WebSphere® IBM WebSphere Partner Gateway Enterprise Edition e Advanced Edition

Versione 6.2

Guida alla configurazione dell'hub

Nota

Prima di utilizzare queste informazioni e il relativo prodotto, leggere le informazioni presenti in “Informazioni particolari” a pagina 443.

Dicembre 2008

Questa edizione si applica alla versione 6.2, release 0, modifica 0 di IBM WebSphere Partner Gateway Enterprise Edition (numero prodotto 5724-L69) e versione 6.2, release 0, modifica 0 di Advanced Edition (numero prodotto 5724-L68) e a tutti i successivi livelli di modifica e release a meno che non diversamente specificato nelle nuove edizioni.

IBM può utilizzare o distribuire qualsiasi informazione fornita dall’utente in qualsiasi modo ritenga appropriato senza incorrere in obblighi verso l’utente.

Indice

Capitolo 1. Informazioni sul presente manuale

In questo documento, viene descritto in che modo configurare il server (R) WebSphere (R) Partner Gateway.

Destinatari

L'amministratore mantiene WebSphere Partner Gateway. Questa pubblicazione presuppone l'esistenza di due tipi di amministratori:

- Amministratore hub
- Amministratore account

L'amministratore hub è l'utente con privilegi avanzati nella comunità. l'amministratore hub è responsabile della configurazione e gestione della comunità hub globale, inclusa la configurazione del partner e l'attivazione della connessione. L'amministratore account ha accesso ad una serie secondaria di funzioni dell'amministratore hub ed è l'utente amministrativo principale per il partner interno o esterno.

Nota: i partner interni ed esterni possono accedere anche ad alcune funzioni. Benché condivisi, i partner interni ed esterni non sempre possono visualizzare o avere l'accesso agli stessi controlli disponibili per il personale dell'amministratore hub e dell'amministratore account.

Convezioni tipografiche

Questo documento utilizza le seguenti convenzioni.

Tabella 1. Convezioni tipografiche

Convenzione	Descrizione
`Font a spaziatura fissa`	Il testo in questo font indica il testo immesso, i valori degli argomenti o le opzioni del comando, gli esempi e gli esempi di codice, o le informazioni che il sistema stampa sulla schermata (testo del messaggio o prompt).
grassetto	Il testo in grassetto indica i controlli dell'interfaccia utente grafica (ad esempio, i nomi dei pulsanti in linea, i nomi o le opzioni dei menu) e le intestazioni della colonna nelle tabelle e il testo.
corsivo	Il testo in corsivo indica enfasi, titoli di manuali, nuovi termini e termini definiti nel testo, nomi di variabili o lettere dell'alfabeto utilizzate come lettere.
`Font a spaziatura fissa corsivo`	Questo tipo di testo indica nomi variabili nel testo a spaziatura fissa.
DirProdotto	*DirProdotto* rappresenta la directory in cui è installato il prodotto. Tutti i nomi del percorso del prodotto di IBM WebSphere Partner Gateway sono relativi alla directory in cui il prodotto WebSphere Partner Gateway è installato sul sistema.

Tabella 1. Convezioni tipografiche (Continua)

Convenzione	Descrizione
%testo% e *$testo*	Il testo contenuto tra il segno percentuale (%) indica il valore della variabile di sistema o della variabile utente di Windows(R) `text`. La notazione equivalente in un ambiente UNIX (R) è $*text*, che indica il valore della variabile di ambiente UNIX *text*.
Testo colorato sottolineato	Il testo colorato sottolineato indica un riferimento incrociato. Fare clic sul testo per andare all'oggetto del riferimento.
Testo in blu	(Solo nei file PDF) un contorno intorno al testo indica un riferimento incrociato. Fare clic sul testo sottolineato per andare all'oggetto del riferimento. Questa convenzione è l'equivalente per i file PDF della convenzione "testo colorato sottolineato" inclusa in questa tabella.
" " (virgolette)	(Solo nei file PDF) Le virgolette racchiudono i riferimenti incrociati ad altre sezioni del documento.
{ }	In una riga di sintassi, le parentesi graffe racchiudono una serie di opzioni dalle quali l'utente deve effettuare un'unica scelta.
[ ]	In una riga di sintassi, le parentesi quadre racchiudono parametri facoltativi.
< >	Le parentesi angolari circondano i singoli elementi di nome per distinguerli l'uno dall'altro. Ad esempio, *<nome_server><none_connettore>*`tmp.log`.
/ o \	Le barre rovesciate (\) vengono utilizzate come separatori nei percorsi di directory delle installazioni di Windows. Per le installazioni UNIX, sostituire le barre rovesciate con quelle in avanti (/).

Documenti correlati

La serie completa della documentazione disponibile con questo prodotto include tutte le informazioni relative all'installazione, alla configurazione e alla gestione ed utilizzo di WebSphere Partner Gateway Connect Enterprise Edition e Advanced Edition.

È possibile scaricare la documentazione o leggerla direttamente online sul seguente sito Web:

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

Nota: delle informazioni importanti su questo prodotto sono disponibili nelle Technote di supporto tecnico e nei Flash rilasciati dopo la pubblicazione di questo documento. E' possibile reperirle sul sito Web di supporto di WebSphere Business Integration:

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

Selezionare l'area di interesse del componente e consultare la sezione Technotes and Flashes.

Novità nella release 6.2

WebSphere Partner Gateway V6.2 supporta le seguenti nuove funzioni:

- Integrazione con WebSphere Transformation Extender utilizzando il framework di estensione di WebSphere Partner Gateway
- Supporto ISA V4 per la trasmissione e la raccolta del file di log
- Aggiornamento certificato e miglioramenti di configurazione
- Collegamenti ai messaggi di errore con dettagli sui messaggi
- Miglioramenti alla pagina Primi passi di WebSphere Partner Gateway
- Script per aggiornare le impostazioni WebSphere Partner Gateway per la rilocazione e la ridistribuzione
- Capacità di eseguire l'IVT (installation verification test) alla fine dell'installazione del componente WebSphere Partner Gateway
- Capacità di esportare e importare la configurazione completa di WebSphere Partner Gateway
- Supporto per l'aggiornamento automatico per ridurre il lavoro di aggiornamento manuale
- Archiver basato sulla console con pianificatore
- Capacità di eseguire la federazione in una cella esistente di WebSphere Application Server
- Supporto per SFTP (Secure File Transfer Protocol)
- Editor CPP/CPA per ebMS (ebXML Message Service)
- Prestazioni dell'archiver migliorate
- Prestazioni migliorate relative alla velocità di elaborazione di documenti per AS2 e file di grandi dimensioni

Per ulteriori dettagli sulle nuove funzioni 6.2, andare a http://www-01.ibm.com/software/integration/wspartnergateway/about/

Capitolo 2. Introduzione alla configurazione dell'hub

Una volta installato WebSphere Partner Gateway e prima di poter scambiare i documenti tra il partner interno ed i partner esterni, è necessario configurare il server di WebSphere Partner Gateway (l'hub).

In questo capitolo vengono riportate le seguenti sezioni:

Panoramica della configurazione dell'hub

L'obiettivo è consentire al partner interno di inviare un documento o una serie di documenti (in maniera elettronica) ad un partner esterno o ricevere un documento o una serie di documenti da un partner esterno. L'hub gestisce la ricezione dei documenti, la conversione in altri formati (se necessaria) e la consegna degli stessi. L'hub può, inoltre, essere configurato per fornire la protezione per i documenti in entrata e in uscita.

I documenti trasferiti tra l'hub ed un partner sono, di solito, in un formato standard e rappresentano una determinata interazione di business. Ad esempio, un partner potrebbe inviare una richiesta di ordine di acquisto come RosettaNet 3A4 PIP, un documento cXML OrderRequest o uno scambio EDI-X12 con una transazione 850. L'hub converte il documento in un formato che può essere utilizzato da un'applicazione sul partner interno. Allo stesso modo, un'applicazione di back-end del partner interno potrebbe inviare una risposta dell'ordine di acquisto nel proprio formato personalizzato che viene convertito in un formato standard. Quindi il documento convertito viene inviato al partner.

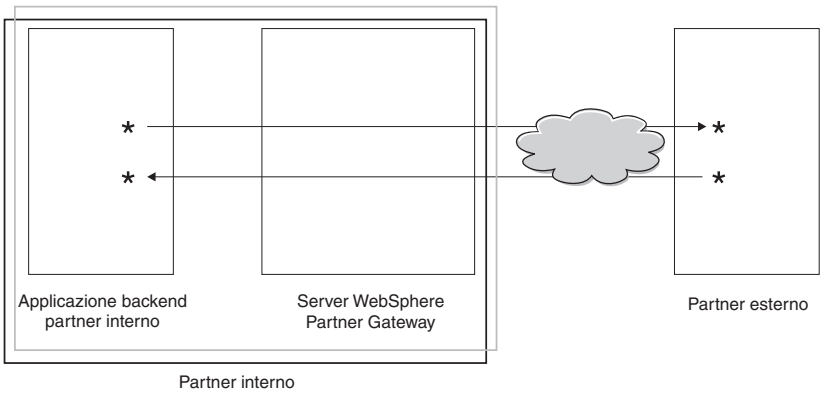


Figura 1. Flusso dei documenti nell'hub

In questa guida, viene descritto il modo in cui configurare l'hub e quindi il modo in cui impostare i partner. È inoltre possibile imparare a configurare la protezione per l'hub.

Notare nella Figura 1 a pagina 5 che il server WebSphere Partner Gateway e l'applicazione di back-end del partner interno sono tutti di proprietà del partner interno. Il partner interno è l'azienda che possiede l'hub. Come descritto nei successivi capitoli, si definisce un profilo per i partner interni come per i partner esterni.

Nota: questo documento mostra come creare le connessioni trasferite dall'applicazione di back-end del partner interno ad una destinazione del partner e da un partner esterno alla destinazione del partner interno. Dopo l'arrivo dei documenti alla destinazione del partner interno, si desidererà forse integrarli con un'applicazione di back-end, come ad esempio WebSphere InterChange Server o WebSphere MQ Broker. Le attività richieste per l'integrazione tra WebSphere Partner Gateway e tali applicazioni di back-end sono definite nel manuale *WebSphere Partner Gateway Enterprise Integration Guide*.

Informazioni necessarie per l'impostazione dell'hub

Per impostare l'hub, è necessario disporre di alcune informazioni sui tipi di scambi in cui parteciperà il partner interno. Ad esempio, sono necessarie le seguenti informazioni:

- Quali tipi di documenti (ad esempio, EDI-X12 o XML personalizzato) il partner interno ed i partner esterni invieranno mediante l'hub?
- Quali tipi di trasporti (ad esempio, HTTP o FTP) il partner interno ed i partner esterni utilizzeranno per inviare i documenti?
- Sarebbe opportuno dividere un documento che arriva sull'hub in più documenti o che singoli documenti vengano raggruppati prima di essere inviati?
- I documenti vengono convertiti prima di essere recapitati?
- I documenti vengono convalidati prima di essere recapitati?
- Un documento sarà controllato per verificare se è un duplicato prima di essere recapitato?
- I documenti vengono codificati o digitalmente firmati o utilizzano altre tecniche di protezione?

Quando queste informazioni vengono stabilite, si è pronti per iniziare la configurazione dell'hub.

Una volta definito l'hub, è possibile definire i partner esterni, mediante le informazioni (come, ad esempio, l'indirizzo IP e i numeri DUNS) fornite dai partner esterni. Come descritto in precedenza, si definisce anche il partner interno come un tipo speciale di partner dell'hub.

Panoramica sui trasporti

I documenti possono essere inviati dai partner a WebSphere Partner Gateway (l'hub) mediante una varietà di trasporti. Un partner può inviare i documenti mediante reti pubbliche utilizzando HTTP, HTTPS, JMS, FTP, FTPS, Script FTP, SMTP o una directory file. Un partner può inviare i documenti mediante una rete VAN (Value Added Network), una rete privata, utilizzando il Trasporto script FTP. È inoltre possibile creare un trasporto personalizzato.

Nota: quando il trasporto directory file viene utilizzato tra un partner e l'hub, l'amministratore deve verificare tutte le problematiche relative alla protezione.

Allo stesso modo, l'hub invia documenti ad applicazioni back-end tramite una varietà di trasporti. I trasporti più comunemente utilizzati tra l'hub e le applicazioni back-end sono HTTP, HTTPS, JMS, Directory di file, Script FTP, FTP SFTP e SMTP.

La Figura 2 mostra i trasporti HTTP, HTTPS, JMS e directory file.

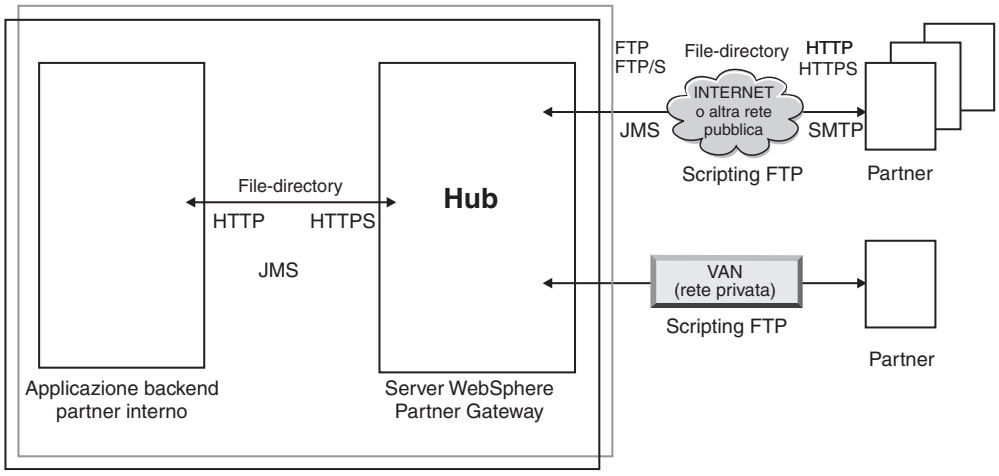


Figura 2. Trasporti più comuni supportati da WebSphere Partner Gateway

Il tipo di trasporto utilizzato per inviare e ricevere i documenti influenza l'impostazione dei destinatari e delle destinazioni. Un *destinatario* è un punto di entrata nell'hub, il punto in cui i documenti inviati dai partner o dalle applicazioni di back-end sono ricevuti sull'hub. Una *destinazione* è un punto di entrata nel computer del partner o nel sistema di back-end, il punto in cui l'hub invia i documenti. Per prepararsi all'utilizzo dei trasporti FTP, FTPS, Script FTP, JMS e directory di file, eseguire la configurazione, come descritto in Capitolo 4, "Preparazione alla configurazione dell'hub", a pagina 33.

Panoramica sulle definizioni del documento

Durante l'impostazione dello scambio di documenti tra i partner esterni ed il partner interno, si specificano vari elementi del documento:

- Il tipo di *impacchettamento* del documento
- Il *protocollo* di business che definisce una classe di documenti che condivide alcune caratteristiche comuni
- Il *tipo di documento* che identifica uno dei documenti forniti dal protocollo di business

L'impacchettamento del documento, il protocollo del documento ed il tipo di documento che costituisce la *definizione del documento*. Utilizzare la definizione del documento fornita dal prodotto di:

- Package: AS
- Protocollo: EDI-X12
- Tipo documento: ISA

Si verifica quando viene ricevuto un documento che è conforme a questa definizione di instradamento. Una volta che l'hub riceve il documento, la fase di spacchettamento del flusso di lavoro in entrata fisso determina che dal documento viene utilizzato l'impacchettamento AS. Si verifica a causa della presenza delle

intestazioni del trasporto, specificate per l'impacchettamento AS. Gli altri tipi di impacchettamento sono rilevati dall'hub in un modo simile, di solito, esaminando le intestazioni del trasporto fornite con il documento. Quando non esistono corrispondenze con alcun tipo di impacchettamento, al documento viene assegnato il tipo di impacchettamento Nessuno. Nel caso dell'impacchettamento AS, gli identificativi di business di provenienza e di destinazione sono ottenuti dalle intestazioni di trasporto del messaggio. Nelle intestazioni di trasporto AS sono riportate anche le altre intestazioni che è possibile specificare se il messaggio sia codificato, compresso o firmato.

Una volta identificato l'impacchettamento, la fase di analisi del protocollo del flusso di lavoro in entrata fisso determina il protocollo ed il tipo di documento. Tale condizione si verifica esaminando il contenuto del messaggio corrente e ricercando le caratteristiche nel documento che identificano il protocollo ed il tipo di documento. La fase del flusso di lavoro per l'analisi del protocollo estrae anche altre informazioni provenienti dal documento a seconda del protocollo in uso.

Una volta definito il documento per utilizzare un particolare package, protocollo e tipo di documento, l'hub può proseguire con l'elaborazione del documento. Quindi, verranno rilevati gli ID di business di provenienza e di destinazione oltre al package, protocollo e al tipo documento. Una volta fornite tali informazioni, l'hub può ricercare una connessione tra i partner mittente e destinatario che dispone del package in entrata, protocollo e del tipo documento.

Una volta rilevata la connessione, l'hub rileva come instradare ed il documento poiché può rilevare le seguenti informazioni aggiuntive:

- Certificati per i partner mittente e destinatario (se richiesto)
- Impostazioni di attributo per l'instradamento mittente e destinatario
- L'azione da eseguire durante l'instradamento del documento
- La mappa di conversione valida (se presente)
- La mappa di convalida valida (se presente)

Impacchettamento

L'impacchettamento fornisce informazioni che riguardano la trasmissione del documento. Come descritto nella sezione precedente, se l'impacchettamento è AS, l'hub utilizza le informazioni contenute nell'intestazione AS per stabilire l'origine e le destinazione per il documento. Se un partner sta inviando un PIP RosettaNet al partner interno, il PIP viene impacchettato come RNIF.

La Figura 3 a pagina 9 mostra i tipi di impacchettamento che è possibile impostare per i documenti trasferiti tra l'hub e un partner esterno e tra l'hub ed un'applicazione di back-end.

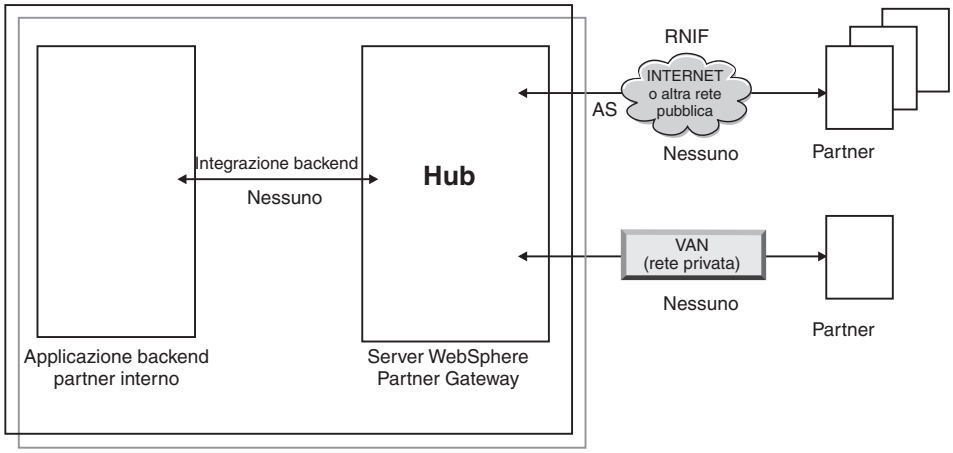


Figura 3. Tipi di impacchettamento del documento

I package sono associati a protocolli specifici. Ad esempio, un partner deve specificare l'impacchettamento RNIF durante l'invio di un documento RosettaNet all'hub.

Integrazione backend: Come descritto in Figura 3, l'integrazione backend è disponibile solo tra l'hub e l'applicazione di back-end. Quando si specifica l'impacchettamento integrazione backend, i documenti inviati dall'hub al sistema back-end hanno informazioni speciali sull'intestazione aggiunte. Similmente, quando un'applicazione invia documenti con l'impacchettamento integrazione backend all'hub, è necessario aggiungere informazioni sull'intestazione. Il package dell'integrazione backend e i requisiti per le informazioni sull'intestazione, sono descritti nel manuale *WebSphere Partner Gateway Enterprise Integration Guide*.

AS: Il package AS è quello più comunemente utilizzato tra i partner e l'hub. Il package AS può essere utilizzato per i documenti che aderiscono agli standard AS1, AS2 e AS3. AS1 è uno standard utilizzato per una trasmissione protetta di documenti su SMTP e AS2 è uno standard utilizzato per la trasmissione protetta di documenti su HTTP o HTTPS. AS3 è un nuovo standard utilizzato per la trasmissione protetta di documenti su FTP o FTPS. I documenti inviati da un partner con l'impacchettamento AS hanno le informazioni sull'intestazione AS1, AS2 o AS3. I documenti inviati ad un partner che prevede le intestazioni AS1, AS2 o AS3 devono essere impacchettati (sull'hub) come AS.

Nessuno: Il package Nessuno consente di inviare e ricevere i documenti tra l'hub ed i partner e tra l'hub ed un'applicazione di back-end. Non viene aggiunta (o non è prevista) alcuna informazione sull'intestazione quando un documento viene impacchettato come Nessuno.

RNIF: Il package RNIF viene fornito sul supporto di installazione. Si carica il package RNIF (insieme ai PIP che si desidera scambiare), come descritto in "documenti RosettaNet" a pagina 107. Il package RNIF consente di inviare i documenti RosettaNet dal partner all'hub o dall'hub al partner.

ebMS: Il meccanismo ebMS (ebXML Message Service) fornisce un metodo standard per trasferire i messaggi di business tra i partner di business ebXML. Fornisce un supporto affidabile per scambiare i messaggi di business senza dipendere dalle soluzioni e dalle tecnologie esclusive. Un messaggio ebXML contiene le strutture per un'intestazione del messaggio (necessarie per l'instradamento e il recapito) ed una sezione di payload.

ebMS fornisce un metodo standard per scambiare i messaggi di business tra i partner di business ebXML. Un messaggio ebXML è una busta di messaggio MIME/Multipart indipendente dal protocollo di comunicazione.

N/A: Alcuni tipi di documenti terminano in WebSphere Partner Gateway o nascono internamente da WebSphere Partner Gateway. Per i tipi di documenti che finiscono in WebSphere Partner Gateway, non è richiesto alcun impacchettamento. I tipi di documenti che hanno origine internamente a WebSphere Partner Gateway non hanno impacchettamento di origine. Pertanto, per tali flussi, l'impacchettamento è specificato come N/A.

Per la maggior parte delle trasmissioni unidirezionali tra un partner esterno ed il partner interno (o viceversa), WebSphere Partner Gateway riceve un documento da un partner esterno e lo invia al partner interno. In WebSphere Partner Gateway, durante la creazione della connessione del partner, specificare il tipo di impacchettamento in cui WebSphere Partner Gateway riceve il documento e il tipo di impacchettamento che WebSphere Partner Gateway utilizza per inviare il documento. Nella Figura 4, un documento impacchettato come AS sta passando da un partner esterno al back-end del partner interno. Il documento viene distribuito alla destinazione partner interno senza intestazioni di trasporto. Nella Figura 4, un'attività è associata allo scambio di documenti.

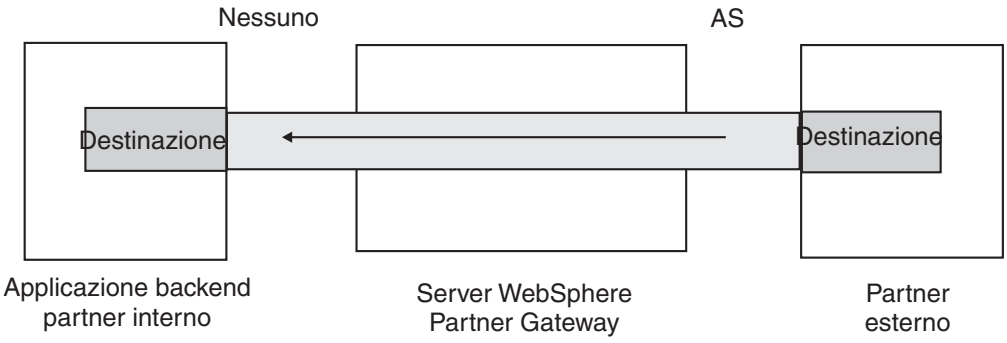


Figura 4. Connessione unidirezionale tipica

Tuttavia, alcuni protocolli richiedono più attività, (come ad esempio la funzione di deenveloping e la conversione) alcune delle quali si verificano come parti dello scambio globale. Ad esempio, se un partner invia uno scambio EDI all'hub, per l'eventuale distribuzione al partner interno, lo scambio viene sottoposto a deenveloping e le singole transazioni EDI vengono elaborate. Lo scambio EDI originale ha un package associato durante l'invio dal partner. Tuttavia, poiché lo scambio stesso non viene consegnato al partner interno (viene sottoposto a deenveloping nell'hub e non si verifica alcuna elaborazione ulteriore dello scambio), l'impacchettamento dello scambio non è valido. Quando si configura l'interazione per l'operazione di deenveloping, di conseguenza, si immette un package sul lato dell'invio ma si specifica N/A per il lato della ricezione.

Il processo per impostare le definizioni del documento richieste per uno scambio EDI è descritto nel Capitolo 10, "Configurazione dei flussi di documenti EDI", a pagina 163.

Protocolli

I protocolli forniti con il sistema sono:

- Binario

Il protocollo Binario può essere utilizzato con package AS, Nessuno e Integrazione backend. Un documento binario non contiene dati sull'origine o la destinazione del documento.

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

  Questi protocolli EDI possono essere utilizzati con package AS o Nessuno. Come descritto in " N/A" a pagina 10, se la transazione EDI o lo scambio che nasce dall'hub o termina all'hub, specificare N/A per il package. X12 e EDIFACT sono standard EDI utilizzati per lo scambio dei dati. EDI-Consent fa riferimento ai tipi di contenuto specificati nella specifica EDI-Consent.
- servizio Web

  Le richieste del servizio Web possono essere utilizzate solo con il package Nessuno.
- cXML

  I documenti cXML possono essere utilizzati solo con il package Nessuno.
- XMLEvent

  XMLEvent è un protocollo speciale utilizzato per fornire la notifica dell'evento per i documenti che fluiscono a e dall'applicazione di back-end. Può essere utilizzato solo con il package Integrazione backend. Questo protocollo è descritto nel manuale *WebSphere Partner Gateway Enterprise Integration Guide*.

Quando si caricano package RNIF, si ottengono anche i protocolli associati (RosettaNet e RNSC). RosettaNet (che è il protocollo utilizzato tra il partner e l'hub) è associato al package RNIF. RNSC (protocollo utilizzato tra l'hub e l'applicazione di back-end del partner interno) è associato al package Integrazione backend.

Per la conversione di transazioni EDI o di documenti XML o ROD, il client DIS (Data Interchange Service) o WTX Design Studio viene utilizzato per creare le mappe di conversione.

Nel client DIS (Data Interchange Service), i dizionari vengono definiti per il protocollo associato a questa conversione. Un dizionario contiene informazioni su tutte le definizioni dei documenti EDI, i segmenti, gli elementi dei dati compositi e gli elementi di dati che costituiscono uno standard EDI. Le definizioni dei documenti di origine per EDI sono fornite da WDI, mentre per ROD e XML, è necessario crearle nel client DIS. Dalla versione 6.2, le mappe standard e di conversione possono essere compilate separatamente. Per informazioni dettagliate su un determinato standard EDI, fare riferimento ai manuali degli standard EDI appropriati. Per informazioni sul client DIS (Data Interchange Service), consultare il manuale *WebSphere Partner Gateway Mapping Guide* o la guida in linea fornita con il client DIS (Data Interchange Service).

Nota: gli ID mittente e destinatario devono essere parte della definizione di documento ROD associata alla mappa di conversione. Le informazioni necessarie per stabilire il tipo di documento ed i valori del dizionario devono essere presenti anche nella definizione del documento. Assicurarsi che lo specialista della mappatura del client Data Interchange Services sia a conoscenza dei requisiti, quando si crea la mappa di conversione.

È possibile creare protocolli personalizzati per definire esattamente il modo in cui si desidera strutturare un documento. Per i documenti XML, è possibile definire un formato XML, come descritto in "Elaborazione documento XML personalizzato" a pagina 151.

Tipo di documento

Il documento può avere vari formati. I tipi di documenti forniti dal prodotto e i relativi protocolli associati sono:

- Binario, che può essere utilizzato con il protocollo binario.
- ISA, che rappresenta lo scambio X12 (busta) e che è associato al protocollo EDI-X12.
- BG, che rappresenta la busta EDI Consent e che è associata al protocollo EDI-Consent
- UNB, che rappresenta la busta EDIFACT e che è associata al protocollo EDI-EDIFACT
- XMLEvent, che può essere utilizzato con il protocollo XMLEvent

Nel seguente elenco vengono descritti altri tipi di documenti e l'origine della definizione:

- PIP RosettaNet PIP (che si carica dal supporto di installazione), che può essere utilizzato con il protocollo RosettaNet
- Un servizio Web (che si carica come un file WSDL), che può essere utilizzato con il protocollo di servizio Web
- Un documento cXML (che si crea specificando il tipo di documento cXML)
- Una transazione EDI specifica, che si importa dal client Data Interchange Services
- Un documento ROD (record-oriented-data) o XML, che si importa dal client Data Interchange Services

È anche possibile creare i propri tipi di documenti, come descritto nella sezione "Elaborazione documento XML personalizzato" a pagina 151.

Panoramica sull'elaborazione del documento

Prima di iniziare a configurare l'hub, è utile revisionare i componenti di WebSphere Partner Gateway e il modo in cui questi vengono utilizzati per elaborare i documenti.

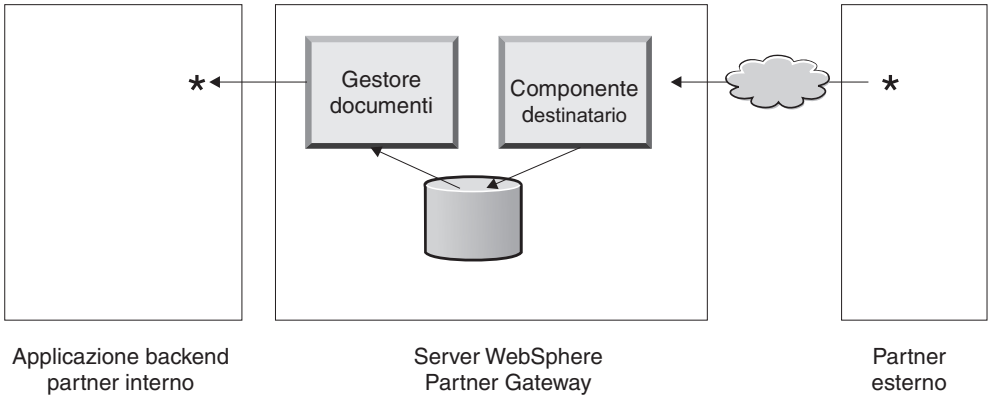


Figura 5. Componenti Destinatario e Gestore documenti

La Figura 5 è un esempio del modo in cui un documento viene inviato da un partner, ricevuto sull'hub, elaborato sull'hub ed inviato all'applicazione di back-end del partner interno.

Nota: a scopo illustrativo, le figure riportate in questo documento mostrano un Destinatario e un Gestore documenti, installati sulla stessa macchina server. (Il terzo componente, ovvero la console, non è illustrata, che costituisce l'interfaccia per WebSphere Partner Gateway.) È possibile avere più occorrenze di questi componenti e possono essere installate su server differenti. Tutti i componenti devono utilizzare lo stesso file system comune. Per informazioni sulle diverse topologie che è possibile utilizzare per impostare WebSphere Partner Gateway, consultare il manuale *WebSphere Partner Gateway Guida all'installazione*.

Un documento viene ricevuto in WebSphere Partner Gateway dal componente Destinatario. Il Destinatario è responsabile del monitoraggio dei trasporti per i documenti in entrata, del richiamo dei documenti in arrivo, dell'esecuzione di determinate elaborazioni e dell'accodamento di essi in modo tale che il Gestore documenti possa richiamarli.

Le istanze dei destinatari sono specifiche al trasporto. Impostare un destinatario per ciascuna tipologia di trasporto che l'hub supporta. Ad esempio, se i partner inviano i documenti su HTTP, impostare il destinatario HTTP per riceverli.

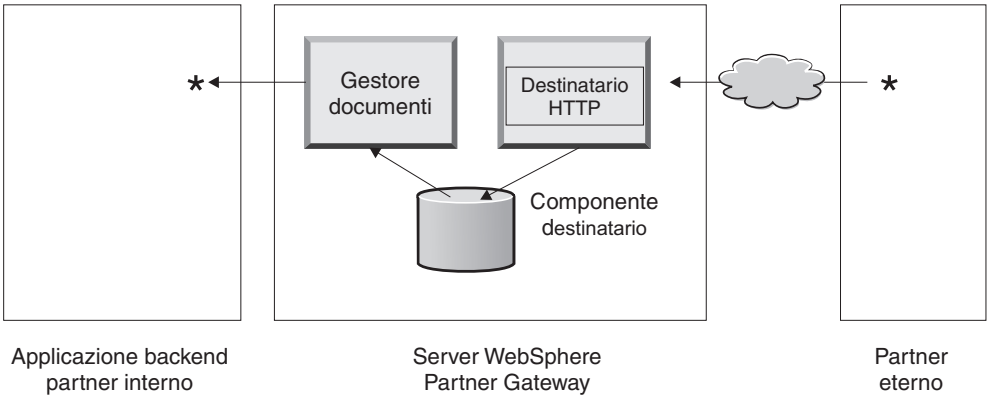


Figura 6. Destinatario HTTP

Se l'applicazione di back-end del partner interno invia i documenti su JMS, impostare un destinatario JMS sull'hub per riceverli.

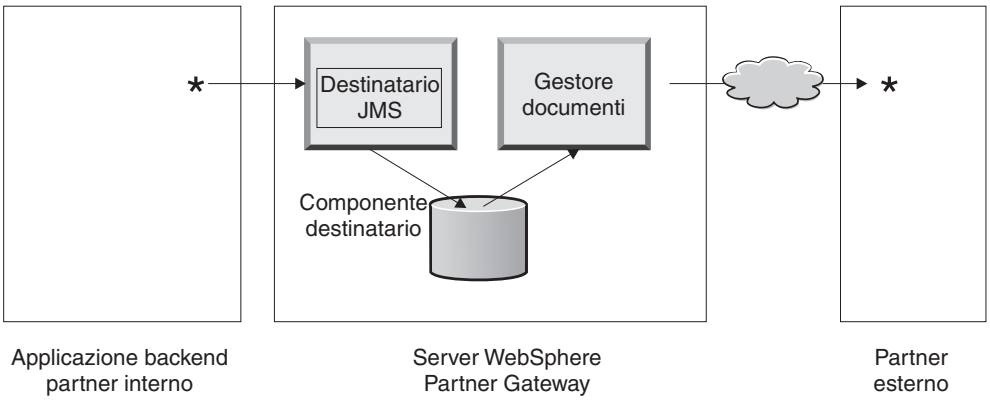


Figura 7. Destinatario JMS

Come descritto nella sezione "Panoramica sui trasporti" a pagina 6, WebSphere Partner Gateway supporta diversi trasporti, ma è anche possibile caricare il proprio

trasporto definito dall'utente per definire un destinatario (come descritto nella sezione " Impostazione di un destinatario per un trasporto definito dall'utente" a pagina 70).

Il destinatario invia il documento ad un file system condiviso. Per più documenti presenti in un singolo file (ad esempio, documenti XML o ROD o scambi EDI inviati insieme), il destinatario suddivide i documenti o gli scambi prima di inviarli al file system condiviso. Il componente Gestore documenti richiama il documento dal file system e determina le informazioni di instradamento e le eventuali conversioni necessarie.

Ad esempio, il partner interno potrebbe inviare un documento EDI-X12 con il package Nessuno all'hub, per il recapito ad un partner che attende il documento EDI-X12 con il package AS2. Il partner fornisce l'URL HTTP dove è necessario recapitare il documento con impacchettamento AS2 e il Gestore documenti impacchetta il documento nel modo previsto dal partner. Il Gestore documenti utilizza la configurazione della destinazione per tale partner (che deve essere stato impostato per l'URL HTTP dove il partner prevede di ricevere i documenti AS2) per inviare il documento al partner.

Configurazione dei componenti di elaborazione del documento con gli handler

Questa sezione descrive, in maniera dettagliata, i componenti di WebSphere Partner Gateway e presenta i vari punti su cui è possibile (oppure è necessario) modificare il comportamento fornito dal prodotto dei componenti per elaborare un documento di business.

Utilizzare *gli handler* per modificare il comportamento fornito dal prodotto di destinatari, destinazioni, fasi del flusso di lavoro fisso ed azioni. Esistono due tipi di handler, quelli forniti da WebSphere Partner Gateway e quelli che sono definiti dall'utente. Per informazioni sulla creazione di handler, consultare il manuale *WebSphere Partner Gateway Programmer Guide*.

Una volta creato un handler, viene caricato per renderlo disponibile. Si caricano solo gli handler definiti dall'utente. Gli handler forniti da WebSphere Partner Gateway sono già disponibili.

Le seguenti sezioni descrivono i punti di elaborazione su cui è possibile specificare gli handler.

Destinatari

I destinatari hanno tre *punti di configurazione* per i quali è possibile specificare gli handler--Preelaborazione, SyncCheck (Controllo sincrono) e Postelaborazione.

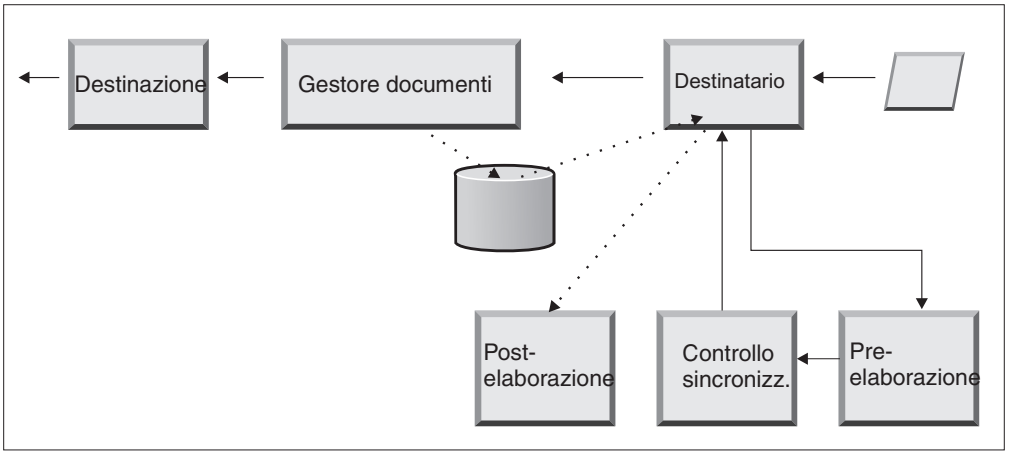


Figura 8. Punti di configurazione del destinatario

L'elaborazione si verifica nel seguente ordine:

1. Il componente destinatario richiama le fasi Preelaborazione e SyncCheck (controllo sincrono) una volta ricevuto il documento.
2. Viene quindi chiamato il Gestore documenti per elaborare il documento.
3. In caso di flussi sincroni, il Gestore documenti fornisce una Risposta sinc. Il componente destinatario quindi richiama la fase Postelaborazione con la risposta restituita dal Gestore documenti.

Le fasi sono descritte nelle seguenti sezioni:

- Preelaborazione

  La fase di Preelaborazione, di solito, viene utilizzata per qualsiasi elaborazione del documento che deve essere completata prima che il documento possa essere elaborato dal Gestore documenti. Ad esempio, se sono ricevuti più documenti ROD in un singolo file, configurare l'handler splitter ROD alla definizione del destinatario. Lo splitter ROD, con gli altri due splitter forniti dal prodotto, è disponibile al momento dell'impostazione di un destinatario. Se si creano ulteriori handler per la fase Preelaborazione, anche questi handler diventano disponibili.

  Per le informazioni sulla configurazione del punto di configurazione Preelaborazione, consultare la sezione " Preelaborazione" a pagina 72.

- SyncCheck

  SyncCheck consente di determinare se WebSphere Partner Gateway deve elaborare il documento in modo sincrono o asincrono. Ad esempio, in caso di documenti AS2 ricevuti su HTTP, determina se un MDN (message disposition notification) deve essere restituito in modo sincrono sulla stessa connessione HTTP. WebSphere Partner Gateway fornisce diversi handler per la verifica sincrona. L'elenco di handler varia, a seconda del trasporto associato al destinatario.

  SyncCheck (controllo sincrono) si applica solo a quei trasporti (come ad esempio HTTP, HTTPS e JMS) che supportano la trasmissione sincrona.

  Nota: per i documenti AS2, cXML, RNIF o SOAP che saranno utilizzati negli scambi sincroni, è necessario specificare l'handler SyncCheck associato al destinatario HTTP o HTTPS.

  Per informazioni sulla configurazione del punto di configurazione SyncCheck, fare riferimento a " SyncCheck" a pagina 75.

- Postelaborazione

  La fase Postelaborazione consente di elaborare il documento di risposta che l'hub invia come risultato di una transazione sincrona.

  Per le informazioni sulla configurazione del punto di configurazione Postelaborazione, consultare la sezione " Postelaborazione" a pagina 76.

