anzeigen, auswählen oder bearbeiten	26
Zertifikate verwalten	26
Details zu digitalen Zertifikaten anzeigen und bearbeiten	26
Ein digitales Zertifikat inaktivieren	27
Gruppen verwalten	27
Gruppenzugehörigkeiten anzeigen und Benutzer zu Gruppen zuordnen	27
Gruppenberechtigungen anzeigen, bearbeiten und zuordnen	27
Gruppendetails anzeigen oder bearbeiten	27
Eine Gruppe löschen	28

Benutzer verwalten	28
Kontakte verwalten	29
Kontaktdetails anzeigen oder bearbeiten	30
Einen Kontakt entfernen	31
Alerts verwalten	31
Alertdetails und Kontakte anzeigen oder bearbeiten	31
Alerts suchen	31
Einen Alert inaktivieren oder aktivieren	32
Einen Alert entfernen	32
Adressen verwalten	33
Eine Adresse bearbeiten	33
Eine Adresse löschen	33

Kapitel 4. Ereignisse und Dokumente anzeigen: Anzeigefunktionen 35

Ereignisanzeige	36
Ereignistypen	37
Tasks der Ereignisanzeige ausführen	37
Ereignisse suchen	37
Ereignisdetails anzeigen	38
AS1/AS2-Anzeige	39
Tasks der AS1/AS2-Anzeige ausführen	39
Nachrichten suchen	40
Nachrichtendetails anzeigen	40
RosettaNet-Anzeige	41
Tasks der RosettaNet-Anzeige ausführen	41
RosettaNet-Prozesse suchen	42
RosettaNet-Prozessdetails anzeigen	42
Unformatierte Dokumente anzeigen	43
Dokumentanzeige	43
Dokumente suchen	43
Dokumentdetails, Ereignisse und unformatierte Dokumente anzeigen	45
Datenprüffehler anzeigen	46
Die Funktion 'Prozess stoppen' verwenden	47

Kapitel 5. Dokumentfluss analysieren: Tools 49

Dokumentanalyse	49
Dokumentstatus	50
Dokumente im System anzeigen	50
Prozess- und Ereignisdetails anzeigen	51
Dokumentvolumenbericht	51
Einen Dokumentvolumenbericht erstellen	52
Einen Dokumentvolumenbericht exportieren	52
Berichte ausdrucken	52
Teilnehmerverbindung testen	53
Web-Server-Ergebniscode	53

Glossar 57

Index 61

Bemerkungen 65

Informationen der Programmierschnittstelle	67
Marken und Servicemarken	68

Zu diesem Handbuch

IBM™ WebSphere™ Business Integration Connect ist ein elektronisches Dokumentverarbeitungssystem zur Verwaltung von B2B-Handelsgemeinschaften. B2B (Business-to-Business) hat sich in den letzten Jahren zu dem Zweck entwickelt, Unternehmen darin zu unterstützen, verschiedene Arten von automatisierten Transaktionen (z. B. Bestellungen und Rechnungen) schnell, bequem und ökonomisch ausführen zu können.

Die in eine Handelsgemeinschaft bzw. Hub-Community von IBM WebSphere Business Integration Connect einbezogenen Parteien sind der Community Manager, der Community Operator und die Teilnehmer der Community (auch einfach als "Teilnehmer" bezeichnet). Zu jeder dieser Parteien gehören Benutzer mit Verwaltungsaufgaben, die über unterschiedliche Berechtigungsstufen verfügen. Außerdem fügen die Benutzer mit Verwaltungsaufgaben reguläre Benutzer mit spezifischen Konsolenzugriffsrechten hinzu.

Dieses Handbuch stellt den Community-Teilnehmern alle erforderlichen Informationen zum Einrichten der Konsole und zum Ausführen von Routinetasks zur Verfügung.

Neuerungen in diesem Release

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 Business Integration Connect.
- Der Community Console wurden neue Eingabehilfefunktionen zur Unterstützung von Sprachausgabeprogrammen hinzugefügt.

Zugehörige Dokumente

Die vollständige, für dieses Produkt verfügbare Dokumentation beschreibt die Funktionen und Komponenten von WebSphere Business Integration Connect Enterprise Edition und Advanced Edition.

Sie können die Dokumentation herunterladen oder online unter der folgenden Adresse lesen:

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

Anmerkung: Wichtige Informationen zu diesem Produkt sind unter Umständen in technischen Hinweisen der technischen Unterstützung und in Flashes verfügbar, die nach der Publizierung dieses Dokuments ausgegeben wurden. Sie sind dann auf der Website der Unterstützung von WebSphere Business Integration verfügbar:

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

Wählen Sie den Bereich der entsprechenden Komponente aus, und blättern Sie zu den technischen Hinweisen und Flashes.

In diesem Handbuch verwendete Konventionen und Terminologie

Typografische Konventionen

In diesem Dokument werden folgende Konventionen verwendet:

Fettdruck	Gibt eine Auswahl in einer Bildschirmansicht an.
Blauer Text	Dieser Text gibt einen Querverweis in Form eines Hyperlinks an und ist nur in blau sichtbar, wenn Sie das Handbuch online anzeigen. Klicken Sie jeweils auf den blauen Text, um zu dem entsprechenden Verweisobjekt zu springen.
Kursivdruck	Gibt eine Variable an.
/	In diesem Dokument werden Schrägstriche (/) als Konvention für Verzeichnispfade verwendet. Ersetzen Sie bei Installationen unter Windows die Schrägstriche durch Backslashes (\). Alle Pfadnamen von WebSphere Business Integration Connect sind relativ zu dem Verzeichnis, in dem das Produkt auf Ihrem System installiert ist.

Begriffe

Die folgenden Begriffe sind einzigartig für dieses Produkt und diese Dokumentverarbeitung. Zusätzliche Begriffe sind im „Glossar“ auf Seite 57 dieses Handbuchs aufgeführt.

Aktion: Wird auch als Geschäftsaktion bezeichnet. Eine Nachricht mit Geschäftsinhalt, z. B. eine Bestellung oder eine Angebotsanfrage. Der Austausch von Geschäftsaktionen und Geschäftssignalen bildet die erforderliche Choreografie zur Ausführung einer durch einen bestimmten PIP angegebenen Geschäftsaktivität.

Geschäftsaktion: Siehe Aktion.

Geschäftsprozess: Ein vordefinierter Satz von Geschäftstransaktionen, die die erforderlichen Schritte zum Erreichen des Geschäftsziels darstellen.

Teilnehmerverbindung: Eine Teilnehmerverbindung definiert die Verbindung zwischen den Umgebungen von zwei spezifischen Teilnehmern der Community, durch die ein eindeutiger Prozess entsprechend der zugeordneten Aktion ausgeführt wird.

Community Console: Die Community Console ist ein webbasiertes Tool für die Konfiguration von WebSphere Business Integration Connect und die Verwaltung des Verarbeitungsablaufs der Geschäftsdokumente in Ihrem Unternehmen zum und vom Community Manager bzw. zu und von den Teilnehmern.

Dokument: Eine Sammlung von Informationen, die einer Unternehmenskonvention unterliegen. In diesem Kontext gibt es mehrere Dokumente in einem Prozess.

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.

Community Manager: Das Unternehmen, das WebSphere Business Integration Connect erworben und an die Mitglieder in seiner Hub-Community verteilt hat. Der Community Manager verfügt über einen Benutzer mit Verwaltungsaufgaben, den Manageradmin, der für den ordnungsgemäßen Zustand und die Wartung des Abschnitts des Community Managers in der Community verantwortlich ist. Funktionen der Community Console, die aus der Anzeige des Community Managers ausgeschlossen sind, beziehen sich auf die Systemkonfiguration.

Community Operator: Die über den gesamten Hub hinweg für die Konfiguration, Wartung und den allgemeinen ordnungsgemäßen Zustand des Systems verantwortlichen Einzelpersonen.

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

Community-Teilnehmer: Der Teilnehmer sendet Geschäftstransaktionen an den Community Manager und empfängt Geschäftstransaktionen vom Community Manager. Die Teilnehmer können auf Funktionen zugreifen, die ihre Rolle innerhalb der Community unterstützen.

RosettaNet-PIP (Partner Interface Process): Ein Modell, das die Aktivitäten, Entscheidungen und Interaktionen der Partnerrolle darstellt, die eine Geschäftstransaktion zwischen zwei Partnern in einer bestimmten Versorgungskette erfüllt. (In WebSphere Business Integration Connect werden diese Partner als "Teilnehmer" bezeichnet.) Jeder in den PIP einbezogene Teilnehmer muss die in einem PIP-Exemplar angegebenen Bedingungen erfüllen. Wenn eine Partei den Dienst nicht wie in der PIP-Implementierungsrichtlinie angegeben ausführt, ist die Geschäftstransaktion null und nichtig.

Prozess: Ein Prozess besteht aus einer Serie von Dokumenten oder Nachrichten, die zwischen Community Manager und Teilnehmer ausgeführt werden. Im Ganzen betrachtet bilden die Dokumente einen vollständigen Geschäftsprozess.

Hilfe anfordern

Onlinehilfe

Die Onlinehilfe ist in jeder Anzeige auf der rechten Seite verfügbar. Siehe Abb. 1.

Anmerkung: Wenn beim Anklicken der Hilfe kein Hilfefenster erscheint, überprüfen Sie, ob Sie einen Pop-upblockierer aktiviert haben.



Abbildung 1. Die Community Console

Kundendienst

Softwareunterstützung:

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

Passport Advantage:

<http://www.ibm.com/software/howtobuy/passportadvantage>

Produktdokumentation

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

Kapitel 1. Einführung

Was ist eine Hub-Community?

Die Hub-Community von IBM WebSphere Business Integration Connect besteht aus drei Einheiten, die für den Austausch von Geschäftsdokumenten in Echtzeit an einen zentralen Hub angeschlossen sind: den Community Operator, den Community Manager und die 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.
- Sicherstellen, dass die Hub-Community für alle Teilnehmer ordnungsgemäß konfiguriert ist.
- 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 Business Integration Connect 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 sind einzigartig für die Community Console von WebSphere Business Integration Connect.

Tabelle 1. Symbole der Community Console

Symbol	Beschreibung
Anklickbare Symbole	
	Klicken Sie hier, um detaillierte Informationen anzuzeigen.
	Klicken Sie hier, um ein ausgewähltes Element zu modifizieren.
	Klicken Sie hier, um eines oder mehrere ausgewählte Elemente zu löschen oder das zugeordnete inaktive Element zu aktivieren.
	Klicken Sie hier, um ein unformatiertes Dokument anzuzeigen.
	Klicken Sie hier, um Gültigkeitsfehler anzuzeigen.
	Klicken Sie hier, um fortzufahren.
	Klicken Sie hier, um anzuhalten.
	Klicken Sie hier, um ein Dokument oder einen Bericht auszudrucken.
	Klicken Sie hier, um einen Bericht zu exportieren.
	Klicken Sie hier, um ein Kalenderdatum auszuwählen.
	Klicken Sie hier, um die Gruppen anzuzeigen, zu der ein Benutzer gehört.
	Klicken Sie hier, um Benutzer innerhalb einer Gruppe anzuzeigen.
	Klicken Sie hier, um basierend auf der ausgewählten Aktion eine neue Aktion zu erstellen.
	Klicken Sie hier, um Informationen aus dem System zu exportieren.
	Klicken Sie hier, um das zugeordnete aktive Element zu inaktivieren.
	Klicken Sie hier, um eine Dokumentflussdefinition zu bearbeiten.
	Klicken Sie hier, um anzuzeigen, wo ein Element verwendet wird.
	Klicken Sie hier, um die Einrichtung der Attribute für die Dokumentflussdefinition anzuzeigen.
	Klicken Sie hier, um eine neue Zuordnung hochzuladen.
	Klicken Sie hier, um eine Zuordnung herunterzuladen.
	Klicken Sie hier, um Attributwerte zu bearbeiten.

Tabelle 1. Symbole der Community Console (Forts.)

Symbol	Beschreibung
	Klicken Sie hier, um RosettaNet-Attributwerte zu bearbeiten.
	Klicken Sie hier, um bei einem Ereignis eines kopierten Dokuments das zu einem früheren Zeitpunkt gesendete Originaldokument anzuzeigen.
	Klicken Sie hier, um die Suchkriterien auszublenden.
	Klicken Sie hier, um Anzeigeberechtigungen darzustellen.
	Rolle ist nicht aktiv. Zum Aktivieren hier klicken.
	Klicken Sie hier, um die Hilfefunktion anzuzeigen.
Durch Symbole angezeigte Informationen	
	Gibt an, dass das Feld eine Eingabe durch den Benutzer erfordert.
	Gibt an, dass ein TPA (Trade Participant Agreement) geschlossen wurde.
	Gibt an, dass ein Teilnehmer oder Gateway inaktiviert ist.
	Gibt an, dass das Dokument gerade bearbeitet wird.
	Gibt an, dass die Dokumentbearbeitung erfolgreich war.
	Gibt an, dass die Dokumentbearbeitung fehlgeschlagen ist.
	Zeigt die Transformationszuordnungen und Verbindungen an, die aktuell die Aktion verwenden.
	Gibt einen synchronen Datenfluss an. Es wird kein Symbol für asynchrone Transaktionen angezeigt.
	Gibt an, dass Daten enthalten sind.
	Gibt an, dass keine Daten enthalten sind.
	Gibt an, dass sich in der ausgeblendeten Sicht eine hierarchische Baumstruktur befindet.
	Gibt an, dass sich in der erweiterten Sicht eine hierarchische Baumstruktur befindet.

Verwendung der Community Console

Nachdem Sie WebSphere Business Integration Connect konfiguriert haben, werden Sie zwei Konsolentools 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 Hubadmin 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 fehlschlagen.

Das Modul **Kontenadmin** der Konsole wird primär zum Einrichten von Business Integration Connect und danach für die Pflege benutzt.

Kapitel 2. Umgebung für Business Integration Connect einrichten

Dieser Abschnitt beschreibt die Tasks, die ein Benutzer mit Verwaltungsaufgaben eines Teilnehmers von Business Integration Connect, der Teilnehmeradministrator, zur Vorbereitung von Business Integration Connect für die Benutzer und die Umgebung des Teilnehmers ausführt.

Zur Konfiguration von Business Integration Connect für Ihr Unternehmen muss der Teilnehmeradministrator folgende Aktivitäten in der unten aufgeführten Reihenfolge von der Community Console aus durchführen.

1. „Bei der Community Console anmelden“
2. „Ein Teilnehmerprofil prüfen“ auf Seite 6
3. „Einen Gateway erstellen“ auf Seite 7
4. „B2B-Funktionalitäten prüfen“ auf Seite 9
5. „Digitale Zertifikate hochladen“ auf Seite 11
6. „Konsolengruppen erstellen“ auf Seite 15
7. „Benutzer erstellen“ auf Seite 15
8. „Kontaktinformationen erstellen“ auf Seite 16
9. „Alerts erstellen und Kontakte hinzufügen“ auf Seite 17
10. „Eine neue Adresse erstellen“ auf Seite 24

Bei der Community Console anmelden

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

Anmerkung: Die Community Console von WBI Connect erfordert die aktivierte Unterstützung von Cookies zur Verwaltung der Sitzungsinformationen. 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 Konsole 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: Diese URLs setzen die Verwendung der standardmäßigen Portnummern voraus. Wenn Sie die standardmäßigen Portnummern geändert haben, ersetzen Sie die Standardnummern durch die von Ihnen angegebenen Werte.

Der Browser zeigt die Bildschirmansicht für die Anmeldung bei der Konsole an. Siehe Abb. 2 auf Seite 6.

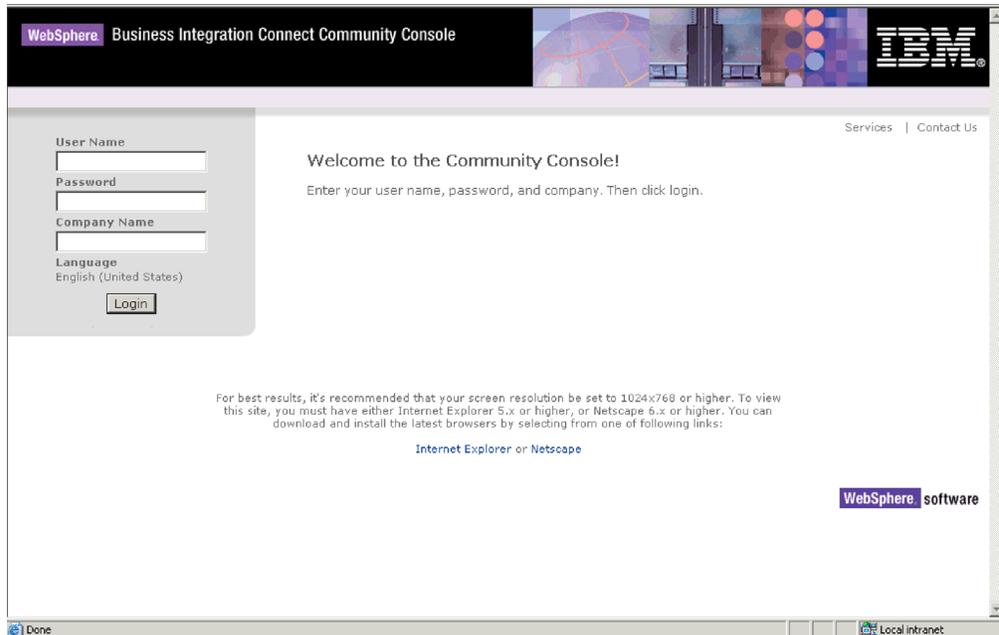


Abbildung 2. Bildschirmansicht für die Anmeldung bei der Community Console

In den meisten Fällen sendet Ihnen der Community Operator den Benutzernamen, das anfängliche Kennwort und den Unternehmensnamen für die Anmeldung bei der Community Console. Sie benötigen diese Informationen für die folgende Prozedur. Haben Sie die Informationen nicht erhalten, kontaktieren Sie den 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 Namen Ihres 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 Konsole an.

Ein Teilnehmerprofil prüfen

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

Die Teilnehmer können in Ihrem Profil alle Attribute bis auf den Teilnehmeranmeldenamen bearbeiten. Außerdem können die 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.

Ein Teilnehmerprofil anzeigen und bearbeiten

1. Klicken Sie auf **Kontenadmin > Profile > Community Teilnehmer**.
2. Klicken Sie zum Bearbeiten auf . Das System zeigt die Bildschirmansicht **Teilnehmerdetails** an.
3. Bearbeiten Sie Ihr Profil nach Bedarf (einige Werte können jedoch nicht geändert werden). In der folgenden Tabelle finden Sie eine Beschreibung der Werte.

Tabelle 2. Werte in den Teilnehmeranzeigen

Wert	Beschreibung
Teilnehmeranmeldename	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.
Teilnehmername	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. <ul style="list-style-type: none"> • DUNS-Nummern müssen neun Ziffern haben, und DUNS+4-Nummern müssen dreizehn Ziffern haben. • Unformatierte ID-Nummern lassen bis zu 60 Alphazeichen, numerische Zeichen und Sonderzeichen zu.
IP-Adresse oder Hostname	<ul style="list-style-type: none"> • Gatewaytyp, z. B. CPS-Teilnehmer. • IP-Adresse oder Hostname des Teilnehmers.