Gestore documenti

I documenti ricevuti dai destinatari sono raccolti dal Gestore documenti dal file system comune per ulteriore elaborazione. Il Gestore documenti utilizza le connessioni del partner per instradare i documenti. Tutti i documenti che utilizzano il Gestore documenti passano attraverso una serie di flussi di lavoro: flusso di lavoro in entrata fisso, flusso di lavoro variabile e flusso di lavoro in uscita fisso. Alla fine del flusso di lavoro in entrata, la connessione del partner viene determinata. La connessione del partner specifica l'azione da eseguire su questo documento. Una volta eseguito il flusso di lavoro variabile, il Gestore documenti esegue il flusso di lavoro in uscita fisso su questo documento.

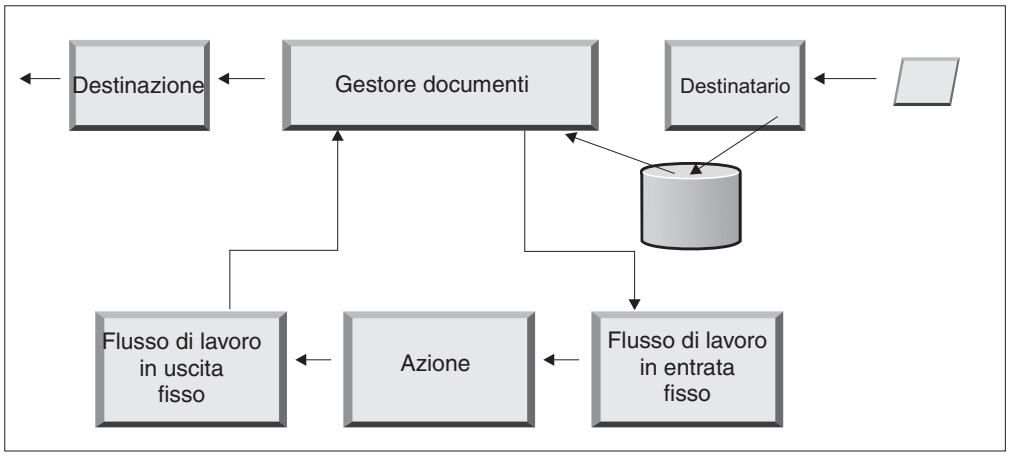


Figura 9. Flussi di lavoro fissi e azioni

La Figura 9 illustra il percorso di un documento PIP RosettaNet PIP o di un servizio Web. Alcuni documenti, tuttavia, richiedono molti flussi configurati. Ad esempio, uno scambio EDI può consistere di più transazioni. Il primo flusso utilizza un'azione per eseguire l'operazione di deenveloping dell'insieme di singole transazioni. Ciascuna di queste transazioni viene quindi reintrodotta ed elaborata in un flusso configurato.

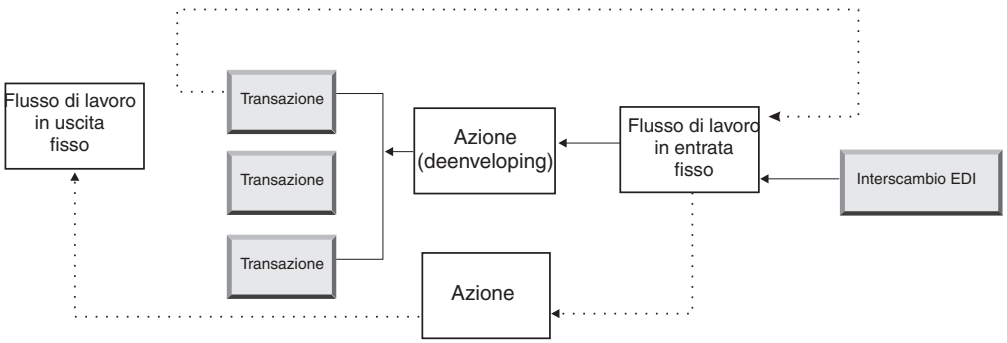


Figura 10. Flussi di lavoro fissi ed azioni per uno scambio EDI

Flusso di lavoro fisso in entrata

Il flusso di lavoro fisso in entrata consiste di un insieme standard di passaggi di elaborazione che fluiscono nel Gestore documenti da un Destinatario. Il flusso di lavoro è fisso perché il numero e i tipi di passaggi è sempre lo stesso. Una volta che l'utente termina, è possibile fornire handler personalizzati per l'elaborazione di questi passaggi: lo spacchettamento del protocollo e l'elaborazione del protocollo. L'ultima fase del flusso di lavoro fisso in entrata effettua una ricerca della connessione del partner, che determina il flusso di lavoro variabile eseguito per questo documento di business.

Se, ad esempio, viene ricevuto un messaggio AS2, il messaggio viene decodificato e gli ID del mittente e del destinatario vengono recuperati. I passaggi del flusso di lavoro fisso in entrata convertono il documento AS2 nel testo normale per una successiva elaborazione da parte di WebSphere Partner Gateway ed estraggono le informazioni per stabilire l'azione per il messaggio.

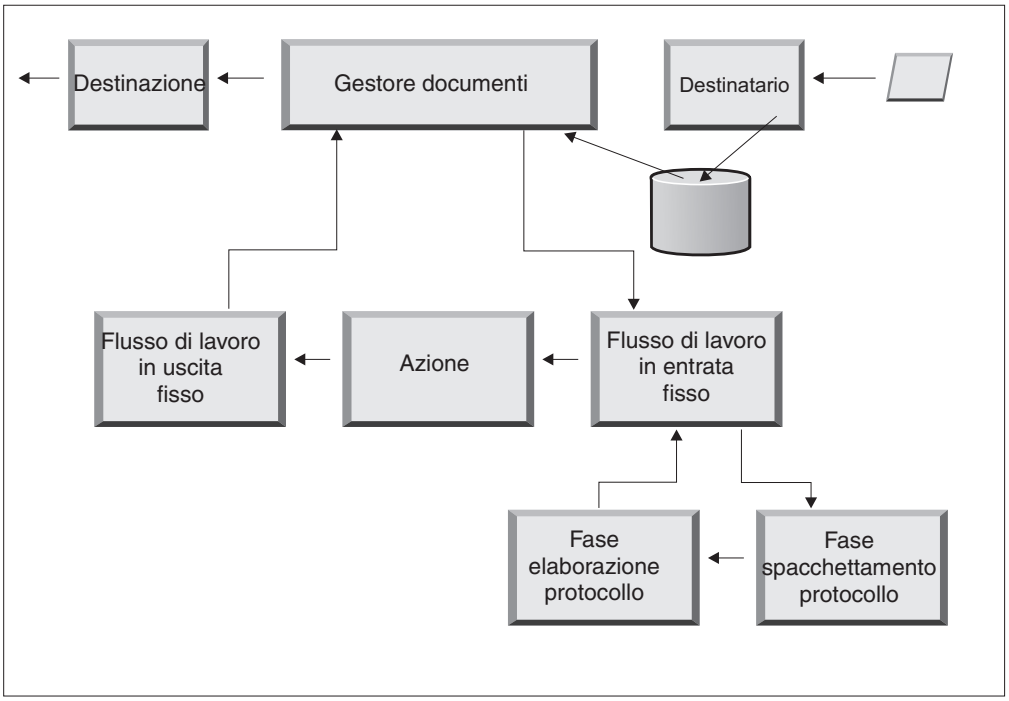


Figura 11. Procedure del flusso di lavoro fisso in entrata

Spacchettamento protocollo: Durante la fase di spacchettamento del protocollo, un documento viene spacchettato in modo che possa essere elaborato ulteriormente. Questo processo può includere la decodifica, la decompressione, la verifica della firma, l'estrazione delle informazioni di instradamento, l'autenticazione dell'utente o l'estrazione delle parti del documento.

WebSphere Partner Gateway fornisce gli handler per l'impacchettamento RNIF, AS, Integrazione backend e Nessuno. Se sono necessari handler per altri protocolli di impacchettamento, possono essere sviluppati come uscite utente. Per informazioni sulla scrittura di uscite utente, consultare il manuale *WebSphere Partner Gateway Programmer Guide*.

Non è possibile modificare la fase Spacchettamento protocollo, tuttavia è possibile aggiungere una logica di business alla fase aggiungendo gli handler.

Per informazioni sulla configurazione di questa fase, consultare la sezione “Configurazione dei flussi di lavoro fissi” a pagina 80.

Fase Elaborazione protocollo: La fase Elaborazione protocollo richiama le informazioni specifiche del protocollo, che potrebbero includere l’analisi del messaggio per determinare le informazioni di instradamento (come, ad esempio, l’ID mittente e l’ID destinatario), le informazioni sul protocollo e le informazioni sul tipo del documento. WebSphere Partner Gateway fornisce l’elaborazione di una varietà di protocolli, come descritto in “ Handler elaborazione protocollo” a pagina 81. L’elaborazione di altri protocolli—ad esempio, CSV (valore separato da virgola)—può essere fornita con una uscita utente.

Non è possibile modificare l’elaborazione del protocollo; tuttavia, è possibile aggiungere una logica di business aggiungendo gli handler.

Per informazioni sulla configurazione di questa fase, consultare la sezione “Configurazione dei flussi di lavoro fissi” a pagina 80.

È possibile utilizzare l’handler predefinito che si applica al protocollo per il documento o è possibile specificare un diverso handler per le procedure del flusso di lavoro fisso per lo spacchettamento e l’elaborazione del protocollo.

Azioni

La fase successiva nell’elaborazione della sequenza si verifica in base alle azioni che sono state impostate per lo scambio del documento. Le azioni consistono in un numero variabile di procedure che possono essere effettuate sul documento. Gli esempi di azioni sono la convalida di un documento (in modo che sia conforme ad un particolare gruppo di regole) e la conversione del documento nel formato richiesto dal destinatario.

Se il documento non ha fasi specifiche richieste, è possibile utilizzare l’azione Pass Through fornita dal prodotto, che non apporta modifiche al documento.

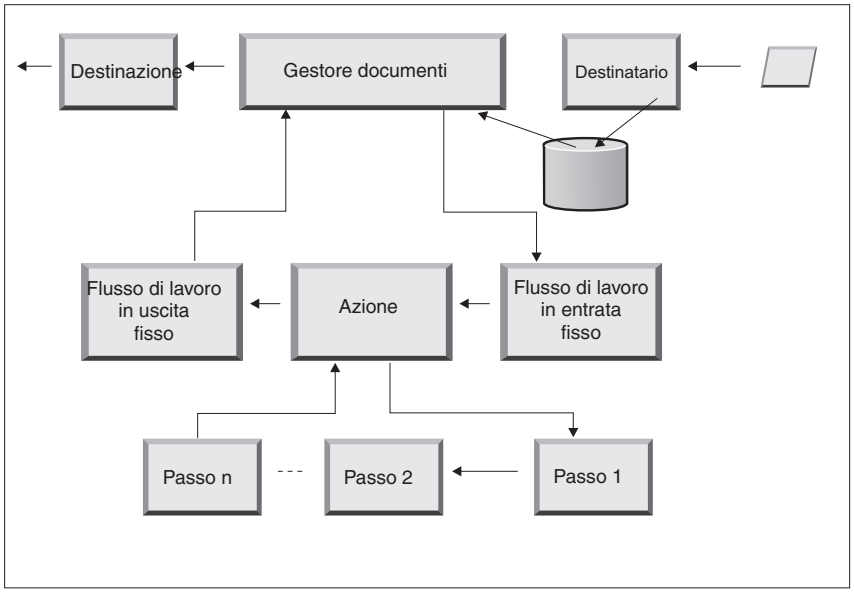


Figura 12. Fasi dell’Azione

Non è possibile modificare un'azione fornita dal prodotto. Tuttavia, è possibile creare un'azione (e aggiungere gli handler all'elenco configurato) o copiare un'azione fornita dal prodotto e quindi modificare l'elenco di handler.

Per le informazioni sulla creazione o sulla copia di un'azione fornita dal prodotto o sulla configurazione di un'azione definita dall'utente, consultare la sezione "Configurazione di azioni" a pagina 82.

Flusso di lavoro fisso in uscita

Il Flusso di lavoro fisso in uscita è formato da una procedura —lo spacchettamento del documento con le informazioni del protocollo. Ad esempio, se un documento è stato impostato per essere ricevuto da un'applicazione di back-end mediante l'impacchettamento Integrazione di backend, determinare informazioni sul''intestazione sono state aggiunte al documento prima che siano trasferite alla destinazione.

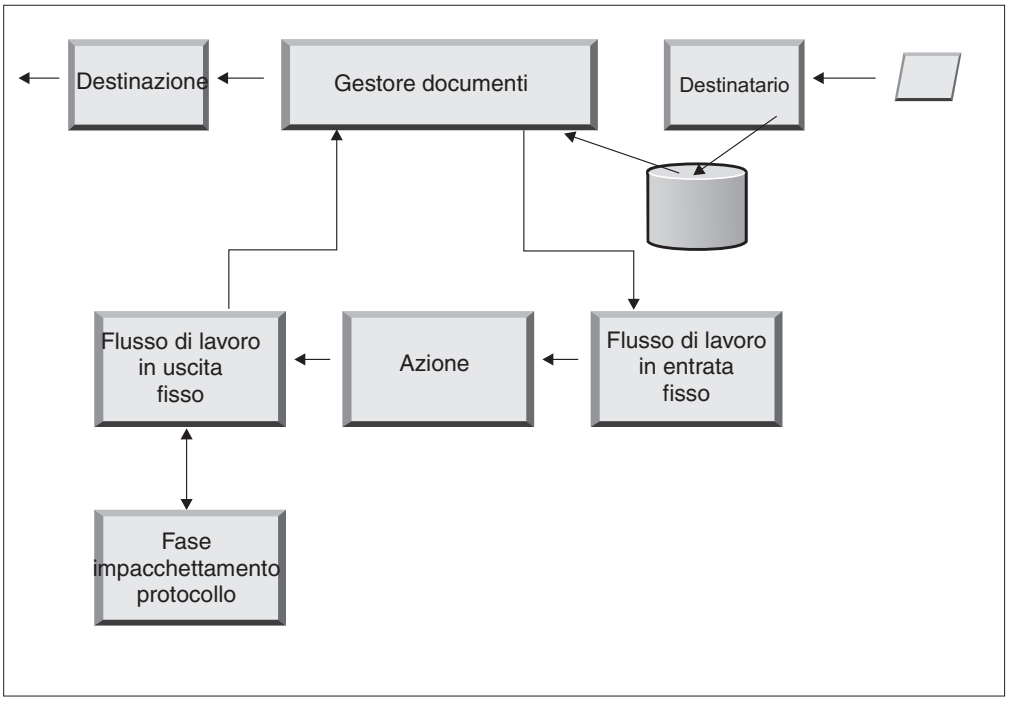


Figura 13. Procedura del flusso di lavoro fisso in uscita

WebSphere Partner Gateway fornisce handler per una varietà di package e protocolli, come descritto in "Flusso di lavoro in uscita" a pagina 81. Se sono necessari handler per altri tipi di impacchettamento, possono essere sviluppati come fasi di uscita utente. Di solito, questi passaggi impiegano uno o più dei seguenti processi:

- Assemblaggio e sviluppo
- Codifica
- Firma
- Compressione
- Configurazione delle intestazioni di trasporto specifiche del protocollo di business

Non è possibile modificare la procedura di Impacchettamento del protocollo, tuttavia è possibile aggiungere una logica di business alla procedura aggiungendo gli handler.

Per informazioni sulla configurazione di questa procedura del flusso di lavoro, fare riferimento a “Configurazione dei flussi di lavoro fissi” a pagina 80.

Destinazioni

Le destinazioni sono state configurate nella console per ogni partner a cui è necessario inviare i messaggi. La configurazione di una destinazione include il trasporto che sarà utilizzato per inviare i messaggi e la configurazione richiesta per inviarla come URL per il processo di ricezione del partner.

Una volta inviato il documento da parte del Gestore documenti, esso viene inviato mediante una destinazione al destinatario previsto. La destinazione dispone di due punti di configurazione—Preelaborazione e Postelaborazione.

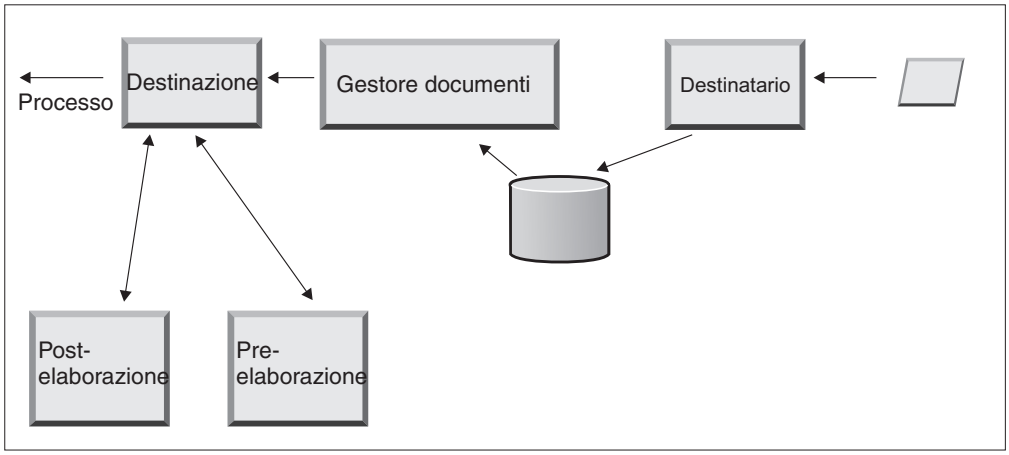


Figura 14. Punti di configurazione della destinazione

- Preelaborazione

  La fase Preelaborazione influenza l’elaborazione di un documento che esso sia inviato al destinatario. Il processo è l’invio corrente del documento. Non viene fornito alcun handler dal sistema per configurare la fase Preelaborazione; tuttavia, è possibile caricare un handler definito dall’utente.
- Postelaborazione

  La fase Postelaborazione agisce sui risultati della trasmissione del documento (ad esempio, sulla risposta ricevuta dal destinatario durante una trasmissione sincrona). Non viene fornito alcun handler dal sistema per configurare la fase Postelaborazione; tuttavia, è possibile caricare un handler definito dall’utente.

Per le informazioni sulla configurazione delle fasi Preelaborazione e Postelaborazione, consultare la sezione “Configurazione degli handler” a pagina 232.

Panoramica della configurazione dell'hub

Una volta analizzate le esigenze di business, come descritto nella sezione "Informazioni necessarie per l'impostazione dell'hub" a pagina 6, impostare l'hub e creare i profili del partner. In questa sezione, viene fornita una panoramica di livello superiore delle attività coinvolte.

Nota: durante la configurazione dell'hub, consultare il manuale *WebSphere Partner Gateway Administrator Guide* per informazioni sui codici di eventi e per dei suggerimenti per la risoluzione dei problemi.

Configurazione dell'hub

Informazioni su questa attività

Come amministratore hub, si eseguono le seguenti attività per configurare l'hub:

1. Eseguire la configurazione preliminare (se richiesta) per i trasporti che si utilizzano. Questo viene descritto in Capitolo 4, "Preparazione alla configurazione dell'hub", a pagina 33.
2. Facoltativamente, personalizzare la console e modificare la password predefinita ed i criteri delle autorizzazioni. Queste attività vengono descritte in Capitolo 6, "Configurazione di Console comunità", a pagina 49.
3. Creare i destinatari per i tipi di trasporti che verranno utilizzati per ricevere i documenti sull'hub (dal partner interno e dai partner esterni). La creazione dei destinatari è descritta nel Capitolo 7, "Definizione dei destinatari", a pagina 55.

   Nota: se il destinatario viene configurato con gli handler definiti dall'utente, è necessario caricare gli handler prima di creare il destinatario. Il caricamento degli handler viene descritto nella sezione " Aggiornamento degli handler definiti dall'utente" a pagina 56.
4. Configurare i passaggi o le azioni del flusso di lavoro in entrata. Si tratta di un Pass Through *opzionale* ed è necessario solo per quelli che hanno requisiti specifici per l'elaborazione del documento non forniti da WebSphere Partner Gateway. Se non è necessario modificare il comportamento fornito dal prodotto dei flussi di lavoro o delle azioni, ignorare questa fase. La configurazione dei passaggi e delle azioni del flusso di lavoro viene descritta in Capitolo 8, "Configurazione delle azioni e delle fasi del flusso di lavoro fisso", a pagina 79.

   Nota: caricare gli handler definiti dall'utente prima di configurare flussi di lavoro ed azioni. Il caricamento di handler definiti dall'utente è descritto in " Aggiornamento degli handler" a pagina 79.
5. Creare le definizioni di documenti (o verificare che quelle richieste siano già disponibili) per definire le tipologie di documenti che è possibile inviare o ricevere sull'hub.
6. Creare le interazioni per indicare la combinazione valida di due definizioni di documenti.

   La creazione delle definizioni di documenti e la creazione delle interazioni sono descritte nel Capitolo 9, "Configurazione dei tipi di documenti", a pagina 101 e nel Capitolo 10, "Configurazione dei flussi di documenti EDI", a pagina 163.
7. Creare un profilo per il partner interno, fornendo le informazioni sul partner interno e stabilendo i tipi di documenti che il partner interno può inviare e ricevere (le capacità B2B del partner interno). La creazione del profilo viene descritta nel Capitolo 3, "Creazione ed impostazione di partner", a pagina 23.

Creazione di partner

Dopo aver configurato l'hub, si crea un profilo per ciascun partner esterno che scambierà documenti con il partner interno. Solo l'amministratore hub può creare i partner.

In qualità di amministratore hub, è possibile impostare le capacità B2B dei partner, stabilire le destinazioni per i partner ed impostare i profili di sicurezza per i partner. In alternativa, queste fasi possono essere eseguite dagli stessi partner.

La creazione dei partner è descritta nel Capitolo 3, "Creazione ed impostazione di partner", a pagina 23. La creazione delle destinazioni è descritta nel Capitolo 11, "Creazione delle destinazioni", a pagina 213. La configurazione dei profili viene descritta nel Capitolo 13, "Abilitazione della sicurezza per gli scambi del documento", a pagina 241.

Definizione delle connessioni del documento

Una volta configurato l'hub e creati i profili del partner, è possibile impostare le connessioni. Le connessioni indicano le combinazioni valide di mittenti e destinatari e i documenti che possono scambiare. La gestione delle connessioni viene descritta nel Capitolo 12, "Gestione connessioni", a pagina 237.

Capitolo 3. Creazione ed impostazione di partner

Esistono due tipologie di partner: partner interni e partner esterni. Il partner interno, di solito, corrisponde all'azienda che possiede il server WebSphere Partner Gateway e che lo utilizza per comunicare con le altre aziende. Il partner interno possiede le applicazioni di backend (applicazioni interne all'azienda proprietaria). Può esserci un numero qualsiasi di partner interni, ma quello predefinito è tipicamente il primo partner definito. Le altre aziende con cui comunica il partner interno sono partner esterni.

Per ogni partner con cui si scambieranno i documenti, sarà necessario creare un profilo del partner. Oltre alla creazione dei profili, sarà anche necessario impostarli, l'impostazione è un processo che implica diverse fasi facoltative ed obbligatorie.

In questo capitolo sono riportate le fasi basilari, necessarie per creare ed impostare un profilo del partner, per comprendere la modalità in base alla quale sono eseguite tali fasi. Per ulteriori informazioni dettagliate su una fase, consultare il riferimento, posto alla fine della fase o della sezione. Questo capitolo include le seguenti sezioni:

Nota: è necessario utilizzare sempre la stessa istanza del browser con cui si accede alla Console comunità per apportare modifiche alla configurazione di WebSphere Partner Gateway. L'utilizzo simultaneo di più istanze del browser può causare l'eliminazione delle modifiche di configurazione.

Creazione dei profili del partner

Informazioni su questa attività

Durante la definizione di un partner in WebSphere Partner Gateway, si tratta della prima fase. Questa fase definisce le informazioni fondamentali sul partner, come ad esempio il nome, il nome di accesso e gli ID di business.

Per creare un partner, è necessario conoscere, almeno, le seguenti informazioni sul partner:

- Il ID di business utilizzato dal partner. Questo può essere:
  - DUNS, che è il Dun standard & il numero Bradstreet associato all'azienda
  - DUNS+4, che è una versione estesa del numero DUNS
  - Figura a mano libera, che può indicare qualsiasi numero selezionato dal partner per identificare l'azienda

Per ciascun partner che si desidera aggiungere alla comunità hub, effettuare la seguente procedura:

1. Fare clic su **Amministrazione account > Profili > Partner**.
2. Fare clic su **Crea**.
3. Per il **Nome accesso azienda**, inserire il nome del partner utilizzato nel campo Azienda durante l'accesso all'hub.
4. Per il **Nome visualizzato partner**, inserire il nome della società o un altro nome descrittivo per il partner. Indica il nome che viene visualizzato nell'elenco **Ricerca del partner**.
5. Selezionare la tipologia di partner. Se si tratta del primo partner, impostare l'azienda che possiede WebSphere Partner Gateway. Quindi, è necessario selezionare **Partner interno**. Nello schermo di configurazione del partner, selezionare la casella di spunta **Partner interno predefinito** se si desidera impostare questo partner interno corrente come quello predefinito. Quando si seleziona questa casella di spunta per gli altri partner, la selezione predefinita viene automaticamente eliminata da questo partner interno. Non è possibile cancellare la selezione in questa pagina. Per il primo partner interno creato, questa casella di spunta viene selezionata per impostazione predefinita.
6. In alternativa, inserire l'ID utente per l'Amministratore. L'ID utente deve essere univoco per tutti i partner. L'amministratore per il partner è in grado di effettuare le attività di gestione valide per questo partner, come ad esempio la gestione delle destinazioni, le capacità B2B e gli utenti. L'Operatore hub dispone sempre dell'accesso completo alla gestione del partner.
7. Selezionare lo stato per il partner. Durante la creazione di un partner, utilizzare il valore predefinito **Abilitato**.
8. In alternativa, inserire la tipologia di azienda nel campo **Tipo fornitore**.
9. In alternativa, inserire il **Sito Web** del partner.
10. Fare clic su **Nuovo** in **ID di business**.
11. Specificare un tipo dall'elenco ed immettere l'identificativo appropriato. WebSphere Partner Gateway utilizza il numero immesso per instradare il documento verso e dal partner.

    Durante l'immissione dell'identificativo, osservare le seguenti indicazioni:

    a. I numeri DUNS devono avere nove cifre uguali.
    b. DUNS+4 deve essere uguale a 13 cifre.
    c. I numeri di ID di figura a mano libera accettano fino a 60 caratteri alfanumerici e speciali.

    Nota: è possibile assegnare più ID di business ad un partner. In alcuni casi, sono necessari più ID di business. Ad esempio, quando l'hub invia e riceve i documenti EDI X12 o EDIFACT, utilizza sia gli ID DUNS che di Forma libera durante lo scambio di documenti.

    Sia il partner interno che i partner esterni coinvolti in questi tipi di flussi del documento devono avere sia un ID DUNS che un ID Figura a mano libera. L'ID Figura a mano libera consente di rappresentare gli ID EDI che dispongono di un identificativo ed un qualificatore. Ad esempio, si supponga che il qualificatore EDI sia "ZZ" e l'identificativo EDI sia "810810810". L'ID Figura a mano libera potrebbe essere specificato come ZZ-810810810.
12. In alternativa, inserire un indirizzo IP per il partner. L'Indirizzo IP viene utilizzato insieme ad una destinazione quando "Convalida IP client" è stato configurato. Inserire un Indirizzo IP procedendo nel modo seguente:

    a. In **Indirizzo IP**, fare clic su **Nuovo**.

b. Specificare la modalità operativa.
c. Inserire l'indirizzo IP del partner.

13. Fare clic su **Salva**.
14. Se è stato inserito un'ID utente dell'Amministratore, verrà presentato con una password, utilizzata dal partner per accedere all'hub. Prendere nota della password. Verrà fornita all'utente Amministratore partner.

Creazione delle destinazioni

Informazioni su questa attività

Una volta creato un profilo per un partner, è necessario stabilire le destinazioni utilizzate dall'hub per inviare i documenti al partner.

Per creare le destinazioni per un partner, effettuare la seguente procedura.

1. Verificare che il profilo del partner per cui si desidera creare le destinazioni, sia stato selezionato.

   Se un profilo è stato appena creato, esso è già stato selezionato. Se non è stato selezionato, attenersi alla seguente procedura:

   a. Fare clic su **Amministrazione account** > **Profili** > **Partner**.
   b. Inserire i criteri di ricerca e fare clic su **Cerca** oppure fare clic su **Cerca** senza inserire i criteri di ricerca per visualizzare un elenco di tutti i partner.
   c. Fare clic sull'icona **Visualizza dettagli** per visualizzare il profilo del partner.
2. Fare clic su **Destinazioni**.
3. Fare clic su **Crea**.
4. Per identificare la destinazione, inserire un **Nome destinazione**.
5. In alternativa indicare lo **Stato** della destinazione.
6. In alternativa, indicare se la destinazione sia **In linea** o **Non in linea**.
7. In alternativa, inserire una **Descrizione** della destinazione.
8. Selezionare un **Trasporto**.
9. Una volta selezionato un trasporto, la sezione **Configurazione della destinazione** di questa pagina è specifica a tale trasporto. Per le informazioni sulla compilazione di questa sezione per ogni trasporto, consultare una di queste sezioni:
   - "Impostazione dei valori globali di trasporto" a pagina 214

     Nota: questi valori sono relativi solo alla destinazione Script FTP.
   - "Impostazione di una destinazione HTTP" a pagina 216
   - "Impostazione di una destinazione HTTPS" a pagina 218
   - "Impostazione di una destinazione FTP" a pagina 219
   - "Impostazione di una destinazione SMTP" a pagina 221
   - "Impostazione di una destinazione JMS" a pagina 222
   - "Impostazione di una destinazione file-directory" a pagina 224
   - "Impostazione di una destinazione FTPS" a pagina 225
   - "Impostazione di una destinazione Script FTP" a pagina 228
   - "Impostazione di una destinazione SFTP" a pagina 227

Impostazione delle capacità B2B

Informazioni su questa attività

Ogni partner dispone delle Capacità B2B che definiscono le tipologie di documenti che il partner è in grado di inviare e ricevere.

In qualità di amministratore hub, è possibile impostare le capacità B2B dei partner o i partner sono in grado di effettuare questa attività in modo autonomo. Utilizzare le Capacità B2B per associare le capacità B2B di un partner ad una definizione del documento.

Per impostare le capacità B2B di ogni partner, effettuare la seguente procedura.

1. Verificare che il profilo del partner per cui si desidera configurare le capacità B2B sia stato selezionato. Il profilo di selezione viene visualizzato vicino alla parte superiore della pagina in grassetto subito dopo **Profilo >**.

   Se un profilo è stato appena creato, esso è già stato selezionato. Se non è stato selezionato, effettuare la seguente procedura:

   a. Fare clic su **Amministrazione account > Profili > Partner**.
   b. Inserire i criteri di ricerca e fare clic su **Cerca** oppure fare clic su **Cerca** senza inserire i criteri di ricerca per visualizzare un elenco di tutti i partner.
   c. Fare clic sull'icona **Visualizza dettagli** per visualizzare il profilo del partner.
2. Fare clic su **Capacità B2B**. Viene visualizzata la pagina Capacità B2B. L'area destra della pagina visualizza i package, i protocolli ed i documenti supportati dal sistema come definizioni del documento.
3. Fare clic sull'icona **Il ruolo non è attivo** della colonna **Imposta origine** per i Package, posti a destra, che contengono i documenti che verranno inviati dai partner esterni al partner interno.
4. Selezionare **Imposta origine** e **Imposta destinazione** se i partner inviano e ricevono gli stessi documenti. La Console visualizza un segno di spunta se la definizione del documento è stata abilitata.

   Nota: la selezione di Imposta origine coincide per tutte le azioni PIP in 2 modi indipendentemente dal fatto che la richiesta ha origine da un partner e la conferma corrispondente da un altro. Ciò è valido anche per Imposta destinazione.
5. Fare clic sull'icona **Espandi**, posta sul livello **Package** per espandere un singolo nodo sul livello di definizione del documento appropriato o selezionare un numero compreso tra **0-4** o **Tutti** per espandere tutte le definizioni del documento visualizzate sul livello scelto.
6. Selezionare nuovamente **Imposta origine**, **Imposta destinazione** o entrambi i ruoli per i livelli inferiori **Protocollo** e **Tipo di documento** per ogni definizione del documento supportata dal sistema.

   Se una definizione è stata attivata sul livello **Tipo di documento**, le definizioni **Azione** e **Attività** (se presenti) saranno attivate automaticamente.
7. In alternativa, fare clic su **Abilitato** nella colonna **Abilitato** per inserire una definizione del documento non in linea. (Quando si seleziona **Imposta origine** o **Imposta destinazione**, il record viene automaticamente abilitato). Fare clic su **Disabilitato** per metterlo in linea.

   Se un package è stato disabilitato, vengono disabilitate anche tutte le definizioni del documento di livello inferiore dello stesso nodo, indipendentemente dal singolo stato in cui sono state precedentemente abilitate. Se una definizione del documento di livello inferiore è stata disabilitata, tutte le

definizioni di livello superiore nello stesso contesto restano abilitate. Quando una definizione del documento è stata disabilitata, tutti gli attributi e le connessioni pre-esistenti continuano a funzionare. La definizione del documento disabilitata limita solo la creazione di nuove connessioni.

8. In alternativa, fare clic sull'icona **Modifica** se si desidera modificare uno degli attributi di un protocollo, package, tipo di documento, azione, attività o segnale. Si visualizzano, quindi, le impostazioni per gli attributi (se disponibili). È possibile modificare gli attributi inserendo un valore o selezionandolo dalla colonna **Aggiorna** e quindi fare clic su **Salva**.

Caricamento dei certificati

Informazioni su questa attività

I certificati consentono ai partner di inviare e ricevere documenti sicuri mediante diversi metodi: codifica, firma digitale o SSL. Se un partner ha ricevuto un certificato da un altro partner, tale partner può utilizzare questi metodi.

Per caricare i certificati per un partner, effettuare la seguente procedura.

1. Verificare che il profilo del partner, per cui si desidera caricare i certificati, sia stato selezionato. Il profilo di selezione viene visualizzato vicino alla parte superiore della pagina in grassetto subito dopo **Profilo >**.

   Se un profilo è stato appena creato, esso è già stato selezionato. Se non è stato selezionato, effettuare la seguente procedura:

   a. Fare clic su **Amministrazione account > Profili > Partner**.
   b. Inserire i criteri di ricerca e fare clic su **Cerca** oppure fare clic su **Cerca** senza inserire i criteri di ricerca per visualizzare un elenco di tutti i partner.
   c. Fare clic sull'icona **Visualizza dettagli** per visualizzare il profilo del partner.
2. Fare clic su **Certificati**.
3. Fare clic su **Carica certificato**.
4. Selezionare il tipo di certificato che si desidera caricare.
5. Immettere una descrizione del certificato.
6. Modificare lo stato in **Abilitato**.
7. Accanto a **Certificato**, fare clic su **Sfoglia** e navigare nella directory in cui è stato salvato il certificato.
8. Selezionare il certificato e fare clic su **Apri**.
9. Se il partner dispone di due certificati di codifica, indicare se si tratta del certificato principale o secondario selezionando Primario o Secondario nell'elenco **Utilizzo del certificato**.
10. Fare clic su **Carica** e fare clic su **Salva**.

Per ulteriori informazioni sull'utilizzo di certificati, consultare il Capitolo 13, "Abilitazione della sicurezza per gli scambi del documento", a pagina 241.

Creazione di utenti

Informazioni su questa attività

Gli utenti sono persone che effettuano l'accesso per svolgere le attività di amministrazione valide per questo partner. I nuovi utenti aggiunti al server LDAP

e alla console di gestione WAS devono essere aggiunti anche nella console WebSphere Partner Gateway affinché siano attivi.

Per creare gli utenti per un partner, effettuare la seguente procedura.

1. Verificare che un profilo del partner, per cui si desidera creare gli utenti, sia stato selezionato. Il profilo di selezione viene visualizzato vicino alla parte superiore della pagina in grassetto subito dopo **Profilo >**. Se un profilo è stato appena creato, esso è già stato selezionato. Se non è stato selezionato, attenersi alla seguente procedura:
   a. Fare clic su **Amministrazione account > Profili > Partner**.
   b. Inserire i criteri di ricerca e fare clic su **Cerca** oppure fare clic su **Cerca** senza inserire i criteri di ricerca per visualizzare un elenco di tutti i partner.
   c. Fare clic sull'icona **Visualizza dettagli** per visualizzare il profilo del partner.
2. Fare clic su **Utenti**.
3. Fare clic su **Crea**.
4. Inserire il nome dell'utente.

   Nota: i nomi utente devono essere univoci per tutti i partner del sistema
5. Verificare che lo stato sia **Abilitato**.
6. In alternativa, inserire il nome fornito, il cognome e le altre informazioni personali dell'utente.
7. Selezionare la **Lingua** e le **Locale di formato** e **Fuso orario** dell'utente.
8. Modificare lo Stato avviso dell'utente in **Abilitato**.
9. Selezionare la Visibilità sottoscritta dell'utente.
10. Fare clic su **Genera automaticamente password** per creare una password per tale utente o inserire e confermare una nuova.
11. Fare clic su **Salva**.

Nota: poiché i nomi utente sono obbligatori su un server LDAP, è necessario che anche i nomi utente siano univoci in WebSphere Partner Gateway. Se si crea un nuovo utente e il nome utente già esiste nello stesso partner o in uno diverso, verrà visualizzato un messaggio di errore che indica, `Un utente con questo nome già esiste`. In tal caso, inserire un altro nome utente nella console e continuare. Se si sta effettuando una migrazione a WebSphere Partner Gateway da una versione precedente in cui i nomi utente non sono stati limitati, viene visualizzato il doppio asterisco (**) accanto a qualsiasi nome utente duplicato, che esiste anche nello stesso profilo partner o in uno diverso. Modificare uno dei nomi utente in modo tale che siano univoci rispetto ad un altro. I nuovi utenti e gruppi che sono aggiunti al server LDAP e alla console di gestione WAS devono essere aggiunti anche nella console WebSphere Partner Gateway affinché siano attivi.

Per consentire il funzionamento di LDAP con WebSphere Partner Gateway, è necessario impostare l'autenticazione del server LDAP mediante la console WebSphere Application Server e l'autorizzazione dell'utente LDAP mediante la Console comunità di WebSphere Partner Gateway. Per informazioni sull'impostazione dell'autenticazione LDAP, consultare il manuale *WebSphere Partner Gateway Guida all'installazione*. Per informazioni sulla gestione degli utente e l'impostazione dell'autorizzazione utente LDAP, consultare la *WebSphere Partner Gateway Administration Guide*.

Per ulteriori informazioni sulla gestione degli utenti, consultare l'argomento "Managing users" nel manuale *WebSphere Partner Gateway Partner Guide*.

Configurazione dell'utente FTP

Informazioni su questa attività

Per abilitare l'utente corrente come utente FTP, eseguire le seguenti operazioni:

1. Verificare che il profilo del partner, per cui si desidera creare i contatti, sia stato selezionato. Il profilo di selezione viene visualizzato vicino alla parte superiore della pagina in grassetto subito dopo **Profilo >**. Se un profilo è stato appena creato, esso è già stato selezionato. Se non è stato selezionato, attenersi alla seguente procedura:
   a. Fare clic su **Amministrazione account > Profili > Partner**.
   b. Inserire i criteri di ricerca e fare clic su **Cerca** oppure fare clic su **Cerca** senza inserire i criteri di ricerca per visualizzare un elenco di tutti i partner.
   c. Fare clic sull'icona Visualizza dettagli per visualizzare il profilo del partner.
2. Fare clic su **Contatti**. Il sistema visualizza lo schermo Elenco contatti.
3. Se la colonna FTP è disabilitata per il contatto, fare clic sull'icona per abilitarla. L'icona passa dallo stato attivo a quello disattivo.
4. Fare clic sul contatto **Nome**. Viene visualizzata la pagina dettagli sul contatto.
5. Modificare **Configurazione FTP**.
6. Immettere **Directory home**, che è il percorso relativo dal valore specificato per bcg.ftp.config.rootdirectory. Questo è un campo obbligatorio.
7. Abilitare o disabilitare l'**Autorizzazione alla scrittura** nella directory home.
8. Abilitare o disabilitare l'autorizzazione all'utilizzo di **Crea/Rimuovi directory**.
9. Selezionare **Numero massimo di accessi**, che è il numero massimo consentito di accessi contemporanei. Se si seleziona Limite personalizzato, immettere il valore personalizzato nella casella di testo.
10. Selezionare **Accessi massimi per lo stesso IP**, che è il numero massimo consentito di accessi contemporanei dallo stesso indirizzo IP. Se si seleziona Limite personalizzato dall'elenco, immettere il valore personalizzato nella casella di testo.
11. Selezionare **Tempo massimo di inattività**, che è il tempo massimo di inattività in secondi dopo che la connessione dell'utente è stata annullata. Se si seleziona Limite personalizzato dall'elenco, immettere il valore personalizzato nella casella di testo.
12. Selezionare **Max. upload**, che è la velocità massima di caricamento in byte/sec. Se si seleziona Limite personalizzato dall'elenco, immettere il valore personalizzato nella casella di testo.
13. Selezionare **Max. Scarica**, che è la velocità massima di scaricamento in byte/sec. Se si seleziona Limite personalizzato dall'elenco, immettere il valore personalizzato nella casella di testo.
14. Fare clic su **Salva**.