4. Klicken Sie auf **Speichern**.

Einen Gateway erstellen

Sie müssen einen Standardgateway erstellen und pflegen. Andernfalls können Sie keine Verbindungen herstellen. Sie können den Standardgateway nicht inaktivieren, da durch diese Aktion der Kanal des Gateways inaktiviert wird. Der Standardgateway kann jedoch geändert werden, indem Sie einen anderen Gateway bestimmen. Die Bildschirmansicht **Gateways** gibt Ihren Standardgateway an.

Die erforderlichen Informationen für das Hinzufügen eines Gateways sind abhängig von dem Transporttyp, den der Gateway verwenden soll.

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

Bei Verwendung im Zusammenhang mit Teilnehmerverbindungen, die die Verbindung zwischen zwei bestimmten Community-Teilnehmern definieren, steuern Gateways das erfolgreiche Routing von Geschäftsdokumenten.

Business Integration Connect verwendet Gateways zum Identifizieren der Adressierung sowie der Quellen- und Zielkonfigurationen.

Erstellen Sie einen Gateway wie folgt:

1. Klicken Sie auf **Kontenadmin > Profile > Gateways**.
2. Klicken Sie in der oberen rechten Ecke der Anzeige auf **Erstellen**.
3. Geben Sie einen eindeutigen Namen für den Gateway ein.
4. Wählen Sie den Status des Gateways aus: **Aktiviert** oder **Inaktiviert**. Dokumente, die durch ein Gateway mit inaktiviertem Status geleitet werden, können nicht verarbeitet werden. Wenn Sie einen Gateway inaktivieren, wird damit auch die Teilnehmerverbindung inaktiviert, die dem Gateway zugeordnet ist.
5. Wählen Sie **Online** oder **Offline** aus. Im Offlinemodus werden die Dokumente in einer Warteschlange gehalten, bis der Gateway wieder online gesetzt wird.
6. Geben Sie eine Beschreibung des Gateways ein.
7. Wählen Sie die Transportmethode des Gateways aus (z. B. HTTP 1.1 oder SMTP). Beispiele zu Transportinformationen finden Sie in Tabelle 3.

Anmerkung: Während der Erstellung eines Benutzerexitgateways kann der Benutzer seine eigene zu verwendende Transportmethode erstellen.

Tabelle 3. Erforderliche Informationen für Transportmethoden

Transport	HTTP	HTTPS	FTP	FTPS	Dateiverzeichnis	JMS	SMTP
Transportprotokollversion	Nur 1.1	1.0 oder 1.1	-			-	-
Ziel-URI	Muss übereinstimmen mit http://...	Muss übereinstimmen mit https://...	Muss übereinstimmen mit ftp://...	Muss übereinstimmen mit ftp://...	Muss übereinstimmen mit file://...	Muss übereinstimmen mit file://...	Muss übereinstimmen mit mailto:...
Benutzername für URI	Erforderlich, falls Authen... erforderlich ist.		Erforderlich, falls Authen... erforderlich ist.	Erforderlich, falls Authen... erforderlich ist.			
Kennwort für URI	Erforderlich, falls Authen... erforderlich ist.		Erforderlich, falls Authen... erforderlich ist.	Erforderlich, falls Authen... erforderlich ist.			
Authen.. erforderlich						Optional	Optional

8. Geben Sie den Benutzernamen für den URI ein (nicht erforderlich für JMS). Dieser Schritt ist immer dann erforderlich, wenn eine Authentifizierung erforderlich wird. Bei Verwendung von FTP ist dies die Anmeldung beim FTP-Server eines Teilnehmers.

Wichtig: Wenn Sie JMS als Transportmethode verwenden, stellt der Ziel-URI die URL für den JNDI-Service dar.

Für MQ-JMS lautet das Format des Ziel-URIs wie folgt:
file:/// <Pfad der benutzerdefinierten MQ-JNDI-Bindungen>.

Dieses Verzeichnis enthält die Datei MQ.bindings für dateibasierte JNDI. Beachten Sie die drei Schrägstriche nach 'file'.

9. Geben Sie das Kennwort für den URI ein (nicht erforderlich für JMS). Dieser Schritt ist immer dann erforderlich, wenn eine Authentifizierung erforderlich wird.
10. Wählen Sie **Ja** oder **Nein** aus, um Authentifizierung anzufordern. Diese ist bei JMS oder SMTP häufig erforderlich. In diesem Fall müssen der Benutzername und das Kennwort ebenfalls konfiguriert werden.
11. Wenn Sie JMS nicht als Transportmethode ausgewählt haben, klicken Sie nun auf **Speichern**. Ist JMS die ausgewählte Transportmethode, gehen Sie weiter zum nächsten Schritt.
12. Geben Sie die übrigen erforderlichen Informationen für den ausgewählten Gatewaytyp ein.
13. Klicken Sie auf **Speichern**. Wiederholen Sie diese Schritte, um zusätzliche Gateways hinzuzufügen.

B2B-Funktionalitäten prüfen

Anmerkung: Bei kleineren Installationen kann dieser Prozess vom Hubadmin 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 Dokumentflussdefinitionen festgelegt. Eine Dokumentflussdefinition 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 Dokumentflussdefinitionen:

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.

Dokumentfluss. 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 Dokumentflussdefinition beinhaltet Attribute (d. h. Informationen), die die Funktionalität der Definition festlegen. Ein Attribut besteht aus einer Einzelinformation, die einem bestimmten Dokumentfluss 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 zeigt die Bildschirmansicht **B2B-Funktionalität** an.
 - Wenn neben dem Paket ein Ordner erscheint und "Aktiviert" in der Spalte **Aktiviert** erscheint, wurde diese Funktionalität durch den Hubadmin 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  unter **Quelle festlegen** bzw. **Ziel festlegen** gibt an, dass die Funktionalität für diese Rolle nicht aktiviert ist (d. h. als Quelle oder Ziel oder beides).
 - 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 Dokumentflusskontextes fest. In einem Zweigege-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 Dokumentflussdefinition einer niedrigeren Ebene fest.
4. Klicken Sie auf  zum Anzeigen und (falls erforderlich) Ändern der Dokumentflussdefinitionen auf der unteren Ebene (z. B. Protokoll oder Dokumentfluss). Sie können auch die Attribute einer Dokumentflussdefinition 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

Mit Hilfe von digitalen Zertifikaten wird die Authentizität von Geschäftsdokumententransaktionen zwischen dem Community Manager und den Teilnehmern geprüft. Außerdem werden sie für die Verschlüsselung und Entschlüsselung verwendet. Verwenden Sie diese Bildschirmanzeige zum Bearbeiten vorhandener und zum Hinzufügen neuer digitaler Zertifikate zu Business Integration Connect.

Nachdem Sie die Zertifikate hochgeladen haben, sind sie von der Konsole aus einsehbar.

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 Business Integration Connect gespeichert; sie können nicht vom System entfernt 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 Paares 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.

Beschreibung

Mit Hilfe von digitalen Zertifikaten können sich Unternehmen identifizieren, wenn sie Geschäfte über das Internet abwickeln. Sie werden auf die gleiche Weise verwendet wie eine ID-Karte oder ein Führerschein. Wenn Unternehmen A sein Zertifikat dem Unternehmen B präsentiert, wird dabei die Identität von Unternehmen A durch das Zertifikat bestätigt.

Nachfolgend wird in einem Beispiel dargestellt, wie digitale Zertifikate ausgestellt und verwendet werden.

Unternehmen A und Unternehmen B möchten miteinander Geschäftstransaktionen über das Internet abwickeln. Unternehmen B, das über ein digitales Zertifikat und ein Schlüsselpaar (öffentlicher und privater Schlüssel) verfügt, fordert eine Kopie des Zertifikats und des öffentlichen Schlüssels von Unternehmen A an.

Unternehmen A, das über kein digitales Zertifikat verfügt, kontaktiert eine Zertifizierungsstelle und fordert ein digitales Zertifikat an. Die Zertifizierungsstelle bestätigt die Identität von Unternehmen A und stellt ihm ein digitales Zertifikat aus. Das Zertifikat beinhaltet ein Schlüsselpaar (öffentlicher und privater Schlüssel), die digitale Unterschrift der Zertifizierungsstelle und Informationen, die das Unternehmen A identifizieren (der Name des Unternehmens und die digitale Unterschrift). Das Zertifikat enthält außerdem eine Seriennummer und ein Ablaufdatum.

Unternehmen A und Unternehmen B tauschen ihre digitalen Zertifikate aus. Die beiden Parteien erachten einander nun als vertrauenswürdig und sind bereit, Internettransaktionen miteinander auszuführen.

Im folgenden Abschnitt werden die verschiedenen Typen digitaler Zertifikate beschrieben.

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 Konsole in Business Integration Connect hochladen und eine Kopie an den Hubbetreiber 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 entsprechende Teil mit dem privaten Schlüssel des Verschlüsselungszertifikats muss über die Konsole auf die Ebene des Hubbetreibers hochgeladen werden. Sie müssen den öffentlichen Abschnitt des Teilnehmerzertifikats über die Konsole in Business Integration Connect hochladen und eine Kopie an den Hubbetreiber 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 Hubbetreiber über die Konsole hochgeladen werden.
- **VTP-Zertifikat (Community Manager).** Dieses Zertifikat wird von der Dokumentverwaltung von Business Integration Connect für die Funktion **Community Participant Simulator** verwendet. Das Zertifikat wird in das Dateisystem kopiert und nicht über die Konsole hochgeladen.

In das Dateisystem kopierte VTP-Zertifikate sind für alle Teilnehmer aktiv, die über die Konsole erstellt werden. Diese Zertifikate prüfen unterzeichnete Doku-

mente, die vom Community Participant Simulator empfangen werden. In das Dateisystem kopierte Zertifikate können über die Konsole 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 Stammzertifikats der Zertifizierungsstelle 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 Stammzertifikats der Zertifizierungsstelle verfügen.
- Der Zielsever muss über eine Kopie des Teilnehmerzertifikats verfügen, falls dieses selbst unterzeichnet ist und in den gesicherten Schlüsselspeicher geladen wurde.
- Der Zielsever muss über eine Kopie des Zertifikats der Zertifizierungsstelle verfügen, falls dieses Zertifikat von einer Zertifizierungsstelle authentifiziert wurde und in den gesicherten Schlüsselspeicher geladen wurde.

Ein digitales Zertifikat laden und definieren

1. Klicken Sie auf **Kontenadmin > Profile > Zertifikate**. Das System zeigt die Bildschirmansicht **Zertifikatliste** an.
2. Klicken Sie in der oberen rechten Ecke der Anzeige auf **Zertifikat laden**. Das System zeigt die Bildschirmansicht **Neues Zertifikat erstellen** an.
3. Wählen Sie den Zertifikattyp 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 einen eindeutigen Namen (Beschreibung) für das Zertifikat im Textfeld des Zertifikatsnamens ein.
5. Wählen Sie **Aktiviert** oder **Inaktiviert** aus.
6. Klicken Sie auf **Durchsuchen**, und navigieren Sie zu dem digitalen Zertifikat.
7. Wählen Sie den Gatewaytyp aus, z. B. CPS-Teilnehmer (nur für SSL-Zertifikate). Mit dieser Funktion können Sie ein Zertifikat basierend auf der Zieladresse auswählen.
8. Klicken Sie auf **Hochladen**.

Konsolengruppen erstellen

Verwenden Sie die Funktion **Gruppe**, um eine Gruppe für einen bestimmten Benutzertyp mit spezifischen Konsolenberechtigungen 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 Konsolenfunktionen, 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 Hubadmin oder vom Teilnehmeradmin überschrieben werden.

Achtung: Administrator- und Standardgruppen werden vom System generiert und können nicht bearbeitet oder gelöscht werden. Der Community Operator verfügt über eine zusätzliche Gruppe: Hubadmin.

Erstellen Sie Gruppen wie folgt:

1. Klicken Sie auf **Kontenadmin > Profile > Gruppen**. Das System zeigt die Bildschirmansicht **Gruppenliste** an.
2. Klicken Sie in der oberen rechten Ecke der Anzeige auf **Erstellen**. Das System zeigt die Bildschirmansicht **Gruppendetails** an.
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 Konsolenzugriffs, 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.

Einen 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 zeigt die Bildschirmansicht **Benutzerliste** an.
2. Klicken Sie in der oberen rechten Ecke der Anzeige auf **Erstellen**. Das System zeigt die Bildschirmansicht **Benutzerdetails** an.
3. Geben Sie den Benutzernamen (Anmeldenamen für den Benutzer) ein.
4. Wählen Sie aus, ob Sie den Konsolenzugriff 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 zeigt die Bildschirmansicht **Benutzerliste** an.
2. Klicken Sie auf  zum Anzeigen der Zielbenutzergruppenzugehörigkeiten.
3. Klicken Sie auf  zum Bearbeiten der Benutzergruppenzugehörigkeiten.
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 nach der Bearbeitung auf .

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 zeigt die Bildschirmansicht **Kontaktdetails** an.
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:

Siehe zum Hinzufügen eines Kontakts zu einem vorhandenen Alert den Abschnitt „Einen neuen Kontakt zu einem vorhandenen Alert hinzufügen“ auf Seite 23.

Siehe zur Erstellung eines volumenbasierten Alerts und zum Hinzufügen von Kontakten zu dem Alert den Abschnitt „Einen volumenbasierten Alert erstellen“ auf Seite 19.

Siehe zur Erstellung eines ereignisbasierten Alerts und zum Hinzufügen von Kontakten zu dem Alert den Abschnitt „Einen 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 in Business Integration Connect 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 Dokumentflussvolumen (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 Dokumentflusses erfolgt, den Sie beim Erstellen des Alerts auswählen. Business Integration Connect beachtet nur Dokumente, die den in Ihrem Alert ausgewählten Dokumentfluss 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 Business Integration Connect 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 Bildschirman-sicht **Alert: Ereignisse** anzeigen. 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.

Einen volumenbasierten Alert erstellen

1. Klicken Sie auf **Kontenadmin** > **Alerts**. Das System zeigt die Bildschirmansicht **Alertsuche** an.
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 **Dokumentfluss** aus.

Die Auswahl für Paket, Protokoll und Dokumentfluss muss mit der Auswahl für Paket, Protokoll und Dokumentfluss des Teilnehmers der Quellen-Community übereinstimmen.

7. Wählen Sie eine der drei Optionen für das Volumen aus (**Erwartet**, **Bereich** oder **Nullvolumen**), und gehen Sie weiter zu 8 auf Seite 20:
 - **Erwartet** - Wählen Sie diese Option aus, wenn die Generierung eines Alerts beim Abweichen des Dokumentflussvolumens von einer exakten Menge erfolgen soll. Führen Sie folgende Schritte aus, um einen Alert für das erwartete Dokumentflussvolumen zu erstellen:
 - a. Geben Sie im Textfenster **Volumen** die Anzahl der erwarteten, innerhalb eines in 8 ausgewählten Zeitrahmens zu empfangenden Dokumentflüsse 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 Dokumentflussvolumen abweichen kann, bevor es zu einer Aktivierung des Alerts kommt. Beispiel:
 - Ist das Volumen = 20 und die Abweichung (%) = 10, wird ein Alert durch ein Dokumentflussvolumen kleiner als 18 oder größer als 22 ausgelöst.
 - Ist das Volumen = 20 und die Abweichung (%) = 0, wird ein Alert durch ein beliebiges Dokumentflussvolumen ungleich 20 ausgelöst.
 - **Bereich**. Wählen Sie die Option **Bereich** zum Generieren eines Alerts aus, wenn das Dokumentflussvolumen außerhalb eines Minimum/Maximum-Bereichs liegen soll. Führen Sie folgende Schritte aus, um einen Alert basierend auf einem Wertebereich zu erstellen:
 - a. Geben Sie im Textfenster **Min** die Mindestanzahl der erwarteten, innerhalb eines in 8 ausgewählten Zeitrahmens zu empfangenden Dokumentflüsse ein. Ein Alert wird nur dann ausgelöst, wenn das Dokumentflussvolumen unter diesen Wert sinkt.

- b. Geben Sie im Textfenster **Max** die maximale Anzahl der erwarteten, innerhalb eines in 8 ausgewählten Zeitrahmens zu empfangenden Dokumentflüsse 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 Dokumentflüsse innerhalb eines in 8 ausgewählten Zeitrahmens auftreten.
8. Wählen Sie für den Zeitrahmen (die Häufigkeit), in dem das System das Dokumentflussvolumen zur Alertgenerierung überwacht, entweder **Täglich** oder **Bereich** aus.
 - **Täglich.** Wählen Sie **Täglich** aus, um das Dokumentflussvolumen an einem oder mehreren Tagen in der Woche oder im Monat zu überwachen. Wählen Sie z. B. die Option **Täglich** aus, wenn Sie das Dokumentflussvolumen 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 Dokumentflussvolumen zwischen zwei bestimmten Tagen in der Woche oder im Monat überwachen möchten. Wählen Sie z. B. die Option **Bereich** aus, um das Dokumentflussvolumen 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 Dokumentflussvolumen für die im nächsten Schritt ausgewählten Tage überwachen soll. Beachten Sie, dass bei Auswahl einer Bereichshäufigkeit das Dokumentflussvolumen 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 .
 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 Alert-eigner dargestellt wird, um dem Alert-eigner zugeordnete Kontakte zu erstellen. Mit dieser Funktion können keine Kontakte für Alertteilnehmer durch den Alert-eigner 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 abonnieren.
20. Klicken Sie auf **Speichern**, um den Kontakt zu speichern. Klicken Sie auf **Speichern & Abonnieren**, 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.

Einen ereignisbasierten Alert erstellen

1. Klicken Sie auf **Kontenadmin > Alerts**. Das System zeigt die Bildschirmanzeige **Alertsuche** an.
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 **Jeder Teilnehmer** aus, um den Alert allen Teilnehmern im System zuzuordnen. Wenn Sie eine Alertsuche ausführen und als Alertteilnehmer **Jeder 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 .
 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 Alert-eigner dargestellt wird, um dem Alert-eigner zugeordnete Kontakte zu erstellen. Mit dieser Funktion können keine Kontakte für Alertteilnehmer durch den Alert-eigner 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**.

Einen neuen Kontakt zu einem vorhandenen Alert hinzufügen

1. Klicken Sie auf **Kontenadmin > Alerts**. Das System zeigt die Bildschirmansicht **Alertsuche** an.
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 zum Anzeigen der Alertdetails auf .
5. Klicken Sie zum Bearbeiten der Alertdetails auf .
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 Alert-eigner dargestellt wird, um dem Alert-eigner zugeordnete Kontakte zu erstellen. Mit dieser Funktion können keine Kontakte für Alertteilnehmer durch den Alert-eigner 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 abonnieren.
12. Klicken Sie zum Speichern des Kontakts auf **Speichern**. Klicken Sie auf **Speichern und abonnieren**, um den Kontakt zu speichern und der Liste der Kontakte für diesen Alert hinzuzufügen.
13. Klicken Sie auf **Speichern**.