Creazione di gruppi

Informazioni su questa attività

Il raggruppamento di utenti consente di gestire immediatamente le autorizzazioni di molti utenti. I nuovi gruppi aggiunti al server LDAP e alla console di gestione WAS devono essere aggiunti anche nella console WebSphere Partner Gateway affinché siano attivi.

Per creare i gruppi per ciascun partner, effettuare la seguente procedura.

1. Verificare che il profilo del partner, per cui si desidera creare i gruppi, sia stato selezionato.

   Se un profilo è stato appena creato, esso è già stato selezionato. Se non è stato selezionato, effettuare la seguente procedura:

   a. Fare clic su **Amministrazione account** > **Profili** > **Partner**.
   b. Inserire i criteri di ricerca e fare clic su **Cerca** oppure fare clic su **Cerca** senza inserire i criteri di ricerca per visualizzare un elenco di tutti i partner.
   c. Fare clic sull'icona **Visualizza dettagli** per visualizzare il profilo del partner.
2. Fare clic su **Gruppi**.
3. Fare clic su **Crea**.
4. Inserire il nome di questo gruppo.
5. Fare clic su **Salva**.
6. Per aggiungere gli utenti a questo gruppo, fare clic su **Appartenenze**.

   Gli utenti, associati a questo partner, sono visualizzati in **Utenti non nel gruppo** o **Utenti nel gruppo**. Per aggiungere un utente ad un gruppo, completare quanto segue:

   a. Fare clic sull'icona **Modifica record** posta accanto al gruppo.
   b. Selezionare l'utente che si desidera aggiungere e fare clic su **Aggiungi a gruppo**.
   c. Fare clic su **Salva**.
7. Per modificare le autorizzazioni degli utenti di questo gruppo, fare clic su **Autorizzazioni**.

   Le autorizzazioni per gli utenti di questo gruppo sono state visualizzate in base al **Modulo**. Per modificare le autorizzazioni di questo gruppo, completare quanto segue:

   a. Fare clic sull'icona **Modifica record** posta accanto al gruppo.
   b. Fare clic sui pallini, posti a destra di ciascun modulo che specifica l'autorizzazione come **Accesso non consentito**, **Sola lettura** oppure **Lettura/scrittura**.
   c. Fare clic su **Salva**.

   Nota: gli utenti possono appartenere a più gruppi. In tal caso, quando le autorizzazioni di diversi gruppi differiscono, l'utente eredita il livello più alto di autorizzazioni, assegnato agli utenti di tutti i gruppi.

Nota: precedentemente l'utente hubadmin era l'unico nome utente con le autorizzazioni di amministrazione del superutente, ma in WebSphere Partner Gateway 6.1, i gruppi sono stati creati in modo tale che tutti gli utenti che sono membri del gruppo hubadmin possono avere le autorizzazioni di superutente. Consente a molti utenti di condividere le responsabilità di hubadmin durante la gestione della protezione della password.

Per ulteriori informazioni sulla gestione dei gruppi, consultare l'argomento "Managing groups" nel manuale *WebSphere Partner Gateway Partner Guide*.

Creazione di contatti

Informazioni su questa attività

WebSphere Partner Gateway consente di creare i contatti che è possibile notificare quando si verificano diversi tipi di eventi. Per creare i contatti per ciascun partner, effettuare la seguente procedura:

1. Verificare che il profilo del partner, per cui si desidera creare i contatti, sia stato selezionato. Il profilo di selezione viene visualizzato vicino alla parte superiore della pagina in grassetto subito dopo **Profilo >**.

   Se un profilo è stato appena creato, esso è già stato selezionato. Se non è stato selezionato, effettuare la seguente procedura:

   a. Fare clic su **Amministrazione account > Profili > Partner**.
   b. Inserire i criteri di ricerca e fare clic su **Cerca** oppure fare clic su **Cerca** senza inserire i criteri di ricerca per visualizzare un elenco di tutti i partner.
   c. Fare clic sull'icona **Visualizza dettagli** per visualizzare il profilo del partner.
2. Fare clic su **Contatti**.
3. Fare clic su **Crea**.
4. Inserire il **Nome fornito** ed il **Cognome** di questo contatto.
5. In alternativa, inserire l'**Indirizzo** di questo contatto.
6. In alternativa, selezionare il **Tipo di contatto**.
7. In alternativa, inserire l'indirizzo **E-mail**, il numero di **Telefono** e il **Numero di fax** di questo contatto.
8. Selezionare la **Lingua** e le **Locale del formato** e il **Fuso orario** del contatto.
9. Modificare lo **Stato avviso** dell'utente in **Abilitato**.
10. Selezionare la **Visibilità sottoscritta** dell'utente.
11. Fare clic su **Salva**.

Per ulteriori informazioni sulla gestione dei contatti, consultare l'argomento "Managing contacts" nel manuale *WebSphere Partner Gateway Partner Guide*.

Creazione di indirizzi

Informazioni su questa attività

WebSphere Partner Gateway consente di creare gli indirizzi per i partner. Per creare un indirizzo per un partner, effettuare la seguente procedura:

1. Verificare che il profilo del partner, per cui si desidera creare gli indirizzi, sia stato selezionato. Il profilo di selezione viene visualizzato vicino alla parte superiore della pagina in grassetto subito dopo **Profilo >**.

   Se un profilo è stato appena creato, esso è già stato selezionato. Se non è stato selezionato, effettuare la seguente procedura:

   a. Fare clic su **Amministrazione account > Profili > Partner**.
   b. Inserire i criteri di ricerca e fare clic su **Cerca** oppure fare clic su **Cerca** senza inserire i criteri di ricerca per visualizzare un elenco di tutti i partner.
   c. Fare clic sull'icona **Visualizza dettagli** per visualizzare il profilo del partner.

2. Fare clic su **Indirizzi**.
3. Fare clic su **Crea nuovo indirizzo**.
4. Selezionare un **Tipo indirizzo**.
5. In alternativa, inserire l'**Indirizzo**.
6. Fare clic su **Salva**.

Per ulteriori informazioni sulla gestione degli indirizzi, consultare l'argomento "Managing addresses" in *WebSphere Partner Gateway Partner Guide*.

Capitolo 4. Preparazione alla configurazione dell'hub

Nei successivi capitoli, saranno impostati i destinatari e le destinazioni, descritti nel Capitolo 2, "Introduzione alla configurazione dell'hub", a pagina 5. A seconda dei tipi di trasporti, utilizzati per ricevere i documenti nei destinatari e per inviarli alle destinazioni, è necessario impostarli.

In questo capitolo vengono riportate le seguenti sezioni:

- " Creazione di una destinazione directory file"
- "Configurazione del server FTP per ricevere i documenti"
- "Configurazione dell'hub per il protocollo di trasporto JMS" a pagina 37
- "Configurazione della compressione RNIF" a pagina 43

Viene fornita anche una breve panoramica degli script FTP richiesti per le destinazioni e i destinatari Script FTP e viene descritto il client Data Interchange Services, che consente di creare le mappe di conversione, convalida e di riconoscimento funzionale per documenti EDI, XML e ROD (record-oriented-data).

- "Utilizzo degli script FTP per le destinazioni e i destinatari di script FTP" a pagina 43
- "Utilizzo delle mappe dal client DIS (Data Interchange Service)" a pagina 44

Se non si desidera impostare questi tipi di destinatari o destinazioni, ignorare questo capitolo e passare al Capitolo 5, "Avvio del server e visualizzazione della Console comunità", a pagina 45.

Creazione di una destinazione directory file

Le versioni di WebSphere Partner Gateway precedenti alla versione 6.1 richiedono la creazione di una directory file per una destinazione directory file. Quindi, nella versione 6.1 la directory specificata per una destinazione directory file verrà creata, se necessario. Se la directory specificata per una destinazione directory file già esiste, sarà utilizzata dalla destinazione.

Configurazione del server FTP per ricevere i documenti

Nota: questa sezione è valida solo per ricevere i documenti su FTP o FTPS dai partner. L'invio dei documenti ai partner è descritto nelle sezioni "Impostazione di una destinazione FTP" a pagina 219 e "Impostazione di una destinazione FTPS" a pagina 225.

Se si desidera utilizzare FTP o FTPS come trasporto per i documenti in entrata, è necessario che un server FTP sia stato installato. Se si desidera utilizzare l'FTP e non è stato installato un server installato, prima di continuare, effettuare la seguente procedura. Accertarsi che uno dei seguenti scenari sia vero per l'installazione:

- Il server FTP viene installato sulla stessa macchina sulla quale è installato WebSphere Partner Gateway.
- Il bcguser sulla macchina WebSphere Partner Gateway dispone dell'accesso di lettura e scrittura nella posizione in cui il server FTP memorizza i file.

Configurazione della struttura di directory richiesta sul server FTP

Informazioni su questa attività

Una volta installato il server FTP, il passo successivo è di creare la struttura di directory richiesta nella directory principale del server FTP. WebSphere Partner Gateway richiede una determinata struttura di directory che il componente Destinatario e i componenti del Gestore documenti utilizzano per identificare correttamente il partner che invia il documento in entrata. La struttura è descritta nella Figura 15.

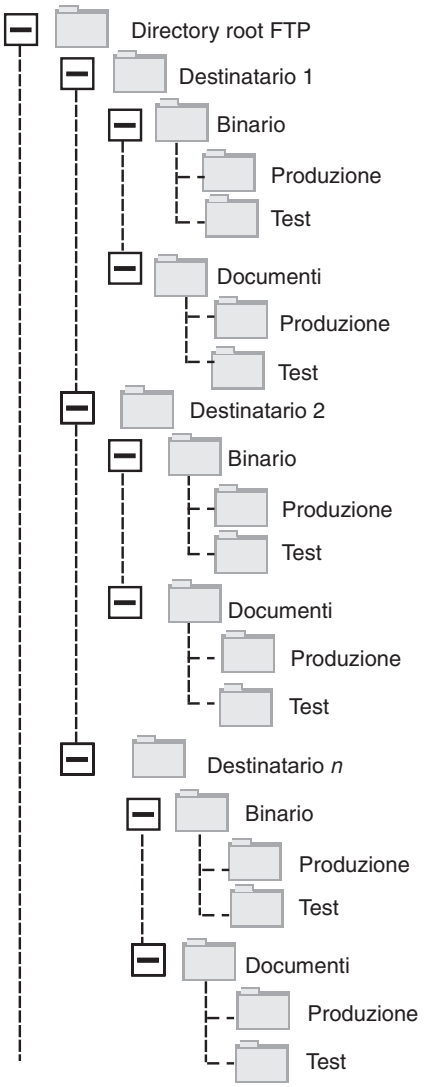


Figura 15. Struttura di directory FTP

Ciascuna directory del partner contiene una directory Binari e una directory Documenti. Entrambe le directory contengono una directory Produzione e una directory Verifica.

La directory Documenti viene utilizzata quando un partner invia un documento XML che contiene le informazioni di instradamento complete (mediante FTP)

all'hub. È necessaria la creazione di una definizione XML personalizzata. Inoltre, i documenti EDI possono essere inviati utilizzando questa directory.

La directory Binari viene utilizzata quando un partner invia altri documenti (mediante FTP) all'hub.

Per ogni partner che utilizza FTP al fine di inviare o ricevere i documenti, creare le seguenti cartelle dalla directory root del server FTP:

1. Creare una cartella per il partner.

   Nota: il nome della cartella deve corrispondere al nome specificato per **Nome accesso azienda** al momento della creazione del partner. La creazione dei partner è descritta nel "Creazione dei profili del partner" a pagina 23.
2. Creare le cartelle secondarie nella cartella del partner definita `Binari` e `Documenti`.
3. Creare le cartelle secondarie nelle cartelle Binari e Documenti denominate `Produzione` e `Verifica`.

Modalità di elaborazione dei file inviati su FTP

È importante comprendere in che modo i file binari e XML vengono elaborati dal server FTP.

File binari

I file binari presentano una struttura di nome di file necessaria perché i file non vengono ispezionati affatto dal Gestore documenti.

La struttura del nome file è: *<To_PartnerID>.<Unique_Filename>*

Quando un file binario viene rilevato dal componente Destinatario, viene scritto nella memoria condivisa e passato nel Gestore documenti per l'elaborazione.

Il nome della directory in cui è stato rilevato il file consente di valutare From Partner Name e la prima parte del nome file consente di valutare To Partner Name. La posizione della directory nella struttura della directory viene utilizzata per valutare se la transazione è una transazione di tipo Produzione o Verifica.

Ad esempio, un file denominato 123456789.abcdefg1234567 viene rilevato nella directory `\ftproot\partnerTwo\binary\production`. Il Gestore documenti è a conoscenza delle seguenti informazioni:

- Il campo `From Partner Name` è `partnerTwo` (poiché il file è stato rilevato nella parte partnerTwo della struttura ad albero di directory).
- Il campo `To Partner Name` è `partnerOne` (poiché la prima parte del nome file è 123456789, che è l'ID DUNS per partnerOne).

  Nota: in tutto il manuale, i numeri DUNS sono solo esempi. WebSphere Partner Gateway richiede che <To_PartnerID> corrisponda ai DUNS del partner destinatario. Nel caso in cui l'ID Duns non venga individuato, la ricerca del canale non avrà esito positivo.
- Il tipo di transazione è Produzione.

Il Gestore documenti ricerca una connessione del partner Produzione da partnerTwo a partnerOne per:

- Package: Nessuno (N/A)
- Protocollo: Binario (1.0)

- Tipo documento: Binario (1.0)

Quindi, il Gestore documenti elabora il file.

I file binari possono essere trasferiti anche via FTP, utilizzando il programma di gestione Generic Preprocess o il programma di gestione FileNamePartnerId. Consultare “Modifica del punto di configurazione Preelaborazione” a pagina 74 per ulteriori dettagli.

File XML

Un file XML instradato mediante le specifiche XML personalizzate non ha requisiti per il nome file poiché il file è stato esaminato dal Gestore documenti e le informazioni di instradamento sono state estratte dal documento stesso.

Quando un file XML è stato rilevato dal destinatario, esso viene scritto nella memoria condivisa e trasferito al Gestore documenti per l’elaborazione.

Il Gestore documenti confronta il file XML nei formati XML che sono stati definiti e seleziona il formato XML richiesto. (L’impostazione dei formati XML viene descritta in “Elaborazione documento XML personalizzato” a pagina 151.) Il campi From Partner Name, To Partner Name, e le informazioni di instradamento sono estratti dal File XML.

La posizione della directory nella struttura della directory viene utilizzata per valutare se la transazione è una transazione di tipo Produzione o Verifica.

Quindi, il Gestore documenti utilizza queste informazioni per rilevare la connessione del partner corretta prima di elaborare il file.

Configurazione aggiuntiva del server FTP

Informazioni su questa attività

Una volta creata la struttura di directory richiesta, configurare il server FTP per ciascun partner della comunità dell’hub. Il modo di configurazione del server FTP dipende dal server che si sta utilizzando. Fare riferimento alla documentazione del server FTP ed eseguire le attività indicate:

1. Aggiungere un nuovo gruppo (ad esempio, Partner).
2. Aggiungere un utente al gruppo creato di recente per ciascun partner che invia o riceve i documenti su FTP.
3. Per ciascun partner, impostare il server FTP per associare il partner in entrata alla rispettiva struttura di directory creata per il partner nella sezione precedente “ Configurazione della struttura di directory richiesta sul server FTP” a pagina 34. Per ulteriori informazioni, fare riferimento alla documentazione del server FTP.

Considerazioni di protezione per il server FTPS

Se si utilizza un server FTPS per ricevere i documenti in entrata, le considerazioni sulla sicurezza per le sessioni SSL sono gestite esclusivamente dal cliente e dal server FTPS che il partner utilizza. Non esiste alcuna configurazione di sicurezza specifica per WebSphere Partner Gateway sui documenti FTPS in entrata. WebSphere Partner Gateway richiama i documenti dal destinatario FTP (descritto nella sezione “ Impostazione di un destinatario FTP” a pagina 60) una volta che il server server ha negoziato correttamente i canali sicuri e ricevuto il documento.

Consultare la documentazione del server FTPS per stabilire i certificati necessari (e il punto in cui sono richiesti) per configurare correttamente un canale sicuro che il partner è in grado di contattare.

Per l'autenticazione del server, fornire il certificato del Destinatario ai partner. Se il certificato viene emesso da un'autorità di certificazione, fornire anche la catena di certificati CA (Certifying Authority). Se l'autenticazione del client è stata supportata dal server FTPS, i certificati di autenticazione del client dei partner devono essere specificati nel server FTPS. Per informazioni su come specificare l'autenticazione del client e dei certificati per l'autenticazione del client, consultare la documentazione del server FTPS.

Configurazione dell'hub per il protocollo di trasporto JMS

In questa sezione, viene descritto come configurare l'hub per utilizzare il trasporto JMS. Se si utilizza il trasporto JMS per inviare documenti dall'hub o ricevere documenti nell'hub, seguire le procedure indicate in questa sezione. Se non si desidera utilizzare un trasporto JMS, saltare questa sezione.

Nota: le procedure contenute in questa sezione descrivono come utilizzare l'implementazione JMS di WebSphere MQ per configurare l'ambiente JMS. Inoltre, le procedure descrivono il modo in cui impostare le code locali. Se si desidera configurare code di trasmissione e remote, fare riferimento alla documentazione di WebSphere MQ.

Anche se questa sezione è specifica per WebSphere MQ, altri provider JMS richiederanno delle procedure simili. Per WebSphere Platform Messaging, consultare l'argomento ″Configuring JMS while WebSphere Partner Gateway is installed on WebSphere Application Server″ nel capitolo 5. ″Integrating WebSphere Process Server with JMS as transport″ nel manuale *WebSphere Partner Gateway Integration Guide*.

Nelle successive sezioni di questo documento, viene descritto il modo in cui impostare le destinazioni o i destinatari JMS (o entrambi). Queste attività vengono descritte in " Impostazione di un destinatario JMS" a pagina 62 e in "Impostazione di una destinazione JMS" a pagina 222.

Creazione di una directory per JMS

Informazioni su questa attività

Si crea prima una directory per JMS. Ad esempio, supporre di voler creare una directory denominata JMS nella directory c:\temp di un'installazione Windows. Queste procedure che è preferibile seguire:

1. Aprire Windows Explorer.
2. Aprire la directory C:\temp.
3. Creare una nuova cartella denominata JMS.

Modifica della configurazione JMS predefinita

Informazioni su questa attività

In questa sezione, si aggiorna il file JMSAdmin.config, che è parte dell'installazione WebSphere MQ, per modificare il contesto factory e l'URL del provider.

1. Spostarsi alla directory `Java\bin` di WebSphere MQ. Ad esempio, in un'installazione Windows, è preferibile navigare in: C:\IBM\MQ\Java\bin

2. Aprire il file JMSAdmin.config utilizzando un editor di testo semplice, come Blocco note o vi.
3. Aggiungere il carattere # all'inizio delle seguenti righe:

   ```
   INITIAL_CONTEXT_FACTORY=com.sun.jndi.ldap.LdapCtxFactory
   PROVIDER_URL=ldap://polaris/o=ibm,c=us
   ```

4. Rimuovere il carattere # dall'inizio delle seguenti righe:

   ```
   #INITIAL_CONTEXT_FACTORY=com.sun.jndi.fscontext.RefFSContextFactory
   #PROVIDER_URL=file:/C:/JNDI-Directory
   ```

5. Modificare la riga `PROVIDER_URL=file:/C:/JNDI-Directory` uguale al nome della directory JMS che si imposta " Creazione di una directory per JMS" a pagina 37. Se, ad esempio, si imposta la directory `c:/temp/JMS`, la riga appare in questo modo:

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

6. Salvare il file.

Creazione di code e del canale

In questa sezione, si utilizza WebSphere MQ per creare le code che si utilizzano per inviare e ricevere i documenti e il canale per questa comunicazione. Si presume che sia stato creato un gestore code. È necessario immettere il nome del gestore code al posto di *<queue_manager_name>* nei seguenti passi. Si presume, inoltre, che un listener per questo gestore code sia stato avviato sulla porta TCP 1414.

1. Aprire il prompt dei comandi.
2. Inserire il seguente comando per avviare il server del comando WebSphere MQ:

   ```
   strmqcsv <queue_manager_name>
   ```

3. Inserire il seguente comando per avviare l'ambiente del comando WebSphere MQ:

   ```
   runmqsc <queue_manager_name>
   ```

4. Inserire il seguente comando per creare una coda WebSphere MQ da utilizzare per mettere in attesa i documenti in entrata inviata all'hub:

   ```
   def ql(<queue_name>)
   ```

   Ad esempio, per creare una coda denominata JMSIN, è preferibile inserire:

   ```
   def ql(JMSIN)
   ```

5. Inserire il seguente comando per creare una coda WebSphere MQ da utilizzare per mettere i documenti in attesa inviati dall'hub:

   ```
   def ql(<queue_name>)
   ```

   Ad esempio, per creare una coda denominata JMSOUT, è preferibile inserire:

   ```
   def ql(JMSOUT)
   ```

6. Inserire il seguente comando per creare un canale WebSphere MQ da utilizzare per i documenti inviati a e dall'hub:

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

   Ad esempio, per creare un canale denominato java.channel, è preferibile inserire:

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

7. Inserire il seguente comando per uscire dall'ambiente del comando WebSphere MQ:

   ```
   end
   ```

Aggiunta di un runtime Java all'ambiente

Informazioni su questa attività

Immettere il seguente comando per aggiungere un runtime Java(TM) al percorso del sistema:

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

dove *DirProdotto* si riferisce alla directory dove WebSphere Partner Gateway è installato.

Definizione della configurazione JMS

Informazioni su questa attività

Per definire la configurazione JMS, effettuare le seguenti procedure:

1. Passare alla directory WebSphere MQ Java (directory (<*path_to_Websphere_MQ_installation_directory*>\java\bin)
2. Avviare l'applicazione JMSAdmin digitando il seguente comando:

   ```
   JMSAdmin
   ```
3. Definire un nuovo contesto JMS digitando i seguenti comandi dal prompt InitCtx>:

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

   Ad esempio, se *context_name* è JMS, il comando sarà:

   ```
   define ctx(JMS)
   change ctx(JMS)
   ```
4. Dal prompt InitCtx/jms>, inserire la seguente configurazione JMS:

   ```
   define qcf(connection_factory_name)
       tran(CLIENT)
       host(<indirizzo_IP_utente>)
       port(1414)
       chan(java.channel)
       qmgr(<queue_manager_name>)
   define q(<name>) queue(<queue_name>) qmgr(<queue_manager_name>)
   define q(<name>) queue(<queue_name>) qmgr(<queue_manager_name>)
   end
   ```

   Nota:

   - Se MQ e WebSphere Partner Gateway sono installati su due macchine diverse, selezionare CLIENT come tipo di trasporto.
   - Se MQ e WebSphere Partner Gateway sono installati sulla stessa macchina, il tipo di trasporto deve essere BINDINGS.

I passi precedenti hanno consentito la creazione del file .bindings, che si trova in una cartella secondaria della cartella specificata al passo 5 a pagina 38. Il nome della cartella secondaria è quello specificato per il contesto JMS.

Come esempio, viene utilizzata la seguente sessione JMSAdmin per definire la factory di connessione della coda come `Hub`, con il seguente indirizzo IP `sample.ibm.com` in cui si trova il Gestore code MQ (<*queue_manager_name*> di `sample.queue.manager`). L'esempio utilizza i nomi di coda e il nome di canale JMS creati in "Creazione di code e del canale" a pagina 38. Notare che l'input di utente segue il > prompt.

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

In questo esempio, il file .bindings si trova nella seguente directory: `c:/temp/JMS/JMS`, dove `c:/temp/JMS` è PROVIDER_URL e `JMS` è il nome del contesto.

Configurazione delle librerie di runtime

Per il Destinatario JMS o la Destinazione JMS, ci sono vari file jar di WebSphere MQ che devono essere visibili per WebSphere Partner Gateway. Questi file jar sono resi visibili inserendoli nel classpath. Se si utilizzerà la modalità Binding MQ per accedere a MQ, anche le librerie native MQ devono trovarsi nel percorso. Consultare la documentazione di WebSphere MQ per ulteriori informazioni sui file jar MQ e sulle librerie native per JMS.

Ci sono vari modi per aggiungere i file jar al classpath di WebSphere Partner Gateway. Un modo consiste nell'inserirli nella directory delle uscite utente ed un secondo modo consiste nell'associarli tramite librerie condivise di WebSphere Application Server.

Metodo di directory di uscite utente:

Per utilizzare questo metodo, inserire i file jar specificati nell'appropriata directory di uscite utente:

- per il Destinatario JMS, inserirli nella directory <root-installazione-WPG>/receiver/lib/userexits
- Per la Destinazione JMS, inserirli nella directory <root-installazione-WPG>/router/lib/userexits

Metodo di librerie condivise di WebSphere Application Server. Informazioni su questa attività

Per utilizzare questo metodo, creare una variabile di libreria condivisa ed associare quindi la variabile all'applicazione Destinatario o Gestore documenti, come illustrato brevemente nei seguenti passi. Per ulteriori informazioni su questa procedura, consultare la documentazione di WebSphere Application Server.

1. Accedere alla console di gestione di WebSphere Application Server
2. Creare la variabile per le librerie condivise completando la seguente procedura:
   a. Passare a **Ambiente** > **Librerie condivise**.
   b. Selezionare un **Ambito** (probabilmente nodo) e fare clic su **Nuovo**.
   c. Immettere il nome della variabile (ad esempio MQ_LIBRARIES), completare le voci di classpath per i file jar MQ e fare clic su **OK**.
3. Associare la variabile di libreria condivisa creata con i componenti di WebSphere Partner Gateway completando le seguenti operazioni:
   a. Passare a **Applicazioni** > **Applicazioni enterprise**.
   b. Selezionare **BCGReceiver** (per i destinatari JMS) o **BCGDocMgr** (per le destinazioni JMS).

c. Selezionare **Riferimenti libreria condivisa**.
d. Selezionare l'applicazione e fare clic su **Librerie condivise di riferimento**.
e. Dall'elenco Disponibile, selezionare la variabile di libreria condivisa creata (ad esempio MQ_LIBRARIES), e spostare la variabile nell'elenco Selezionato. Fare quindi clic su **OK**.

Configurazione del gateway JMS e del destinatario con MQ esterno

Informazioni su questa attività

Quelle seguenti sono le operazioni da eseguire per creare un bridge di comunicazione tra WebSphere Partner Gateway e MQ mediante la console di gestione di WebSphere Application Server:

1. Creare una produzione connessione code JMS.
   a. Collegarsi alla console di gestione di WebSphere Application Server.
   b. Passare a **Risorse > JMS > Produzione connessione code**.
   c. Selezionare un **Ambito** e fare clic su **Nuovo**.
      - Per la configurazione del gateway, selezionare l'ambito del server/nodo del Document Manager (L'ambito del nodo è utile nel caso dei cluster. Per la modalità semplice, selezionare un ambito server).
      - Per la configurazione del destinatario, selezionare l'ambito del server/nodo del destinatario. (L'ambito del nodo è utile nel caso dei cluster. Per la modalità semplice, selezionare un ambito server).
   d. Selezionare l'opzione **Provider di messaggistica WebSphere MQ** e fare clic su **OK**.
   e. Immettere il **Nome** e il **nome JNDI**. Questi sono dei valori obbligatori.
   f. Immettere i valori corretti per il **Gestore code**, per l'**Host** (IP della macchina in cui è in esecuzione il gestore code), per la **porta**, per il **canale** e per il **tipo di trasporto**. I campi restanti sono facoltativi.

      Nota:
      - Se MQ e WebSphere Partner Gateway sono installati su due macchine diverse, selezionare CLIENT come tipo di trasporto.
      - Se MQ e WebSphere Partner Gateway sono installati sulla stessa macchina, il tipo di trasporto deve essere BINDINGS.

      Per ulteriori dettagli, fare riferimento al centro informazioni di WebSphere Application Server al seguente indirizzo: http://publib.boulder.ibm.com/infocenter/wasinfo/v6r1/index.jsp?topic=/com.ibm.websphere.nd.multipla...
2. Creare la coda JMS.
   a. Collegarsi alla console di gestione di WebSphere Application Server.
   b. Passare a **Risorse > JMS > Code**.
   c. Selezionare un **Ambito** e fare clic su **Nuovo**.
      - Per la configurazione del gateway, selezionare l'ambito del server/nodo del Document Manager (L'ambito del nodo è utile nel caso dei cluster. Per la modalità semplice, selezionare un ambito server).
      - Per la configurazione del destinatario, selezionare l'ambito del server/nodo del destinatario. (L'ambito del nodo è utile nel caso dei cluster. Per la modalità semplice, selezionare un ambito server).
   d. Immettere il **Nome** e il **nome JNDI**. Questi sono dei valori obbligatori.

e. Immettere i valori corretti per il **Gestore code**, per l'**Host** (IP della macchina in cui è in esecuzione il gestore code), per la **porta**, per il **canale** e per il **tipo di trasporto**. I campi restanti sono facoltativi.

f. Riavviare i server relativi che hanno subito delle modifiche, ad esempio DocumentManager/Receiver/bcgserver nel caso di installazione distribuita semplice.

3. Configurare il gateway JMS su WebSphere Partner Gateway.
   a. Accedere alla console di gestione di WebSphere Partner Gateway.
   b. Fare clic su **Amministrazione account > Profili > Destinazioni**.
   c. Fare clic su **Crea**.
   d. Immettere il **Nome destinazione**. È un campo obbligatorio.
   e. Selezionare **JMS** nel campo del trasporto.
   f. Immettere i valori per i seguenti campi obbligatori:
      - Indirizzo: immettere l'indirizzo di destinazione fornendo il nome host e la porta corretti degli oggetti Produzione connessioni code o Coda, creati in WebSphere Application Server. L'indirizzo deve essere in formato corbaloc:iiop: <hostname>: <bootstrapportnumber>, dove:
        – corbaloc:iiop - indica il protocollo utilizzato per la comunicazione tra il client (WebSphere Partner Gateway) e il server (WebSphere Application Server).
        – <hostname> - nome host o indirizzo IP della macchina su cui è installato WebSphere Application Server, per cui sono stati creati gli oggetti Produzione connessione code e Coda.
        – <bootstrapportnumber> - il numero della porta bootstrap del server dove gli oggetti Produzione connessione code e Coda vengono collegati. Per acquisire il numero della porta bootstrap, è possibile accedere alla console di gestione di WebSphere Application Server, passare a **Server > Server delle applicazioni > <nome server> Porte** e verificare l'indirizzo bootstrap. In caso di modalità distribuita, i numeri porta sono diversi per il destinatario e il gateway. Accedere al server corrispondente (bcgreceiver per il destinatario e bcgdocmgr per il gateway) per ottenere il numero della porta di avvio corretto.
      - Nome produzione JMS: il nome JNDI fornito per la Produzione della connessione code JMS.
      - Nome coda JMS: il nome JNDI fornito per la coda JMS.
      - Nome factory JNDI JMS: è la produzione da utilizzare per la comunicazione JNDI. Dato che si sta utilizzando WebSphere Application Server, è possibile specificare il valore com.ibm.websphere.naming.WsnInitialContextFactory.

4. Configurare il destinatario JMS su WebSphere Partner Gateway.
   a. Accedere alla console di gestione di WebSphere Partner Gateway.
   b. Fare clic su **Amministrazione hub > Configurazione hub > Destinatari**.
   c. Fare clic su **Crea destinatario**.
   d. Immettere il **Nome destinatario**. È un campo obbligatorio.
   e. Selezionare **JMS** nel campo del trasporto.
   f. Immettere i valori appropriati per i campi richiesti, come descritto nel passo :3f.

Configurazione della compressione RNIF

I messaggi di business Rosettanet ed il loro allegati sono compressi ed impacchettati utilizzando la busta S/MIME per trasferire documenti di grandi dimensioni. Inoltre, il supporto decompressione viene fornito per i messaggi di business Rosettanet. Viene fornita un'opzione per comprimere il payload da solo o con allegati. Per un miglioramento delle prestazioni, comprimere il contenuto di servizio ed i suoi allegati prima della codifica, la firma o la codifica di trasferimento come per Rosettanet 2.0 Technical Advisory Specification. Nel rispettivo canale Rosettanet WebSphere Partner Gateway, selezionare la compressione attributo oggetto di instradamento per avere uno dei seguenti valori:

- Nessuno
- Payload
- Payload e allegato

A parte l'opzione di compressione selezionata, è inoltre possibile selezionare altri attributi di criteri del filtro come **Comprimi tipo contenuto** e **Comprimi dimensione**. È possibile selezionare il payload o gli allegati per la compressione dal pool di allegati utilizzando i criteri del filtro. **Comprimi tipo contenuto** prevede che "Tutto" o Tipi mime validi siano separati da virgole. Se viene selezionata l'opzione **Payload** nella compressione base, allora il payload sarà compresso indipendentemente dal valore specificato nell'attributo oggetto di instradamento **Comprimi tipo contenuto**. Solo gli allegati sono selezionati per la compressione in base ai tipi di contenuto specificato. L'attributo dell'oggetto di instradamento **Comprimi dimensione** prevede "Tutto" o limite dimensione valida. Il limite dimensione valida indica la dimensione minima accettabile per la compressione.

Quando viene inviato un documento Rosettanet compresso, la decompressione S/MIME viene eseguita sul contenuto dei servizi ed i suoi allegati.

Utilizzo degli script FTP per le destinazioni e i destinatari di script FTP

Il trasporto Script FTP consente di inviare dati ad un servizio FTP, inclusa una VAN (Value Added Network). Si controllano le operazioni sul server FTP mediante un file di script che contiene i comandi FTP.

Specificare questo script quando viene creata una destinazione o un destinatario Script FTP. WebSphere Partner Gateway sostituisce i valori correnti immessi al momento della creazione del destinatario o della destinazione per i segnaposto nello script FTP.

Le operazioni definite nello script di input vengono tradotte in azioni sul server FTP. Lo script di input è costituito di un gruppo o di comandi FTP supportati. I parametri di questi comandi possono prendere la forma di una variabile, che verrà risolta in fase di runtime.

Per le informazioni sulla creazione di uno script FTP per un destinatario Script FTP, consultare la sezione " Impostazione di un destinatario Script FTP" a pagina 65. Per le informazioni sulla creazione di uno script FTP per una destinazione Script FTP, consultare la sezione "Impostazione di una destinazione Script FTP" a pagina 228.

Utilizzo delle mappe dal client DIS (Data Interchange Service)

Per eseguire l'operazione di deenveloping di EDI, la conversione e la convalida o per effettuare conversioni in documenti ROD, XML e EDI, importare le mappe associate dal client Data Interchange Services. Data Interchange Services è un programma installato separatamente che risiede, di solito, su un computer differente da quello su cui è in esecuzione WebSphere Partner Gateway.

Lo specialista della mappatura di Data Interchange Services crea mappe descrivendo come documenti specifici devono essere convertiti e convalidati.

Per creare qualsiasi mappa viene richiesta la definizione dei documenti di origine e destinazione. Le definizioni dei documenti di origine per EDI sono fornite da WDI, mentre per ROD e XML, è necessario crearle utilizzando il client DIS. Per EDI, importare il file .eif, il file standard nel client DIS. In caso di ROD, creare lo standard utilizzando il client DIS. Importare DTD/XSD per creare lo standard per XML. Le mappe di conversione e standard possono essere compilate separatamente.

Ad esempio, è possibile che sia disponibile un ordine di acquisto creato da un'applicazione di back-end che si desidera convertire e inviare ad un partner esterno come un ordine di acquisto EDI X12 standard (850). Lo specialista della mappatura Data Interchange Services dovrebbe scrivere una mappa in cui viene descritto in dettaglio come convertire ciascun campo o parte di dati dal programma nel formato X12. Quindi, la mappa viene esportata direttamente in WebSphere Partner Gateway, oppure in un file da importare in seguito utilizzando uno script del comando.

Per informazioni su come importare le mappe dal client Data Interchange Services, vedere " Importazione manuale di mappe" a pagina 198.

Completamento delle attività di configurazione post-installazione

Dopo aver installato WebSphere Partner Gateway, è necessario configurarlo. Di norma, questa configurazione comporta l'utilizzo della console di gestione di WebSphere Partner Gateway per impostare l'hub. In base ai requisiti della propria comunità commerciale, potrebbe anche essere necessario configurare l'infrastruttura di WebSphere Application Server che ospita i componenti di WebSphere Partner Gateway. Alcune di queste attività sono qui elencate, insieme ai link ad istruzioni dettagliate per l'esecuzione di ciascuna di esse.

- "Modifica dell'intensità della codifica" a pagina 250
- "Configurazione di SSL con Autenticazione client" a pagina 251

Capitolo 5. Avvio del server e visualizzazione della Console comunità

In questo capitolo viene descritto il modo in cui avviare il server WebSphere Partner Gateway e visualizzare la Console comunità. Sono incluse le seguenti sezioni:

- "Avvio dei componenti di WebSphere Partner Gateway"
- " Accesso alla console Comunità" a pagina 46

Per informazioni su come avviare i Cluster dalla console di gestione di WebSphere Application Server Network Deployment, consultare il Capitolo 1. "Managing the WebSphere Partner Gateway component applications" nel manuale *WebSphere Partner Gateway Administration Guide*.

Avvio dei componenti di WebSphere Partner Gateway

Informazioni su questa attività

Per avviare il server, è necessario avviare ognuno dei tre componenti di WebSphere Partner Gateway: la Console, il Gestore documenti e il Destinatario.

1. Modificare la directory \<*DirProdotto*\bin.
2. Immettere il seguente comando per avviare il Console:
   - Per i sistemi UNIX:
     ```
     ./bcgStartServer.sh console
     ```
   - Per i sistemi basati su Windows:
     ```
     bcgStartServer console
     ```
3. Immettere il seguente comando per avviare il Destinatario:
   ```
   ./bcgStartServer.sh receiver
   ```

   o
   ```
   bcgStartServer receiver
   ```
4. Immettere il seguente comando per avviare il Gestore documenti:
   ```
   ./bcgStartServer.sh router
   ```

   o
   ```
   bcgStartServer router
   ```

Le istruzioni precedenti si applicano ad un'installazione in modalità distribuita che installa ciascun componente nel proprio server delle applicazioni. Se è stato installato WebSphere Partner Gateway utilizzando la modalità semplice, tutti e tre i componenti sono installati sullo stesso server. Immettere il seguente comando per avviare il server in modalità semplice che ospita tutti e tre i componenti:

```
./bcgStartServer.sh
```

o

```
bcgStartServer
```

Le realease precedenti di WebSphere Partner Gateway hanno utilizzato un server separato di guida che deve essere anche avviato. Non è più richiesto poiché il server di aiuto è stato avviato automaticamente nell'applicazione della console.

Una volta avviati i componenti, collegarsi alla Console comunità, come descritto in " Accesso alla console Comunità". Per ulteriori dettagli sull'avvio dei server dalla console di gestione WebSphere Application Server, consultare *WebSphere Partner Gateway Administrator Guide*.

Per informazioni sull'avvio del client Data Interchange Services, consultare il manuale *WebSphere Partner Gateway Mapping Guide*.

Accesso alla console Comunità

Informazioni su questa attività

Questa sezione fornisce le procedure per la visualizzazione e l'accesso alla Console comunità. La risoluzione dello schermo consigliata è 1024x768.

Nota: la Console comunità di WebSphere Partner Gateway richiede l'attivazione del supporto dei cookie per conservare le informazioni sulla sessione. Nessuna informazione personale viene memorizzata nel cookie, che scade quando il browser viene chiuso.

1. Aprire un browser web ed immettere il seguente URL per visualizzare la console:

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

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

   Dove <*hostname*> e <*domain*> sono il nome e l'ubicazione del computer in cui si trova il componente della Console comunità.

   Nota: questi URL presumono l'utilizzo dei numeri porta predefiniti. Se i numeri porta predefiniti sono stati modificati, sostituirli con i valori specificati.

Nella maggior parte dei casi, l'amministratore hub ha inviato il nome utente, la password iniziale e il nome di accesso azienda che verranno utilizzati per accedere alla Console comunità. E' necessario acquisire queste informazioni per la seguente procedura. Se queste informazioni non sono state ricevute, contattare l'amministratore hub.

Per accedere alla Console comunità (queste istruzioni sono appropriate per i partner interni ed esterni):

1. Immettere il **Nome utente** per la propria azienda.
2. Immettere la **Password** per la propria azienda.
3. Immettere il **Nome di accesso azienda**, ad esempio, IBM.
4. Fare clic su **Accesso**. Quando si accede per la prima volta, è necessario creare una nuova password.
5. Immettere una nuova password, quindi digitare la nuova password una seconda volta nella casella di testo Verifica.
6. Fare clic su **Salva**. Il sistema visualizza lo schermo di immissione iniziale della console.

Nota: se WebSphere Partner Gateway è stato configurato utilizzando LDAP, è necessario immettere la Password e il Nome utente LDAP. Il Nome di accesso

azienda non è pertinente in questo scenario, quindi non verrà richiesto di immettere queste informazioni. Inoltre, il sistema non richiederà di modificare la propria password.