Eine 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 zeigt die Bildschirmansicht **Adressen** an.
2. Klicken Sie in der oberen rechten Ecke der Bildschirmansicht auf **Erstellen** > **Neu** > **Adresse**. Das System zeigt die Bildschirmansicht **Adressen** an.
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. Verbindungen und Benutzer der Community verwalten: Kontenadmin

Die Funktionen im Modul **Kontenadmin** steuern, wie und von wem IBM WebSphere Business Integration Connect 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 beschäftigen haben, sind Sie mit diesen Funktionen bereits vertraut.

Tabelle 4. Funktionen von Kontenadmin

Welche Funktion möchten Sie verwenden?

„Gateways verwalten“
„Zertifikate verwalten“ auf Seite 26
„Gruppen verwalten“ auf Seite 27
„Benutzer verwalten“ auf Seite 28
„Kontakte verwalten“ auf Seite 29
„Alerts verwalten“ auf Seite 31
„Adressen verwalten“ auf Seite 33

Gateways verwalten

Verwenden Sie die Funktion **Gateways** zum Anzeigen von Gatewayinformationen, 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 einen Gateway inaktivieren, wird damit auch die Teilnehmerverbindung inaktiviert, die dem Gateway zugeordnet ist. Der Gateway

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

1. Klicken Sie auf **Kontenadmin > Profile > Gateways**. Das System zeigt die Bildschirmansicht **Gateway-Liste** an.
2. Klicken Sie auf , und Details zu Gateways anzuzeigen.
3. Klicken Sie auf , um Details zu Gateways zu bearbeiten.
4. Bearbeiten Sie die Informationen wie erforderlich. In der folgenden Tabelle werden die Werte für Gateways beschrieben.

Tabelle 5. Werte in der Gatewayanzeige

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	Der URI der Zieladresse.
Online oder Offline	Im Offlinemodus werden die Dokumente in einer Warteschlange gehalten, bis der 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 den Standardgateway an.

5. Klicken Sie auf **Speichern**.

Standardgateways anzeigen, auswählen oder bearbeiten

1. Klicken Sie auf **Kontenadmin > Profile > Gateways**. Das System zeigt die Bildschirmansicht **Gateway-Liste** an.
2. Klicken Sie in der oberen rechten Ecke der Anzeige auf **Standardgateways anzeigen**. Das System zeigt die Bildschirmansicht **Standardgateway-Liste** an.
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 , um die Details zu den Zertifikaten anzuzeigen. Das System zeigt die Bildschirmansicht **Zertifikatdetails** an.
3. Klicken Sie auf , um das Zertifikat zu bearbeiten.

4. Bearbeiten Sie die Daten wie erforderlich.
5. Klicken Sie auf **Speichern**.

Ein digitales Zertifikat inaktivieren

1. Klicken Sie auf **Kontenadmin > Profile > Zertifikate**. Das System zeigt die Bildschirmansicht **Zertifikatliste** an.
2. Klicken Sie auf , um die Details zu den Zertifikaten anzuzeigen. Das System zeigt die Bildschirmansicht **Zertifikatdetails** an.
3. Klicken Sie auf , 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 zeigt die Bildschirmansicht **Gruppenliste** an.

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  zum Anzeigen einer Liste von Benutzern innerhalb einer Gruppe. Erscheint dieses Symbol nicht, hat die Gruppe keine Mitglieder. Klicken Sie im Untermenü auf **Zugehörigkeiten**.
3. Klicken Sie auf , um die Benutzer innerhalb einer Gruppe zu bearbeiten.
4. Klicken Sie auf die Schaltfläche **Der Gruppe hinzufügen**, um Benutzer der Gruppe zuzuordnen.
5. Klicken Sie auf  zum Speichern und Beenden.

Gruppenberechtigungen anzeigen, bearbeiten und zuordnen

1. Klicken Sie auf **Kontenadmin > Profile > Gruppen**. Das System zeigt die Bildschirmansicht **Gruppenliste** an.
2. Klicken Sie auf , 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 zeigt die Bildschirmansicht **Gruppenliste** an.

2. Klicken Sie auf , um die Gruppendetails (Name und Beschreibung) anzuzeigen. Das System zeigt die Bildschirmansicht **Gruppendetails** an.
3. Klicken Sie auf , 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 eine zusätzliche Gruppe: Hubadmin.

Eine Gruppe löschen

1. Klicken Sie auf **Kontenadmin > Profile > Gruppen**. Das System zeigt die Bildschirmansicht **Gruppenliste** an.
2. Klicken Sie auf , um die Gruppendetails anzuzeigen. Das System zeigt die Bildschirmansicht **Gruppendetails** an.
3. Klicken Sie auf , um die 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 zeigt die Bildschirmansicht **Benutzerliste** an.

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

Tabelle 7. Werte in der Benutzerlistenanzeige

Wert	Beschreibung
Benutzername	Der Anmeldeame für die Konsole.
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 Alertsabskriptionen für diesen Benutzer ebenfalls entfernt.
Anmeldestatus	Bei aktiviertem Status kann sich der Benutzer bei der Konsole anmelden.

2. Klicken Sie auf , um die Benutzerdetails anzuzeigen.
3. Klicken Sie auf , um die Benutzerdetails zu bearbeiten.
4. Bearbeiten Sie die Informationen wie erforderlich. Die folgende Tabelle beschreibt die Werte in der Bildschirmansicht **Benutzerdetails**.

Tabelle 8. Benutzerdetails

Wert	Beschreibung
Benutzername	Der Anmeldename für den Konsolenbenutzer.
Aktiviert	Aktivieren oder Inaktivieren des Konsolenzugriffs.
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 (Universal Time Coordinated). Das System verwendet UTC für seine Zeitzoneberechnungen. 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 Benutzer *Hubadmin* als Superuser für die Systemkonfiguration verantwortlich ist, werden die von ihm ausgewählte Locale und Zeitzone der Community Console zum neuen Standardwert für alle Benutzer der Community Console. 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 Manager 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 Bildschirmansicht **Kontakte** erscheinen.

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	<ul style="list-style-type: none"> • 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 abonnieren.
Subskribiert	Ist diese Option ausgewählt, werden diesem Kontakt einer oder mehrere Alerts zugeordnet. Wird der Kontakt aus dem System entfernt, werden damit auch alle Alertsabonnierungen aus dem System entfernt.
Alertstatus	Wenn der Alertstatus aktiviert ist, empfängt dieser Kontakt alle abonnierten Alerts.

2. Klicken Sie auf , um die Kontaktdetails anzuzeigen. Das System zeigt die Bildschirmansicht **Kontaktdetails** an.
3. Klicken Sie auf , um die Kontaktdetails zu bearbeiten.
4. Bearbeiten Sie die Informationen wie erforderlich. In der folgenden Tabelle werden die 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 abonnierten Alerts. Wählen Sie Inaktivieren aus, wenn dieser Kontakt nicht mehr alle Alerts erhalten soll.
Subskribiert	Dieser Wert wird vom System ausgefüllt.
Sichtbarkeit	<ul style="list-style-type: none"> • 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 abonnieren.

5. Klicken Sie auf **Speichern**.

Einen Kontakt entfernen

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

Alerts verwalten

Die Alerts in Business Integration Connect 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.

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 zeigt die Bildschirmansicht **Alertsuche** an.
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 zeigt die Bildschirmansicht **Alertsuche - Ergebnisse** an.
4. Klicken Sie auf , um die Details eines Alerts anzuzeigen.
5. Klicken Sie auf , 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 zeigt die Bildschirmansicht **Alertsuche** an.
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).

Table 11. Alertsuchkriterien für Teilnehmer

Wert	Beschreibung
Alerttyp	Alert für Umfang oder Ereignis bzw. alle Alerttypen.
Alertname	Der Name des Alerts.
Alertstatus	Aktiviert oder inaktiviert 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.

Table 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	Aktiviert oder inaktiviert 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.

Einen Alert inaktivieren oder aktivieren

1. Klicken Sie auf **Kontenadmin > Alerts**. Das System zeigt die Bildschirmansicht **Alertsuche** an.
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.

Einen Alert entfernen

1. Klicken Sie auf **Kontenadmin > Alerts**. Das System zeigt die Bildschirmansicht **Alertsuche** an.
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 **X**, um den Alert zu 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.

Eine Adresse bearbeiten

1. Klicken Sie auf **Kontenadmin > Profile > Adressen**. Das System zeigt die Bildschirmansicht **Adressen** an.
2. Suchen Sie die zu bearbeitende Adresse, und klicken Sie auf .
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**.

Eine Adresse löschen

1. Klicken Sie auf **Kontenadmin > Profile > Adressen**. Das System zeigt die Bildschirmansicht **Adressen** an.
2. Suchen Sie die zu löschende Adresse, und klicken Sie auf .
3. Bestätigen Sie, dass Sie die Adresse löschen möchten.

Kapitel 4. Ereignisse und Dokumente anzeigen: Anzeigefunktionen

Das Anzeigemodul umfasst folgende Funktionen:

- Ereignisanzeige
- AS1/AS2-Anzeige
- RosettaNet-Anzeige
- Dokumentanzeige
- Gateway-Warteschlange

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

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, des Ereigniscodes und der Ereignisposition suchen. Der Hubadmin 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.

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.

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.

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 Empfänger Prozess), Teilnehmerverbindung, Gatewaytyp, Dokumentstatus, Protokoll, Dokumentfluss 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.