Capitolo 6. Configurazione di Console comunità

In questo capitolo viene descritto il modo in cui configurare la Console comunità per specificare gli elementi visualizzati dai partner, il modo in cui accedono alla console e il tipo di accesso alle varie attività della console. Questo capitolo include le seguenti sezioni:

- "Specifica delle informazioni sulla locale e del marchio della console"
- "Impostazione della politica di password" a pagina 51
- "Configurazione delle autorizzazioni" a pagina 52

Non è necessario effettuare nessuna di queste attività, se si desidera utilizzare le impostazioni predefinite fornite da WebSphere Partner Gateway.

Nota: è necessario utilizzare sempre la stessa istanza del browser con cui si accede alla Console comunità per apportare modifiche alla configurazione di WebSphere Partner Gateway. L'utilizzo simultaneo di più istanze del browser può causare l'eliminazione delle modifiche di configurazione.

Specifica delle informazioni sulla locale e del marchio della console

Informazioni su questa attività

Per impostazione predefinita, le pagine della Console comunità vengono presentate in lingua inglese. L'IBM fornisce le conversioni del contenuto in altre lingue come un gruppo di file che è possibile caricare. Altri elementi della console, forniti dalla IBM per le varie locale, sono grafici di banner. Facoltativamente, è possibile caricare i grafici logo di cui si dispone. Inoltre, è possibile caricare i fogli di stile personalizzati di cui si dispone utilizzati per formattare il testo delle pagine.

Si effettuano queste attività utilizzando la pagina Caricamento locale. Per visualizzare la pagina Caricamento locale:

1. Fare clic su **Amministrazione hub > Configurazione console > Configurazione locale**.
2. Fare clic su **Crea**.
3. Selezionare una posizione dall'elenco **Locale**.

La Console visualizza la pagina Caricamento locale.

Dalla pagina Caricamento locale, è possibile scegliere di effettuare le seguenti attività:

- Marchiare la console, caricando un banner unico o un logo (o entrambi)
- Caricare i file che l'IBM fornisce in modo che è possibile localizzare il contenuto degli elementi sulla console

Marchio della console

Informazioni su questa attività

È possibile personalizzare il modo in cui la Console comunità appare modificando le immagini di marchio. Il marchio della Console comunità comporta l'importazione di due immagini: lo sfondo di intestazione e il logo aziendale.

- lo sfondo di intestazione viene visualizzato nella parte superiore della Console comunità.
- lo logo della società viene visualizzato in alto a destra della Console comunità.

Le immagini devono essere file in formato .JPG conformi a determinate specifiche, perché si adattino alla finestra di Console comunità.

- Per vedere le specifiche richieste per il banner e il logo, fare clic su **Specifiche immagine** sulla finestra di Caricamento locale.
- Per vedere gli esempi di intestazione o immagine di logo, scorrere in basso nella parte **Immagini di esempio** della pagina e fare clic su **sample_headerback.jpg** o su **sample_logo.jpg**.
- Per scaricare gli esempi di un banner e un logo per utilizzare un modello per la creazione del banner e del logo, fare clic su immagini di **Esempio (sfondo di intestazione e logo aziendale)**.

Dopo aver creato il banner o il logo (o entrambi), effettuare le seguenti procedure:

1. Per caricare il banner personalizzato, effettuare le seguenti attività:
   - Nel campo **Banner**, immettere il percorso e il nome del file di immagine che si desidera utilizzare per l'intestazione/banner.
   - Fare clic su **Sfoglia** per navigare nel file .jpg che contiene il banner e selezionarlo.
2. Per caricare il logo personalizzato, effettuare una delle seguenti procedure:
   - Nel campo **Logo**, immettere il percorso e il nome del file che si desidera utilizzare per il logo aziendale.
   - Fare clic su **Sfoglia** per navigare nel file .jpg che contiene il logo e selezionarlo.
3. Fare clic su **Carica**.

Nota: quando si sostituisce lo sfondo di intestazione e il logo aziendale, è necessario riavviare la Console comunità per attivare le modifiche.

Modifica del foglio di stile

Informazioni su questa attività

Se si desidera specificare un foglio di stile differente da quello predefinito (ad esempio, se si desidera font e colori dimensionati in modo differente), effettuare questi passaggi:

1. Eseguire una delle seguenti attività:
   - Nel campo **CSS**, immettere il percorso e il nome del file che contiene il foglio di stile personalizzato.
   - Fare clic su **Sfoglia** per navigare nel file che contiene il foglio di stile e selezionarlo.
2. Fare clic su **Carica**.

Localizzazione dei dati sulla console

Informazioni su questa attività

Se si ricevono i bundle di risorse o gli altri file di locale dall'IBM, è possibile utilizzare la pagina Caricamento locale per caricarli. I bundle di risorsa includono le seguenti informazioni:

- Le **Etichette della console**, che contengono stringhe di testo che rappresentano tutto il testo nell'interfaccia
- Le **Descrizioni di evento**, che contengono stringhe di testo utilizzate per visualizzare dettagli sull'evento (ad esempio, "Un tentativo è stato effettuato per creare una connessione duplicata")
- **Nomi di evento**, che contengono stringhe di testo che rappresentano nomi di evento (ad esempio, "La connessione già esiste")
- **Descrizione di evento EDI**, che contengono stringhe di testo utilizzate per visualizzare i dettagli sull'evento EDI (ad esempio, "Errore di riconciliazione FA. Nessun ID attività trovato per le transazioni nel riconoscimento EDI ").
- **Nomi di evento EDI**, che contengono le stringhe di testo che rappresentano nomi di evento EDI (come ad esempio "Errore di riconciliazione FA")
- **Testo di evento esteso**, che contengono stringhe di testo che forniscono informazioni aggiuntive sugli eventi (ad esempio, la causa dell'evento e le informazioni sulla risoluzione dei problemi)

Per caricare un bundle di risorsa o un altro file della locale:

1. Per ogni bundle di risorsa o file, effettuare una delle seguenti attività:
   - Immettere il nome e il percorso del file.
   - Fare clic su **Sfoglia** per navigare nel file, e selezionare il file.
2. Una volta terminato il caricamento dei file, fare clic su **Carica**.

Impostazione della politica di password

È possibile impostare una politica della password per la comunità hub, se si desidera utilizzare i valori diversi da quelli impostati (dal sistema) come predefiniti. La politica della password si applica a tutti gli utenti che accedono alla Console comunità.

È possibile modificare i seguenti elementi della politica della password:

- Lunghezza minima, che rappresenta il numero minimo di caratteri che il partner deve utilizzare per la password. Il valore predefinito è di 8 caratteri.
- Tempo di scadenza, che rappresenta il numero di giorni entro i quali la password scade. Il valore predefinito è di 30 giorni.
- Unicità, che specifica il numero di password da conservare in un file di cronologia. Un partner non può utilizzare una password vecchia se questa si trova in un file di cronologia. Il valore predefinito è di 10 password.
- Caratteri speciali, che, quando selezionato, indica che le password devono contenere almeno tre dei seguenti tipi di caratteri speciali:
  – Caratteri maiuscoli
  – Caratteri minuscoli
  – Caratteri numerici
  – Caratteri speciali

  Questa impostazione consente i requisiti di protezione più severi quando le password vengono composte dei caratteri inglesi (ASCII). L'impostazione predefinita è disattivata. Si consiglia che i Caratteri speciali rimangano disattivati quando le password vengono composte di caratteri internazionali. I gruppi di caratteri di lingua non inglese potrebbero non contenere i tre richiesti al di fuori dei quattro tipi di carattere.

  I caratteri speciali supportati dal sistema sono i seguenti: '#', '@', '$', '&', '+'.

- Verifica della variazione di nome, che, quando selezionata, impedisce l'utilizzo di password che comprendono una variazione facilmente individuabile dell'accesso utente o nel nome completo Questo campo viene selezionato per impostazione predefinita.

Per modificare i valori predefiniti:

1. Fare clic su **Amministrazione hub > Configurazione di console > Politica di password**. Viene visualizzata la pagina Politica di password.
2. Fare clic sull'icona **Modifica**.
3. Modificare gli eventuali valori predefiniti in quelli che si desidera utilizzare per la politica della password.
4. Fare clic su **Salva**.

Configurazione delle autorizzazioni

Le autorizzazioni rappresentano i privilegi di cui un utente deve disporre per accedere ai vari moduli della Console.

Modalità di concessione delle autorizzazioni agli utenti

Prima di configurare le autorizzazioni, è utile comprendere il modo in cui le autorizzazioni sono concesse ai singoli utenti. Tutti e tre tipi di entità nella comunità hub–l' Amministratore hub, il Partner interno e i Partner esterni–possono avere un utente Amministratore. Durante la creazione di un partner o di un Partner interno, è anche possibile creare un utente Amministratore per la determinata entità.

Nota: nel caso del partner Operatore hub, durante l'installazione vengono creati automaticamente due utenti amministrativi: un utente Amministratore e l'utente hubadmin.

Durante la creazione del partner (come definito nella sezione "Creazione dei profili del partner" a pagina 23), fornire le informazioni di accesso al partner (come, ad esempio il nome e la password utilizzati per l'accesso). Una volta eseguito l'accesso da parte del partner, all'interno dell'organizzazione il partner crea ulteriori utenti. Il partner crea anche gruppi e assegna gli utenti a tali gruppi. Ad esempio, un'organizzazione potrebbe necessitare di un gruppo di persone che controllano il volume dei documenti. Il partner deve creare un gruppo Volume e aggiungere gli utenti ad esso.

Nota: in qualità di amministratore hub, è anche possibile definire gli utenti e i gruppi per un partner.

L'amministratore per il partner deve quindi assegnare le autorizzazioni al gruppo specifico di utenti. Ad esempio, l'Amministratore potrebbe decidere che il gruppo Volume vede solo il Volume documento e i report di Analisi documento. L'Amministratore, utilizzando la pagina Dettagli gruppo, abilita il modulo dei report dei documenti, ma disabilita tutti gli altri moduli per il gruppo Volume.

L'impostazione eseguita dall'utente, come amministratore hub, sulla pagina Autorizzazioni determina se un modulo viene elencato nella pagina Dettagli gruppo.

Alcuni moduli vengono limitati a determinati membri della comunità hub (ad esempio, gli amministratori hub, come hubadmin). Quindi, anche se si abilita uno

di questi moduli destinati per essere utilizzati da un partner, il modulo non viene visualizzato nella pagina Dettagli gruppo del partner.

Abilitazione e disabilitazione delle autorizzazioni

Informazioni su questa attività

Dalla pagina Elenco autorizzazioni, è possibile determinare le autorizzazioni disponibili da assegnare ai gruppi di utenti mediante la relativa abilitazione o disabilitazione. In caso contrario, tuttavia, definire le nuove autorizzazioni.

Per modificare le autorizzazioni predefinite:

1. Fare clic su **Amministrazione hub > Configurazione console > Autorizzazioni**. Viene visualizzato l'Elenco autorizzazioni.
2. Se si desidera modificare i valori predefiniti, effettuare le seguenti procedure:
   a. Fare clic sull'impostazione corrente (**Abilitata** o **Disabilitata**) per modificare l'impostazione.
   b. Quando viene richiesto di confermare la modifica, fare clic su **OK**.

Capitolo 7. Definizione dei destinatari

In questo capitolo viene descritto il modo in cui impostare i destinatari in WebSphere Partner Gateway. Sono incluse le seguenti sezioni:

Nota: è necessario utilizzare sempre la stessa istanza del browser con cui si accede alla Console comunità per apportare modifiche alla configurazione di WebSphere Partner Gateway. L'utilizzo simultaneo di più istanze del browser può causare l'eliminazione delle modifiche di configurazione.

Panoramica sui destinatari

Come descritto nella "Panoramica sull'elaborazione del documento" a pagina 12, il *destinatario* è responsabile dell'accettazione dei documenti in entrata, provenienti da un determinato trasporto. Un'istanza del destinatario è stata configurata per una determinata distribuzione.

I documenti, ricevuti da un destinatario sull'hub, possono provenire da partner esterni (per un'eventuale consegna al partner interno) o da un'applicazione di back-end del partner interno (per un'eventuale consegna ai partner esterni).

La Figura 16 a pagina 56 mostra un server WebSphere Partner Gateway con quattro destinatari impostati. Due destinatari (HTTP/S e FTP/S) sono validi per i documenti provenienti dai partner. Questi due destinatari rappresentano un indirizzo URI HTTP e una directory FTP. Vengono fornite le informazioni su questi destinatari ai partner per indicare il punto in cui è necessario inviare i documenti. Gli altri due destinatari (JMS e directory file) sono validi per i documenti provenienti dall'applicazione di back-end del partner interno. Questi destinatari indicano una coda ed una directory.

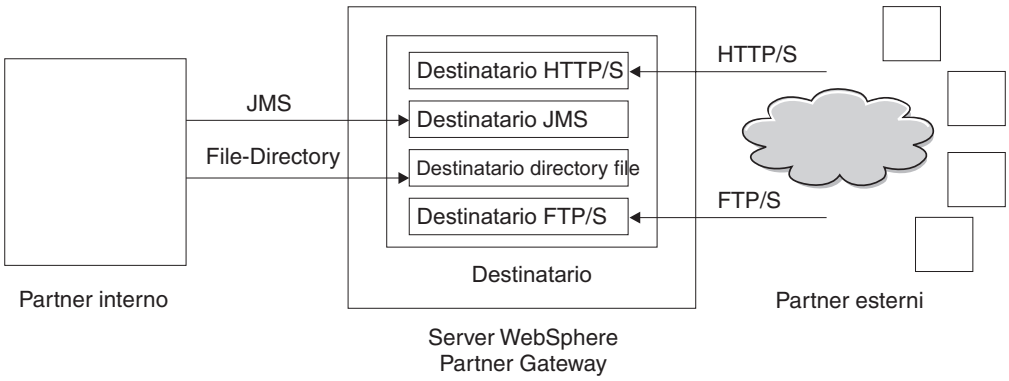


Figura 16. Trasporti e destinatari associati

Impostare almeno un destinatario per ciascun tipo di trasporto sul quale saranno inviati i documenti all'hub. Ad esempio, sarà disponibile un destinatario HTTP per ricevere eventuali documenti inviati mediante il trasporto HTTP o HTTPS. Se i partner esterni inviano i documenti su FTP, un destinatario FTP è stato impostato.

Se si dispone di requisiti speciali per alcuni documenti ricevuti, potrebbe essere necessario impostare più destinatari per un determinato trasporto. In tal caso, è necessario indicare ai partner tali requisiti e richiedere l'invio di tali documenti agli indirizzi specifici in modo tale che sia possibile eseguire un'elaborazione appropriata del destinatario.

Il Destinatario viene rilevato quando un messaggio viene ricevuto su uno dei destinatari. Alcuni destinatari rilevano i messaggi eseguendo il polling dei relativi trasporti a intervalli regolari o su base pianificata per stabilire se sono arrivati nuovi messaggi. I destinatari di WebSphere Partner Gateway, basati sul polling, sono: JMS, FTP, SMTP, File e Script FTP. Il destinatario HTTP/S si basa sul richiamo, significa che riceve la notifica dal trasporto alla ricezione dei messaggi. I trasporti definiti dall'utente possono essere sia su base polling che sul richiamo.

Aggiornamento degli handler definiti dall'utente

Informazioni su questa attività

Mediante la specifica di un handler per il destinatario, è possibile modificare i punti di configurazione per i destinatari. L'handler può essere fornito da WebSphere Partner Gateway o definito dall'utente. In questa sezione, viene descritto come caricare un handler definito dall'utente. Consultare questa sezione solo per gli handler definiti dall'utente. Gli handler forniti da WebSphere Partner Gateway sono già disponibili.

Per caricare un handler, effettuare la seguente fase:

1. Dal menu principale, fare clic su **Amministrazione hub > Configurazione hub > Handler** .
2. Fare clic su **Destinatario**.

   Viene visualizzato l'elenco degli handler attualmente definiti per i destinatari. Gli handler, forniti da WebSphere Partner Gateway, presentano un ID fornitore di **Prodotto**.
3. Dalla pagina Elenco handler, fare clic su **Importa**.
4. Nella pagina Importa handler, specificare il percorso al file XML che descrive l'handler o utilizzare **Sfoglia** per cercare il determinato file XML.

Una volta caricato un handler, è possibile utilizzarlo per personalizzare i punti di configurazione dei destinatari.

Programmi generici di gestione pre-elaborazione

Il programma di gestione di configurazione Pre-elaborazione è disponibile su tutti i tipi di destinatari ma non è applicabile ai destinatari SMTP. La seguente tabella descrive gli attributi che è possibile impostare per un programma di gestione Pre-elaborazione:

Tabella 2. Programma generico di gestione pre-elaborazione

Attributi	**Descrizione**
From Packaging Name	Questo attributo indica il package associato al documento. Questo valore deve corrispondere al tipo di impacchettamento specificato nella definizione del documento.
From Packaging Version	Questo attributo indica la versione del package specificato in **From Packaging Name**. Ad esempio, se il documento dispone di un tipo di package impostato su Nessuno, tale valore sarà N/A.
From Protocol Name	Questo attributo indica il protocollo associato al documento. Questo valore deve corrispondere al protocollo specificato nella definizione del documento.
From Protocol Version	Questo attributo indica la versione del protocollo specificato in **From Protocol Name**.
From Process Code	Questo attributo indica il processo (tipo di documento) associato a questo documento. Questo valore deve corrispondere al tipo di documento indicato nella definizione del documento.
From Process Version	Questo attributo indica la versione del processo specificato in **From Process Code**.
METADICTIONARY	Questo attributo indica il nome del dizionario al quale è associata la definizione del documento. Questo valore deve corrispondere al protocollo specificato nel campo From Protocol Name.
METADOCUMENT	Questo attributo indica il nome della definizione associato a questo documento. Tale valore deve corrispondere al processo specificato nel campo From Process Code.
METASYNTAX	Questo attributo indica la sintassi del documento che verrà elaborata in questo destinatario; i valori consentiti sono ediIchg(scambio EDI) / xml / rod (file non codificato).
ENCODING	Questo attributo indica la codifica caratteri del documento. Il valore predefinito è ASCII.
BCG_BATCHDOCS	Questo attributo viene impostato su **ON** se si desidera che i documenti vengano elaborati in un batch.
SenderId, ReceiverId	Questo attributo indica l'ID destinatario e l'ID mittente, i quali sono gli ID di business dei partecipanti, così come sono configurati nei loro profili.

Impostazione dei valori globali di trasporto

Informazioni su questa attività

Impostare gli attributi globali di trasporto validi per tutti i destinatari degli script FTP. Se non sono stati definiti i destinatari degli script FTP, ignorare questa sezione.

1. Per visualizzare l'Elenco destinatari, fare clic su **Amministrazione hub > Configurazione hub > Destinatari**.
2. Nell'Elenco destinatari, fare clic su **Attributi globali di trasporto**.
3. Se i valori predefiniti sono appropriati per la configurazione, fare clic su **Annulla**. Altrimenti, continuare con gli altri passaggi descritti in questa sezione.
4. Fare clic sull'icona **Modifica**, posta accanto a **Attribuiti globali visualizzati per categoria**.
5. Verificare e, se necessario, modificare i valori **Trasporto script FTP** e **Script FTP - Destinatari e destinazioni**.

   Il trasporto Script FTP utilizza un meccanismo di blocco che evita l'accesso simultaneo di più istanze Script FTP allo stesso destinatario. Quando un trasporto FTP è pronto per inviare documenti, richiede questo blocco. I valori predefiniti sono stati forniti per la durata di attesa dell'istanza del destinatario al fine di ottenere il blocco e il numero di volte in base al quale tenta di richiamarlo se il blocco è in uso. È anche possibile utilizzare questi valori predefiniti o modificarli. Per modificare uno o più valori, immettere il nuovo o i nuovi valori. È possibile modificare:

   - Valori **Trasporto Script FTP**
     - **Conteggio tentativi blocco**, che indica il numero di volte in base al quale il destinatario tenta di ottenere un blocco se il blocco è attualmente in uso. Il valore predefinito è 3.
     - **Intervallo tentativi del blocco (secondi)**, che indica il tempo tra un tentativo e l'altro per ottenere il blocco. Il valore predefinito è 260 secondi.
   - Valori **Script FTP - Destinatari e destinazioni**
     - **Tempo max di blocco (secondi)**, che indica la durata in cui il destinatario gestisce il blocco. Il valore predefinito è 240 secondi.
     - **Tempo max di coda (secondi)**, che indica la durata di attesa del destinatario in una coda per ottenere il blocco. Il valore predefinito è 740 secondi.
6. Fare clic su **Salva**

Impostazione di un destinatario HTTP/S

Informazioni su questa attività

Il Destinatario ha un servlet bcgreceiver predefinito che consente di ricevere i messaggi POST HTTP/S. Creare uno o più destinatari HTTP per accedere ai messaggi ricevuti dal servlet.

La seguente procedura descrive le fasi richieste per un destinatario HTTP/S.

1. Per visualizzare la pagina Elenco destinatari, fare clic su **Amministrazione hub > Configurazione hub > Destinatari**.
2. Nella pagina Elenco destinatari, fare clic su **Crea destinatario**.

Dettagli destinatario

Informazioni su questa attività

Nella sezione **Dettagli destinatario**, effettuare la seguente procedura:

1. Inserire un nome per il destinatario. Ad esempio, è possibile chiamare il destinatario HttpReceiver1. È un campo obbligatorio. Il nome immesso sarà visualizzato nell'Elenco destinatari.
2. In alternativa, indicare lo stato del destinatario. **Abilitato** è il valore predefinito. Un destinatario abilitato è in grado di accettare i documenti. Un destinatario disabilitato non è in grado di accettare i documenti.
3. In alternativa, inserire una descrizione del destinatario.
4. Selezionare **HTTP/S** dall'elenco **Trasporto**.

Configurazione destinatario

Informazioni su questa attività

Nella sezione **Configurazione destinatario**, effettuare la seguente procedura:

1. In alternativa, specificare la modalità operativa. La modalità operativa definisce la natura della trasmissione. Ad esempio, se si desidera verificare uno scambio di documenti prima di inserirlo in produzione, è preferibile inserire **Verifica**. Quello predefinito è **Produzione**.
2. Inserire l'indirizzo URI per il destinatario HTTP/S. Il nome deve iniziare con **bcgreceiver**. Ad esempio, è possibile inserire bcgreceiver/Receiver. I documenti che arrivano nel server su HTTP/S vengono ricevuti in /bcgreceiver/Receiver.
3. Per autenticare un destinatario HTTP/S utilizzando l'attributo di intestazione, impostare il flag **Abilita autenticazione di base** su true. Il valore predefinito è false.
4. Verificare e, se necessario, modificare i valori **Trasporto HTTP/S**. È possibile modificare:
   - **Timeout max sincrono (secondi)**, per indicare il numero di secondi in cui può restare attiva una connessione sincrona. Il valore predefinito è 300 secondi.
   - **Numero max di connessioni sincrone contemporanee**, per indicare quante connessioni sincrone sono consentite dal sistema. Il valore predefinito è 100 connessioni.

Nota: è possibile modificare i valori di **Instradamento sincronizzato**.

Handler

Se si ricevono file contenenti più scambi EDI o documenti XML o ROD che devono essere divisi, configurare l'handler splitter appropriato nel punto di configurazione Preelaborazione.

Se si desidera inviare o ricevere certi tipi di documenti di business (RosettaNet, cXML, SOAP e AS2) tramite uno scambio sincrono, specificare un handler per il protocollo associato nel punto di configurazione SyncCheck.

È anche possibile modificare i punti di configurazione Postelaborazione per il destinatario.

Per modificare un punto di configurazione, consultare la sezione " Modifica dei punti di configurazione" a pagina 72. Altrimenti, fare clic su **Salva**.

Impostazione di un destinatario FTP

Informazioni su questa attività

Un destinatario FTP esegue il polling del server FTP ad un intervallo fisso per cercare nuovi documenti.

Le seguenti fasi descrivono le informazioni da specificare per un destinatario FTP.

1. Per visualizzare la pagina Elenco destinatari, fare clic su **Amministrazione hub > Configurazione hub > Destinatari**.
2. Nella pagina Elenco destinatari, fare clic su **Crea destinatario**.

Risultati

Dettagli destinatario

Informazioni su questa attività

Nella sezione **Dettagli destinatario**, effettuare la seguente procedura:

1. Inserire un nome per il destinatario. Ad esempio, è possibile chiamare il destinatario FTPReceiver1. È un campo obbligatorio. Il nome immesso sarà visualizzato nell'Elenco destinatari.
2. In alternativa, indicare lo stato del destinatario. **Abilitato** è il valore predefinito. Un destinatario abilitato è in grado di accettare i documenti. Un destinatario disabilitato non è in grado di accettare i documenti.
3. In alternativa, inserire una descrizione del destinatario.
4. Selezionare **Directory FTP** dall'elenco **Trasporto**.

Configurazione destinatario

Informazioni su questa attività

Nella sezione **Configurazione destinatario**, effettuare la seguente procedura:

1. Nel campo **Directory root FTP**, inserire la directory root del server FTP. Il Gestore documenti esegue il polling delle directory secondarie del partner all'interno della directory root FTP per l'instradamento del documento. Questo campo è obbligatorio. Per le informazioni sull'impostazione della directory per un server FTP, consultare la sezione "Configurazione del server FTP per ricevere i documenti" a pagina 33.

   Nota: immettere il percorso per la directory FTP root. Non includere le directory secondarie del partner.
2. Facoltativamente, inserire un valore per **Intervallo file invariato** per indicare il numero di secondi in cui la dimensione del file deve rimanere invariata prima che il Gestore documenti recuperi il documento per l'elaborazione. In tal modo, questo intervallo invariato assicura che un documento ha completato la trasmissione (e non è ancora in transito) quando Gestore documenti lo recupera. Il valore predefinito è 3 secondi.
3. Facoltativamente, inserire un valore per **Numero di thread**, per indicare il numero di documenti che Gestore documenti elabora simultaneamente. Si consiglia come valore predefinito 1.
4. Facoltativamente, inserire un valore per **Estensioni file da escludere** per indicare i tipi di documenti che il Gestore documenti deve ignorare (escludere dall'elaborazione), se individua i documenti nella directory FTP. Ad esempio, se

si desidera che il Gestore documenti ignori i file del foglio di calcolo, nel cui caso è preferibile inserire l'estensione associata ad essi. Dopo aver immesso l'estensione, fare clic su **Aggiungi**. L'estensione viene quindi aggiunta all'elenco delle estensioni del file da ignorare. Il valore predefinito è che nessun tipo di file viene escluso.

Nota: non utilizzare un punto che precede l'estensione del nome file (ad esempio: .exe o . txt). Utilizzare solo i caratteri che denotano l'estensione file.

Handler

Se si ricevono file contenenti più scambi EDI o documenti XML o ROD che devono essere divisi, configurare l'handler splitter appropriato nel punto di configurazione Preelaborazione.

Per modificare il punto di configurazione Preelaborazione, consultare la sezione " Modifica dei punti di configurazione" a pagina 72. Altrimenti, fare clic su **Salva**.

Impostazione di un destinatario SMTP (POP3)

Informazioni su questa attività

Un destinatario SMTP esegue il polling del server di posta POP3 (in base alla pianificazione specificata) per ricercare nuovi documenti.

Le seguenti fasi descrivono le informazioni da specificare per un destinatario SMTP (POP3).

1. Per visualizzare la pagina Elenco destinatari, fare clic su **Amministrazione hub > Configurazione hub > Destinatario**.
2. Nella pagina Elenco destinatari, fare clic su **Crea destinatario**.

Risultati

Dettagli destinatario

Informazioni su questa attività

Nella sezione **Dettagli destinatario**, effettuare la seguente procedura:

1. Inserire un nome per il destinatario. Ad esempio, è possibile chiamare il destinatario POP3Receiver1. È un campo obbligatorio. Il nome immesso sarà visualizzato nell'Elenco destinatari.
2. In alternativa, indicare lo stato del destinatario. **Abilitato** è il valore predefinito. Un destinatario abilitato è in grado di accettare i documenti. Un destinatario disabilitato non è in grado di accettare i documenti.
3. In alternativa, inserire una descrizione del destinatario.
4. Selezionare **POP3** dall'elenco **Trasporto** .

Configurazione destinatario

Informazioni su questa attività

Nella sezione **Configurazione destinatario** della pagina, effettuare la seguente procedura:

1. Facoltativamente, indicare la Modalità operativa. La Modalità operativa definisce la natura della trasmissione. Ad esempio, se si desidera verificare uno

scambio di documenti prima di inserirlo in produzione, è preferibile inserire **Verifica**. Quello predefinito è **Produzione**.

2. Inserire l'ubicazione del server POP3 laddove viene recapitata la posta. Ad esempio, è possibile immettere un indirizzo IP.
3. Facoltativamente, inserire un numero di porta. Se non si inserisce nulla, viene utilizzato il valore di 110.
4. Inserire l'ID utente e la password necessaria per accedere al server di posta, se sono necessari un ID utente e la password.
5. Facoltativamente, inserire un valore per **Numero di thread**, per indicare il numero di documenti che Gestore documenti elabora simultaneamente. Si consiglia come valore predefinito 1.

Pianificazione

Informazioni su questa attività

Nella sezione **Pianifica** della pagina, effettuare la seguente procedura:

1. Selezionare **Pianificazione basata sull'intervallo** o **Pianificazione basata sul calendario**.
2. Eseguire uno di questi passaggi:
   - Se si seleziona **Pianificazione basata sull'intervallo**, selezionare il numero di secondi che dovrebbero intercorrere prima che si effettui di nuovo il polling del POP3 (o accettare il valore predefinito). Se si seleziona il valore predefinito, si effettua il polling del server POP3 ogni 5 secondi.
   - Se si seleziona **Pianificazione basata sul calendario**, scegliere il tipo di pianificazione (**Pianificazione giornaliera**, **Pianificazione settimanale** o **Pianificazione personalizzata**).
     - Se si seleziona **Pianificazione giornaliera**, immettere le ore e i minuti in cui effettuare il polling del POP3.
     - Se si seleziona **Pianificazione settimanale**, selezionare uno o più giorni della settimana oltre all'ora del giorno.
     - Se si seleziona **Pianificazione personalizzata**, selezionare l'ora del giorno e scegliere **Intervallo** o **Giorni selettivi** per la settimana e il mese. Con **Intervallo**, si specifica la data di inizio e quella di fine. (Ad esempio, fare clic su **Lun** e **Ven**, se si desidera effettuare il polling del server ad una certa ora solo settimanalmente). Con **Giorni selettivi**, si scelgono i giorni specifici della settimana e del mese.

Impostazione di un destinatario JMS

Informazioni su questa attività

Un destinatario JMS esegue il polling di una coda JMS (in base alla pianificazione specificata) per ricercare nuovi documenti.

Le seguenti fasi descrivono le informazioni da specificare per un destinatario JMS.

1. Per visualizzare la pagina Elenco destinatari, fare clic su **Amministrazione hub > Configurazione hub > Destinatari**.
2. Nella pagina Elenco destinatari, fare clic su **Crea destinatario**.

Nota: per informazioni sulla configurazione delle librerie di runtime in modo che WebSphere Partner Gateway possa rilevare i file jar di WebSphere MQ requisiti, consultare "Configurazione delle librerie di runtime" a pagina 40.

Dettagli destinatario

Informazioni su questa attività

Nella sezione **Dettagli destinatario**, effettuare la seguente procedura:

1. Inserire un nome per il destinatario. Ad esempio, è possibile chiamare il destinatario JMSReceiver1. È un campo obbligatorio. Il nome inserito sarà visualizzato nell'Elenco destinatari.
2. In alternativa, indicare lo stato del destinatario. **Abilitato** è il valore predefinito. Un destinatario abilitato è in grado di accettare i documenti. Un destinatario disabilitato non è in grado di accettare i documenti.
3. In alternativa, inserire una descrizione del destinatario.
4. Selezionare **JMS** dall'elenco **Trasporto** .

Configurazione destinatario

Informazioni su questa attività

Nella sezione **Configurazione destinatario** della pagina, effettuare la seguente procedura:

1. Facoltativamente, indicare il Tipo di operazione. Il Tipo di operazione definisce la natura della trasmissione. Ad esempio, se si desidera verificare uno scambio di documenti prima di inserirlo in produzione, è preferibile inserire **Verifica**. Quello predefinito è **Produzione**.
2. Inserire l'URL del provider JMS. Il valore deve corrispondere a quello immesso (il percorso del file system del file di binding) al momento della configurazione di WebSphere Partner Gateway per JMS (passo 5 a pagina 38). Inoltre, è possibile specificare la cartella secondaria per il contesto JMS come parte dell'URL del provider JMS.

   Ad esempio, senza il contesto JMS, immettere `c:/temp/JMS`. Con il contesto JMS, immettere `c:/temp/JMS/JMS`.
3. Inserire l'ID utente e la password necessaria per accedere alla coda JMS, se sono necessari un ID utente e la password.
4. Inserire un valore per il nome di coda JMS. È un campo obbligatorio. Il nome deve corrispondere a quello specificato con il comando `define q` al momento della creazione del file di binding (passo 4 a pagina 39).

   Se viene immessa la cartella secondaria per il contesto JMS al passo 2, immettere solo il nome della coda qui (ad esempio `inQ`). Se non è stata immessa la cartella secondaria per il contesto JMS nell'URL del provider JMS, specificare tale cartella prima del nome factory (ad esempio `JMS/inQ`).
5. Inserire un valore per il nome factory JMS. Questo è un campo obbligatorio. Questo nome deve corrispondere a quello specificato con il comando `define qcf` al momento della creazione del file di bind (passo 4 a pagina 39).

   Se viene immessa la cartella secondaria per il contesto JMS al passo 2, immettere solo il nome factory qui (ad esempio, `Hub`). Se non è stata immessa la cartella secondaria per il contesto JMS nell'URL del provider JMS, specificare tale cartella prima del nome factory (ad esempio `JMS/Hub`).
6. Facoltativamente, inserire il package dell'URL del provider.
7. Inserire un nome factory JNDI. Questo è un campo obbligatorio. Il valore di com.sun.jndi.fscontext.RefFSContextFactory è l'unico probabilmente utilizzato, se si imposta la configurazione JMS per WebSphere MQ come descritto in "Configurazione dell'hub per il protocollo di trasporto JMS" a pagina 37.

8. In alternativa, inserire un valore per la **Scadenza**, per indicare il numero di secondi in cui il destinatario monitora la coda JMS per i documenti. Questo campo è facoltativo.
9. Facoltativamente, inserire un valore per **Numero di thread**, per indicare il numero di documenti che Gestore documenti elaborerà simultaneamente. Si consiglia come valore predefinito 1.

Ad esempio, se si desidera impostare un destinatario al fine di corrispondere l'esempio di configurazione JMS, riportato nella sezione "Configurazione dell'hub per il protocollo di trasporto JMS" a pagina 37, è necessario:

1. Inserire il valore **JMSReceiver** nella casella **Nome destinatari**.
2. Immettere uno dei seguenti valori nella casella **URL del provider JMS**:
   - **file:///C:/TEMP/JMS/JMS** nel caso di Windows
   - **file:///opt/temp** nel caso di UNIX.
3. Inserire il valore **inQ** nella casella **Nome coda JMS**.
4. Inserire il valore **Hub** nella casella **Nome factory JMS**.

Handler

Se si ricevono file contenenti più scambi EDI o documenti XML o ROD che devono essere divisi, configurare l'handler splitter appropriato nel punto di configurazione Preelaborazione.

Per modificare i punti di configurazione per questo destinatario, consultare la sezione " Modifica dei punti di configurazione" a pagina 72. Altrimenti, fare clic su **Salva**.

Impostazione di un destinatario Directory file

Informazioni su questa attività

Un destinatario Directory file esegue il polling di una directory in base ad un intervallo fisso per ricercare nuovi documenti.

Le seguenti fasi descrivono le informazioni da specificare per un destinatario directory file.

1. Per visualizzare la pagina Elenco destinatari, fare clic su **Amministrazione hub > Configurazione hub > Destinatari**.
2. Nella pagina Elenco destinatari, fare clic su **Crea destinatario**.

Dettagli destinatario

Informazioni su questa attività

Nella sezione **Dettagli destinatario**, effettuare la seguente procedura:

1. Inserire un nome per il destinatario. Ad esempio, è possibile chiamare il destinatario FileReceiver1. È un campo obbligatorio. Il nome inserito sarà visualizzato nell'Elenco destinatari.
2. In alternativa, indicare lo stato del destinatario. **Abilitato** è il valore predefinito. Un destinatario abilitato è in grado di accettare i documenti. Un destinatario disabilitato non è in grado di accettare i documenti.
3. In alternativa, inserire una descrizione del destinatario.
4. Selezionare **Directory file** dall'elenco **Trasporto** .

Configurazione destinatario

Informazioni su questa attività

Nella sezione **Configurazione destinatario** della pagina, effettuare la seguente procedura:

1. Inserire un valore per **Percorso root del documento** per indicare dove i documenti saranno ricevuti.

   Se la directory principale non esiste, viene creata una nuova directory per il destinatario. Ma, se la directory principale esiste già, verrà utilizzata dal destinatario. Ciò vale solo da WebSphere Partner Gateway 6.1.1 in poi.

   Il prefisso `file://` è facoltativo.

   Ad esempio, se si desidera specificare la directory `c:\wpg\receivers\file1` come Percorso root del documento, immettere `c:\wpg\receivers\file1` o `file://c:\wpg\receivers\file1`.
2. In alternativa, inserire un valore per **Intervallo di polling** per indicare la frequenza con cui effettuare il polling della directory per i nuovi documenti. Se non viene inserito nulla, il polling della directory viene effettuato ogni 5 secondi.
3. Facoltativamente, inserire un valore per **Intervallo file invariato** per indicare il numero di secondi in cui la dimensione del file deve rimanere invariata prima che il Gestore documenti recuperi il documento per l'elaborazione. In tal modo, questo intervallo invariato assicura che un documento ha completato la trasmissione (e non è ancora in transito) quando Gestore documenti lo recupera. Il valore predefinito è 3 secondi.
4. Facoltativamente, inserire un valore per **Numero di thread**, per indicare il numero di documenti che Gestore documenti elabora simultaneamente. Si consiglia come valore predefinito 1.

Handler

Se si ricevono file contenenti più scambi EDI o documenti XML o ROD che devono essere divisi, configurare l'handler splitter appropriato nel punto di configurazione Preelaborazione.

Per modificare il punto di configurazione Preelaborazione, consultare la sezione " Modifica dei punti di configurazione" a pagina 72. Altrimenti, fare clic su **Salva**.

Impostazione di un destinatario Script FTP

Informazioni su questa attività

Un destinatario Script FTP è un destinatario di polling che viene eseguito in base alla pianificazione impostata. Il comportamento di un destinatario Script FTP è regolato da uno script di comandi FTP.

A differenza del destinatario FTP, che esegue il polling di una directory sul server FTP, il destinatario Script FTP esegue il polling di directory su un altro server (ad esempio, VAN).

Nota:

1. Se il database non è attivo e l'utente blocco è impostato su "Sì", il destinatario Script FTP potrebbe non funzionare in quanto non riceverà il blocco dal database.

2. Il partner deve assicurarsi che il documento sia completo perché il destinatario Script FTP possa riceverlo. Questa operazione può essere eseguita facendo in modo che il Server FTP tenga il documento bloccato fino a quando non è completo oppure facendo in modo che il partner scriva il documento in una directory temporanea e sposti quindi il documento completato nella directory utilizzata dal destinatario Script FTP.

Creazione dello script FTP

Informazioni su questa attività

I server FTP possono avere requisiti specifici per i comandi consentiti. Per utilizzare un destinatario Script FTP, creare un file che include tutti i comandi FTP richiesti dal server FTP a cui si è connessi. (È necessario ricevere queste informazioni dall'amministratore del server FTP.)

1. Creare uno script per i destinatari, per indicare le azioni che si desidera eseguire. Di seguito è riportato un esempio di script di connessione al server FTP specificato (con nome e password specificati), passando alla directory specificata sul server FTP e ricevendo tutti i file in quella directory.

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

   I segnaposto (ad esempio, %BCGSERVERIP%) sono stati sostituiti quando il destinatario è in servizio dai valori inseriti al momento della creazione di una determinata istanza di un destinatario Script FTP. In questo esempio, %BCGOPTION% è il nome della directory nel comando `cd`. I parametri dello script e i relativi campi associati Destinatario Script FTP sono riportati nella Tabella 3:

Tabella 3. Modalità in cui i parametri sono associati alle voci del campo del destinatario Script FTP

Parametro dello script	Voce del campo del destinatario Script FTP
%BCGSERVERIP%	IP server
%BCGUSERID%	ID utente
%BCGPASSWORD%	Password
%BCGOPTIONx%	Opzione*x*, in **Attributi definiti dall'utente**

2. Salvare il file.

Comandi script FTP

È possibile utilizzare i seguenti comandi, quando si crea lo script:

- ascii, binario, passivo, epsv

  Questi comandi non vengono inviati al server FTP. Modificano la modalità di trasferimento (ascii, binario o passivo) al server FTP.
- cd

  Questo comando passa alla directory specificata.
- delete

  Questo comando rimuove un file dal server FTP.
- get

  Questo comando utilizza un singolo argomento, il nome del file da recuperare dal sistema remoto. Il file richiesto viene trasferito in WebSphere Partner

Gateway. Utilizzare questo comando solo per recuperare un singolo file il cui nome è noto, altrimenti il comando `mget` utilizzare il comando con caratteri globali.

- getdel

  Questo comando è uguale al comando `get`, escluso per il fatto che il file viene rimosso dal sistema remoto quando WebSphere Partner Gateway ottiene il file per l'elaborazione.

- mget

  Questo comando utilizza un singolo argomento, che descrive un gruppo di file da recuperare. La descrizione può includere i caratteri jolly standard ('*' e '?'). Uno o più file vengono quindi recuperati dal sistema remoto.

- mgetdel

  Questo comando utilizza un singolo argomento, che descrive un gruppo di file da recuperare ed eliminare dal server FTP. La descrizione può includere i caratteri jolly standard ('*' e '?'). Uno o più file vengono quindi recuperati ed eliminati dal sistema remoto.

- mkdir

  Questo comando rimuove una directory dal server FTP.

- mputren

  Questo comando è una combinazione dei comandi mput e rename. Ad esempio, il comando **mputren * *.tmp /destination/*** copia il file dalla destinazione al server FTP con l'estensione **.tmp**. Una volta completato il processo di scaricamento del documento, il file viene ridenominato e copiato nella directory **/destination** nella root FTP.

- open

  Questo comando utilizza tre parametri - l'indirizzo IP del server FTP, il nome utente e una password. Tali parametri consentono di mappare le variabili %BCGSERVERIP%, %BCGUSERID% e %BCGPASSWORD%.

  Quindi, la prima riga dello script del destinatario Script FTP deve essere:

  ```
  open %BCGSERVERIP% %BCGUSERID% %BCGPASSWORD%
  ```

- quit

  Questo comando termina una connessione esistente ad un server FTP.

- quote

  Questo comando indica che tutto ciò che segue QUOTE deve essere inviato al sistema remoto come comando. In tal modo, si inviano i comandi ad un server FTP remoto che potrebbe non essere definito nel protocollo FTP standard.

- rename

  Questo comando ridenomina un file sul server FTP.

- rmdir

  Questo comando rimuove una directory dal server FTP.

- site

  Questo comando può essere utilizzato per inviare comandi specifici del sito al sistema remoto. Il sistema remoto stabilisce se il contenuto di questo comando è valido.

Dettagli destinatario

Informazioni su questa attività

Le seguenti fasi descrivono le informazioni da specificare per un destinatario Script FTP.

1. Per visualizzare la pagina Elenco destinatari, fare clic su **Amministrazione hub > Configurazione hub > Destinatari**.
2. Nella pagina Elenco destinatari, fare clic su **Crea destinatario**.

Nella sezione **Dettagli destinatario**, effettuare la seguente procedura:

1. Inserire un nome per il destinatario. Ad esempio, è possibile chiamare il destinatario FTPScriptingReceiver1. È un campo obbligatorio. Il nome inserito sarà visualizzato nell'Elenco destinatari.
2. In alternativa, indicare lo stato del destinatario. **Abilitato** è il valore predefinito. Un destinatario abilitato è in grado di accettare i documenti. Un destinatario disabilitato non è in grado di accettare i documenti.
3. In alternativa, inserire una descrizione del destinatario.
4. Selezionare **Script FTP** dall'elenco Trasporto.

Configurazione destinatario

Informazioni su questa attività

Nella sezione **Configurazione destinatario** della pagina, effettuare la seguente procedura:

1. Facoltativamente, indicare il Tipo di operazione. Il Tipo di operazione definisce la natura della trasmissione. Ad esempio, se si desidera verificare uno scambio di documenti prima di inserirlo in produzione, è preferibile inserire **Verifica**. Quello predefinito è **Produzione**.
2. Immettere l'indirizzo IP del server FTP a cui ci si connette. Il valore immesso sostituisce %BCGSERVERIP% quando si esegue lo script FTP.
3. Inserire l'ID utente e la password necessari per accedere al server. I valori immessi sostituiscono %BCGUSERID% e %BCGPASSWORD% quando si esegue lo script FTP.
4. Indicare se il destinatario funziona in modalità SSL (secure sockets layer). In tal caso, sarà necessario scambiare i certificati con i partner, come descritto nel Capitolo 13, "Abilitazione della sicurezza per gli scambi del documento", a pagina 241.
5. Caricare il file di script seguendo questi passi:
   a. Fare clic su **Carica file di script**.
   b. Immettere il nome del file che contiene lo script per l'elaborazione dei documenti oppure utilizzare **Sfoglia** per navigare nel file.
   c. Selezionare il **Tipo di codifica del file script**.
   d. Fare clic su **Carica file** per caricare il file di script nella casella di testo **File di script al momento caricato**.
   e. Se il file di script è quello che si desidera utilizzare, fare clic su **Salva**.
   f. Fare clic su **Chiudi finestra**.
6. Nel campo **Scadenza connessione**, inserire il numero di secondi in cui un socket rimane aperto senza traffico.
7. Nel campo **Utente blocco**, indicare se il destinatario richiede un blocco, in modo tale che nessuna altra istanza di uno Script FTP possa avere l'accesso simultaneo alla stessa directory del server FTP.

Risultati

Nota: i valori di **Attributi globali script FTP** sono già riempiti e non è possibile modificarli in questa pagina. Per modificare questi valori, si utilizza la pagina Attributi globali di trasporto, come descritto in " Impostazione dei valori globali di trasporto" a pagina 58.

Attributi definiti dall'utente

Informazioni su questa attività

Se si desidera specificare attributi aggiuntivi, eseguire questi passaggi. Il valore immesso per l'opzione sostituisce %BCGOPTION*x*% quando viene eseguito lo script FTP (dove *x* corrisponde al numero dell'opzione).

1. Fare clic su **Nuovo**.
2. Immettere un valore accanto a **Opzione 1**
3. Se si dispone di attributi aggiuntivi da specificare, fare di nuovo clic su **Nuovo** ed immettere in valore.
4. Ripetere il passaggio 3 per tutti gli attributi che si desidera definire.

Si supponga, ad esempio che lo script FTP sia come segue:

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

%BCGOPTION% in questo caso dovrebbe essere della directory.

Pianificazione

Specificare se si desidera la pianificazione basata sul calendario o quella basata sull'intervallo.

- Se si seleziona **Pianificazione basata sull'intervallo**, selezionare il numero di secondi che dovrebbero intercorrere prima che si effettui il polling del server FTP (o accettare il valore predefinito).
- Se si seleziona **Pianificazione basata sul calendario**, scegliere il tipo di pianificazione (**Pianificazione giornaliera**, **Pianificazione settimanale** o **Pianificazione personalizzata**).
  - Se si seleziona **Pianificazione giornaliera**, immettere il giorno in cui effettuare il polling del server FTP.
  - Se si seleziona **Pianificazione settimanale**, selezionare uno o più giorni della settimana oltre all'ora del giorno.
  - Se si seleziona **Pianificazione personalizzata**, selezionare l'ora del giorno e scegliere **Intervallo** o **Giorni selettivi** per la settimana e il mese. Con **Intervallo**, si specifica la data di inizio e quella di fine. (Ad esempio, fare clic su **Lun** e **Ven**, se si desidera effettuare il polling del server ad una certa ora solo settimanalmente). Con **Giorni selettivi**, si scelgono i giorni specifici della settimana e del mese.

Handler

Se si ricevono file contenenti più scambi EDI o documenti XML o ROD che devono essere divisi, configurare l'handler splitter appropriato nel punto di configurazione Preelaborazione.

Per modificare il punto di configurazione Preelaborazione, consultare la sezione " Modifica dei punti di configurazione" a pagina 72. Altrimenti, fare clic su **Salva**.

Impostazione di un destinatario per un trasporto definito dall'utente

Informazioni su questa attività

Se un destinatario è stato definito per un trasporto definito dall'utente, i nomi del campo e le altre informazioni sono stati definiti all'interno del file che descrive il trasporto.

Quindi effettuare la seguente procedura:

1. Fare clic su **Amministrazione hub > Configurazione hub > Destinatario**.
2. Fare clic su **Gestisci tipi di trasporti**.
3. Inserire il nome di un file XML che definisce il trasporto (o utilizzare **Sfoglia** per navigare nel file).
4. Fare clic su **Carica**.

   Nota: dall'Elenco destinatari, è anche possibile eliminare un tipo di trasporto definito dall'utente. È impossibile eliminare un trasporto fornito da WebSphere Partner Gateway. Inoltre, non è possibile eliminare un trasporto definito dall'utente una volta utilizzato per creare un destinatario.
5. Fare clic su **Crea destinatario**.
6. Inserire un nome per il destinatario. È un campo obbligatorio. Il nome inserito sarà visualizzato nell'Elenco destinatari.
7. In alternativa, indicare lo stato del destinatario. **Abilitato** è il valore predefinito. Un destinatario abilitato è in grado di accettare i documenti. Un destinatario disabilitato non è in grado di accettare i documenti.
8. In alternativa, inserire una descrizione del destinatario.
9. Selezionare il trasporto definito dall'utente dall'elenco.
10. Completare i campi (che saranno univoci per ciascun trasporto definito dall'utente).
11. Se si desidera modificare i punti di configurazione per questo destinatario, consultare la sezione " Modifica dei punti di configurazione" a pagina 72. Altrimenti, fare clic su **Salva**.

Impostazione di un destinatario SFTP

Informazioni su questa attività

Questo fornisce supporto per l'utilizzo di SFTP (SSH-FTP) come protocollo per il trasferimento di documenti di business. SFTP fornisce la riservatezza, l'autenticazione e l'integrità del messaggio per i dati. Il componente Destinatario SFTP rende possibile l'utilizzo del Server SFTP durante lo scambio di documenti con i partner commerciali. Durante la ricezione dei documenti, viene eseguito il polling del server SFTP per i nuovi documenti. È necessario eseguire le modifiche al programma di installazione per l'installazione dell'adattatore come un adattatore di risorsa. L'adattatore della risorsa deve essere installato con le istanze del gestore documenti e destinatario.

L'adattatore richiama i file dal server SFTP e li memorizza nella directory locale. Notifica l'MDB dei file salvati e una volta che l'MDB ha ricevuto i file, è possibile eliminare tali file dalla directory locale o è possibile conservarli nella directory archivio per la configurazione.

La seguente procedura descrive le fasi richieste per un destinatario HTTP/S.

1. Fare clic su **Amministrazione hub > Configurazione hub > Destinatari** per visualizzare la pagina Elenco destinatari.
2. Nella pagina Elenco destinatari, fare clic su **Crea destinatario**.

Dettagli destinatario

Informazioni su questa attività

Nella sezione **Dettagli destinatario**, effettuare la seguente procedura:

1. Inserire un nome per il destinatario. Ad esempio, è possibile chiamare il destinatario SFTPReceiver1. Questo è un campo obbligatorio. Il nome immesso sarà visualizzato nell'Elenco destinatari.
2. In alternativa, indicare lo stato del destinatario. **Abilitato** è il valore predefinito. Un destinatario abilitato è in grado di accettare i documenti. Un destinatario disabilitato non è in grado di accettare i documenti.
3. In alternativa, inserire una descrizione del destinatario.
4. Selezionare **SFTP** dall'elenco **Trasporto**.

Configurazione destinatario

Informazioni su questa attività

Nella sezione **Dettagli destinatario**, effettuare la seguente procedura:

1. Immettere la **Modalità operativa**. Effettuare una selezione dall'elenco a discesa o fare clic su **Nuovo** per creare una modalità.
2. Nel campo **IP host SFTP**, immettere l'URL del server SFTP. Accetta un massimo di 100 caratteri. È anche possibile immettere indirizzi IP, IPv4 e IPv6.
3. Immettere il valore del **Numero porta**.
4. **Directory eventi remota** è la directory di sistema in cui l'adattatore scarica i file di evento dal sito FTP.
5. In **Tipo di autenticazione**, selezionare **Di base** (nome utente/password) o **Certificato client** (autenticazione chiave pubblica).
6. Immettere **Id utente** e **Password** per nome utente/password. Se il tipo di autenticazione è autenticazione chiave pubblica, è necessario utilizzare il **File di chiavi private** (chiavi) e la **Passphrase** (certificati configurati) nella console.
7. In **Intervallo polling SFTP**, immettere il periodo di tempo di attesa dell'adattatore per il polling.
8. In **Frequenza polling**, immettere il numero di cicli di polling trascorsi i quali l'adattatore verificherà i nuovi file nel server SFTP.
9. **Quantità polling** è il numero di eventi che l'adattatore invia all'esportazione durante ogni periodo di polling
10. **Intervallo tentativi** è il periodo di tempo di attesa dell'adattatore intercorso tra i tentativi per stabilire una nuova connessione dopo un errore durante le operazioni in entrata.
11. **Limite di tentativi** è il numero di volte per cui l'adattatore tenta di ristabilire una connessione in entrata dopo un errore.

12. **Codifica EIS** è la codifica del server FTP. Utilizzare questo valore per la connessione di controllo al server FTP.
13. Immettere il **Numero di thread**.
14. Fare clic su **Salva** per salvare la configurazione.

Modifica dei punti di configurazione

Il numero dei punti di configurazione disponibili ed il numero degli handler associati per questi punti di configurazione variano a seconda del tipo del destinatario impostato. Ad esempio, il punto di configurazione SyncCheck è disponibile solo con i destinatari HTTP/S e JMS.

Per determinati protocolli di business (RosettaNet, cXML, SOAP, e AS2) che vengono coinvolti negli scambi sincroni, è necessario specificare un handler per il punto di configurazione SyncCheck. È anche possibile modificare il modo in cui i destinatari elaborano i documenti applicando un handler definito dall'utente caricato (o un processo fornito dal prodotto) ai punti Preelaborazione e Postelaborazione del destinatario.

Per applicare un handler scritto dall'utente per questi punti di configurazione, è necessario caricare l'handler, come descritto nella sezione " Aggiornamento degli handler definiti dall'utente" a pagina 56. È anche possibile utilizzare un handler fornito dal prodotto, che è già disponibile e non deve essere caricato.

Preelaborazione

L'handler di configurazione Preelaborazione è disponibile su tutte le tipologie di destinatari ma non è valido per i destinatari SMTP.

Attributi di Preelaborazione

La Tabella 4 descrive gli attributi da impostare per un handler Preelaborazione ed elenca gli handler splitter a cui si applicano gli attributi.

Gli attributi ROD utilizzati come esempio in questa tabella corrispondono a quelli utilizzati in " Esempio da ROD a EDI" a pagina 345. Nell'esempio, gli attributi ROD sono contenuti nella mappa S_DT_ROD_TO_EDI.eif, che include la seguente definizione del documento:

- Package: Nessuno (versione N/A)
- Protocollo: ROD_TO_EDI_DICT (versione ALL)
- Tipo documento: DTROD-TO-EDI_ROD (versione ALL)

Gli attributi metadictionary e metadocument ROD associati a questo flusso sono ROD_TO_EDI_DICT e DTROD-TO-EDI_ROD.

Tabella 4. Attributi handler splitter

Attributo	Descrizione	Handler splitter
Codifica	La codifica del carattere del documento. Il valore predefinito è ASCII.	ROD Generic XML EDI

Tabella 4. Attributi handler splitter (Continua)

Attributo	Descrizione	Handler splitter
BATCHDOCS	Quando BCG_BATCHDOCS è attivo, lo splitter aggiunge ID di batch al documento quando i documenti vengono separati. Se i documenti vengono convertiti in transazioni EDI da sottoporre a enveloping, l'Enveloper utilizza ID batch per verificare che le transazioni siano state posizionate nello stesso scambio EDI (se possibile) prima di essere recapitate. L'Enveloper deve disporre dell'attributo batch impostato su **On** (valore predefinito). Fare riferimento a "Modalità batch" a pagina 182.	ROD Generic XML
From Packaging Name	L'impacchettamento associato al documento. Questo valore deve corrispondere al tipo di impacchettamento specificato nella definizione del documento. Ad esempio, per un documento che dispone di un tipo di impacchettamento impostato su Nessuno, questo valore deve essere **Nessuno**.	ROD Generic
From Packaging Version	La versione di impacchettamento specificata in From Packaging Name. Ad esempio, se il documento dispone di un tipo di impacchettamento impostato su Nessuno, questo valore deve essere **N/A**.	ROD Generic
From Protocol Name	Il protocollo associato al documento. Questo valore deve corrispondere al protocollo specificato nella definizione del documento. Ad esempio, per un documento ROD, questo valore può essere **ROD-TO-EDI_DICT**.	ROD Generic
From Protocol Version	La versione del protocollo specificata in From Protocol Name. Ad esempio per il protocollo ROD-TO-EDI_DICT, il valore deve essere **ALL**.	ROD Generic
From Process Code	Il processo (tipo di documento) associato a questo documento. Questo valore deve corrispondere al tipo di documento indicato nella definizione del documento. Ad esempio, per un documento ROD, questo valore può essere DTROD-TO-EDI_ROD.	ROD Generic
From Process Version	La versione del processo specificata in From Process Code. Ad esempio, per DTROD-TO-EDI_ROD, questo valore deve essere **ALL**.	ROD Generic
Metadictionary	L'attributo metadictionary fornisce le informazioni che consentono a WebSphere Partner Gateway di interpretare i dati. Ad esempio, per un documento ROD, questo valore può essere **ROD-TO-EDI_DICT**.	ROD Generic
Metadocument	L'attributo metadocument fornisce le informazioni che consentono a WebSphere Partner Gateway di interpretare i dati. Ad esempio, per un documento ROD, questo valore può essere **DTROD-TO-EDI_ROD**.	ROD Generic
Metasyntax	L'attributo metasyntax descrive il formato del documento che sta per essere suddiviso. Il valore predefinito è **rod**.	ROD Generic
SenderId	ID del partner che esegue l'invio.	Generic
ReceiverId	ID del partner destinatario.	Generic

Notes:

1. Solo un tipo di documento ROD per istanza del destinatario è supportato.

2. Se un destinatario dispone di più handler splitter configurati (ad esempio, se ha gli handler splitter ROD, XML e EDI configurati), l'handler splitter ROD deve essere l'ultimo nell'**Elenco configurato**.

Modifica del punto di configurazione Preelaborazione

Informazioni su questa attività

Per modificare il punto di configurazione Preelaborazione, effettuare la seguente procedura:

1. Selezionare **Preelaborazione** dall'elenco **Handler del punto di configurazione**.

   Vengono forniti cinque programmi di gestione Pre-elaborazione (per impostazione predefinita) e vengono riportati nell'**Elenco disponibili**.

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

   Nota: gli handler Preelaborazione non sono validi per i destinatari SMTP.
2. Se si ricevono più scambi EDI o documenti XML o ROD da separare, assicurarsi di selezionare l'handler splitter appropriato. Per configurare la fase Preelaborazione:
   a. Selezionare un handler dall'**Elenco disponibile** e fare clic su **Aggiungi**. L'handler si sposta dall'**Elenco disponibile** all'**Elenco configurato**, come descritto nella sezione Figura 17:

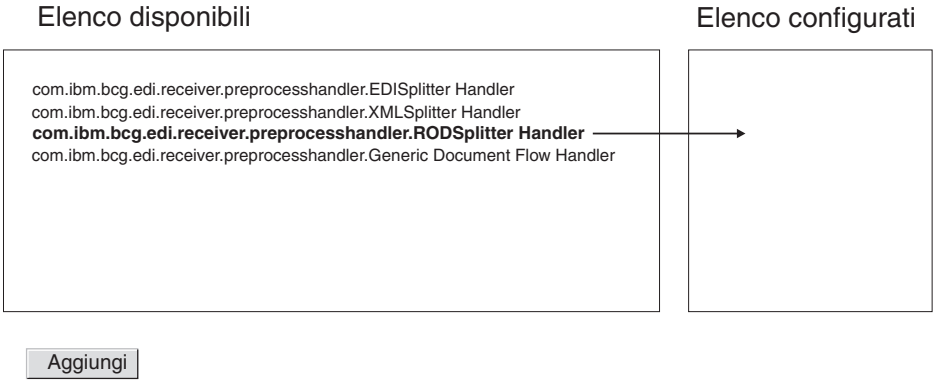


Figura 17. Configurazione della fase Preelaborazione per un destinatario

   b. Ripetere questo passaggio per ciascun handler che si desidera aggiungere all'elenco configurato.

      Per i destinatari, gli handler sono stati chiamati nell'ordine in cui sono visualizzati nell'**Elenco configurato**. Il primo handler valido elabora la richiesta e i successivi handler dell'elenco non sono stati chiamati.
   c. Configurare l'handler selezionandolo e facendo clic su **Configura**:
      - Se è stato aggiunto EDISplitterHandler, è possibile modificare l'attributo Codifica. Il valore predefinito per la codifica è ASCII.
      - Se è stato aggiunto XMLSplitterHandler, è possibile modificare l'attributo BCGBATCHDOC. Il valore predefinito è **ON**. Per le informazioni su questo attributo, consultare la sezione "Attributi di Preelaborazione" a pagina 72.

- Se è stato aggiunto RODSplitterHandler, è possibile modificare i valori di 11 attributi. La codifica, BATCHDOCS e Metasyntax presentano valori predefiniti. Per gli altri attributi, è necessario immettere un valore per From Packaging Name, From Packaging Version, From Protocol Name, From Protocol Version, From Process Code, From Process Version, Metadictionary, e Metadocument. Per le informazioni su tali attributi, consultare la sezione "Attributi di Preelaborazione" a pagina 72.
- Se è stato aggiunto GenericDocumentFlowHandler, è possibile specificare i valori di 13 attributi. La codifica e BATCHDOCS hanno valori predefiniti. Gli attributi SenderId e ReceiverId vengono pre-configurati per GenericDocumentFlowHandler senza alcun valore predefinito. Per gli altri attributi, digitare un valore per From Packaging Name, From Packaging Version, From Protocol Name, From Protocol Version, From Process Code, From Process Version, Metadictionary, Metadocument e Metasyntax. Per le informazioni su tali attributi, consultare la sezione "Attributi di Preelaborazione" a pagina 72.
- Se è stato aggiunto FileNamePartnerId, non prevede i parametri di configurazione. Prevede il file ricevuto per seguire questa convenzione di denominazione:

  ```
  <anystring>bcgrcv<Receiver ID>bcgsdr<Sender ID>bcgend<anystring>
  ```

  dove

  Receiver ID ,Sender ID
  Sono gli ID di business dei partecipanti come configurati nei relativi profili.

  bcgrcv, bcgsdr
  Sono costanti di stringhe che segnano l'inizio degli ID di business del mittente e del destinatario.

  bcgend
  È una costante di stringa che determina la fine della stringa della convenzione di denominazione richiesta

  anystring
  indica il carattere alfanumerico scelto dall'utente

  Questo handler può essere configurato solo per i destinatari Script FTP o Directory file. Per ricevere i file binari su Script FTP o Directory file, è possibile configurare questo handler per il destinatario.

SyncCheck

Informazioni su questa attività

Il punto di configurazione SyncCheck è disponibile solo per i destinatari HTTP/S e JMS.

Per specificare un handler per un protocollo di business coinvolto in uno scambio sincrono, procedere nel modo seguente:

1. Selezionare **SyncCheck** dall'elenco **Handler del punto di configurazione**.
   i sei handler SyncCheck sono forniti (per impostazione predefinita) per un destinatario HTTP/S. Questi handler sono mostrati nell'**Elenco disponibile**:
   - com.ibm.bcg.server.sync.As2SyncHdlr
   - com.ibm.bcg.server.sync.CxmlSyncHdlr
   - com.ibm.bcg.server.sync.RnifSyncHdlr

- com.ibm.bcg.server.sync.SoapSyncHdlr
- com.ibm.bcg.server.sync.DefaultAsynchronousSyncCheckHandler
- com.ibm.bcg.server.sync.DefaultSynchronousSyncCheckHandler
- com.ibm.bcg.server.sync.EBMSSyncCheckHandler

Ad esempio, se si configura il destinatario HTTP/S, l'Elenco disponibile appare nel modo seguente:

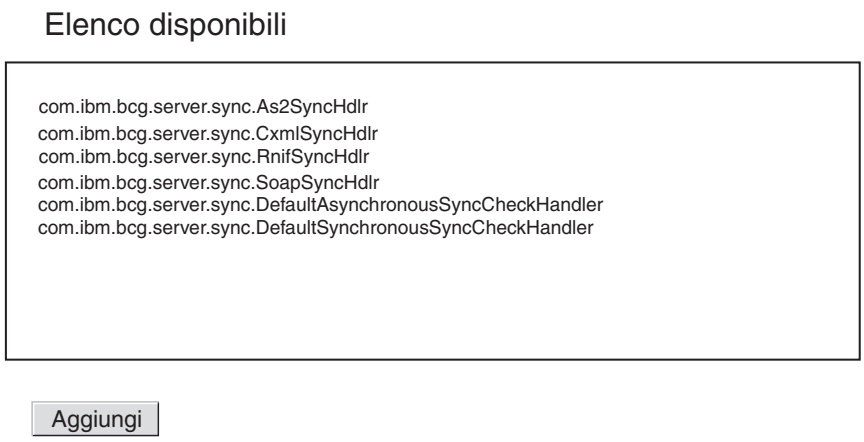


Figura 18. Elenco di handler disponibili per il punto di configurazione HTTP/S SyncCheck

Come è possibile notare dalla convenzione di denominazione, i primi quattro handler sono specifici ai quattro tipi di documento che possono essere utilizzati per le transazioni sincrone. Qualsiasi richiesta che utilizza DefaultAsynchronousSyncCheckHandler viene considerata come richiesta sincrona. Qualsiasi richiesta che utilizza DefaultSynchronousSyncCheckHandler viene considerata come richiesta sincrona.

È possibile utilizzare DefaultAsynchronousSyncCheckHandler e DefaultSynchronousSyncCheckHandler con gli altri destinatari (come, ad esempio un destinatario JMS).

2. Se si ricevono documenti sincroni su questo destinatario, effettuare la seguente procedura:
   a. Selezionare uno o più handler dall'**Elenco disponibile** e fare clic su **Aggiungi**.
   b. Ripetere questa procedura, se si desidera aggiungere altri handler all'elenco. Per i destinatari, gli handler sono stati chiamati nell'ordine in cui sono visualizzati nell'**Elenco configurato**. Il primo handler disponibile elabora la richiesta e gli altri handler dell'elenco non sono chiamati.

   Per i destinatari HTTP e HTTPS, è opportuno elencare l'handler SyncCheck specifico (ad esempio, com.ibm.bcg.server.sync.As2SyncHdlr per le transazioni AS2) prima di elencare gli handler SyncCheck predefiniti.

Postelaborazione

Informazioni su questa attività

Per impostazione predefinita non viene fornito alcun handler per la fase Postelaborazione e, di conseguenza, nessun handler viene elencato nell'**Elenco disponibile**. Tuttavia, è possibile caricare un handler per questo punto di configurazione per tutte le tipologie dei destinatari che supportano la comunicazione sincrona. I tipi di handler disponibili per la fase Postelaborazione sono:

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

Aggiungere un handler Postelaborazione caricando un handler conforme ad una di queste tipologie di handler. Viene utilizzata l'opzione **Importa** della pagina Elenco handler per caricare un handler definito dall'utente. Quando un handler del destinatario definito dall'utente è stato caricato, l'handler è stato aggiunto all'Elenco handler. Viene inoltre visualizzato nell'Elenco disponibile per il tipo del punto di configurazione al quale appartiene.

Per modificare il punto di configurazione Postelaborazione, procedere nel modo seguente:

1. Selezionare **Postelaborazione** dall'elenco **Handler del punto di configurazione**.
2. Selezionare un handler definito dall'utente nell'**Elenco disponibile** e fare clic su **Aggiungi**. L'handler si sposta dall'**Elenco disponibile** all'**Elenco configurato**

Modifica dell'elenco configurato

Informazioni su questa attività

Se è necessario modificare l'ordine degli handler, eliminare un handler o configurare gli attributi dell'handler, procedere nel modo seguente:

- Rimuovere un handler selezionandolo nell'**Elenco configurato** e facendo clic su **Rimuovi**. L'handler viene spostato nell'**Elenco disponibile**.
- Disporre nuovamente l'ordine in base al quale l'handler viene utilizzato selezionandolo e facendo clic su **Sposta su** o **Sposta giù**.
- Configurare l'handler selezionandolo nell'**Elenco configurato** e facendo clic su **Configura**. Verrà visualizzato l'elenco degli attributi da configurare.

Capitolo 8. Configurazione delle azioni e delle fasi del flusso di lavoro fisso

In questo capitolo, vengono descritte le attività facoltative che è possibile eseguire per configurare flussi di lavoro fissi ed azioni in entrata e in uscita. Se non è necessario modificare il comportamento fornito dal prodotto dei flussi di lavoro o delle azioni, ignorare questo capitolo.

Questo capitolo include le seguenti sezioni:

Nota: è necessario utilizzare sempre la stessa istanza del browser con cui si accede alla Console comunità per apportare modifiche alla configurazione di WebSphere Partner Gateway. L'utilizzo simultaneo di più istanze del browser può causare l'eliminazione delle modifiche di configurazione.

Aggiornamento degli handler

Informazioni su questa attività

Se si modificano i componenti, caricare prima gli handler per determinati componenti prima di creare o configurare i componenti. È necessario caricare solo gli handler definiti dall'utente per i componenti necessari. Ad esempio, se si aggiunge una fase di convalida, è necessario caricare l'handler dalla pagina Azioni di **Handler** (come descritto nelle fasi da 1 a 4 a pagina 80).

Nota: come menzionato nella sezione "Configurazione dei componenti di elaborazione del documento con gli handler" a pagina 14, solo gli handler definiti dall'utente sono caricati. Gli handler forniti da WebSphere Partner Gateway sono già disponibili.

È possibile modificare i flussi di lavoro fissi e le azioni e creare nuove azioni. Si modificano questi componenti dagli handler associati.

Nota: è possibile elencare i validi tipi di handler per le azioni ed i flussi di lavoro fissi facendo clic su **Amministrazione hub > Configurazione hub > Handler > Azione > Tipi di handler** o **Amministrazione hub > Configurazione hub > Handler > Flusso di lavoro fisso > Tipi di handler**. Utilizzare questo elenco per confermare che l'handler è un tipo valido prima di caricarlo. È necessario che sia uno dei tipi consentiti o non sarà caricato correttamente.

Per caricare un handler, effettuare la seguente fase:

1. Dal menu principale, fare clic su **Amministrazione hub > Configurazione hub > Handler** .
2. Selezionare il tipo di handler (**Azione** o **Flusso di lavoro fisso**).

   Viene visualizzato l'elenco degli handler attualmente definiti per un determinato componente. Vengono elencati gli handler forniti da WebSphere Partner Gateway. Presentano un ID fornitore di **Prodotto**.
3. Dalla pagina Elenco handler, fare clic su **Importa**.

4. Nella pagina Importa handler, specificare il percorso al file XML che descrive l'handler o utilizzare **Sfoglia** per cercare il determinato file XML.
5. Fare clic su **Carica**.

Dopo il caricamento dell'handler, è possibile utilizzarlo per creare nuove azioni e flussi di lavoro.

Nota: è possibile aggiornare gli handler definiti dall'utente caricando il file XML modificato. Per un handler di azione, ad esempio, fare clic su **Amministrazione hub > Configurazione hub > Handler > Azione**, quindi fare clic su **Importa**.

Non è possibile modificare o eliminare gli handler forniti da WebSphere Partner Gateway.

Configurazione dei flussi di lavoro fissi

Informazioni su questa attività

Il Capitolo 2, "Introduzione alla configurazione dell'hub", a pagina 5 viene descritto nelle due fasi del flusso di lavoro fisso in entrata che è possibile configurare, una per spacchettare un protocollo e una per analizzare quest'ultimo. Per i flussi di lavoro in uscita, esiste una fase per lo spacchettamento del protocollo.

Se si utilizza un handler definito dall'utente per configurare una fase del flusso di lavoro, caricare l'handler come descritto nella sezione " Aggiornamento degli handler" a pagina 79.

Per configurare un flusso di lavoro fisso, effettuare le seguenti fasi:

1. Fare clic su **Amministrazione hub > Configurazione hub > Flusso di lavoro fisso**.
2. Fare clic su **In entrata** o **In uscita**.
3. Fare clic sull'icona **Visualizza i dettagli** accanto al nome della fase che si desidera configurare.

   Viene visualizzata la fase, insieme all'elenco di handler già configurati per questa fase. Per un elenco degli handler predefiniti, vedere "Flussi di lavoro in entrata" a pagina 81 e "Flusso di lavoro in uscita" a pagina 81.
4. Fare clic sull'icona **Modifica** per modificare l'elenco degli handler.
5. Eseguire una o più delle seguenti attività per ciascuna fase si desidera modificare.
   a. Aggiungere un handler selezionandolo nell'**Elenco disponibile** e facendo clic su **Aggiungi**. (È possibile che sia visualizzato un handler nell'**Elenco disponibile**, se è stato caricato un handler definito dall'utente o se è stato precedentemente rimosso un handler dall'**Elenco configurato**). L'handler viene spostato nell'**Elenco configurato**.
   b. Rimuovere un handler selezionandolo nell'**Elenco configurato** e facendo clic su **Rimuovi**. L'handler viene spostato nell'**Elenco disponibile**.
   c. Riorganizzare l'ordine in base al quale gli handler sono chiamati selezionando l'handler e facendo clic su **Sposta su** o su **Sposta giù**.

      Gli handler vengono chiamati nell'ordine in cui sono riportati nell'**Elenco configurato**. Il primo handler disponibile che può elaborare la richiesta è l'unico che gestisce la richiesta. Se si anticipa la ricezione di un grande numero di documenti di un certo tipo (ad esempio, documenti ROD), è

possibile spostare l'handler associato a quel tipo di documento (in questo esempio, com.ibm.bcg.edi.business.process.RODScannerHandler) nella parte iniziale dell'elenco.

6. Fare clic su **Salva**.

Flussi di lavoro in entrata

In questa sezione, vengono elencati gli handler configurati per i flussi di lavoro in entrata.

Handler spacchettamento protocollo

Per impostazione predefinita, la fase di spacchettamento del protocollo dispone dei seguenti handler configurati:

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

Handler elaborazione protocollo

Per impostazione predefinita, la fase di elaborazione del protocollo dispone dei seguenti handler configurati:

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

L'attributo ″Content-Types″ è associato a BinaryChannelParseHandler, XMLRouterBizHandler, EDIRouterBizProcessHandler e cXMLChannelParseHandler. Questi handler sono stati inseriti con l'elenco predefinito dei tipi di contenuti. Se il documento ricevuto include un'intestazione content type, configurata per uno degli handler precedenti, tale handler viene applicato.

Flusso di lavoro in uscita

Per impostazione predefinita, la fase di Impacchettamento del protocollo dispone dei seguenti handler configurati:

- com.ibm.bcg.server.pkg.NullPackagingHandler
- com.ibm.bcg.ediint.ASPackagingHandler
- com.ibm.bcg.edi.server.EDITransactionHandler
- com.ibm.bcg.rosettanet.pkg.RNOPPackagingHandler
- com.ibm.bcg.server.pkg.RNPassThruPackagingHandler
- com.ibm.bcg.cxml.cXMLPackagingHandler
- com.ibm.bcg.soap.SOAPPackagingHandler
- com.ibm.bcg.eai.EAIPackagingHandler

Configurazione di azioni

Il Capitolo 2, “Introduzione alla configurazione dell’hub”, a pagina 5 descrive le azioni che possono essere effettuate da una o più fasi. WebSphere Partner Gateway fornisce una serie di azioni predefinite. È possibile aggiungere all’elenco di azioni caricando uno o più handler di azioni (che sono fasi nell’azione), che è possibile utilizzare in un’azione. È, inoltre, possibile creare nuove azioni come descritto in “Creazione di azioni” a pagina 98.

Nota: è impossibile modificare le azioni fornite da WebSphere Partner Gateway, anche se è possibile copiare una di queste e modificarla, come descritto in “Copia di un’azione” a pagina 99.

Se si utilizza un handler definito dall’utente per configurare un’azione, caricare l’handler come descritto nella sezione “ Aggiornamento degli handler” a pagina 79.

Azioni fornite dal prodotto

Questa sezione fornisce i dettagli sulle azioni fornite dal prodotto WebSphere Partner Gateway riguardo all’obiettivo e all’eventuale configurazione richiesta per utilizzarle. Il Capitolo 9, “Configurazione dei tipi di documenti”, a pagina 101 fornisce ulteriori informazioni dettagliate sul momento in cui utilizzare alcune di queste azioni.

Il nome di alcune azioni include Bidirezionale. Il termine *Bidirezionale* significa che i formati di origine e di destinazione possono essere invertiti e l’azione può essere ancora utilizzata. Ad esempio, per l’azione “Conversione bidirezionale di RosettaNet e XML con convalida”, il documento di origine può essere RosettaNet e il documento di destinazione XML o il documento di origine può essere XML e il documento di destinazione RosettaNet.

Di seguito sono riportate le varie Azioni fornite in WebSphere Partner Gateway:

- “Pass Through” a pagina 83
- “Annullamento del partner interno del processo RosettaNet” a pagina 83
- “Pass Through di RosettaNet con registrazione del processo” a pagina 84
- “Conversione bidirezionale di RosettaNet e del contenuto del servizio di RosettaNet con convalida” a pagina 85
- “Conversione bidirezionale di RosettaNet e del contenuto del servizio RosettaNet senza convalida del contenuto” a pagina 86
- “Conversione bidirezionale di XML personalizzato del partner interno in RosettaNet con verifica duplicati del contenuto e convalida” a pagina 87
- “Conversione bidirezionale di RosettaNet e XML con convalida” a pagina 85
- “Conversione bidirezionale di XML personalizzati con convalida” a pagina 88
- “Conversione bidirezionale dell’XML personalizzato con verifica duplicati e convalida” a pagina 89
- “Pass Through XML personalizzato con verifica e convalida duplicati” a pagina 89
- “Pass Through XML personalizzato con verifica duplicati” a pagina 90
- “Pass Through XML personalizzato con convalida” a pagina 91
- “Deenveloping di EDI” a pagina 91
- “Convalida EDI e conversione EDI” a pagina 92
- “Conversione ROD (FlatFile) e convalida EDI” a pagina 93

Pass Through

Obiettivo

Questa azione viene utilizzata quando non si verifica alcuna elaborazione speciale sul documento, come, ad esempio, la convalida o la conversione. Il documento di origine viene inviato al percorso di destinazione nello stato in cui si trova.

Configurazione

Non è richiesta alcuna azione.

Modifica

Questa azione può essere copiata in una nuova azione. Le nuove fasi possono essere aggiunte prima delle fasi esistenti. Ad esempio, una fase di convalida personalizzata convalida il documento di origine o altre elaborazioni personalizzate.

Fasi

Questa azione contiene le seguenti fasi, eseguite in sequenza:

1. **com.ibm.bcg.passthrough.No_op** – consente di indicare che l'intestazione content type del documento di destinazione non deve provenire dal contenuto del documento.
2. **com.ibm.bcg.outbound.OutboundDocFactory** - è sempre richiesto. Effettua l'elaborazione richiesta di WebSphere Partner Gateway sul documento di destinazione. Si tratta dell'ultima fase ed è stata aggiunta automaticamente dalla Console alle azioni esistenti o alle azioni create di recente. Questa fase non viene visualizzata nell'elenco di handler configurati.

Annullamento del partner interno del processo RosettaNet

Obiettivo

Questa azione è valida per l'annullamento di un processo RNIF RosettaNet da parte del partner interno (backend). Quando l'applicazione di backend (partner interno) invia un documento Evento XML con il codice eventi 800/801, in questo passo viene creato un documento 0A1 per essere inviato al partner esterno e viene annullato il processo PIP corrispondente.

Configurazione

Il processo RNIF annullato deve essere già stato configurato in WebSphere Partner Gateway e WebSphere Partner Gateway deve aver già ricevuto il documento RosettaNet che ha avviato il processo annullato.

Modifica

Questa azione non può essere modificata o copiata poiché questa azione è specifica all'annullamento del processo PIP RosettaNet.

Fasi

Questa azione contiene le seguenti fasi, eseguite in sequenza:

1. **com.ibm.bcg.server.pkg.UnPackagingFactory** - determina la classe di spacchettamento corretta per RNIF o presume che il documento non sia RNIF e nessuno spacchettamento viene eseguita.
2. **com.ibm.bcg.validation.ValidationFactory** - convalida il documento RN di origine per il contenuto del servizio RNIF appropriato.
3. **com.ibm.bcg.outbound.OutboundDocFactory** - è sempre richiesto. Effettua l'elaborazione richiesta di WebSphere Partner Gateway sul documento di destinazione. Si tratta dell'ultima fase ed è stata aggiunta automaticamente dalla Console alle azioni esistenti o alle azioni create di recente. Questa fase non viene visualizzata nell'elenco di handler configurati.

Pass Through di RosettaNet con registrazione del processo

Obiettivo

Questa azione viene utilizzata quando il documento RNIF di origine RosettaNet viene autorizzato in WebSphere Partner Gateway. Utilizzare questa fase quando il contenuto del servizio del documento RNIF non viene estratto o convertito. Anche se si tratta di un Pass Through, l'elaborazione RNIF è ancora effettuata con le notifiche di ricezione create.

Configurazione

Non è richiesta alcuna azione

Modifica

Questa azione può essere copiata e modificata. Le nuove fasi possono essere aggiunte prima delle fasi esistenti per un'ulteriore elaborazione personalizzata.