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

Die Anzeigen RosettaNet und AS1/AS2 umfassen zusätzliche Suchkriterien für den Hubadmin. Weitere Informationen finden Sie im Handbuch für Administratoren von WebSphere Business Integration Connect.

Tabelle 14. Anzeigen

Welche Funktion möchten Sie verwenden?	Siehe
Ereignisanzeige	Seite 36
RosettaNet-Anzeige	Seite 41
AS1/AS2-Anzeige	Seite 43
Dokumentanzeige	Seite 43

Ereignisanzeige

Verwenden Sie die Ereignisanzeige zum Anzeigen und Untersuchen von Ereignissen.

Ein Ereignis informiert Sie darüber, dass im System etwas Besonderes aufgetreten 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 15. 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 16. Tasks der Ereignisanzeige

Was möchten Sie tun?	Siehe
Ereignisse suchen.	Seite 37
Ereignisdetails anzeigen.	Seite 38

Ereignisse suchen

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

Ereignisse werden in der Bildschirmansicht **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 17. 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, wie oft Suchergebnisse aktualisiert werden (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 Bildschirmansicht 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 neben dem anzuzeigenden Ereignis auf . Das System zeigt die Ereignisdetails und zugeordneten Dokumente an.
5. Klicken Sie neben dem ggf. anzuzeigenden Dokument auf .
6. Klicken Sie auf , um ggf. das unformatierte Dokument anzuzeigen.
7. Klicken Sie auf  zum Anzeigen von Gültigkeitsfehlern.

Tipp: Ist in der Ereignisanzeige die Kopie eines Dokuments zu sehen, zeigen Sie das zuvor gesendete Originaldokument durch Auswahl in **Dokumentdetails**  an.

AS1/AS2-Anzeige

Verwenden Sie die AS1/AS2-Anzeige zum Anzeigen von gepackten B2B-Transaktionen und B2B-Prozessdetails, die das Übertragungsprotokoll AS1 oder AS2 (Applicability Statement 1 oder 2) verwenden. Sie können die Choreografie 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 weiß der Sender des Dokuments sicher, 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 Dokumentfluss, den Gatewaytyp, den Synchronstatus und die Dokumentdetails anzeigen. Beim Anzeigen der Dokumentdetails werden zusätzliche Dokumentverarbeitungsinformationen dargestellt.

Tasks der AS1/AS2-Anzeige ausführen

Tabelle 18. Tasks der AS1/AS2-Anzeige

Was möchten Sie tun?	Siehe
Nachrichten suchen	Seite 42
Unformatierte Dokumente anzeigen	Seite 43

Nachrichten suchen

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

Tabelle 19. 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 . 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.
Dokumentfluss	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 Bildschirmansicht der 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 neben der anzuzeigenden Nachricht auf . Das System zeigt die Nachricht und die zugeordneten Dokumentdetails an.

Tabelle 20. 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.
Quelleneilnehmer	Der Teilnehmer, der einen Geschäftsprozess einleitet.
Zielteilnehmer	Der Teilnehmer, der den Geschäftsprozess empfängt.
Zeitmarke der Einleitung	Datum und Uhrzeit des Verarbeitungsbegins des Dokuments.
Gatewaytyp	Test oder Produktion. 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: <ul style="list-style-type: none"> • 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  zum Anzeigen des unformatierten Dokuments.

RosettaNet-Anzeige

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 die Choreografie 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 basierend auf spezifischen Suchkriterien dar.

Tasks der RosettaNet-Anzeige ausführen

Tabelle 21. Tasks der RosettaNet-Anzeige

Was möchten Sie tun?	Siehe
RosettaNet-Prozesse suchen.	Seite 42
RosettaNet-Prozessdetails anzeigen.	Seite 42
Unformatierte Dokumente anzeigen.	Seite 43

RosettaNet-Prozesse suchen

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

Tabelle 22. 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 . Test ist nur auf Systemen verfügbar, die den Testgatewaytyp unterstützen.
Protokoll	Für die Teilnehmer verfügbare Protokolle.
Dokumentfluss	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 zeigt die Bildschirmansicht **RosettaNet-Anzeige - Suche** an.
2. Wählen Sie die Suchkriterien aus den Dropdown-Listen aus.
3. Klicken Sie auf **Suchen**. Das System zeigt die Ergebnisse Ihrer Suche an.

Tabelle 23. Dokumentverarbeitungsdetails

Wert	Beschreibung
Teilnehmer	Die in den Geschäftsprozess einbezogenen Teilnehmer.
Zeitmarken	Datum und Uhrzeit des Verarbeitungsbeginns des ersten Dokuments.
Dokumentfluss	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 neben dem anzuzeigenden RosettaNet-Prozess auf . Das System zeigt Details und zugeordnete Dokumente zu dem ausgewählten Prozess an.
5. Klicken Sie neben dem anzuzeigenden Dokument auf . Das System zeigt das Dokument und die zugeordneten Ereignisdetails an.

Unformatierte Dokumente anzeigen

1. Klicken Sie auf **Anzeigen > RosettaNet-Anzeige**. Das System zeigt die Bildschirmansicht **RosettaNet-Anzeige - Suche** an.
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 neben dem anzuzeigenden Prozess auf . Das System zeigt Prozessdetails und zugeordnete Dokumente für den ausgewählten Prozess an.
5. Klicken Sie neben dem Dokumentfluss auf  zum Anzeigen des unformatierten Dokuments.

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 46.
- Die Anzeige des unformatierten Dokuments stellt den HTTP-Header mit dem unformatierten Dokument dar.

Dokumentanzeige

Verwenden Sie die Dokumentanzeige zur Ansicht der einzelnen Dokumente, aus denen ein Prozess besteht. Sie können Suchkriterien zum Anzeigen von unformatierten Dokumenten sowie zugeordneten Dokumentverarbeitungsdetails und Ereignissen verwenden.

Beim Anzeigen von cXML-Dokumentdetails werden alle Dokumente im Zusammenhang mit der ausgewählten Anforderung oder Antwort unter dem Header **Zugeordnete Dokumente** angezeigt. Das Vergrößerungsglassymbol fehlt dann beim ersten Dokument. Das Symbol repräsentiert das aktuell in den oben genannten Details angezeigte Dokument.

Tabelle 24. Tasks der Dokumentanzeige

Was möchten Sie tun?	Siehe
Dokumente suchen	Seite 37
Dokumentdetails, Ereignisse und unformatierte Dokumente anzeigen	Seite 45
Datenprüffehler anzeigen	Seite 46
Die Funktion 'Prozess stoppen' verwenden	Seite 47

Dokumente suchen

1. Klicken Sie auf **Anzeigen > Dokumentanzeige**. Das System zeigt die Bildschirmansicht **Dokumentanzeige - Suche** an.

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

Tabelle 25. Suchkriterien der Dokumentanzeige

Wert	Beschreibung
Startdatum und -zeit	Datum und Uhrzeit der Prozesseinleitung.
Enddatum und -zeit	Datum und Uhrzeit der Fertigstellung des Prozesses.
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 Gatewaytyp	Suchen im sendenden oder empfangenden Dokumentfluss. Produktion oder Test . 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.
Dokumentfluss	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 Filter	Die IP-Adresse des Quellenteilnehmers. 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 anzusehen, wählen Sie **Debugging** aus.

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

Tabelle 26. Mit Hilfe der Dokumentanzeige verfügbare Dokumentinformationen

Wert	Beschreibung
Teilnehmer	Die in den Geschäftsprozess einbezogenen Quellenteilnehmer (Sender) und Zielteilnehmer (Empfänger).
Zeitmarken	Das Datum und die Uhrzeit des Verarbeitungsbeginns und -endes des Dokuments.
Dokumentfluss	Der Geschäftsprozess, der gerade ausgeführt wird.
Gatewaytyp	Test oder Produktion. 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 zeigt die Bildschirmansicht **Dokumentanzeige - Suche** an.
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 zum Anzeigen der Details und Ereignisse eines Dokuments neben diesem Dokument auf . Das System zeigt Prozessdetails und Ereignisse für das ausgewählte Dokument an. Klicken Sie in der Ereignisanzeige auf das Symbol in Form eines blauen Pfeils, um die Ereignisdetails anzuzeigen.
 - Klicken Sie neben dem Dokument auf  zum Anzeigen des unformatierten Dokuments mit HTTP-Header. Das System zeigt dann den Inhalt des unformatierten Dokuments an.

Beim Anzeigen von Dokumentdetails werden folgende Dokumentverarbeitungsinformationen angezeigt:

Tabelle 27. Dokumentverarbeitungswerte, mit der Dokumentanzeige verfügbar

Wert	Beschreibung
Referenz-ID	Die eindeutige Identifikationsnummer, die dem Dokument durch das System zugeordnet wird.
Dokument-ID	Die eindeutige Identifikationsnummer, die dem Dokument durch den Quellenteilnehmer zugeordnet wird.
Dokumentzeitmarke Gateway	Datum und Uhrzeit der Erstellung durch den Teilnehmer.
Verbindungsdokumentfluss	Der Gateway, durch den das Dokument geleitet wird.
Quelle und Ziel	Vom System für ein Dokument ausgeführte Aktionen, um die Kompatibilität des Dokuments mit Geschäftsanforderungen der Teilnehmer untereinander sicherzustellen.
Eingangszeitmarke	Die in den Geschäftsprozess einbezogenen Quellen- und Zielteilnehmer.
Zeitmarke Endstatus	Das Datum und die Uhrzeit, zu der das System das Dokument vom Teilnehmer empfangen hat.
Quellen- und Zielgeschäfts-ID	Das Datum und die Uhrzeit, zu der das Dokument vom System erfolgreich zum Zielteilnehmer weitergeleitet wurde.
Quellen- und Zieldokumentfluss	Die Geschäftsidentifikationsnummer des Quellen- und des Zielteilnehmers, z. B. DUNS.
	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  klicken.