Fasi

Questa azione contiene le seguenti fasi, eseguite in sequenza:

1. **com.ibm.bcg.rosettanet.passthru.ProcessLoggingFactory** - questa fase imposta i metadati del documento RosettaNet in BDO (Business Document Object).
2. **com.ibm.bcg.passthrough.No_op** - consente di indicare che l'intestazione content type del documento di destinazione non deve provenire dal contenuto del documento.
3. **com.ibm.bcg.outbound.OutboundDocFactory** - è sempre richiesto. Effettua l'elaborazione richiesta di WebSphere Partner Gateway sul documento di destinazione. Si tratta dell'ultima fase ed è stata aggiunta automaticamente dalla Console alle azioni esistenti o alle azioni create di recente. Questa fase non viene visualizzata nell'elenco di handler configurati.

Conversione bidirezionale di RosettaNet e del contenuto del servizio di RosettaNet con convalida

Obiettivo

Questa azione viene utilizzata per i documenti RNIF RosettaNet. Durante la ricezione di un documento RNIF dal partner esterno, il payload (RNSC - RosettaNet Service Content) sarà estratto dal documento impacchettato RNIF da inviare all'applicazione di backend (partner interno). La convalida si verifica sul documento RNIF incluso RNSC. Quando proviene dall'applicazione di backend (partner interno) il documento RNSC sarà convalidato.

Configurazione

Il package PIP RosettaNet per il documento RosettaNet deve essere caricato.

Modifica

Questa azione non può essere copiata e modificata.

Fasi

Questa azione contiene le seguenti fasi, eseguite in sequenza:

1. **com.ibm.bcg.server.pkg.UnPackagingFactory** - determina la classe di spacchettamento corretta per RNIF o presume che il documento non sia RNIF e nessuno spacchettamento viene eseguita.
2. **com.ibm.bcg.validation.ValidationFactory** - effettua la convalida e utilizza il seguente BusinessProcesses per convalidare i documenti RNIF 1.1, RNIF 2.0 e RNSC. - RNSignal0A1Validation (la convalida di WebSphere Partner Gateway ha creato segnali RNIF o il messaggio 0A1) - ValidationNoOp (restituisce BusinessDocument senza eseguire elaborazioni, sarà definito quando viene ritentato WBIC per segnali RNIF o il messaggio 0A1) - RN11Validation (consente di convalidare il messaggio RNIF 1.1) - RN20Validation (consente di convalidare il messaggio RNIF 2.0) - RNSCValidation (consente di convalidare l'evento XML e il messaggio RNSC)
3. **com.ibm.bcg.translation.protocol.StdRNandRNSCProtFactory** - consente di estrarre RNSC dal documento RNIF o di creare le informazioni RNIF per RNSC.
4. **com.ibm.bcg.sponsor.SponsorBusProcessFactory** - viene utilizzato durante l'elaborazione dei documenti 0A1 RosettaNet per aggiornare il motore di stato di RosettaNet.
5. **com.ibm.bcg.outbound.OutboundDocFactor**y - è sempre richiesto. Effettua l'elaborazione richiesta di WebSphere Partner Gateway sul documento di destinazione. Si tratta dell'ultima fase ed è stata aggiunta automaticamente dalla Console alle azioni esistenti o alle azioni create di recente. Questa fase non viene visualizzata nell'elenco di handler configurati.

Conversione bidirezionale di RosettaNet e XML con convalida

Obiettivo

Questa azione viene utilizzata per i documenti RNIF RosettaNet che è necessario convertire in un documento XML personalizzato o viceversa. Durante la ricezione di un documento RNIF dal partner esterno, il payload (RNSC - RNIF Service Content) sarà estratto dal package RNIF, convalidato e convertito in un documento XML con i documenti di destinazione convertiti e convalidati per l'invio all'applicazione di backend (partner interno). Quando proviene dall'applicazione di

backend (partner interno), XML sarà convalidato e convertito in RNSC, che viene convalidato.

Configurazione

- Il package PIP RosettaNet per il documento RosettaNet deve essere caricato
- Richiede la configurazione della mappa di convalida (XML SCHEMA) sul documento XML di origine o di destinazione
- Richiede la configurazione della mappa di conversione XSLT per questa azione

Modifica

Questa azione non può essere copiata e modificata.

Fasi

Questa azione contiene le seguenti fasi, eseguite in sequenza:

1. **com.ibm.bcg.server.pkg.UnPackagingFactory** - determina la classe di spacchettamento corretta per RNIF o presume che il documento non sia RNIF e nessuno spacchettamento viene eseguita.
2. **com.ibm.bcg.validation.ValidationFactory** – per convalidare il documento XML o RNIF di origine.
3. **com.ibm.bcg.translation.protocol.RNXsltProtFactory** – converte il documento RNSC in / da XML.
4. **com.ibm.bcg.validation.OutboundValidationFactory** - convalida il documento XML convertito risultante.
5. **com.ibm.bcg.sponsor.SponsorBusProcessFactory** - viene utilizzato durante l'elaborazione dei documenti 0A1 RosettaNet per aggiornare il motore di stato di RosettaNet.
6. **com.ibm.bcg.outbound.OutboundDocFactory** - è sempre richiesto. Effettua l'elaborazione richiesta di WebSphere Partner Gateway sul documento di destinazione. Si tratta dell'ultima fase ed è stata aggiunta automaticamente dalla Console alle azioni esistenti o alle azioni create di recente. Questa fase non viene visualizzata nell'elenco di handler configurati.

Conversione bidirezionale di RosettaNet e del contenuto del servizio RosettaNet senza convalida del contenuto

Obiettivo

Questa azione viene utilizzata per i documenti RNIF RosettaNet. Durante la ricezione di un documento RNIF da un partner esterno, il payload (RNSC - RosettaNet Service Content) sarà estratto dal documento impacchettato RNIF da inviare all'applicazione di backend (partner interno). La convalida si verifica sul documento RNIF e non su RNSC. Quando proviene dall'applicazione di backend (partner interno) il documento RNSC non sarà convalidato.

Configurazione

Il package PIP RosettaNet per il documento RosettaNet deve essere caricato.

Modifica

Questa azione non può essere copiata e modificata.

Fasi

Questa azione contiene le seguenti fasi, eseguite in sequenza:

1. **com.ibm.bcg.server.pkg.UnPackagingFactory** - determina la classe di spacchettamento corretta per RNIF o presume che il documento non sia RNIF e nessuno spacchettamento viene eseguita.
2. **com.ibm.bcg.validation.ValidationWithoutContentFactory** – effettua la convalida eccetto su RNSC.
3. **com.ibm.bcg.translation.protocol.StdRNandRNSCProtFactory** - consente di estrarre RNSC dal documento RNIF o di creare le informazioni RNIF per RNSC.
4. **com.ibm.bcg.sponsor.SponsorBusProcessFactory** - viene utilizzato durante l'elaborazione dei documenti 0A1 RosettaNet per aggiornare il motore di stato di RosettaNet.
5. **com.ibm.bcg.outbound.OutboundDocFactory** - è sempre richiesto. Effettua l'elaborazione richiesta di WebSphere Partner Gateway sul documento di destinazione. Si tratta dell'ultima fase ed è stata aggiunta automaticamente dalla Console alle azioni esistenti o alle azioni create di recente. Questa fase non viene visualizzata nell'elenco di handler configurati.

Conversione bidirezionale di XML personalizzato del partner interno in RosettaNet con verifica duplicati del contenuto e convalida

Obiettivo

Questa azione viene utilizzata per i documenti RNIF RosettaNet che è necessario convertire in un documento XML personalizzato o viceversa. Durante la ricezione di un documento RNIF dal partner esterno, il payload (RNSC - RNIF Service Content) sarà estratto dal package RNIF, convalidato e convertito in un documento XML da inviare all'applicazione di backend (partner interno). Quando proviene dall'applicazione di backend (partner interno), verrà eseguita una verifica di ID duplicata sull'XML che verrà quindi convalidato e convertito in RNSC; verrà quindi eseguita la convalida. In modo analogo all'azione ″Conversione bidirezionale di RosettaNet e XML con convalida″ ma con un'ulteriore Verifica duplicati, l'azione viene eseguita sul documento XML di origine.

Configurazione

- Il formato XML del documento di origine necessita della configurazione delle Chiavi della verifica duplicati
- Il package PIP RosettaNet per il documento RosettaNet deve essere caricato
- Richiede la configurazione della mappa di convalida (XML SCHEMA) sul documento XML di origine o di destinazione
- Richiede la configurazione della mappa di conversione XSLT per questa azione

Modifica

Questa azione non può essere copiata e modificata, appena è specifica ad un documento RNIF.

Fasi

Questa azione contiene le seguenti fasi, eseguite in sequenza:

1. **com.ibm.bcg.duplicate.ContentDuplicateProcessFactory** - per un XML personalizzato ricevuto effettua una verifica di ID duplicati.

2. **com.ibm.bcg.server.pkg.UnPackagingFactory** - determina la classe di spacchettamento corretta per RNIF o presume che il documento non sia RNIF e nessuno spacchettamento viene eseguita.
3. **com.ibm.bcg.validation.ValidationFactory** – per convalidare il documento XML o RNIF di origine.
4. **com.ibm.bcg.translation.protocol.RNXsltProtFactory** – converte il documento RNSC in / da XML.
5. **com.ibm.bcg.validation.OutboundValidationFactory** - convalida il documento XML convertito risultante.
6. **com.ibm.bcg.sponsor.SponsorBusProcessFactory** - viene utilizzato durante l'elaborazione dei documenti 0A1 RosettaNet per aggiornare il motore di stato di RosettaNet.
7. **com.ibm.bcg.outbound.OutboundDocFactory** - è sempre richiesto. Effettua l'elaborazione richiesta di WebSphere Partner Gateway sul documento di destinazione. Si tratta dell'ultima fase ed è stata aggiunta automaticamente dalla Console alle azioni esistenti o alle azioni create di recente. Questa fase non viene visualizzata nell'elenco di handler configurati.

Conversione bidirezionale di XML personalizzati con convalida

Obiettivo

Questa azione viene utilizzata con i documenti XML personalizzati, provenienti da un partner esterno o dal partner interno. Il documento di origine è stato convalidato, convertito nel documento di destinazione ed il documento di destinazione è stato convalidato.

Configurazione

- Richiede la configurazione della mappa di convalida (XML SCHEMA) sul documento di origine
- Richiede la configurazione della mappa di conversione XSLT per questa azione
- Richiede la configurazione della mappa di convalida (XML SCHEMA) sul documento di destinazione

Modifica

Questa azione può essere copiata e modificata. Le fasi di conversione e di convalida possono essere sostituite con le fasi definite dall'utente o aggiungere le ulteriori fasi definite dall'utente.

Fasi

Questa azione contiene le seguenti fasi, eseguite in sequenza:

1. **com.ibm.bcg.validation.ValidationFactory** – questa fase convalida il documento XML personalizzato ricevuto.
2. **com.ibm.bcg.translation.protocol.translators.xslt.XSLTranslationFactory** – effettua la conversione.
3. **com.ibm.bcg.validation.OutboundValidationFactory** - convalida il documento XML convertito risultante.
4. **com.ibm.bcg.outbound.OutboundDocFactory** - è sempre richiesto. Effettua l'elaborazione richiesta di WebSphere Partner Gateway sul documento di destinazione. Si tratta dell'ultima fase ed è stata aggiunta automaticamente dalla Console alle azioni esistenti o alle azioni create di recente. Questa fase non viene visualizzata nell'elenco di handler configurati.

Conversione bidirezionale dell'XML personalizzato con verifica duplicati e convalida

Obiettivo

Questa azione viene utilizzata con i documenti XML personalizzati. Può essere utilizzata per i documenti che provengono dal partner esterno o dal partner interno. La verifica di ID duplicati viene eseguita sul documento di origine, la convalida sul documento di origine, la conversione del documento di origine nel documento di destinazione e la convalida del documento di destinazione. Questa azione è simile all'azione "Conversione bidirezionale di XML personalizzati con convalida" tranne con la fase aggiuntiva di Verifica duplicati.

Configurazione

- Il formato XML del documento di origine necessita della configurazione delle Chiavi della verifica duplicati
- Richiede la configurazione della mappa di convalida (XML SCHEMA) sul documento di origine
- Richiede la configurazione della mappa di conversione XSLT per questa azione
- Richiede la configurazione della mappa di convalida (XML SCHEMA) sul documento di destinazione

Modifica

Questa azione può essere copiata e modificata. Le fasi che possono essere sostituite con le fasi definite dall'utente sono ValidationFactory, XSLTTranslationFactory e OutboundValidationFactory o aggiungere le ulteriori fasi definite dall'utente.

Fasi

Questa azione contiene le seguenti fasi, eseguite in sequenza:

1. **com.ibm.bcg.duplicate.ContentDuplicateProcessFactory** - verifica un documento duplicato in base all'ID documenti.
2. **com.ibm.bcg.validation.ValidationFactory** - questa fase convalida il documento XML personalizzato ricevuto.
3. **com.ibm.bcg.translation.protocol.translators.xslt.XSLTranslationFactory** - questa fase converte il documento XML personalizzato ricevuto in formato XML di destinazione.
4. **com.ibm.bcg.validation.OutboundValidationFactory** - questa fase convalida il documento XML di destinazione convertito dalla fase di conversione precedente.
5. **com.ibm.bcg.outbound.OutboundDocFactory** - è sempre richiesto. Effettua l'elaborazione richiesta di WebSphere Partner Gateway sul documento di destinazione. Si tratta dell'ultima fase ed è stata aggiunta automaticamente dalla Console alle azioni esistenti o alle azioni create di recente. Questa fase non viene visualizzata nell'elenco di handler configurati.

Pass Through XML personalizzato con verifica e convalida duplicati

Obiettivo

Questa azione viene utilizzata con i documenti XML personalizzati. Può essere utilizzata per i documenti che provengono da un partner esterno o dal partner interno. La verifica duplicati di ID viene eseguita e la convalida viene effettuata sul documento di origine. Questa azione è simile all'azione "Pass Through XML

personalizzato con verifica e convalida duplicati" tranne quando viene eseguita un'ulteriore verifica di convalida del documento di origine.

Configurazione

- Il formato XML del documento di origine necessita della configurazione delle Chiavi della verifica duplicati
- Richiede la configurazione della mappa di convalida (XML SCHEMA) sul documento XML di origine

Modifica

Questa azione può essere copiata e modificata. Le fasi che è possibile sostituire con le fasi definite dall'utente sono ValidationFactory o aggiungere le ulteriori fasi definite dall'utente.

Fasi

Questa azione contiene le seguenti fasi, eseguite in sequenza:

1. **com.ibm.bcg.duplicate.ContentDuplicateProcessFactory** - verifica un documento duplicato in base all'ID documenti. Il formato XML per questo documento di origine deve avere la configurazione dell'ID duplicato.
2. **com.ibm.bcg.validation.ValidationFactor**y - questa fase convalida il documento XML personalizzato di origine.
3. **com.ibm.bcg.passthrough.No_op** - consente di indicare che l'intestazione content type del documento di destinazione non deve provenire dal contenuto del documento.
4. **com.ibm.bcg.outbound.OutboundDocFactory** - è sempre richiesto. Effettua l'elaborazione richiesta di WebSphere Partner Gateway sul documento di destinazione. Si tratta dell'ultima fase ed è stata aggiunta automaticamente dalla Console alle azioni esistenti o alle azioni create di recente. Questa fase non viene visualizzata nell'elenco di handler configurati.

Pass Through XML personalizzato con verifica duplicati

Obiettivo

Questa azione viene utilizzata con i documenti XML personalizzati. Può essere utilizzata per i documenti provenienti da un partner esterno o dal partner interno. La verifica duplicati di ID viene eseguita sul documento di origine.

Configurazione

Il formato XML del documento di origine necessita della configurazione delle Chiavi di verifica duplicati.

Modifica

Questa azione non può essere copiata in una nuova azione, mentre la possibile modifica aggiunge una fase di convalida, che è stata definita nell'azione "Pass Through XML personalizzato con verifica e convalida duplicati".

Fasi

Questa azione contiene le seguenti fasi, eseguite in sequenza:

1. **com.ibm.bcg.duplicate.ContentDuplicateProcessFactory** - verifica un documento duplicato in base all'ID documenti. Il formato XML per questo documento di origine deve avere la configurazione dell'ID duplicato.
2. **com.ibm.bcg.passthrough.No_op** - consente di indicare che l'intestazione content type del documento di destinazione non deve provenire dal contenuto del documento.
3. **com.ibm.bcg.outbound.OutboundDocFactory** - è sempre richiesto. Effettua l'elaborazione richiesta di WebSphere Partner Gateway sul documento di destinazione. Si tratta dell'ultima fase ed è stata aggiunta automaticamente dalla Console alle azioni esistenti o alle azioni create di recente. Questa fase non viene visualizzata nell'elenco di handler configurati.

Pass Through XML personalizzato con convalida

Obiettivo

Questa azione viene utilizzata con i documenti XML personalizzati, provenienti da un partner esterno o dal partner interno. La convalida viene eseguita sul documento di origine.

Configurazione

Richiede la configurazione della mappa di convalida (XML SCHEMA) sul documento XML di origine.

Modifica

Questa azione può essere copiata e modificata. La fase ValidationFactory può essere sostituita con la fase definita dall'utente o aggiungere le ulteriori fasi definite dall'utente.

Fasi

Questa azione contiene le seguenti fasi, eseguite in sequenza:

1. **com.ibm.bcg.validation.ValidationFactory** - questa fase convalida il documento XML personalizzato di origine.
2. **com.ibm.bcg.passthrough.No_op** - consente di indicare che l'intestazione content type del documento di destinazione non deve provenire dal contenuto del documento.
3. **com.ibm.bcg.outbound.OutboundDocFactory** - è sempre richiesto. Effettua l'elaborazione richiesta di WebSphere Partner Gateway sul documento di destinazione. Si tratta dell'ultima fase ed è stata aggiunta automaticamente dalla Console alle azioni esistenti o alle azioni create di recente. Questa fase non viene visualizzata nell'elenco di handler configurati.

Deenveloping di EDI

Obiettivo

Questa azione viene utilizzata con gli scambi EDI, provenienti da un partner esterno. Lo scambio EDI sarà sottoposto a deenveloping (le transazioni EDI estratte), tali transazioni EDI saranno nuovamente introdotte in WebSphere Partner Gateway per la singola elaborazione. Il documento dello scambio EDI non viene elaborato all'interno di WebSphere Partner Gateway.

Configurazione

Configurazione facoltativa nelle Definizioni documento.

Modifica

Questa azione non può essere copiata e modificata

Fasi

Questa azione contiene le seguenti fasi, eseguite in sequenza:

1. **com.ibm.bcg.edi.business.process.EDIDenvFactory** – esegue l'operazione di deenveloping dello scambio EDI.
2. **com.ibm.bcg.outbound.OutboundDocFactory** - è sempre richiesto. Effettua l'elaborazione richiesta di WebSphere Partner Gateway sul documento di destinazione. Si tratta dell'ultima fase ed è stata aggiunta automaticamente dalla Console alle azioni esistenti o alle azioni create di recente. Questa fase non viene visualizzata nell'elenco di handler configurati.

Convalida EDI e conversione EDI

Obiettivo

Questa azione viene utilizzata per le transazioni EDI che erano state sottoposte a deenveloping da uno scambio EDI dall'azione Deenveloping di EDI. Provengono da un partner esterno. I documenti della transazione EDI saranno convalidati e quindi convertiti.

Configurazione

- Configurazione facoltativa nelle Definizioni documento
- Mappe di convalida facoltative per la transazione EDI di origine dal client DIS o WTX design studio.
- Mappe di conversione dal client DIS o WTX design studio.
- Connessione partecipante da qualsiasi package / EDI - Qualsiasi / Da qualsiasi a nessuno / EDI - Qualsiasi / Qualsiasi deve essere impostato con un'azione definita come Deenveloping EDI.

Modifica

Questa azione può essere copiata e modificata per aggiungere ulteriori fasi di uscita utente.

Fasi

Questa azione contiene le seguenti fasi, eseguite in sequenza:

1. **com.ibm.bcg.edi.business.process.EDISourceValidationFactory** – convalida la transazione EDI. Questa fase emette RF EDI una volta elaborate tutte le transazioni EDI dallo scambio EDI.
2. **com.ibm.bcg.edi.business.process.EDITranslatorFactory** – converte la transazione EDI nel documento di destinazione.
3. **com.ibm.bcg.outbound.OutboundDocFactory** - è sempre richiesto. Effettua l'elaborazione richiesta di WebSphere Partner Gateway sul documento di destinazione. Si tratta dell'ultima fase ed è stata aggiunta automaticamente dalla Console alle azioni esistenti o alle azioni create di recente. Questa fase non viene visualizzata nell'elenco di handler configurati.

Conversione XML e convalida EDI
Obiettivo

Questa azione viene utilizzata per i documenti XML personalizzati dal partner interno. Il documento XML di origine viene convertito in una transazione EDI e convalidato. Viene poi inviato al backend o ad un partner esterno. I formati XML vengono utilizzati per identificare le informazioni sull'instradamento.

Configurazione

- Configurazione facoltativa nelle Definizioni documento.
- Mappe di convalida facoltative per la transazione EDI di destinazione dal client DIS.
- Mappe di conversione dal client DIS o WDI Design Studio.

Modifica

Questa azione può essere copiata e modificata per rimuovere la fase EDITargetValidationFactory o per aggiungere ulteriori fasi di uscita utente.

Fasi

Questa azione contiene le seguenti fasi, eseguite in sequenza:

1. **com.ibm.bcg.edi.business.process.XMLTranslatorFactory** – converte il documento XML di origine in una transazione EDI di destinazione.
2. **com.ibm.bcg.edi.business.process.EDITargetValidationFactory** – convalida la transazione EDI di destinazione.
3. **com.ibm.bcg.outbound.OutboundDocFactory** - è sempre richiesto. Effettua l'elaborazione richiesta di WebSphere Partner Gateway sul documento di destinazione. Si tratta dell'ultima fase ed è stata aggiunta automaticamente dalla Console alle azioni esistenti o alle azioni create di recente. Questa fase non viene visualizzata nell'elenco di handler configurati.

Conversione ROD (FlatFile) e convalida EDI
Obiettivo

Questa azione viene utilizzata per i documenti (ROD/File di testo) dal partner interno. Il documento ROD di origine e lo converte in una transazione EDI e convalidato.

Configurazione

- Configurazione facoltativa nelle Definizioni documento
- Mappe di convalida facoltative per la transazione EDI di destinazione dal client DIS
- Lo standard ROD deve essere definito nel client DIS e compilato utilizzando una mappa di conversione fittizia.
- Lo splitter ROD / Processore documento generico deve essere aggiunto nello stesso modo utilizzato per l'handler processi nel destinatario. Questo per conoscere il formato e il documento del dizionario.

Modifica

Questa azione può essere copiata e modificata per rimuovere la fase EDITargetValidationFactory o per aggiungere ulteriori fasi di uscita utente.

Fasi

Questa azione contiene le seguenti fasi, eseguite in sequenza:

1. **com.ibm.bcg.edi.business.process.RODTranslatorFactory** – converte il documento ROD di origine nella transazione EDI di destinazione.
2. **com.ibm.bcg.edi.business.process.EDITargetValidationFactory** – convalida la transazione EDI di destinazione.
3. **com.ibm.bcg.outbound.OutboundDocFactory** - è sempre richiesto. Effettua l'elaborazione richiesta di WebSphere Partner Gateway sul documento di destinazione. Si tratta dell'ultima fase ed è stata aggiunta automaticamente dalla Console alle azioni esistenti o alle azioni create di recente. Questa fase non viene visualizzata nell'elenco di handler configurati.

Suddivisione ebMS e analisi

Obiettivo

Questa azione è per i documenti ebMS da un partner esterno. Gli allegati del payload saranno estratti e introdotti nuovamente in WebSphere Partner Gateway per la singola elaborazione. Il documento ebMS non viene elaborato ulteriormente in WebSphere Partner Gateway.

Configurazione

Non sono richieste ulteriori configurazioni.

Modifica

Questa azione non può essere copiata e modificata.

Fasi

Questa azione contiene le seguenti fasi, eseguite in sequenza:

1. **com.ibm.bcg.server.EBMSSplitAndParse** – gli allegati del payload sono stati estratti in singoli documenti.
2. **com.ibm.bcg.outbound.OutboundDocFactory** - è sempre richiesto. Effettua l'elaborazione richiesta di WebSphere Partner Gateway sul documento di destinazione. Si tratta dell'ultima fase ed è stata aggiunta automaticamente dalla Console alle azioni esistenti o alle azioni create di recente. Questa fase non viene visualizzata nell'elenco di handler configurati.

Convalida scambio EDI

Obiettivo

La convalida dello scambio EDI viene utilizzata durante l'integrazione asincrona con WTX. Le singole transazioni vengono estratte dallo scambio eseguendo il deenveloping dello scambio. L'azione di deenveloping estrarrà ogni transazione dallo scambio. Ogni transazione creerà un documento che verrà inoltrato direttamente per la convalida

Configurazione

- Connessione partecipante da <qualsiasi package> / EDI – xxxx / XXX a Nessuno / EDI – xxxx / XXX deve essere impostata con un'azione definita come "Convalida scambio EDI".
- Facoltativamente, un utente FA può configurare una mappa FA.

- Deve essere definito un canale per il riconoscimento funzionale per il passaggio.

Conversione WTX
Obiettivo

EDI, XML e ROD o i file di testo vengono convertiti utilizzando WTX.

La conversione di EDI tramite WTX può essere asincrona o sincrona. La conversione sincrona è maggiormente utilizzata quando una transazione convalidata e sottoposta a deenveloping viene inviata a WTX per l'elaborazione, ma qui la transazione verrebbe nuovamente sottoposta a enveloping poiché è necessario per l'elaborazione in WTX. Una volta che la transazione EDI è stata convalidata correttamente, viene trasferita all'azione Transazione EDI di conversione WTX. In modalità asincrona, le transazioni EDI vengono convertite nel backend, dove WTX viene distribuito sul programma di avvio WESB/WMB o WTX.

Configurazione per sincrono

- Connessione partecipante da <qualsiasi package> / EDI – xxxx / XXX a Nessuno / EDI – xxxx / XXX deve essere impostata con un'azione definita come Deenveloping EDI
- Connessione partecipante da <N/A> / XXXXXXX/ YYYYY a Nessuno / ZZZZZZ / BBBBBBB deve essere impostata con un'azione definita come "Convalida EDI" & "Transazione EDI Conversione WTX".
- Una mappa di conversione WTX deve essere associata anche a questo canale.

Configurazione per asincrono

- Connessione partecipante da <qualsiasi package> / EDI – xxxx / XXX a Nessuno / EDI – xxxx / XXX deve essere impostata con un'azione definita come Deenveloping EDI
- Connessione partecipante da <N/A> / <versione edi>/ transazione a <N/A> / <versione edi> / transazione deve essere impostata con un'azione definita come Convalida EDI.
- Connessione partecipante da <N/A> / <versione edi> / transazione a <BI> / <scambio edi> / <ISA> / <UNB> / <UCS> deve essere impostata con un'azione definita come Convalida EDI & REENVELOPING EDI.

Configurazione per ROD e XML

- Conversione ROD - Connessione partecipante da <qualsiasi package> / <qualsiasi protocollo (file di testo) > / <qualsiasi file di testo> a <Qualsiasi> / <ANY> / <Qualsiasi> Il formato deve essere impostato con un'azione definita come "Conversione WTX".
- Conversione XML - Connessione partecipante da <qualsiasi package> / <qualsiasi protocollo> / <qualsiasi XML> a <Qualsiasi> / <ANY> / <Qualsiasi> Il formato deve essere impostato con un'azione definita come "Conversione WTX".

Busta WTX
Obiettivo

Quando si utilizza WTX in modalità asincrona, vengono convertite e create transazioni EDI dopo la conversione WTX. Questa viene inviata a WebSphere partner Gateway per l'enveloping.

Configurazione

- Connessione da <Backend> / <Dizionario EDI> / <Documento EDI> {EDI Trx} a <N/A> / <EDI X12/EDIFACT> / <EDI ISA/UNB> con azione Pass Through configurazione profilo enveloper all'estremità della destinazione. (Canale-A).
- Connessione da <NA> / <Scambio EDI> / <EDI ISA/UNB> a <ANY PACKAGE> / <EDI X12/EDIFACT> / <EDI ISA/UNB> con azione Pass through. (Canale-B)
-

ReEnveloper EDI
Obiettivo

Il ReEnveloper viene utilizzato per eseguire l'enveloping di singole transazioni. Esso recupera le intestazioni dell'enveloper dalla busta di origine e inserisce ogni transazione di cui è stato eseguito il deenveloping.

Configurazione

- Un canale tra origine come transazione e Destinazione come Scambio EDI con il profilo busta impostato
- Impostare l'azione come ReEnveloper EDI

Convalida busta Soap

La richiesta del servizio web nel complesso verrà convalidata per lo schema SOAP1.1 come per gli standard del settore. La Busta SOAP di azione contiene le seguenti fasi, eseguite in sequenza:

1. **com.ibm.bcg.validation.WebserviceFactory** – esegua la convalida della richiesta del servizio Web e restituisce l'handler WebserviceValidation.
2. **com.ibm.bcg.outbound.OutboundDocFactory** - sempre richiesto. Effettua l'elaborazione richiesta di WebSphere Partner Gateway sul documento di destinazione. Si tratta dell'ultima fase ed è stata aggiunta automaticamente dalla Console alle azioni esistenti o alle azioni create di recente. Questa fase non viene visualizzata nell'elenco di handler configurati.

Convalida corpo SOAP

Questa funzione convalida il Corpo SOAP o il payload disponibile nella Busta SOAP. La convalida Payload è supportata solo per i payload XML nella Busta SOAP. Il puntatore di posizione dello schema standard del settore in Payload XML viene utilizzato per la convalida basata sullo schema. Facoltativamente, è possibile associare lo schema al rispettivo canale del servizio Web per la convalida del payload. Lo schema che si è esplicitamente associato al canale del servizio Web ha la precedenza sullo schema posizionato in XML payload. In mancanza del puntatore di posizione dello schema in XML payload, associare uno schema nel canale di servizio Web. Gli attributi dell'oggetto di instradamento per la richiesta e la risposta del servizio Web sono i seguenti:

- **ResponseValidation** – imposta il valore di questo attributo su "No" sul lato di destinazione, se non si desidera convalidare un documento di risposta. Il valore predefinito di questo attributo è "Yes".
- **ContentValidation** – questo attributo consente di abilitare o disabilitare la convalida del contenuto su XML payload. Per impostazione predefinita, viene abilitata la convalida del contenuto. Se si imposta su "No", verrà eseguita la convalida della grammatica.

Il Corpo SOAP di azione contiene le seguenti fasi eseguite in sequenza:

1. **com.ibm.bcg.validation.ValidationFactory** – esegue la convalida della richiesta del servizio Web.
2. **com.ibm.bcg.outbound.OutboundDocFactory** - sempre richiesto. Effettua l'elaborazione richiesta di WebSphere Partner Gateway sul documento di destinazione. Si tratta dell'ultima fase ed è stata aggiunta automaticamente dalla Console alle azioni esistenti o alle azioni create di recente. Questa fase non viene visualizzata nell'elenco di handler configurati.

Per aggiornare WebSphere Partner Gateway affinché includa la convalida della funzione del payload nella busta SOAP, consultare la Administration Guide.

Deenveloping SOAP

La Busta SOAP deve essere sottoposta a deenveloping e l'elemento del Corpo SOAP deve essere introdotto per un'ulteriore elaborazione. Gli attributi dell'oggetto di instradamento per il Deenveloping della busta SOAP sono i seguenti:

- **Deenveloping busta SOAP** - supporta solo la comunicazione asincrona. Nessun errore SOAP o risposta SOAP viene restituita poiché si tratta di un supporto profilo di base del servizio Web one-Way. In caso di comunicazione sincrona, Deenveloping busta SOAP genera un errore nel documento e registra l'evento errore.
- **Re-instradare il documento sottoposto a deenveloping** - questo è un attributo dell'oggetto di instradamento collegato dell'azione **Deenveloping busta SOAP**. Se questo attributo di oggetto instradamento viene impostato su ″Sì″, l'azione **Deenveloping busta SOAP** deve introdurre il Corpo SOAP estratto dalla Busta SOAP come nuovo documento in WebSphere Partner Gateway. Inoltre, l'allegato deve essere anche introdotto come nuovo documento. Tutti i documenti appena introdotti restituiscono un errore nel package N/A. Per instradarli ulteriormente, è necessario configurare il canale basato sui package N/A per il payload estratto e i documenti allegati.
- **Payload di consumo** - questo attributo è collegato all'attributo **Re-instradare il documento sottoposto a deenveloping**. Viene utilizzato per l'omissione del payload dopo l'estrazione. Se il valore di questo attributo e il valore di **Re-instradare il documento sottoposto a deenveloping** è impostato su ″Sì″, il payload non viene estratto o instradato dalla busta SOAP. Gli allegati da soli vengono instradati. Nel caso in cui questo attributo sia impostato su ″No″ e **Re-instradare il documento sottoposto a deenveloping** è impostato su ″Sì″, il Payload e gli allegati vengono instradati separatamente. Il valore predefinito di questo attributo è ″No″.

L'azione Deenveloping Busta SOAP contiene le seguenti operazioni eseguite in sequenza:

1. **com.ibm.bcg.validation.SOAPDeEnveloperFactory** – esegue la convalida della richiesta del servizio Web e restituisce l'handler SOAPDeEnveloper.
2. **com.ibm.bcg.outbound.OutboundDocFactory** - sempre richiesto. Effettua l'elaborazione richiesta di WebSphere Partner Gateway sul documento di destinazione. Si tratta dell'ultima fase ed è stata aggiunta automaticamente dalla Console alle azioni esistenti o alle azioni create di recente. Questa fase non viene visualizzata nell'elenco di handler configurati.

Qualora all'interno di istanze si desidera eseguire il deenveloping SOAP con l'allegato e instradare solo gli allegati non il payload del corpo SOAP, la configurazione è la seguente:

- bcg.soap.ConsumePayload = Y (per impostazione predefinita questo valore è N)

- bcg.soap.Re-RouteDe-EnvelopedDocument = Y (per impostazione predefinita questo valore è Y)

Quando si desidera eseguire il deenveloping SOAP con l'allegato e instradare il payload e gli allegati separatamente, la configurazione è la seguente:

- bcg.soap.ConsumePayload = N (per impostazione predefinita questo valore è N)
- bcg.soap.Re-RouteDe-EnvelopedDocument = Y (per impostazione predefinita questo valore è Y)

Per aggiornare WebSphere Partner Gateway affinché includa la funzione del payload di convalida nella Busta SOAP, consultare *WebSphere Partner Gateway Administrator Guide*.

Modifica di un'azione definita dall'utente

Informazioni su questa attività

Per configurare un'azione definita dall'utente, effettuare le seguenti fasi:

1. Fare clic su **Ammin hub > Configurazione hub > Azioni**.
2. Fare clic sull'icona **Visualizza i dettagli** accanto all'azione definita dall'utente che si desidera configurare.

   Viene elencata l'azione e l'elenco degli handler (fasi dell'azione) già configurati.
3. Effettuare una delle seguenti fasi per ogni azione che si desidera modificare.
   a. Aggiungere una fase selezionando l'handler associato dall'**Elenco disponibile** e facendo clic su **Aggiungi**. L'handler viene spostato nell'**Elenco configurato**.
   b. Rimuovere un handler selezionandolo nell'**Elenco configurato** e facendo clic su **Rimuovi**. L'handler viene spostato nell'**Elenco disponibile**.
   c. Riorganizzare l'ordine in base al quale gli handler sono chiamati selezionando l'handler e facendo clic su **Sposta su** o su **Sposta giù**.
   d. In tal modo, un handler deve essere elaborato più volte selezionandolo e facendo clic su **Ripeti**.

      Quindi tutti gli handler configurati per un'azione vengono chiamati e le fasi, che gli handler rappresentano, vengono effettuate nell'ordine in cui sono state visualizzate nell'**Elenco configurato**.
   e. Configurare l'handler selezionandolo nell'**Elenco configurato** e facendo clic su **Configura**. Viene visualizzato l'elenco di attributi che è possibile configurare.
4. Fare clic su **Salva**.

Creazione di azioni

È possibile creare un'azione in uno dei seguenti modi:

- Creare una nuova azione ed associare gli handler all'azione.
- Copiare un'azione fornita dal prodotto e, se necessario, modificare gli handler ad esso associati.

Creazione di una nuova azione

Informazioni su questa attività

Per creare una nuova azione, effettuare le seguenti fasi:

1. Fare clic su **Ammin hub > Configurazione hub > Azioni**.
2. Fare clic su **Crea**.

3. Inserire un nome per l'azione. Questo campo è obbligatorio.
4. Inserire una descrizione facoltativa dell'azione.
5. Indicare se l'azione è abilitata per l'uso.
6. Per ogni fase che viene richiamata come parte dell'azione, aggiungere l'handler selezionandolo dall'**Elenco disponibile** e fare clic su **Aggiungi**. L'handler viene spostato nell'**Elenco configurato**.

   Gli handler vengono chiamati dall'azione nell'ordine in cui sono stati riportati nell'**Elenco configurato**. Verificare che gli handler siano stati posizionati nell'ordine corretto. È possibile utilizzare **Sposta su** o **Sposta giù** per disporre di nuovo l'ordine degli handler o **Ripeti** per fare in modo che l'handler debba essere elaborato più volte.
7. Configurare un handler selezionandolo dall'**Elenco configurato** e facendo clic su **Configura**. Viene visualizzato l'elenco di attributi che è possibile configurare.
8. Fare clic su **Salva**.

Copia di un'azione
Informazioni su questa attività

Per creare un'azione copiando quella esistente, effettuare le seguenti fasi:

1. Fare clic su **Ammin hub > Configurazione hub > Azioni**.
2. Dall'Elenco azioni, fare clic sull'icona **Copia** accanto all'azione che si desidera copiare.
3. Inserire un nome per l'azione. Questo campo è obbligatorio.
4. Inserire una descrizione facoltativa dell'azione.
5. Indicare se l'azione è abilitata per l'uso.
6. Si noti che una o più fasi si trovano già nell'**Elenco configurati**. Queste sono le fasi associate all'azione che si desidera effettuare: Ad esempio, se è stata clonata l'azione Annullamento del processo RosettaNet del partner interno fornita dal prodotto, verrà visualizzato il seguente elenco degli handler disponibili e configurati:

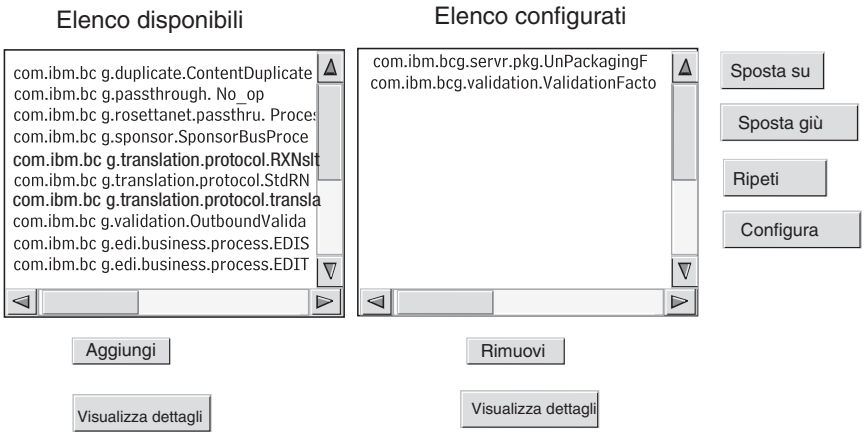


Figura 19. Clonazione di un'azione

   Per modificare l'**Elenco configurato**, eseguire una o più delle seguenti fasi:

   a. Aggiungere una fase selezionando l'handler associato dall'**Elenco disponibile** e facendo clic su **Aggiungi**. L'handler viene spostato nell'**Elenco configurato**.

b. Rimuovere una fase selezionando l'handler associato dall'**Elenco configurato** e facendo clic su **Rimuovi**. L'handler viene spostato nell'**Elenco disponibile**.

c. Riorganizzare l'ordine in base al quale gli handler sono chiamati selezionando l'handler e facendo clic su **Sposta su** o su **Sposta giù**.

   Tutti gli handler configurati per un'azione vengono chiamati e le fasi, associate agli handler, vengono effettuate nell'ordine in cui sono state visualizzate nell'**Elenco configurato**.

d. Configurare il gestore selezionandolo nell'**Elenco configurato** e facendo clic su **Configura**. Viene visualizzato l'elenco di attributi che è possibile configurare.

7. Fare clic su **Salva**.

Capitolo 9. Configurazione dei tipi di documenti

In questo capitolo viene descritto come configurare i documenti non EDI che saranno scambiati con i partner esterni e con le applicazioni di back-end. La configurazione dei tipi di documenti e delle interazioni per i documenti EDI (con l'eccezione dei documenti EDI trasmessi) è descritta nel Capitolo 10, "Configurazione dei flussi di documenti EDI", a pagina 163. Il Capitolo 10, "Configurazione dei flussi di documenti EDI", a pagina 163 descrive il modo in cui configurare le interazioni ed i tipi di documenti per i documenti XML e ROD (record-oriented-data).

In questo capitolo, vengono descritti i seguenti argomenti:

Nota: è necessario utilizzare sempre la stessa istanza del browser con cui si accede alla Console comunità per apportare modifiche alla configurazione di WebSphere Partner Gateway. L'utilizzo simultaneo di più istanze del browser può causare l'eliminazione delle modifiche di configurazione.

Panoramica dei tipi di documenti

Una definizione del documento è costituita almeno da un package, un protocollo e da un tipo di documento. Per determinati protocolli, è possibile specificare un'azione, un'attività e un segnale. Le definizioni del documento specificano le tipologie di documenti che saranno elaborati da WebSphere Partner Gateway.