Tipp: Informationen zur Fehlerbehebung bei nicht verarbeiteten Dokumenten finden Sie im Abschnitt „Datenprüffehler anzeigen“ auf Seite 46.

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 28. Farbig markierte Dokumentprüffehler

Wert	Beschreibung
Rot	Erster Gültigkeitsfehler
Orange	Zweiter Gültigkeitsfehler
Grün	Dritter Gültigkeitsfehler

Nachfolgend ist ein Beispiel für verschachtelte XML-Gültigkeitsfehler aufgeführt:

Das Datenelement *ContactInformation* ist der erste Gültigkeitsfehler. Dieser Tag befindet sich an der falschen Position. Die korrekte Position ist direkt nach *PartnerRoleDescription*.

Das Datenelement *FreeFormText* ist der zweite Gültigkeitsfehler. Dieser Tag ist doppelt vorhanden.

Das Datenelement *John* ist der dritte Gültigkeitsfehler. Dieses Feld erfordert mindestens sechs Zeichen.

```

<?xml version="1.0" encoding="UTF-8"?><!DOCTYPE Pip3 A7PurchaseOrderUpdateNotification
SYSTEM "3A7_MS_V02_00_PurchaseOrderUpdateNotification.dtd">
<Pip3A7PurchaseOrderUpdateNotification>
  <fromRole>
  <PartnerRoleDescription>
  <GlobalPartnerRoleClassificationCode>Seller</GlobalPartnerRoleClassificationCode>
  <PartnerDescription>
    <ContactInformation>
      <ContactName>
        <FreeFormText>John</FreeFormText>
        <FreeFormText>John</FreeFormText>
      </contactName>
      <EmailAddress>John@example.com</EmailAddress>
      <telephoneNumber>
        <CommunicationsNumber>+1-234-567-8998-8</CommunicationsNumber>
      </telephoneNumber>
      <fascimileNumber>
        <CommunicationsNumber>+1-234-567-8998-7</CommunicationsNumber>
      </fascimileNumber>
    </ContactInformation>
  <BusinessDescription>
    <GlobalBusinessIdentifier>123456789</GlobalBusinessIdentifier>
    <GlobalSupplyChainCode>InformationTechnology</GlobalSupplyChainCode>
    <BusinessDescription>
    <GlobalPartnerClassificationCode>Carrier</GlobalPartnerClassificationCode>
  </PartnerDescription>
</PartnerRoleDescription>

```

Beispiel für nicht verschachtelte XML-Gültigkeitsfehler:

```
<billTo>
  <PartnerRoleDescription>
    <EmailAddress>frances@sample.com</EmailAddress>
  <ContactInformation>
    <contactName>
      <FreeFormText>String</FreeFormText>
    </contactName>
    <facsimileNumber>
      <CommunicationsNumber>String</CommunicationsNumber>
    </facsimileNumber>
    <telephoneNumber>
      <CommunicationsNumber>+888-999-0000</CommunicationsNumber>
    </telephoneNumber>
  </ContactInformation>
</billTo>
```

Das Datenelement *EmailAddress* ist der erste nicht verschachtelte Gültigkeitsfehler. Dieser Tag befindet sich an der falschen Position. Die korrekte Position ist direkt nach *ContactInformation*

Das Datenelement der Telefonnummer ist der zweite nicht verschachtelte Gültigkeitsfehler. Dieses Feld erfordert zwei weitere Zeichen für den Landescode.

Zum Anzeigen von Gültigkeitsfehlern in einem unformatierten Dokument siehe „Unformatierte Dokumente anzeigen“ auf Seite 43.

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

Die 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. Während dieser Zeit zeigt die Dokumentanzeige das Dokument weiterhin mit dem Status **Im Vorgang** an.

Kapitel 5. Dokumentfluss 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, Dokumentfluss 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 29. Tools

Welche Funktion möchten Sie verwenden?	Siehe
Dokumentanalyse	Seite 49
Dokumentvolumenbericht	Seite 51
Teilnehmerverbindung testen	Seite 53

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 Bildschirmansicht **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 30. 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: <ul style="list-style-type: none">• 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 zeigt die Bildschirmansicht **Dokumentanalyse - Suche** an.
2. Wählen Sie die Suchkriterien aus den Dropdown-Listen aus.

Tabelle 31. Dokumentsuchkriterien

Wert	Beschreibung
Startdatum und -zeit	Datum und Uhrzeit der Prozesseinleitung.
Enddatum und -zeit	Datum und Uhrzeit der Fertigstellung des Prozesses.
Quellteilnehmer	Der Teilnehmer, der den Geschäftsprozess eingeleitet hat (nur Community Manager).
Zielteilnehmer	Der Teilnehmer, der den Geschäftsprozess empfangen hat (nur Community Manager).
Suchen in Gatewaytyp	Suchen im sendenden oder empfangenden Dokumentfluss. 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.
Dokumentfluss	Ein spezifischer Geschäftsprozess.
Sortieren nach	Sortieren der Ergebnisse nach Name des sendenden Teilnehmers oder des empfangenden Teilnehmers.
Aktualisieren	Steuert, wie oft Suchergebnisse periodisch aktualisiert werden (nur Community Manager).
Aktualisierungsrate	Steuert, wie oft Suchergebnisse aktualisiert werden (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 zeigt die Bildschirmansicht **Dokumentanalyse - Suche** an.
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 neben den anzuzeigenden Quellen- und Zielteilnehmern auf . 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 32. 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.

Einen Dokumentvolumenbericht erstellen

1. Klicken Sie auf **Tools > Dokumentvolumenbericht**. Das System zeigt die Bildschirmansicht **Dokumentvolumenbericht - Suche** an.
2. Wählen Sie die Suchkriterien aus den Dropdown-Listen aus.

Tabelle 33. 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 Gatewaytyp	Suchen im sendenden oder empfangenden Dokumentfluss. 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.
Dokumentfluss	Ein spezifischer Geschäftsprozess.
Sortieren nach	Sortieren der Ergebnisse nach diesen Kriterien (Dokumentfluss oder Zieldokumentfluss).
Ergebnisse pro Seite	Anzahl der angezeigten Einträge pro Seite.

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

Einen Dokumentvolumenbericht exportieren

1. Klicken Sie auf **Tools > Dokumentvolumenbericht**. Das System zeigt die Bildschirmansicht **Dokumentvolumenbericht - Suche** an.
2. Wählen Sie die Suchkriterien aus den Dropdown-Listen aus.
3. Klicken Sie auf **Suchen**. Das System zeigt den Bericht an.
4. Klicken Sie zum Exportieren des Berichts auf . Navigieren Sie zum Speichern der Datei zur gewünschten Position.

Anmerkung: Berichte werden als Dateien mit durch Kommas getrennten Werten (.CSV) gespeichert. Dateinamen haben das Suffix “.csv”.

Berichte ausdrucken

1. Klicken Sie auf **Tools > Dokumentvolumenbericht**. Das System zeigt die Bildschirmansicht **Dokumentvolumenbericht - Suche** an.
2. Wählen Sie die Suchkriterien aus den Dropdown-Listen aus.
3. Klicken Sie auf **Suchen**. Das System zeigt den Bericht an.
4. Klicken Sie zum Ausdrucken des Berichts auf .

Teilnehmerverbindung testen

Mit der Funktion **Teilnehmerverbindung testen** können Sie den Gateway oder Web-Server testen. Wenn Sie Community Manager sind, können Sie auch einen bestimmten Teilnehmer auswählen. Bei diesem Test wird eine leere Anforderung POST an einen Gateway oder 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 zeigt die Bildschirmansicht **Teilnehmerverbindung testen** an.
2. Wählen Sie die Testkriterien aus den Dropdown-Listen aus.

Tabelle 34. 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 spezifischste 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 definitiven Satz, wie vom Ursprungsserver verfügbar, dar, 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 einer 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 unauthorisierten 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 den 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 den Gateway oder den übergeordneten Server zum Erfüllen der Anforderung keine rechtzeitige Antwort.
- 505 - HTTP Version Not Supported

Glossar

A

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

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

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 Konsole wie ein Teilnehmer agiert, 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.

Dokumentflussdefinition. Stellt dem System alle notwendigen Informationen zum Empfangen, Verarbeiten und Weiterleiten von Dokumenten zwischen Community-Teilnehmern zur Verfügung. Typen von Dokumentflussdefinitionen sind Paket, Protokoll, Dokumentfluss, 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 den 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 einen bestimmten 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 Konsole zum Ausführen verschiedener Funktionen verfügt.

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 Antwortgeschäftssaktion.

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, Konsolenzugriffsberechtigungen 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 Business Integration Connect, sind Teilnehmer Partner). 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.

Versuchszahl. 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.