Il termine impacchettamento indica la logica richiesta per impacchettare un documento secondo una specifica, come ad esempio, AS2. Un flusso di protocollo è la logica richiesta per elaborare un documento che aderisce ad un certo protocollo, come ad esempio, EDI-X12. Un tipo di documento descrive come deve essere il documento.

Nelle sezioni successive vengono descritte brevemente le fasi generali per impostare un tipo di documento tra il partner interno ed un partner.

Fase 1: Verificare che la definizione del documento sia disponibile

Informazioni su questa attività

Verificare se esiste una definizione del documento (da quelle predefinite con il sistema). Se il flusso non esiste, crearlo caricando i file necessari o creando manualmente una definizione personalizzata.

Per stabilire la definizione del documento, è possibile modificare determinati attributi. Gli attributi sono utilizzati per eseguire varie funzioni di elaborazione e instradamento dei documenti, come ad esempio la convalida, la verifica di codifica e il conteggio dei tentativi. Gli attributi impostati sul livello della definizione del documento forniscono un'impostazione globale per il package, protocollo o tipo di documento associato. Gli attributi disponibili variano, in base alla definizione del documento. Gli attributi per le definizioni del documento EDI, ad esempio, hanno diversi attributi rispetto alle definizioni del documento RosettaNet.

Ad esempio, se viene specificato un valore per **Ora per riconoscere** sul package AS, si applica a tutti i documenti del package con AS. (**Ora per riconoscere** specifica l'intervallo di attesa di una notifica MDN (message disposition notification) prima di inviare nuovamente la richiesta originale.) Se, in seguito, si imposta l'attributo **Ora per riconoscere** al livello Capacità B2B, tale impostazione sovrascrive quella impostata a livello di definizione del documento.

Per gli attributi, che è possibile impostare su tutti i livelli della definizione del documento, i valori impostati al livello del tipo di documento hanno la priorità su quelli impostati al livello del protocollo e gli attributi impostati al livello del protocollo hanno la precedenza su quelli impostati al livello del package.

Prima di poter creare le interazioni, è necessario disporre del tipo di documento elencato nella pagina Gestisci le definizioni di documento. Per gestire la definizione documento, consultare *Hub administration tasks Chapter of WebSphere Partner Gateway Administrator Guide.*

Fase 2: Creare le interazioni

Informazioni su questa attività

Creare le interazioni per i tipi di documenti definiti. L'interazione indica a WebSphere Partner Gateway le azioni da eseguire su un documento. Per alcuni scambi, sono necessari solo due flussi, uno per descrivere il documento ricevuto nell'hub (dal partner o partner interno) e l'altro che descrive il documento inviato dall'hub (al partner esterno o partner interno). Se, tuttavia, l'hub invia o riceve uno scambio EDI che verrà diviso in singole transazioni o in cui sono richiesti i riconoscimenti, verranno create effettivamente più transazioni per eseguire lo scambio. Per gestire le interazioni, consultare *Hub administration tasks Chapter of WebSphere Partner Gateway Administrator Guide.*

Fase 3: Creare i profili del partner, le destinazioni e le capacità B2B

Informazioni su questa attività

Creare i profili del partner per i partner esterni e per il partner interno. Definire le destinazioni (che determinano dove saranno inviati i documenti) e le capacità B2B, che specificano i documenti che il partner interno e i partner esterni sono in grado di inviare e ricevere. La pagina Capacità B2B elenca tutti i tipi di documenti definiti.

È possibile impostare attributi sul livello delle capacità B2B. Gli attributi impostati su questo livello sovrascrivono quelli impostati al livello della definizione del documento. Ad esempio, se si imposta **Ora per riconoscere** su 30 al livello della definizione del documento per il package AS ma poi viene impostato su 60 al livello delle capacità B2B, viene utilizzato il valore 60. L'impostazione di un

attributo al livello B2B consente di personalizzare l'attributo per un determinato partner.

Fase 4: Attivare le connessioni

Informazioni su questa attività

Attivare le connessioni tra il partner interno e i partner esterni. Le connessioni disponibili si basano sono basate sulle interazioni create. Le interazioni sono basate sulle capacità B2B. Le interazioni dipendono dalle definizioni del documento disponibili.

Per alcuni scambi, viene richiesta una sola connessione. Ad esempio, se un partner invia un documento binario ad un'applicazione di back-end del partner interno, risulta necessaria solo una connessione. Tuttavia, per lo scambio di scambi EDI in cui lo scambio è sottoposto a deenveloping e le singole transazioni vengono convertite, vengono stabilite più connessioni.

Nota: per gli scambi EDI passati come tali, è richiesta una sola connessione.

È possibile impostare attributi sul livello della connessione. Gli attributi impostati su questo livello sostituiscono quelli impostati sul livello delle capacità B2B. Ad esempio, se si imposta **Ora di notifica** su 60 per il package AS2 a livello delle capacità B2B, ma poi lo si imposta su 120, il valore utilizzato è 120. L'impostazione di un valore per un attributo al livello della connessione consente di personalizzare ulteriormente l'attributo, in base ai requisiti di instradamento dei partner e delle applicazioni richiamate.

Un esempio di flusso

Informazioni su questa attività

Per impostazione predefinita, sono abilitati molti metodi di impacchettamento. Per illustrate la procedura generale al fine di stabilire le definizioni del documento, tenere presente il caso in cui si dispone di un accordo con un partner esterno per ricevere uno scambio EDI che aderisca allo standard EDI-X12. Il partner invia il documento nel formato di impacchettamento AS2. Si specifica che lo scambio venga inviato senza conversione ad un'applicazione di back-end, senza impacchettamento.

1. Nella pagina Gestisci le definizioni di documento, verificare che la definizione del documento (che descrive la tipologia del documento che si presenta nell'hub dal partner) sia stata abilitata.
   a. Fare clic su **Amministrazione hub > Configurazione hub> Definizione documento**.
   b. Fare clic sull'icona **Espandi** accanto a **Package: AS**. Si noti che **EDI-X12** è già elencato.
   c. Fare clic sull'icona **Espandi** accanto a **Protocollo: EDI-X12**. Il **Tipo documento: ISA** è già stato elencato.
2. Durante la visualizzazione della pagina Gestisci la definizione di documento, verificare che la seconda definizione del documento (che descrive il tipo di documento che si presenta nell'applicazione di back-end) sia stata abilitata.
   a. Fare clic sull'icona **Espandi** accanto a **Package: Nessuno**. Si noti che **EDI-X12** è già elencato.
   b. Fare clic sull'icona **Espandi** accanto a **Protocollo: EDI-X12**. Il **Tipo documento: ISA** è già stato elencato.

3. Creare un'interazione che descrive se il tipo di documento sarà un tipo di origine o del destinatario.
   a. Durante la visualizzazione della pagina Gestisci la definizione di documento, fare clic su **Crea interazioni**.
   b. Nella colonna Origine, espandere **Package: AS**, **Protocollo: EDI-X12 (ALL)** e poi fare clic su **Tipo documento: ISA** in modo tale che il pallino sia selezionato.
   c. Nella colonna Destinazione, espandere **Package: Nessuno**, **Protocollo: EDI-X12 (ALL)** e poi fare clic su **Tipo documento: ISA** in modo tale che il pallino sia selezionato.
   d. In questo esempio, non si verifica alcuna conversione. Quindi, non effettuare alcuna selezione dall'elenco **Mappa di conversione**.
   e. Nell'elenco **Azione**, selezionare **Pass Through**.
   f. Fare clic su **Salva**.

Quindi, è necessario specificare che l'hub sia in grado di accettare scambi EDI-X12 (standard ISA) impacchettati come AS. Si specifica anche che l'hub è in grado di inviare scambi EDI-X12 (standard ISA) senza impacchettamento. Si specifica, inoltre, che non ha luogo alcuna conversione con lo scambio; si verifica il passaggio all'applicazione di back-end (dopo aver rimosso le intestazioni AS).

Non è stato ancora specificato il partner che è in grado di inviare questa tipologia di scambio all'hub. Definire quando si desidera impostare il profilo del partner e le capacità B2B del partner. (Si definisce inoltre un profilo e le capacità B2B per il sistema di back-end del partner interno). Una volta effettuate tali attività, creare una connessione tra il partner e l'applicazione di back-end. Per questo esempio, la Figura 20 mostra la connessione tra il partner e l'applicazione di back-end del partner interno.

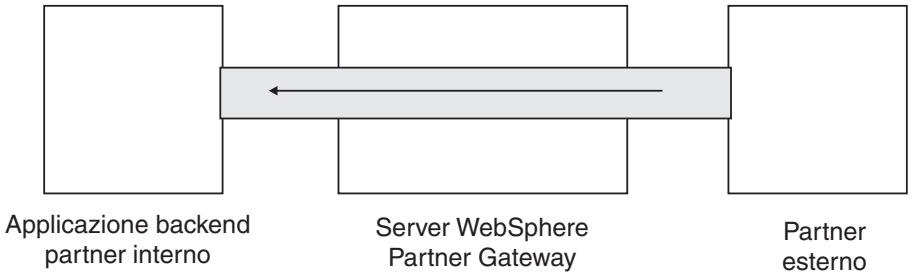


Figura 20. Una connessione unidirezionale da un partner al partner interno

Verificare che esista una connessione utilizzando la pagina Gestisci connessioni (**Amministrazione account > Connessioni**). Nella pagina Gestisci connessioni, selezionare il partner dall'elenco **Origine**, il partner interno dall'elenco **Destinazione** e fare clic su **Cerca**. Viene visualizzata l'unica connessione disponibile. Se necessario, è possibile modificare gli attributi e le azioni, descritte nelle sezioni successive.

Esistono tre tipi di definizioni del documento - quelle fornite con il sistema che è possibile selezionare dalla console, quelle già definite ma non ancora definite nella Console comunità (caricare queste definizioni mediante l'installazione di WebSphere Partner Gateway o da un'altra ubicazione) e quelle create dall'utente. Per ogni tipologia della definizione del documento, è possibile (o a volte è necessario) specificare gli attributi o caricare le mappe che definiscono ulteriormente il tipo di documento.

Documenti binari

Il documento binario viene trasmesso mediante l'hub nello stato in cui si trova, e, quindi, lo scambio dei documenti binari tra un partner esterno ed un'applicazione di back-end del Partner interno è un processo semplice. A partire dalle release versione 6.1.1 è possibile creare più partner interni. Prima di poter stabilire le connessioni tra loro, è necessario che i profili e le capacità B2B del partner interno e dei partner esterni siano definiti. In caso non si utilizzi il partner interno predefinito, l'ID destinatario del partner interno deve essere impostato esplicitamente. Quando il documento binario viene instradato tramite il trasporto HTTP utilizzando l'autenticazione di base, l'ID destinatario può essere passato tramite l'attributo **X-aux-receiver-id** . È inoltre possibile inviare i documenti binari all'hub tramite il partner esterno utilizzando il protocollo FTP. Il protocollo binario è già disponibile per i package AS, Nessuno e Integrazione backend; di conseguenza, la "Fase 1: Verificare che la definizione del documento sia disponibile" a pagina 101 è già stata realizzata.

Nota: è possibile aggiungere gli attributi a qualsiasi livello (Package, Protocollo o Tipo documento) per modificare l'elaborazione predefinita facendo clic sull'icona **Modifica i valori dell'attributo**. Per impostazione predefinita, nessun attributo è stato associato al protocollo binario o al tipo di documento.

Allo stesso modo, per impostazione predefinita vengono fornite quattro interazioni che coinvolgono documenti binari e per queste interazioni non è necessarie che sia eseguita la "Fase 2: Creare le interazioni" a pagina 102. Le interazioni vengono fornite per i seguenti scambi:

Tabella 5. Interazioni fornite dal prodotto

Package/Protocollo/Tipo documento di origine	Package/Protocollo/Tipo documento di destinazione
AS/Binario/Binario	Integrazione Backend/Binario/Binario
Integrazione Backend/Binario/Binario	AS/Binario/Binario
AS/Binario/Binario	Nessuno/Binario/Binario
Nessuno/Binario/Binario	AS/Binario/Binario

Per lo scambio di documenti binari, è necessario eseguire:

- "Fase 3: Creare i profili del partner, le destinazioni e le capacità B2B" a pagina 102, che viene descritto in Capitolo 3, "Creazione ed impostazione di partner", a pagina 23 e Capitolo 11, "Creazione delle destinazioni", a pagina 213.
- "Fase 4: Attivare le connessioni" a pagina 103, che viene descritto in Capitolo 12, "Gestione connessioni", a pagina 237.

Documenti EDI con azione Pass Through

WebSphere Partner Gateway fornisce la capacità di eseguire il deenveloping e convertire gli scambi EDI, un processo descritto in Capitolo 10, "Configurazione dei flussi di documenti EDI", a pagina 163.

La Figura 21 a pagina 106 mostra il flusso di uno scambio EDI, trasmesso da un partner al partner interno.

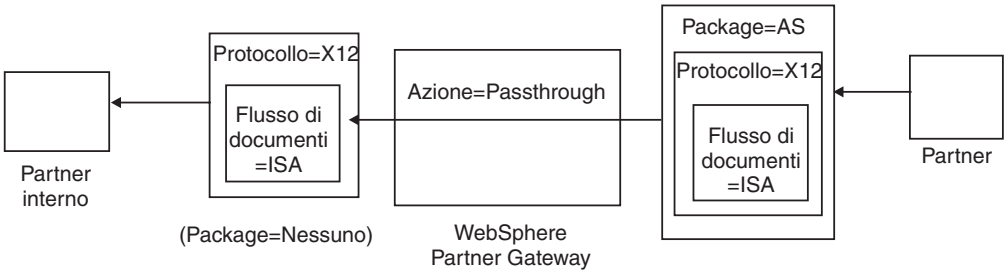


Figura 21. Scambio EDI in entrata con azione Pass Through

In questo esempio, le intestazioni AS2 sono state rimosse, altrimenti lo scambio resta invariato e fluisce attraverso il sistema alla destinazione del partner interno.

Nella conversione sincrona della transazione EDI che utilizza WTX (Da EDI a qualsiasi), se la conversione ha più di un output, in base all'indicatore di instradamento l'elemento child passerà direttamente al flusso di lavoro in uscita oppure verrà reinstradato nel flusso di lavoro in entrata fisso per fare in modo che passi attraverso un nuovo canale. In caso di conversione asincrona, WTX invierà le transazioni EDI a WPG per l'enveloping. È necessario impostare le connessioni per i due canali - <nessuno> / <Dizionario EDI> / <Documento EDI > {EDI Trx} con Pass Through e <NA> / <Scambio EDI> / <,EDI ISA / UNB> a <Qualsiasi package> / <EDI X12 / <FACT> / <EDI ISA / UNB con azione Pass Through.

Creazione delle definizioni del documento

Informazioni su questa attività

Il tipo di documento per gli scambi passthrough EDI è già stato fornito (per impostazione predefinita) nella pagina Gestisci le definizioni di documento, come descritto nella sezione "Un esempio di flusso" a pagina 103. Se si desidera modificare gli attributi che includono i valori predefiniti o impostare un attributo che non ha alcun valore assegnato, per effettuare tali attività è possibile utilizzare la pagina Gestisci le definizioni di documento.

Ad esempio, si supponga di voler modificare l'attributo **Ora di notifica** per un documento EDI impacchettato con AS. Questi sono i passaggi che si desidera effettuare:

1. Fare clic su **Amministrazione hub > Configurazione hub> Definizione documento**.
2. Fare clic sull'icona **Modifica i valori dell'attributo** accanto a **Package: AS**.
3. Scorrere la sezione della pagina **Attributi del contesto della definizione di documento**.
4. Nella riga **Ora per riconoscere**, digitare un valore differente nella colonna **Aggiornamento**.
5. Fare clic su **Salva**.

In questo esempio, è stato modificato un attributo. Gli attributi per il protocollo (ad esempio, EDI-X12) e il tipo di documento (ad esempio, ISA) non sono relativi all'azione Pass Through. Questo attributo si applica a tutti i documenti inclusi nel formato di impacchettamento AS.

Creazione delle interazioni

Informazioni su questa attività

Per creare l'interazione per uno scambio EDI con l'azione Pass Through, procedere nel modo seguente:

1. Fare clic su **Amministrazione hub > Configurazione hub> Definizione documento**.
2. Fare clic su **Crea interazione**.
3. In **Origine**, espandere **Package: AS** e **Protocollo: EDI-X12** e poi selezionare **Tipo di documento: ISA**.
4. In **Destinazione**, espandere **Package: Nessuno** e **Protocollo: EDI-X12** e poi selezionare **Tipo documento: ISA**.
5. Nell'elenco **Azione**, selezionare **Pass Through**.

Le fasi da 1 a 5 consentono a WebSphere Partner Gateway di accettare uno scambio EDI-X12 impacchettato come AS da un partner di origine, inviare uno scambio EDI-X12 senza impacchettamento al partner di destinazione e ottenere il passaggio dello scambio dall'origine alla destinazione.

Se si desidera impostare un'interazione con il documento di origine impacchettato come Nessuno/EDI-X12/ISA e il documento di origine impacchettato come AS/EDI-X12/ISA, espandere **Package: Nessuno** nella fase 3 (nella colonna **Origine**) ed espandere **Package: AS** nella fase 4 (nella colonna **Destinazione**).

---

documenti RosettaNet

RosettaNet è un'organizzazione che fornisce standard aperti per supportare lo scambio dei messaggi di business tra i partner. Per ulteriori informazioni su RosettaNet, vedere http://www.rosettanet.org. Gli standard includono il RNIF (RosettaNet Implementation) e le specifiche PIP (Partner Interface Process). RNIF definisce il modo in cui i partner trasmettono i messaggi fornendo un framework di impacchettamento dei messaggi, protocolli di trasferimento e sicurezza. Ci sono due versioni emesse: 1.1 e 2.0. Una Un PIP definisce un processo di business pubblico e i formati di messaggi basati su XML per supportare il processo.

WebSphere Partner Gateway supporta la messaggistica RosettaNet utilizzando RNIF 1.1 e 2.0. Quando l'hub riceve Un messaggio PIP, convalida e converte il messaggio da inviare al sistema di back-end appropriato. WebSphere Partner Gateway fornisce un protocollo per impacchettare il messaggio convertito in IL messaggio RNSC (RosettaNet Service Content) che il sistema di back-end può gestire. Per informazioni sull'impacchettamento utilizzato su questi messaggi per fornire le informazioni di instradamento, consultare il manuale *WebSphere Partner Gateway Enterprise Integration Guide*.

L'hub può anche ricevere i messaggi RNSC dai sistemi di back-end e creare il messaggio PIP appropriato ed inviare il messaggio al partner commerciale appropriato (un partner). Fornire le definizioni del documento per la versione RNIF e PIP che si desidera utilizzare.

Oltre a fornire la capacità di instradamento per i messaggi RosettaNet, WebSphere Partner Gateway conserva uno stato per ogni messaggio gestito. Ciò consente di inviare nuovamente i messaggi che hanno esito negativo fino a che il numero di tentativi raggiunge una soglia specificata. lo meccanismo di Notifica dell'evento avvisa i sistemi di back-end se un messaggio PIP non può essere recapitato. Inoltre,

l'hub può creare automaticamente PIP 0A1 da inviare ai partner appropriati se riceve determinati messaggi di Notifica eventi dai sistemi di back-end. Per ulteriori informazioni sulla notifica degli eventi, consultare il manuale *WebSphere Partner Gateway Enterprise Integration Guide*.

Package del tipo di documenti RNIF e PIP

Per supportare il sistema di messaggistica RosettaNet, WebSphere Partner Gateway fornisce due gruppi di file compressi denominati package. lo *package RNIF* sono costituiti da definizioni del documento richieste per supportare il protocollo RNIF. Questi package sono contenuti nella directory B2BIntegrate.

Per RNIF V1.1, i package sono:

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

Per RNIF V02.00, i package sono:

- Package_RNIF_V02.00.zip
- Package_RNSC_1.0_RNIF_V02.00.zip

Il primo package di ciascuna coppia fornisce le definizioni del documento richieste per supportare le comunicazioni RosettaNet con i partner e il secondo package fornisce le definizioni del documento richieste per supportare le comunicazioni RosettaNet con i sistemi di back-end.

Il secondo gruppo di package è costituito dai package del tipo di documento PIP. Ogni package del tipo di documento PIP include una directory Packages, che contiene un file XML e una directory GuidelineMaps che comprende i file XSD. Il file XML specifica le definizioni del documento che stabiliscono il modo in cui WebSphere Partner Gateway gestisce PIP e definisce i segnali ed i messaggi scambiati. I file XSD specificano il formato dei messaggi PIP e definiscono i valori consentiti per gli elementi XML dei messaggi. I file compressi per PIP 0A1 presentano anche un file XML che l'hub utilizza come modello per creare i documenti 0A1.

lo PIP per cui WebSphere Partner Gateway fornisce i package del tipo di documento PIP sono:

- PIP 0A1 Notifica di errore v1.0
- PIP 0A1 Notifica di errore V02.00.00
- PIP 2A1 Distribuzione informazioni nuovo prodotto V02.00.00
- PIP 2A12 Distribuzione master prodotto V01.03.00
- PIP 3A1 Richiesta quotazione V02.00.00
- PIP 3A2 Richiesta prezzo e disponibilità R02.01.00
- PIP 3A4 Richiesta ordine di acquisto V02.02.00
- PIP 3A4 Richiesta ordine di acquisto V02.00
- PIP 3A5 Query stato ordine R02.00.00
- PIP 3A6 Distribuzione stato ordine V02.02.00
- PIP 3A7 Notifica acquisto OrderUpdate V02.02.00
- PIP 3A8 Richiesta modifica ordine di acquisto V01.02.00
- PIP 3A8 Richiesta modifica ordine di acquisto V01.03.00
- PIP 3A9 Richiesta cancellazione ordine di acquisto V01.01.00
- PIP 3B2 Notifica anticipo spedizione V01.01.00

- PIP 3B3 Distribuzione stato spedizione R01.00.00
- PIP 3B11 Notifica ordine di spedizione R01.00.00A
- PIP 3B12 Richiesta ordine di spedizione V01.01.00
- PIP 3B13 Notifica conferma ordine di spedizione V01.01.00
- PIP 3B14 Richiesta cancellazione ordine di spedizione V01.00.00
- PIP 3B18 Notifica documentazione di spedizione V01.00.00
- PIP 3C1 Restituzione prodotto V01.00.00
- PIP 3C3 Notifica della fattura V01.01.00
- PIP 3C4 Notifica della fattura rifiutata V01.00.00
- PIP 3C6 Notifica dell'avviso di pagamento V01.00.00
- PIP 3C7 Notifica di auto-fatturazione V01.00.00
- PIP 3D8 Distribuzione attività in esecuzione V01.00.00
- PIP 4A1 Notifica di previsione strategica V02.00.00
- PIP 4A3 Notifica di previsione soglia release V02.00.00
- PIP 4A4 Notifica di previsione pianificazione release R02.00.00A
- PIP 4A5 Notifica di replica previsione V02.00.00
- PIP 4B2 Notifica di ricezione della spedizione V01.00.00
- PIP 4B3 Notifica di consumo V01.00.00
- PIP 4C1 Distribuzione di report inventario V02.03.00
- PIP 4C1 Distribuzione di report inventario V02.01
- PIP 5C1 Distribuzione elenco prodotto V01.00.00
- PIP 5C2 Richiesta registrazione progetto V01.00.00
- PIP 5C4 Distribuzione stato registrazione V01.02.00
- PIP 5D1 Richiesta sped. da magazzino e autorizzazione addebito V01.00.00
- PIP 6C1 Query concessione servizio V01.00.00
- PIP 6C2 Richiesta garanzia reclamo V01.00.00
- PIP 7B1 Distribuzione attività in esecuzione V01.00.00
- PIP 7B5 Notifica ordine attività industriale V01.00.00
- PIP 7B6 Notifica replica ordine attività industriale V01.00.00

Per ogni PIP, esistono quattro Package del tipo di documento PIP:

- Per il sistema di messaggistica RNIF 1.1 con i partner
- Per il sistema di messaggistica RNIF 1.1 con i sistemi di back-end
- Per il sistema di messaggistica RNIF 2.0 con i partner
- Per il sistema di messaggistica RNIF 2.0 con i sistemi di back-end

Ciascun package del tipo di documento PIP segue una convenzione di denominazione specifica che consente di identificare se il package sia valido per i messaggi tra WebSphere Partner Gateway e i partner o tra WebSphere Partner Gateway ed i sistemi di back-end. La convenzione di denominazione identifica inoltre la versione RNIF, PIP e la versione PIP supportata dal package. Per i package del tipo di documento PIP utilizzati per il sistema di messaggistica tra WebSphere Partner Gateway e i partner, il formato è:

`BCG_Package_RNIF<RNIF_version>_<PIP><PIP_version>.zip`

Per i package del tipo di documento PIP utilizzati per il sistema di messaggistica tra WebSphere Partner Gateway ed i sistemi di back-end, il formato è:

```
BCG_Package_RNSC<Backend_Integration_version>_RNIF<RNIF_version>_
<PIP><PIP_version>.zip
```

Ad esempio, il file BCG_Package_RNIF1.1_3A4V02.02.zip è valido per la convalida dei documenti per la versione 02.02 di PIP 3A4 inviati tra i partner e WebSphere Partner Gateway mediante il protocollo RNIF 1.1. Per i package del tipo di documento PIP per comunicare con i sistemi di back-end, il nome del package deve identificare anche il protocollo utilizzato per inviare il contenuto RosettaNet ai sistemi di back-end. Per informazioni sull'impacchettamento utilizzato per questi messaggi, consultare il manuale *WebSphere Partner Gateway Enterprise Integration Guide*.

Creazione delle definizioni del documento

Informazioni su questa attività

Per il sistema di messaggistica RosettaNet, WebSphere Partner Gateway richiede i package RNIF per la versione di RNIF utilizzata per inviare i messaggi. Per ciascun PIP supportato da WebSphere Partner Gateway, richiede due package del tipo di documento PIP per la versione RNIF. Ad esempio, per supportare il PIP 3A4 sul RNIF 2.0, WebSphere Partner Gateway richiede i seguenti package:

- Package_RNIF_V02.00.zip
- Package_RNSC_1.0_RNIF_V02.00.zip
- BCG_Package_RNIFV02.00_3A4V02.02.zip
- BCG_Package_RNSC1.0_RNIFV02.00_3A4V02.02.zip

Il primo package supporta il sistema di messaggistica RosettaNet con i partner ed il secondo package supporta il sistema di messaggistica RosettaNet con i sistemi di back-end. Il terzo ed il quarto package consentono a WebSphere Partner Gateway di trasmettere i messaggi 3A4 tra i partner ed i sistemi di back-end mediante RNIF 2.0.

Per caricare un package RosettaNet:

1. Fare clic su **Amministrazione hub > Configurazione hub> Definizione documento**.
2. Fare clic su **Carica/Scarica package**.
3. Selezionare **No** per **Package WSDL**.
4. Fare clic su **Sfoglia** e selezionare il package RNIF per la comunicazione con i partner.

   I package RNIF sono ubicati, per impostazione predefinita, nella directory B2BIntegrate/Rosettanet sul supporto di installazione. Se, ad esempio si stava caricando il package RNIF versione 2.00, si deve accedere alla directory B2BIntegrate/Rosettanet e scegliere: Package_RNIF_V0200.zip.
5. Accertarsi che **Salva nel database** sia stato impostato su **Sì**.
6. Fare clic su **Carica**.
7. Fare nuovamente clic su **Sfoglia** e selezionare il package RNIF per la comunicazione con le applicazioni di back-end.

   Se, ad esempio si stava caricando il package RNIF versione 2.00, si deve accedere alla directory B2BIntegrate/Rosettanet e scegliere Package_RNSC_1.0_RNIF_V02.00.zip.
8. Fare clic su **Carica**.

   I package richiesti per comunicare con i partner o con il sistema di back-end sono stati installati nel sistema. Se è stata controllata la pagina Gestisci le

definizioni di documento, viene visualizzata una voce **Package: RNIF/Protocollo: RosettaNet**, che rappresenta il tipo di impacchettamento per comunicare con i partner e **Package: Integrazione backend/Protocollo: RNSC**, che indica il tipo di impacchettamento per comunicare con le applicazioni di back-end.

9. Per ciascun PIP che si desidera supportare, caricare il package del tipo di documento PIP per PIP e per la versione RNIF supportati. Ad esempio, per caricare PIP 3A6 (Notifica avviso di pagamento Advice) da inviare ad un partner, effettuare la seguente procedura:
   a. Fare clic su **Sfoglia** e selezionare BCG_Package_RNIFV02.00_3C6V02.02 dalla directory B2BIntegrate/Rosettanet.
   b. Accertarsi che **Salva nel database** sia stato impostato su **Sì**.
   c. Fare clic su **Carica**.

   Quindi, il PIP 3C6V02.02 viene visualizzato come un tipo di documento posto al di sotto di **Package: RNIF/Protocollo: RosettaNet** nella pagina Gestisci le definizioni di documento. Viene visualizzata anche un'attività, un'azione e due segnali. Sono inclusi nel caricamento del PIP.

   Per caricare il PIP 3A6 da inviare ad un'applicazione di back-end, eseguire questi passaggi:
   a. Fare clic su **Sfoglia** e selezionare BCG_Package_RNSC1.0_RNIFV02.00_3C6V02.02.zip.
   b. Accertarsi che **Salva nel database** sia stato impostato su **Sì**.
   c. Fare clic su **Carica**.

   Quindi, il PIP 3C6V02.02 viene visualizzato come tipo di documento, posto al di sotto di **Package: Integrazione backend/Protocollo: RNSC** nella pagina Gestisci le definizioni di documento. Se WebSphere Partner Gateway non fornisce un package per il PIP o la versione PIP che si desidera utilizzare, è possibile creare una propria e caricarla. Per ulteriori informazioni, consultare la sezione "Creazione dei package di definizione del documento PIP" a pagina 355.

Configurazione dei valori dell'attributo

Informazioni su questa attività

Per le definizioni del documento PIP, la maggior parte dei valori di attributo è già stata impostata e non è necessario configurarla. Tuttavia, non è necessario impostare i seguenti attributi:

Package RNIF (1.0)

- **GlobalSupplyChainCode** - identificare il tipo di catena di fornitura utilizzata dal partner. I tipi sono Componenti elettronici, Informazioni delle tecnologie e Produzione del semiconduttore. Questo attributo non presenta un valore predefinito.

Package RNIF (V02.00)

- **Codifica** - Impostare se i PIP devono avere un payload codificato, un contenitore e un payload codificato e nessuna codifica. Il valore predefinito è Nessuno.
- **Ric sinc richiesto** - Impostato su sì se il partner desidera ricevere la notifica di ricezione. Impostare su No se è richiesto 200.
- **Sinc supportata** - Impostare se il PIP supporta gli scambi di messaggi sincroni. Il valore predefinito è No.

I PIP per cui WebSphere Partner Gateway fornisce i package del tipo di documento PIP non sono sincroni. Quindi, non è necessario modificare gli attributi Ric sinc richiesto e Sinc supportata per questi PIP.

Nota: il comportamento dell'attributo Ric sinc richiesto si differenzia dai PIP ad uno o due modi. Per un PIP a 2 modi, quando Ric sinc richiesto è impostato su No, questa impostazione ha la precedenza sull'impostazione Sì di Non-rifiuto di ricevuta. Ad esempio, supporre di inviare un 3A7 con le seguenti impostazioni:

- SiqReq=Y
- NonRepofRec=Y
- SyncSupported=Y
- SyncAckReq=N

Per un PIP a due modi, viene ricevuto un messaggio di errore sul documento in entrata. Su un PIP a un modo, tuttavia, il documento in entrata viene visualizzato sulla console e 0KB 200 è stato restituito al partner.

Per impostare gli attributi, procedere nel modo seguente:

1. Fare clic su **Amministrazione hub > Configurazione hub> Definizione documento**.
2. Fare clic sulle icone **Espandi** per espandere in maniera individuale un nodo al livello della definizione del documento appropriato o selezionare **Tutti** per espandere tutti i nodi della definizione del documento visualizzati.
3. Nella colonna **Azioni**, fare clic sull'icona **Modifica valori attributo** per il package (ad esempio, Package: RNIF (1.1) o Package: RNIF (V02.00)) che si desidera modificare.
4. Nella sezione **Attributi del contesto della definizione di documento**, andare alla colonna **Aggiornamento** dell'attributo che si desidera impostare e selezionare o inserire il nuovo valore. Ripetere tale passaggio per ogni attributo che si desidera impostare.
5. Fare clic su **Salva**.

Nota: è anche possibile aggiornare gli attributi RosettaNet sul livello della connessione facendo clic su **Attributi** per l'origine o la destinazione e inserire o modificare i valori nella colonna **Aggiornamento**. Consultare la sezione "Specifica e modifica di attributi" a pagina 238.

Creazione delle interazioni

Informazioni su questa attività

Il seguente processo descrive il modo in cui creare un'interazione tra un sistema di back-end e un partner. È necessario creare un'interazione per ciascun PIP da inviare e uno per ciascun PIP da ricevere.

Prima di iniziare, verificare che le definizioni del documento RNIF appropriate siano state caricate e che i package per il PIP che si desidera utilizzare siano stati caricati. Se si desidera generare un PIP 0A1 (Notification of Failure), verificare che sia stato caricato tale PIP, come descritto nella fase 9 a pagina 111.

Per creare un'interazione per un particolare PIP, procedere nel modo seguente:

1. Fare clic su **Amministrazione hub > Configurazione hub> Definizione documento**.
2. Fare clic su **Crea interazione**.

3. Espandere l'albero **Origine** al livello **Azione** ed espandere l'albero **Destinazione** al livello **Azione**.
4. Nelle strutture ad albero, selezionare le definizioni del documento da utilizzare per il contesto di origine e quello di destinazione. Ad esempio, se il partner è l'iniziatore di un PIP 3C6 (un PIP di un'unica azione), selezionare le seguenti definizioni del documento:

Tabella 6. PIP 3C6 avviato da un partner

Origine	**Destinazione**
Package: RNIF (V02.00)	Package: Integrazione Backend (1.0)
Protocollo: RosettaNet (V02.00)	Protocollo: RNSC (1.0)
Tipo di documento: 3C6 (V01.00)	Tipo di documento: 3C6 (V01.00)
Attività: Notify of Remittance Advice	Attività: Notify of Remittance Advice
Azione: Remittance Advice Notification Action	Azione: Remittance Advice Notification Action

Se il sistema di back-end è l'iniziatore del PIP 3C6, selezionare le seguenti definizioni del documento:

Tabella 7. PIP 3C6 iniziato da un sistema di back-end

Origine	**Destinazione**
Package: Integrazione Backend (1.0)	Package: RNIF (V02.00)
Protocollo: RNSC (1.0)	Protocollo: RosettaNet (V02.00)
Tipo di documento: 3C6 (V01.00)	Tipo di documento: 3C6 (V01.00)
Attività: Notify of Remittance Advice	Attività: Notify of Remittance Advice
Azione: Remittance Advice Notification Action	Azione: Remittance Advice Notification Action

Per un PIP a doppia azione, come ad esempio 3A4 avviato da un partner, selezionare le seguenti definizioni del documento per la prima azione:

Tabella 8. PIP 3A4 avviato da un partner

Origine	**Destinazione**
Package: RNIF (V02.00)	Package: Integrazione Backend (1.0)
Protocollo: RosettaNet (V02.00)	Protocollo: RNSC (1.0)
Tipo di documento: 3A4 (V02.02)	Tipo di documento: 3A4 (V02.02)
Attività: Request Purchase Order	Attività: Request Purchase Order
Azione: Purchase Order Request Action	Azione: Purchase Order Request Action

Se un sistema di back-end avvia il PIP 3A4 a doppia azione, selezionare le seguenti definizioni del documento per la prima azione:

Tabella 9. PIP 3A4 inizializzato da un sistema di back-end

Origine	**Destinazione**
Package: Integrazione Backend (1.0)	Package: RNIF (V02.00)
Protocollo: RNSC (1.0)	Protocollo: RosettaNet (V02.00)
Tipo di documento: 3A4 (V02.02)	Tipo di documento: 3A4 (V02.02)
Attività: Request Purchase Order	Attività: Request Purchase Order
Azione: Purchase Order Request Action	Azione: Purchase Order Request Action

5. Nel campo Azione, selezionare **Conversione bidirezionale di RosettaNet e del contenuto del servizio di RosettaNet con convalida**.
6. Fare clic su **Salva**.
7. Se si imposta un PIP a doppia azioni, ripetere i passaggi necessari per creare l'interazione per la seconda azione. Ad esempio, selezionare le seguenti definizioni del documento per la seconda azione per un PIP 3A4 avviato da un partner. Si tratta dell'azione in cui il sistema di back-end invia la risposta.

Tabella 10. PIP 3A4 avviato da un partner (seconda azione)

Origine	Destinazione
Package: Integrazione Backend (1.0)	Package: RNIF (V02.00)
Protocollo: RNSC (1.0)	Protocollo: RosettaNet (V02.00)
Tipo di documento: 3A4 (V02.02)	Tipo di documento: 3A4 (V02.02)
Attività: Request Purchase Order	Attività: Request Purchase Order
Azione: Purchase Order Confirmation Action	Azione: Purchase Order Confirmation Action

Per la seconda azione per un sistema di back-end che ha avviato il PIP 3A4, selezionare le seguenti definizioni del documento:

Tabella 11. PIP 3A4 avviato da un sistema di back-end (seconda azione)

Origine	Destinazione
Package: RNIF (V02.00)	Package: Integrazione Backend (1.0)
Protocollo: RosettaNet (V02.00)	Protocollo: RNSC (1.0)
Tipo di documento: 3A4 (V02.02)	Tipo di documento: 3A4 (V02.02)
Attività: Request Purchase Order	Attività: Request Purchase Order
Azione: Purchase Order Confirmation Action	Azione: Purchase Order Confirmation Action

8. Se si desidera generare una notifica di errore 0A1, creare un'interazione per XMLEvent.
   a. Fare clic su **Amministrazione hub > Configurazione hub> Definizione documento**.
   b. Fare clic su **Crea interazione**.
   c. Espandere la struttura ad albero **Origine** al livello **Tipo di documento** ed espandere la struttura ad albero **Destinazione** al livello **Tipo di documento**.
   d. Selezionare le seguenti definizioni del documento:

Tabella 12. Definizione del documento Evento XML

Origine	Destinazione
Package: Integrazione Backend (1.0)	Package: Integrazione Backend (1.0)
Protocollo: XMLEvent (1.0)	Protocollo: XMLEvent (1.0)
Tipo di documento: XMLEvent (1.0)	Tipo di documento: XMLEvent (1.0)

   e. Nel campo Azione, selezionare **Pass Through**.
   f. Fare clic su **Salva**.
9. Creare un'interazione per XMLEvent su 0A1 RNSC.
   a. Fare clic su **Amministrazione hub > Configurazione hub> Definizione documento**.
   b. Fare clic su **Crea interazione**.

c. Espandere l'albero **Origine** al livello **Tipo di documento** ed espandere l'albero **Destinazione** al livello **Attività**.
d. Selezionare le seguenti definizioni del documento:

Tabella 13. Definizione del documento Evento XML su 0A1

Origine	Destinazione
Package: Integrazione Backend (1.0)	Package: Integrazione Backend (1.0)
Protocollo: XMLEvent (1.0)	Protocollo: RNSC (1.0)
Tipo di documento: XMLEvent (1.0)	Tipo di documento: 0A1 (V02.00)
	Attività: Distribute Notification of Failure.

e. Nel campo Azione, selezionare **Conversione bidirezionale di RosettaNet e XML con convalida**.
f. Fare clic su **Salva**.

Nota: Per abilitare o disabilitare i XMLEvent, consultare *la sezione Enabling or disabling XMLEvents di Enterprise Integration Guide*

Visualizzazione dei documenti RosettaNet

Informazioni su questa attività

Il Visualizzatore RosettaNet riporta le informazioni sui documenti RosettaNet. È possibile visualizzare i documenti non elaborati, gli eventi ed i dettagli di elaborazione dei documenti associati mediante determinati criteri di ricerca. Queste informazioni sono utili nel caso in cui si tenti di stabilire se un documento sia stato consegnato correttamente o determinare la causa di un problema.

Per avviare il Visualizzatore RosettaNet, procedere nel modo seguente:

1. Fare clic su **Visualizzatori > Visualizzatore RosettaNet**.
2. Selezionare dagli elenchi i criteri di ricerca corretti, come descritto in Tabella 14.

Tabella 14. Criteri di ricerca RosettaNet

Valore	Descrizione
Data e ora di inizio	La data e l'ora in cui il processo è stato avviato.
Data e ora di fine	La data e l'ora in cui il processo è stato completato.
Partner di origine e di destinazione	Identifica i partner di origine (che inizia) e di destinazione (che riceve) (solo partner interno).
Partner	Indica se la ricerca viene applicata a tutti i partner o al solo partner interno.
Il mio ruolo è	Indica se vengono ricercati i documenti in cui il partner è di destinazione o di origine.
ID di business di origine	Il numero di identificazione di business del partner di inizializzazione, ad esempio, DUNS.
Modalità operativa	Produzione o verifica. La verifica è disponibile solo sui sistemi che supportano la modalità operativa di verifica.
Protocollo	I protocolli disponibili per i partner.
Tipo di documento	Il processo di business specifico.
ID istanza processo	Numero di identificazione univoco assegnato al processo. I criteri possono comprendere il carattere jolly dell'asterisco (*).
Ordina per	Ordinare i risultati per: • Data e ora di destinazione • Tipo di documento Il valore predefinito è Data e ora di destinazione.