Index

A

- Adressen
 - bearbeiten 33
 - Beschreibung 24, 33
 - löschen 33
 - Werte 33
- Aktion, Definition vi, 10
- Aktivität, Definition 9
- Alert aktivieren 32
- Alert inaktivieren 32
- Alerts
 - Alert entfernen 32
 - Alert inaktivieren 32
 - Alertdetails und Kontakte anzeigen oder bearbeiten 31
 - Beschreibung 17, 31
 - ereignisbasierten Alert erstellen 21
 - Kontakt zu vorhandenem Alert hinzufügen 23
 - suchen 31
 - Suchkriterien 32
 - Suchkriterien, Teilnehmer 31
 - volumenbasierten Alert erstellen 19
- Anzeige
 - Alertdetails und Kontakte 31
 - Details zu Gateways 25
 - Gatewayliste 25
 - Gruppenberechtigungen 27
 - Gruppendetails 27
 - Kontaktdetails 30
- Anzeigen
 - AS1/AS2-Anzeige 39
 - Beschreibung 35
 - Dokumentanzeige 43
 - Dokumentdetails 45
 - Dokumente
 - Dokumentanalyse 50
 - Dokumentverarbeitungsdetails, RosettaNet-Anzeige 42
 - Ereignisanzeige 36
 - Ereignisdetails, Ereignisanzeige 38
 - Ereignisse 45
 - Gültigkeitsfehler 46
 - Nachrichtendetails, AS1/AS2-Anzeige 40
 - Prozess- und Ereignisdetails, Dokumentanalyse 51
 - RosettaNet-Anzeige 41
 - RosettaNet-Prozessdetails 42
 - unformatierte Dokumente 43, 45
- AS1/AS2-Anzeige 43
 - Beschreibung 39
 - Nachrichten suchen 40
 - Nachrichtendetails anzeigen 40
 - Paketdetails 41
 - Suchkriterien 40
- Authentifizierung erforderlich 8

B

- B2B-Funktionalitäten, Beschreibung 9
- Bearbeiten
 - Adresse 33
 - Alertdetails und Kontakte 31
 - Details zu Gateways 25

- Bearbeiten (*Forts.*)
 - Gruppendetails 27
 - Kontaktdetails 30
- Bei Konsole anmelden 5, 6
- Benutzer
 - Beschreibung 15, 28
 - neuen Benutzer erstellen 16
 - Werte 28
 - zu Gruppen zuordnen 16
- Benutzername für URI 8
- Berichte ausdrucken
 - Dokumentvolumenbericht 52

C

- Community Console
 - anzeigen 5
 - Benutzer 1
 - Definition vi
 - Verwendung 4
- Community Manager
 - Beschreibung vii, 1
- Community Operator
 - Beschreibung vii, 1
- Community-Teilnehmer
 - Beschreibung vii, 1

D

- Debugereignisse 4, 37
- Digitale Unterschrift, Definition 11
- Digitales VIP-Zertifikat
 - Definition 13
- Dokument
 - Definition vi
 - Details, Dokumentanzeige 44
 - suchen 43
 - Verarbeitungswerte, Dokumentanzeige 45
- Dokumentanalyse
 - Beschreibung 49
 - Dokumente anzeigen 50
 - Prozess- und Ereignisdetails anzeigen 51
 - Suchkriterien 50
- Dokumentanzeige
 - Beschreibung 43
 - Dokumentdetails 44
 - Dokumentverarbeitungswerte 45
 - Suchkriterien 44
 - Werte 40, 41, 44, 45
- Dokumentfluss, Definition 9, 10
- Dokumentprotokoll, Definition vi
- Dokumentstatus
 - Definitionen 49
 - Dokumentvolumenbericht 51
- Dokumentvolumenbericht
 - ausdrucken 52
 - Beschreibung 51
 - Dokumentstatus 51
 - erstellen 52
 - exportieren 52

Dokumentvolumenbericht (*Forts.*)

Suchkriterien 52

DUNS+4 7

DUNS-Nummern 7

E

Entfernen

Alert 32

Kontakt 31

Entschlüsselung

Definition 12

Ereignisanzeige

Beschreibung 36

Ereignisdetails anzeigen 38

Suchkriterien 38

Ereignisse

suchen 37

Suchkriterien 38

Ereignistypen 37

Beschreibungen 37

Ergebniscode

Web-Server 53

Erstellen

Dokumentvolumenbericht 52

ereignisbasierter Alert 21

Gateways 7

neue Gruppe 15

neuer Benutzer 16

volumenbasierter Alert 19

Zertifikatablaufalert 21

Exportieren

Dokumentvolumenbericht 52

F

Fälschungssicherer Herkunftsnachweis, Definition 12

Fehlerereignistyp 37

Fehlerfelder

Gültigkeitsfehler 46

FTP 8

G

Gateways

Beschreibung 25

Details zu Gateways anzeigen oder bearbeiten 25

erstellen 7

Liste anzeigen 25

Werte 26

Geschäftsaktion, Definition vi

Geschäftsprozess, Definition vi

Gruppen 27

Benutzer zuordnen 16

Berechtigungen anzeigen, bearbeiten und zuordnen 27

Beschreibung 27

erstellen 15

Gruppendetails anzeigen oder bearbeiten 27

Gruppenzugehörigkeiten anzeigen 27

löschen 28

Werte 27

Gültigkeitsfehler

anzeigen 46

H

Hilfe viii

Hilfe anfordern viii

HTTP 8

HTTPS 8

Hub-Community

Beschreibung 1

I

Informationsereignistyp 37

J

JMS 8

K

Kennwort für URI 8

Konsole anzeigen 5

Kontakt zu vorhandenem Alert hinzufügen 23

Kontakte

Beschreibung 16, 29

Details 30

Kontakt entfernen 31

Kontaktdetails anzeigen oder bearbeiten 30

Werte 27, 30

Kontenadmin, Funktionen 5, 25

Kritischer Ereignistyp 37

Kundendienst viii

L

Löschen

Adresse 33

Gruppe 28

M

MQ-JMS 9

MQ-JNDI-Bindungen 9

O

Öffentlicher Schlüssel, Definition 12

Onlinehilfe viii

P

Paket, Definition vii, 9

Paketdetails

AS1/AS2-Anzeige 41

Passport Advantage viii

Privater Schlüssel, Definition 12

Protokoll, Definition 9

Prozess, Definition vii

R

RosettaNet, Definition vii

RosettaNet-Anzeige

Beschreibung 41

Dokumentverarbeitung, Details 42

RosettaNet-Anzeige (*Forts.*)
 Prozessdetails anzeigen 42
 Prozesse suchen 42
 Suchkriterien 42

S

Schlüssel, Definition 12
Selbst unterzeichneter Schlüssel, Definition 12
SMTP 8
Softwareunterstützung viii
SSL-Clientzertifikat, Definition 13, 14
Standardgateway
 anzeigen 26
 auswählen 26
 bearbeiten 26
Suchen
 Alerts 31
 Dokumente 43
 Ereignisse 37
 Nachrichten, AS1/AS2-Anzeige 40
 RosettaNet-Prozesse 42
Suchkriterien
 Alerts 32
 AS1/AS2-Anzeige 40
 Dokumentanalyse 50
 Dokumentanzeige 44
 Dokumentvolumenbericht 52
 Ereignisanzeige 38
 RosettaNet-Anzeige 42
Symbole 2

T

Teilnehmer
 Beschreibung 1
Teilnehmerprofil
 anzeigen 6
 bearbeiten 6
 Beschreibung 6
 Werte 7
Teilnehmerverbindung, Definition vi
Teilnehmerverbindung testen
 Beschreibung 53
 Web-Server-Ergebniscode 53
 Werte 53
Tools
 Beschreibung 49
 Dokumentanalyse 49
 Dokumentvolumenbericht 51
 Teilnehmerverbindung testen 53
Transportmethode
 erforderliche Informationen 8
Transportprotokollversion 8
Typografische Konventionen vi

U

Unformatierte Dokumente
 anzeigen 43
Unformatierte ID-Nummern 7
Unternehmenswebsite viii

V

Verschlüsselung
 Definition 11
 Zertifikat, Definition 14
Von Konsole abmelden 5

W

Warnungsereignistyp 37
Web-Server-Ergebniscode 53
Werte
 Adressen 33
 Dokumentanzeige 40, 41, 44, 45
 Gateways 26
 Kontakte 27, 30
 Teilnehmerprofil 7
 Teilnehmerverbindung testen 53

X

X.509-Zertifikat, Definition 12

Z

Zertifikat für digitale Unterschrift, Definition 13
Zertifikat für digitale Unterschriften, Definition 14
Zertifikate
 Ablaufalert, erstellen 21
 Typen und unterstützte Formate 13
Ziel-URI 8
Zuordnen
 Benutzer zu Gruppen 16
 Gruppenberechtigungen 27
 Gruppenzugehörigkeit 27

Bemerkungen

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

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

IBM Europe
Director of Licensing
92066 Paris La Defense Cedex
France

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

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

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

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

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

Die Bereitstellung solcher Informationen kann von bestimmten Bedingungen abhängig sein, in einigen Fällen auch von der Zahlung einer Gebühr.

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

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

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

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

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

COPYRIGHT- UND BERECHTIGUNGSHINWEIS

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

Alle Rechte vorbehalten.

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

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

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

Informationen der Programmierschnittstelle

Informationen der Programmierschnittstelle (soweit vorhanden) unterstützen Sie beim Erstellen von Anwendungssoftware mit Hilfe dieses Programms.

Mit allgemeinen Programmierschnittstellen können Sie Anwendungssoftware schreiben, die die Dienste der durch dieses Programm bereitgestellten Tools übernehmen.

Diese Informationen können jedoch auch Informationen zur Diagnose, Modifikation und Optimierung enthalten. Sie werden Ihnen als Unterstützung beim Debugging Ihrer Anwendungssoftware zur Verfügung gestellt.

Achtung: Verwenden Sie diese Informationen zu Diagnose, Modifikation und Optimierung nicht als Programmierschnittstelle, da Änderungen vorbehalten sind.

Marken und Servicemarken

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

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

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

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

Java und alle Java-basierten Marken sind in gewissen Ländern Marken der Sun Microsystems.

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



WebSphere Business Integration Connect Enterprise Edition und Advanced Edition Version 4.2.2.

IBM