Tabella 14. Criteri di ricerca RosettaNet (Continua)

Valore	Descrizione
Decrescente o Crescente	Decrescente visualizza la data/ora più recente o il testo a partire dalla prima lettera dell'alfabeto. Crescente visualizza la data/ora meno recente o il testo a partire dall'ultima lettera dell'alfabeto. I valore predefinito è Decrescente.
Risultati per pagina	Specifica il numero di risultati visualizzati per pagina

3. Fare clic su **Cerca**.

Documenti CIDX

CIDX è un'associazione di business robusta ed indica il corpo degli standard, il cui obiettivo è migliorare la semplicità, la velocità ed il costo per condurre l'azienda elettronicamente tra le aziende chimiche e i relativi partner di business. CIDX comprende varie iniziative che guidano gli standard per l'industria chimica. In questo documento viene trattata l'iniziativa Chem eStandards di CIDX. Chem eStandards rappresenta standard uniformi di scambio dati, sviluppati in modo specifico dall'acquisto, dalla vendita e dalla consegna di prodotti chimici. Chem eStandards è costituito da:

- Specifiche messaggi di ChemXML o Chem eStandards: v2.0, v2.0.1, v2.0.2, v3.0 e v4.0.
- Specifica della sicurezza e busta di Chem eStandards: v2.0 e v3.0

Per l'impacchettamento, CIDX utilizza sempre RNIF 1.1. È importante osservare che RNIF 1.1 è sempre asincrono. Quindi, gli scambi del documento CIDX sono sempre asincroni.

CIDX è costituito da funzioni di impacchettamento e dalle transazioni, mentre RosettaNet è costituito da funzioni di impacchettamento e da PIP (partner interchange processes). CIDX utilizza l'è costituito da funzioni di impacchettamento RNIF 1.1. Le transazioni sono definite dallo standard ChemXML. Ciascuna versione dello standard ChemXML definisce le transazioni. Tutte le transazioni di ChemXML, in una determinata versione dello standard ChemXML, hanno la stessa versione dello standard ChemXML. A differenza di RosettaNet, CIDX non richiede la conformità per elaborare la definizione. CIDX riguarda la struttura della transazione e lo scambio dei messaggi in modo sicuro.

Per continuare il confronto, RosettaNet è il responsabile di amministrazione per lo standard RosettaNet come CIDX è il responsabile di amministrazione dello standard CIDX. RosettaNet definisce l'impachettamento RNIF e i PIP. I messaggi di RosettaNet possono utilizzare RNIF 1.1 o RNIF 2.0. I PIP definiti da RosettaNet forniscono il gruppo messaggi e la coreografia del processo. CIDX utilizza sempre RNIF 1.1 come definito da RosettaNet. Poiché CIDX è il corpo di amministrazione, la busta RNIF deve essere costruita nel modo definito dalla specifica della sicurezza e dalla busta di Chem eStandards. Questa specifica si basa sull'implementazione di RosettaNet. CIDX NON utilizza i PIP definiti da RosettaNet. Invece, CIDX utilizza la specifica messaggi di Chem eStandards.

Per ulteriori informazioni su CIDX, consultare l'indirizzo http://www.cidx.org. Gli standard di CIDX possono essere scaricati dall'indirizzo: http://www.cidx.org. È possibile trovare Chem eStandards Envelope and Security Version 3.0 all'indirizzo http://www.cidx.org/Portals/0/Publications/Envelope_and_Security_v3.0.pdf.

WebSphere Partner Gateway supporta il seguente Chem eStandards:

- Specifica della sicurezza e busta Chem eStandards v3.0.
- Specifiche messaggi di Chem eStandards o ChemXML v4.0.

Package del tipo di documento RNIF e PIP per CIDX

CIDX utilizza RNIF1.1. Per supportare CIDX, WebSphere Partner Gateway fornisce due gruppi di file compressi, definiti package. lo *package RNIF* sono costituiti da definizioni del documento richieste per supportare il protocollo RNIF. Questi package sono contenuti nella directory B2BIntegrate.

Per RNIF V1.1, i package sono:

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

Il primo package fornisce le definizioni del documento richieste per supportare le comunicazioni CIDX con i partner e il secondo package fornisce le definizioni del documento richieste per supportare le comunicazioni CIDX con i sistemi di back-end.

Il secondo gruppo di package è costituito dai package del tipo di documento PIP. Ogni package del tipo di documento PIP include una directory Packages, che contiene un file XML e una directory GuidelineMaps che comprende i file XSD. Il file XML specifica le definizioni del documento che stabiliscono il modo in cui WebSphere Partner Gateway gestisce PIP e definisce i segnali ed i messaggi scambiati. I file XSD specificano il formato dei messaggi PIP e definiscono i valori consentiti per gli elementi XML dei messaggi. I file compressi per PIP 0A1 presentano anche un file XML che l'hub utilizza come modello per creare i documenti 0A1.

Per CIDX, WebSphere Partner Gateway fornisce i package del tipo di documento per Order Create di E41 ChemXML versione 4.0 e Order Response di E42 ChemXML versione 4.0

La convenzione di denominazione dei package CIDX forniti coincide con i package forniti per RosettaNet. Ad esempio, BCG_Package_RNIF1.1_E414.0.zip è valido per la convalida dei documenti v4.0 per il PIP E41 inviato tra i partner e WPG mediante RNIF1.1

Creazione delle definizioni del documento

Informazioni su questa attività

Per il sistema di messaggistica CIDX, WebSphere Partner Gateway richiede i package RNIF per la versione di RNIF utilizzata per inviare i messaggi. Per ciascun PIP supportato da WebSphere Partner Gateway, richiede due package del tipo di documento PIP per la versione RNIF. Ad esempio, per supportare il PIP E41 in RNIF1.1, WebSphere Partner Gateway richiede i seguenti package:

- Package_RNIF_1.1.zip
- Package_RNSC_1.0_RNIF_1.1.zip
- BCG_Package_RNIF1.1_E414.0.zip
- BCG_Package_RNSC1.0RNIF1.1_E414.0.zip

Il primo package supporta il sistema di messaggistica CIDX con i partner e il secondo package supporta il sistema di messaggistica CIDX con i sistemi di

back-end. Il terzo ed il quarto package consentono a WebSphere Partner Gateway di trasmettere i messaggi E41 tra i partner ed i sistemi di back-end.

Per caricare i package CIDX:

1. Fare clic su **Amministrazione hub > Configurazione hub> Definizione documento**.
2. Fare clic su **Carica/Scarica package**.
3. Selezionare **No** per **Package WSDL**.
4. Fare clic su **Sfoglia** e selezionare il package RNIF per la comunicazione con i partner.

   I package RNIF sono situati, per impostazione predefinita, nella directory B2BIntegrate/rosettanet del supporto di installazione. Se, ad esempio si stava caricando il package RNIF versione 2.00, si deve accedere alla directory B2BIntegrate/rosettanet e scegliere: Package_RNIF_V0200.zip.
5. Accertarsi che **Salva nel database** sia stato impostato su **Sì**.
6. Fare clic su **Carica**.
7. Fare nuovamente clic su **Sfoglia** e selezionare il package RNIF per la comunicazione con le applicazioni di back-end.

   Se, ad esempio si stava caricando il package RNIF versione 2.00, si deve accedere alla directory B2BIntegrate/rosettanet e scegliere Package_RNSC_1.0_RNIF_V02.00.zip.
8. Fare clic su **Carica**.

   I package richiesti per comunicare con i partner o con il sistema di back-end sono stati installati nel sistema. Se è stata controllata la pagina Gestisci le definizioni di documento, viene visualizzata una voce **Package: RNIF/Protocollo: Rosettanet**, che rappresenta il tipo di impacchettamento per comunicare con i partner e **Package: Integrazione backend/Protocollo: RNSC**, che indica il tipo di impacchettamento per comunicare con le applicazioni di back-end.
9. Per ogni PIP che si desidera supportare, caricare il package del tipo di documento PIP per il PIP e per la versione di RNIF supportati.

   Ad esempio, per caricare il PIP E41 CIDX (Order Create) da inviare ad un partner, procedere nel modo seguente:

   a. Fare clic su **Sfoglia** e selezionare **BCG_Package_RNIF1.1_E414.0.zip** nella directory B2BIntegrate/Rosettanet.
   b. Accertarsi che **Salva nel database** sia stato impostato su **Sì**.
   c. Fare clic su **Carica**.

   Quindi, il PIP E41 viene visualizzato come tipo di documento, posto al di sotto di Package: RNIF/Protocollo: RosettaNet nella pagina Gestisci le definizioni di documento. Viene visualizzata anche un'attività, un'azione e due segnali. Sono inclusi nel caricamento del PIP.

   Per caricare il PIP E41 da inviare all'applicazione di back-end, procedere nel modo seguente:

   a. Fare clic su **Sfoglia** e selezionare **BCG_Package_RNSC1.0RNIF1.1_E414.0.zip**.
   b. Accertarsi che **Salva nel database** sia stato impostato su **Sì**.
   c. Fare clic su **Carica**.

   Quindi il PIP E41 viene visualizzato come tipo di documento posto al di sotto di Package: Integrazione backend/Protocollo: RNSC nella pagina Gestisci le definizioni di documento.

Configurazione dei valori dell'attributo

Informazioni su questa attività

Per le definizioni del documento RNIF, la maggior parte dei valori di attributo è già stata impostata e non è necessario configurarla. Tuttavia, non è necessario impostare i seguenti attributi:

Package RNIF (1.1)

- **GlobalSupplyChainCode** - identificare il tipo di catena di fornitura utilizzata dal partner. I tipi sono Componenti elettronici, Informazioni delle tecnologie e Produzione del semiconduttore. Questo attributo non presenta un valore predefinito.

Per impostare gli attributi, procedere nel modo seguente:

1. Fare clic su **Amministrazione hub > Configurazione hub> Definizione documento**.
2. Fare clic sulle icone **Espandi** per espandere in maniera individuale un nodo al livello della definizione del documento appropriato o selezionare **Tutti** per espandere tutti i nodi della definizione del documento visualizzati.
3. Nella colonna **Azioni**, fare clic sull'icona **Modifica valori attributo** per il package (ad esempio, Package: RNIF (1.1) o Package: RNIF (V02.00)) che si desidera modificare.
4. Nella sezione **Attributi del contesto della definizione di documento**, andare alla colonna **Aggiornamento** dell'attributo che si desidera impostare e selezionare o inserire il nuovo valore. Ripetere tale passaggio per ogni attributo che si desidera impostare.
5. Fare clic su **Salva**.

Nota: è anche possibile aggiornare gli attributi RosettaNet sul livello della connessione facendo clic su **Attributi** per l'origine o la destinazione e inserire o modificare i valori nella colonna **Aggiornamento**. Consultare la sezione "Specifica e modifica di attributi" a pagina 238.

Creazione delle interazioni

Informazioni su questa attività

Il seguente processo descrive il modo in cui creare un'interazione tra un sistema di back-end e un partner. È necessario creare un'interazione per ciascun PIP da inviare e uno per ciascun PIP da ricevere.

Prima di iniziare, verificare che le definizioni del documento RNIF appropriate siano state caricate e che i package per il PIP che si desidera utilizzare siano stati caricati.

Per creare un'interazione per un particolare PIP, procedere nel modo seguente:

1. Fare clic su **Amministrazione hub > Configurazione hub> Definizione documento**.
2. Fare clic su **Crea interazione**.
3. Espandere l'albero **Origine** al livello **Azione** ed espandere l'albero **Destinazione** al livello **Azione**.
4. Nelle strutture ad albero, selezionare le definizioni del documento da utilizzare per il contesto di origine e quello di destinazione. Ad esempio, se il partner è

l'iniziatore di un PIP E41, selezionare le seguenti definizioni del documento:

Tabella 15. PIP 3C6 avviato da un partner

Origine	Destinazione
Package:RNIF(1.1)	Package: Integrazione di backEnd (1.1)
Protocollo:RosettaNet(1.1)	Protocollo: RNSC (1.0)
Tipo di documento: E41 (4.0)	Tipo di documento: E41 (4.0)
Attività: OrderCreate	Attività:OrderCreate
Azione: Order Create	Azione: Order Create

Per un PIP a doppia azione, come ad esempio 3A4 avviato da un partner, selezionare le seguenti definizioni del documento per la prima azione:

Tabella 16. PIP 3A4 avviato da un partner

Origine	Destinazione
Package: RNIF (V02.00)	Package: Integrazione Backend (1.0)
Protocollo: RosettaNet (V02.00)	Protocollo: RNSC (1.0)
Tipo di documento: 3A4 (V02.02)	Tipo di documento: 3A4 (V02.02)
Attività: Request Purchase Order	Attività: Request Purchase Order
Azione: Purchase Order Request Action	Azione: Purchase Order Request Action

5. Nel campo Azione, selezionare **Conversione bidirezionale di RosettaNet e del contenuto del servizio di RosettaNet con convalida**.
6. Fare clic su **Salva**.

Visualizzazione dei documenti CIDX

Informazioni su questa attività

Il Visualizzatore RosettaNet riporta le informazioni sui documenti CIDX. È possibile visualizzare i documenti non elaborati, gli eventi ed i dettagli di elaborazione dei documenti associati mediante determinati criteri di ricerca. Queste informazioni sono utili nel caso in cui si tenti di stabilire se un documento sia stato consegnato correttamente o determinare la causa di un problema.

Per avviare il Visualizzatore RosettaNet, procedere nel modo seguente:

1. Fare clic su **Visualizzatori > Visualizzatore RosettaNet**.
2. Selezionare i criteri di ricerca appropriati.
3. Fare clic su **Cerca**.

Documenti ebMS

Il meccanismo ebMS fornisce un metodo standard per scambiare i messaggi di business tra i partner di business ebXML. ebMS (ebXML Messaging Service) fornisce un supporto affidabile per scambiare i messaggi di business senza dipendere dalle soluzioni e dalle tecnologie esclusive. Questa sezione mostra come impostare le definizioni e le interazioni del documento per questi documenti.

Creazione delle definizioni del documento

Informazioni su questa attività

Il sistema di messaggistica ebMS richiede che un file XML CPA (Collaboration Profile Agreement) sia caricato prima di poter definire i documenti.

Per caricare un file XML CPA, procedere nel modo seguente:

1. Fare clic su **Amministrazione hub** > **Configurazione hub** > **ebMS**.
2. Fare clic su **Carica CPA**.
3. Fare clic su **Sfoglia** e selezionare il package CPA appropriato.
4. Verificare che **Versione ebMS** 2.0 sia stata selezionata.
5. Fare clic su **Carica**.

Durante il processo di caricamento CPA, all'utente sarà richiesto di selezionare il partner interno dai partner presenti in CPA. Il partner interno viene considerato come il gestore nel flusso ebMS e tutte le destinazioni nel flusso ebMS per il partner interno utilizzeranno l'impacchettamento N/A o l'integrazione di backend. Tuttavia, sulla console il partner sarà riportato solo come partner esterno.

Quindi ebMS viene visualizzato come un package e come un protocollo in ebMS e Package: Integrazione di backend nella pagina Gestisci le definizioni di documento.

Inoltre, è possibile configurare Il flusso ebMS in WebSphere Partner Gateway senza CPA. A tal fine, creare le definizioni del documento ebMS, le capacità B2B dalla console WebSphere Partner Gateway come descritto nella sezione "Panoramica dei tipi di documenti" a pagina 101. In effetti, mentre si carica CPA, tutte le configurazioni verranno eseguite automaticamente. In mancanza di CPA, seguire la procedura riportata in questa sezione.

Configurazione dei valori dell'attributo

Informazioni su questa attività

Per le definizioni del documento ebMS, la maggior parte dei valori degli attributi è già stata impostata e non è necessario configurarla. Tuttavia, non è necessario impostare i seguenti attributi:

Package ebMS

- **Ora per riconoscere in min** - Impostare l'intervallo di attesa per una notifica prima di inviare nuovamente la richiesta originale. Questo attributo funziona insieme al Conteggio tentativi. Le unità sono espresse in minuti. Il valore predefinito è 30.
- **Conteggio tentativi** - Impostare il numero di volte per cui inviare una richiesta se non viene ricevuto un riconoscimento. Questo attributo funziona insieme all'attributo Ora per riconoscere. Il valore predefinito è 3.
- **Non-rifiuto richiesto** - Indica se memorizzare il documento originale nella memoria di non rifiuto. Il valore predefinito è Sì.

  Nota: in WebSphere Partner Gateway 6.1, le informazioni di non rifiuto sono ottenute dai parametri della connessione partner. I parametri della connessione partner sono ottenuti dopo una ricerca con esito positivo della connessione partner. Per impostazione predefinita, il non rifiuto è impostato su "Sì"; questo significa che, se per qualche ragione le informazioni non sono disponibili dalla connessione partner, il documento verrà inserito nella memoria di non rifiuto.

- **Memorizzazione messaggio richiesta** - Indica se memorizzare il documento nella memorizzazione messaggio. Il valore predefinito è Sì.

  Nota: A partire da WebSphere Partner Gateway 6.1.1, le informazioni della memorizzazione messaggio vengono ottenute dai parametri della connessione partner. I parametri della connessione partner sono ottenuti dopo una ricerca con esito positivo della connessione partner. Per impostazione predefinita, la memorizzazione messaggio è impostata su ″Sì″, che indica che il documento verrà conservato nella memorizzazione messaggio.
- **Non-rifiuto di ricevuta** - Impostare se memorizzare la ricezione nella memoria di non rifiuto. Il valore predefinito è Sì.
- **Intervallo tentativi** - Impostare l'intervallo di attesa del sistema tra i tentativi. Questo attributo funziona insieme al Conteggio tentativi. Il valore predefinito è 5 minuti.

Per impostare gli attributi, procedere nel modo seguente:

1. Fare clic su **Amministrazione hub > Configurazione hub > Definizione documento**.
2. Fare clic sulle icone **Espandi** per espandere in maniera individuale un nodo al livello della definizione del documento appropriato o selezionare **Tutti** per espandere tutti i nodi della definizione del documento visualizzati.
3. Nella colonna **Azioni**, fare clic sull'icona **Modifica i valori dell'attributo** per il package che si desidera modificare.
4. Nella sezione **Attributi del contesto della definizione di documento**, andare alla colonna **Aggiornamento** dell'attributo che si desidera impostare e selezionare o inserire il nuovo valore. Ripetere tale passaggio per ogni attributo che si desidera impostare.
5. Fare clic su **Salva**.

Nota: è anche possibile aggiornare gli attributi ebMS sul livello della connessione facendo clic su **Attributi** per l'origine o la destinazione e inserire o modificare i valori nella colonna **Aggiornamento**. Consultare la sezione "Specifica e modifica di attributi" a pagina 238.

Creazione delle interazioni

Informazioni su questa attività

Il seguente processo descrive il modo in cui creare un'interazione tra un sistema di back-end e un partner.

Prima di iniziare, verificare che le definizioni del documento ebMS appropriate siano state caricate.

Per creare un'interazione per un determinato partner, procedere nel modo seguente:

1. Fare clic su **Amministrazione hub** > **Configurazione hub** > **Definizione documento**.
2. Fare clic su **Crea interazione**.
3. Espandere la struttura ad albero Origine al livello Azione ed espandere la struttura ad albero Destinazione al livello Azione.
4. Nelle strutture ad albero, selezionare le definizioni del documento da utilizzare per il contesto di origine e quello di destinazione. Ad esempio, se il partner è l'iniziatore di un messaggio ebMS, selezionare le seguenti definizioni del

documento:

Tabella 17. ebMS avviato da un partner

Origine	Destinazione
Package: ebMS	Package: Integrazione Backend (1.0)
Protocollo: ebMS	Protocollo: ebMS
Tipo di documento: ALMService	Tipo di documento: ALMService
Attività: ALMService	Attività: ALMService
Azione: Remittance ALMBusiness	Azione: ALMBusiness

Se il sistema di back-end è l'iniziatore di ebMS, selezionare le seguenti definizioni del documento:

Tabella 18. ebMS avviato dal sistema di back-end

Origine	Destinazione
Package: Integrazione Backend (1.0)	Package: ebMS
Protocollo: ebMS	Protocollo: ebMS
Tipo di documento: ALMService	Tipo di documento: ALMService
Attività: ALMService	Attività: ALMService
Azione: ALMBusiness	Azione: Remittance ALMBusiness

5. In alternativa, nel campo Azione selezionare **Suddivisione ebMS e analisi**.

   La selezione di questo handler estrae i payload dal messaggio ebMS, proveniente dal partner e introduce i payload nuovamente nel flusso come se provenissero dal partner in modo separato. Questo handler non deve essere selezionato quando il sistema di back-end avvia il messaggio. Se questo handler non è stato selezionato, nel campo Azione selezionare Pass Through
6. Fare clic su **Salva**.

   Nota: in alcuni flussi ebMS, ad esempio nelle specifiche STAR, l'elemento Servizio ebMS (il valore Servizio ebMS coincide con il valore Definizione del flusso di documenti del canale WPG) non è un indirizzo URI ma una stringa. In tal caso, come per la specifica ebMS 2.0, un attributo di tipo deve essere presente con l'elemento Servizio nel messaggio SOAP ebMS. Ad esempio, in una specifica STAR, l'attributo di tipo deve includere il valore "STARBOD." È possibile configurare un attributo sulla destinazione degli attributi Definizione del flusso di documenti. (Consultare la Tabella 20 a pagina 139).

Associazione di CPA ebMS alla configurazione di WebSphere Partner Gateway

Informazioni su questa attività

Questa sezione fornisce l'associazione tra CPA (Collaboration Profile Agreement) e la configurazione di WebSphere Partner Gateway UI. Le funzioni vengono elencate insieme alla configurazione di WebSphere Partner Gateway UI corrispondente.

1.

Funzione
Elemento/Attributo

1.1 IdCPA 1

Importato/Configurato manualmente: importato

Configurazione di WebSphere Partner Gateway UI:

CPAID è configurato tramite i canali associati tra due partner. È possibile visualizzare il valore passando a **Amministrazione hub > ebMS** nella console di WebSphere Partner Gateway. Fare clic su Cerca e poi sull'icona Visualizza dettagli dai risultati della ricerca visualizzati.

2.

Funzione
Elemento/Attributo

1.2. Stato 1

Importato/Configurato manualmente: importato ma non memorizzato in WebSphere Partner Gateway. Inoltre, non è possibile configurarlo manualmente.

Configurazione di WebSphere Partner Gateway UI:

Non è possibile configurare questo attributo in WebSphere Partner Gateway. Il valore viene controllato durante l'importazione di CPA. Uno dei seguenti stati viene visualizzato durante l'importazione:

- Concordato: il CPA può essere importato.
- Firmato: il CPA può essere importato e la firma viene verificata prima dell'importazione.
- Suggerito: non è possibile importare il CPA.

3.

Funzione
Elemento/Attributo

1.3 Avvio 1

Importato/Configurato manualmente: importato.

Configurazione di WebSphere Partner Gateway UI:

Non è possibile configurare questo attributo in WebSphere Partner Gateway. Può essere impostato solo dall'importazione di CPA. È possibile visualizzare il valore passando a **Amministrazione hub > ebMS** nella console di WebSphere Partner Gateway. Fare clic su Cerca e poi sull'icona Visualizza dettagli dai risultati della ricerca visualizzati.

4.

Funzione
Elemento/Attributo

1.4 Fine 1

Importato/Configurato manualmente: importato.

Configurazione di WebSphere Partner Gateway UI:

Non è possibile configurare questo attributo in WebSphere Partner Gateway. Può essere impostato solo dall'importazione di CPA. È possibile visualizzare il valore passando a **Amministrazione hub > ebMS** nella console di WebSphere Partner Gateway. Fare clic su Cerca e poi sull'icona Visualizza dettagli dai risultati della ricerca visualizzati.

5.

Funzione
Elemento/Attributo

1.5 Conversation Constraints 0, 1 (9.5) - invocationLimit 0,1 - concurrentConversations 0, 1

Importato/Configurato manualmente: importato.

Configurazione di WebSphere Partner Gateway UI:

Non è possibile configurare questo attributo in WebSphere Partner Gateway. Può essere impostato solo dall'importazione di CPA. È possibile visualizzare il valore passando a **Amministrazione hub > ebMS** nella console di WebSphere Partner Gateway. Fare clic su Cerca e poi sull'icona Visualizza dettagli dai risultati della ricerca visualizzati.

6.

Funzione
Elemento/Attributo

1.6 Informazioni sulla parte 2
partyName 1

Importato/Configurato manualmente: importato.

Configurazione di WebSphere Partner Gateway UI:

Per visualizzare i valori, passare a **Amministrazione account > Profili > Partner**. Fare clic su Cerca e poi sull'icona Visualizza dettagli dai risultati della ricerca visualizzati per il partner in CPA.

7.

Funzione
Elemento/Attributo

1.6 Informazioni sulla parte 2
defaultMshChannelId 1

Importato/Configurato manualmente: importato ma non memorizzato in WebSphere Partner Gateway. Inoltre, non è possibile configurarlo manualmente.

Configurazione di WebSphere Partner Gateway UI:

I valori vengono utilizzati durante l'importazione del CPA per impostare gli attributi canale degli elementi del segnale **Activity- MSHService** come il Ping, lo stato richiesta, il MessageError e il riconoscimento. Questi valori di canale vengono nuovamente sovrascritti se esiste qualsiasi elemento ″OverrideMshActionBinding″ in CPA per qualsiasi elemento di azione specifico.

8.

Funzione
Elemento/Attributo

1.6 Informazioni sulla parte 2
defautMshPackageId 1

Importato/Configurato manualmente: importato ma non memorizzato in WebSphere Partner Gateway. Inoltre, non è possibile configurarlo manualmente.

Configurazione di WebSphere Partner Gateway UI:

I valori vengono utilizzati durante l'importazione del CPA per impostare gli attributi canale degli elementi del segnale **Activity- MSHService** come il Ping, lo stato richiesta, il MessageError e il riconoscimento. Questi valori di canale vengono nuovamente sovrascritti se esiste qualsiasi elemento ″OverrideMshActionBinding″ in CPA per qualsiasi elemento di azione specifico.

9.

Funzione
Elemento/Attributo

1.6 Informazioni sulla parte 2
PartyId 1, *

Importato/Configurato manualmente: importato.

Configurazione di WebSphere Partner Gateway UI:

Per visualizzare i valori, passare a **Amministrazione account > Profili > Partner**. Fare clic su Cerca e poi sull'icona Visualizza dettagli dai risultati della ricerca visualizzati per il partner in CPA.

10.

Funzione
Elemento/Attributo

1.6 Informazioni sulla parte 2
type

Importato/Configurato manualmente: non importato e non è possibile configurarlo.

11.

Funzione
Elemento/Attributo

1.6 Informazioni sulla parte 2
PartyRef 1,*= (8.4.2)
- xlink:type F
- xlink:href 1
- type Fixed
- schemaLocation Implied

Importato/Configurato manualmente: non importato e non è possibile configurarlo.

12.

Funzione
Elemento/Attributo

1.6 Informazioni sulla parte 2
1.6.3 CollaborationRole 1,*

Importato/Configurato manualmente: importato.

Configurazione di WebSphere Partner Gateway UI:

WebSphere Partner Gateway supporta più elementi del ruolo di collaborazione.

13.

Funzione
Elemento/Attributo

1.6 Informazioni sulla parte 2

```
.6.3.1 ProcessSpecification 1
- name 1
- version 1
- xlink:type 1
- xlink:href
1 - uuid ImpliedReference 0,*  (8.4.4.6)
- URI 0, 1
 Transforms 1
  Transform
1 - Algorithm Fixed
 DigestMethod 1
  DigestValue 1
```

Importato/Configurato manualmente: non importato.

Configurazione di WebSphere Partner Gateway UI:

Impossibile configurarlo.

14.

Funzione
Elemento/Attributo

1.6 Informazioni sulla parte 2

```
1.6.3.2 Role 1   (8.4.5)
- name 1
- xlink:type Fixed
- xlink:href 1
```

Importato/Configurato manualmente: l'attributo **xlink:href** viene importato, altri attributi non vengono importati.

Configurazione di WebSphere Partner Gateway UI:

Il valore può essere configurato in attributi di canale **Amministrazione account > Connessioni > Connessioni partner**. Ricercare i canali e accedere all'attributo canale - **Role**.

15.

Funzione
Elemento/Attributo

1.6 Informazioni sulla parte 2

1.6.3.3 ApplicationCertificateRef 0,1 (8.4.6)

Importato/Configurato manualmente: importato.

Configurazione di WebSphere Partner Gateway UI:

Non è possibile configurare il valore. Il certificato specificato per l'attributo **certId** viene caricato nel file system ma non in WebSphere Partner Gateway.

16.

Funzione
Elemento/Attributo

1.6 Informazioni sulla parte 2

1.6.3.4 ApplicationSecurityDetailsRef 0, 1 (8.4.7)
- securityId 1

Importato/Configurato manualmente: non importato.

Configurazione di WebSphere Partner Gateway UI:

Impossibile configurarlo.

17.

Funzione
Elemento/Attributo

1.6.3.5 ServiceBinding 1

1.6.3.5.1 Service 1 (8.4.9)
- type Implied

Importato/Configurato manualmente: importato.

Configurazione di WebSphere Partner Gateway UI:

- **Service** : è il nome della definizione del documento. Per visualizzare il valore, passare a **Amministrazione hub > Definizioni documento**. Il valore del servizio verrà visualizzato come Tipo di documento e Attività nel package ebMS e nel package di integrazione di backend.
- **Type**: viene utilizzato come attributo canale in **Amministrazione account > Connessioni > Connessioni partner**. Ricercare i canali e accedere all'attributo canale **Service Type**.

18.

Funzione
Elemento/Attributo

1.6.3.5 ServiceBinding 1

1.6.3.5.1 Service 1 (8.4.9)
- type Implied

Importato/Configurato manualmente: importato.

Configurazione di WebSphere Partner Gateway UI:

- **Service** : è il nome della definizione del documento. Per visualizzare il valore, passare a **Amministrazione hub > Definizioni documento**. Il valore del servizio verrà visualizzato come Tipo di documento e Attività nel package ebMS e nel package di integrazione di backend.
- **Type**: viene utilizzato come attributo canale in **Amministrazione account > Connessioni > Connessioni partner**. Ricercare i canali e accedere all'attributo canale **Service Type**.

19.

Funzione
Elemento/Attributo

1.6.3.5.2 CanSend 0, * (8.4.10)

```
ThisPartyActionBinding 1
- action 1
- packageId 1
- xlink:href  Implied -
xlink:type Fixed
BusinessTransactionCharacteristics 1
- isNonRepudiationRequired
  All implied
isNonRepudiationReceiptRequired
- isConfidential
- isAuthenticated
- isAuthorizationRequired
- isTamperProof
- isIntelligibleCheckRequired
- timeToAcknowledgeReceipt
- timeToAcknowledgeAcceptance
- timeToPerform
- retryCountChannelId 1,*
ActionContext 0, 1
- binaryCollaboration 1
- businessTransactionActivity 1
- requestOrResponseAction 1
CollaborationActivity 0, 1
- name 1
OtherPartyActionBinding 0, 1
CanReceive 0, 1
```

Importato/Configurato manualmente: importato.

Configurazione di WebSphere Partner Gateway UI:

- **CanSend** – Viene creato un canale da **Integrazione backend > ebMS > Nome servizio > Azione del partnerA** a **ebMS > Nome servizio > Azione del partnerB** (il partnerB contiene l'elemento **CanReceive** collegato all'elemento **OtherPartyActionBinding**).
- **Azione** – importato e creato come un elemento Azione nell'**Attività** contenuta nella definizione del documento.
- **packageId** – Gli attributi dell'ID package di riferimento vengono memorizzati come attributi canale.
- Xlink:href e xlink:type: non importati e non è possibile configurarli.
- **isNonRepudiationRequired, isNonRepudiationReceiptRequired, isIntelligibleCheckRequired, timeToAcknowledgeReceipt, timeToPerform**: questi attributi vengono configurati come attributi del canale.

- **isConfidential, isAuthenticated, isTamperProof, isAuthorizationRequired, timeToAcknowledgeAcceptance, retryCount** - Non vengono importati e non sono configurabili.
- **ChannelId** 1, * : viene accettato solo un valore per WebSphere Partner Gateway. Gli attributi di riferimento vengono impostati come attributi canale.
- **binaryCollaboration, businessTransactionActivity, requestOrResponseAction, CollaborationActivity** – Non vengono importati e non sono configurabili.
- **OtherPartyActionBinding** - Importato. Il riferimento viene utilizzato per creare il canale.
- **CanReceive** - Importato e considerato sincrono se esiste qualsiasi altro canale per la stessa connessione.

20.

Funzione
Elemento/Attributo

1.6.3.5.2 CanSend 0, * (8.4.10)

```
1.6.3.5.3 CanReceive 0, *  (8.4.11)
ThisPartyActionBinding 1
OtherPartyActionBinding 0, 1
CanSend 0, 1
```

Importato/Configurato manualmente: importato.

Configurazione di WebSphere Partner Gateway UI:

- **CanReceive** – Viene creato un canale da **ebMS > Nome servizio > Azione del partnerA** a **Integrazione backend > ebMS > Nome servizio > Azione del partnerB** (il partnerB contiene l'elemento **CanSend** collegato all'elemento **OtherPartyActionBinding**).
- **OtherPartyActionBinding** - Importato. Il riferimento viene utilizzato per creare il canale.
- **CanSend** - Importato e considerato sincrono se esiste qualsiasi altro canale per la stessa connessione.

21.

Funzione
Elemento/Attributo

1.6.3.5.2 CanSend 0, * (8.4.10)

```
1.6.4 Certificate 1, * (8.4.18)
- certId  KeyInfo
```

Importato/Configurato manualmente: importato.

Configurazione di WebSphere Partner Gateway UI:

I certificati vengono memorizzati nel file system e questo deve essere caricato manualmente in WebSphere Partner Gateway sotto **Amministrazione account > Profili > Certificati**.

22.

Funzione
Elemento/Attributo

1.6.3.5.2 CanSend 0, * (8.4.10)

```
1.6.5 SecurityDetails 0, *   (8.4.18)
- securityId 1 TrustedAnchor 0, *
AnchorCertificateRef 1, *
SecurityPolicy 0, 1
```

Importato/Configurato manualmente: non importato. Solo i certificati di riferimento vengono caricati nel file system.

23.

Funzione

Elemento/Attributo

1.6.3.5.2 CanSend 0, * (8.4.10)

```
1.6.6 DeliveryChannel 1, * (8.4.22)
- channelId 1
- transportId 1
- docExchangeId1
MessagingCharacteristics 1
- syncReplyMode All implied
- ackRequested attribute
- ackSignatureRequested
- duplicateElimination
- actor
```

Importato/Configurato manualmente: importato.

Configurazione di WebSphere Partner Gateway UI:

- **channelId** : gli attributi di riferimento vengono impostati come attributi canale.
- **transportId**: gli attributi di riferimento vengono utilizzati per creare il gateway e vengono impostati come gateway predefinito per il canale.
- **docExchangeId**: gli attributi di riferimento vengono impostati come attributi canale.
- **syncReplyMode, ackRequested, ackSignatureRequested, duplicateElimination, actor**: tali attributi vengono importati e configurati come attributi canale.

24.

Funzione

Elemento/Attributo

1.6.3.5.2 CanSend 0, * (8.4.10)

```
1.6.7 Transport 1, * (8.4.24)
- transportId 1
TransportSender 0, 1 (8.4.25)
TransportProtocol 1
- version 1
ImpliedAccessAuthentication 0, *
TransportClientSecurity 0, 1
TransportSecurityProtocol 1
- version 1
ImpliedClientCertificateRef  0, 1
- certId 1
ServerSecurityDetailsRef 0, 1
- securityId 1
EncryptionAlgorithm 0, *
- minimumStrength All Implied
- oid
- w3c
- enumeratedType
```

Importato/Configurato manualmente: non importato.

25.

Funzione

Elemento/Attributo

1.6.3.5.2 CanSend 0, * (8.4.10)

```
1.6.7 Transport 1, * (8.4.24)
TransportReceiver 0, 1 (8.4.33)
TransportProtocol 1
- version 1
ImpliedEndpoint 1, *
- uri 1
- type  ImpliedAccessAuthentication 0, *
TransportServerSecurity 0, 1
TransportSecurityProtocol 1
- version 1
ServerCertificateRef 1
- certId 1
ClientSecurityDetailsRef 0, 1
- SecurityId 1
EncryptionAlgorithm 0, *
- minimumStrength All Implied
- oid
- w3c
- enumeratedType
```

Importato/Configurato manualmente: importato.

Configurazione di WebSphere Partner Gateway UI:

- **Transport Protocol**: definisce il protocollo del gateway.
- **Version** : definisce la versione del protocollo del gateway.
- **URL**: definisce l'URL del gateway. Questi valori possono essere visualizzati in **Amministrazione account > Profili > Ricerca del partner**. Per tutti i partner e per il partner selezionato, fare clic sulla scheda **Destinazione**. I valori rimanenti dell'attributo non vengono importati.

26.

Funzione

Elemento/Attributo

1.6.3.5.2 CanSend 0, * (8.4.10)

```
1.6.8 DocExchange (8.4.39)
- docExchangeId 1 1.6.8.2.1
ebXMLSenderBinding 0, 1 (8.4.40)
- version ReliableMessaging 0, 1
Retries 0, 1
RetryInterval 0, 1
MessageOrderSemantics 1
PersistDuration 0, 1
SenderNonRepudiation 0, 1
NonRepudiationProtocol 1
- version 1 Implied
HashFunction 1
SignatureAlgorithm 1
- oid All implied
- w3c
- enumeratedType
SigningCertificateRef 1
- certId 1
SenderDigitalEnvelope 0, 1
DigitalEnvelopeProtocol 1
- version 1  EncryptionAlgorithm 1
```

```
- minimumStrength All Implied
- oid
- w3c
- enumeratedType
```

Importato/Configurato manualmente: importato.

Configurazione di WebSphere Partner Gateway UI:

Retries, RetryInterval, MessageOrderSemantics, PersistDuration, HashFunction, SignatureAlgorithm, DigitalEnvelopeProtocol, EncryptionAlgorithm : questi valori vengono importati e memorizzati come attributi di canale, in **Amministrazione account > Connessioni > Connessioni partner**. Ricercare i canali e andare in **Attributi canale**. I valore rimanenti non vengono importati e non è possibile configurarli.

27.

Funzione
Elemento/Attributo

1.6.3.5.2 CanSend 0, * (8.4.10)

```
1.6.8.2 ebXMLReceiverBinding 0, 1 (8.4.53)
- version 1
ReliableMessaging 0, 1
Retries 0, 1
RetryInterval 0, 1
MessageOrderSemantics 1
ReceiverNonRepudiation 0, 1
NonRepudiationProtocol 1
- version 1
HashFunction 1
SigningAlgorithm 1
- oid All Implied
- w3c
- enumeratedType
SigningSecurityDetailsRef 1
- securityId 1
ReceiverDigitalEnvelope 0, 1
DigitalEnvelopeProtocol 1
- version 1
EncryptionAlgorithm 1
- minimumStrength All Implied
- oid
- w3c
- enumeratedType
EncryptionCertificateRef 1
- certId 1
NamespaceSupported 0, *
- location 1
- version Implied
```

Importato/Configurato manualmente: importato.

Configurazione di WebSphere Partner Gateway UI:

Retries, RetryInterval, MessageOrderSemantics, PersistDuration, HashFunction, SignatureAlgorithm, DigitalEnvelopeProtocol, EncryptionAlgorithm : questi valori vengono importati e memorizzati come attributi di canale, in **Amministrazione account > Connessioni > Connessioni partner**. Ricercare i canali e andare in **Attributi canale**. I valore rimanenti non vengono importati e non è possibile configurarli.

28.

Funzione
Elemento/Attributo

1.6.3.5.2 CanSend 0, * (8.4.10)

```
1.6.9  OverrideMshActionBinding 0, *  (8.4.58)
- action 1
- channelId
```

Importato/Configurato manualmente: importato.

Configurazione di WebSphere Partner Gateway UI:

Per l'azione specificata, gli attributi canale vengono impostasti mediante l'utilizzo dell'ID canale di riferimento.

29.

Funzione
Elemento/Attributo

1.6.3.5.2 CanSend 0, * (8.4.10)

```
1.7 SimplePart (8.5)
- id 1
- mimetype 1
- mimparameters  Implied
- xlink:role
 ImpliedNamespaceSupported 0, *
```

Importato/Configurato manualmente: importato.

Configurazione di WebSphere Partner Gateway UI:

Mimetype: i valori vengono importati e memorizzati come attributi canale. I valori restanti non vengono importati e non è possibile configurarli.

30.

Funzione
Elemento/Attributo

1.6.3.5.2 CanSend 0, * (8.4.10)

```
1.8 Packaging (8.6)
- id 1
ProcessingCapabilities 1, *
- parse 1
- generate 1
CompositeList 0, *
Composite 0, *
- mimetype 1
- id 1
- mimeparameters ImpliedConstituent 1, *
- idref 1
- excludeFromSignature Implied
- minOccurs Implied
- maxOccurs Implied
SignatureTransform 0, 1
Transform 1, *
EncryptionTransform 0, 1
Transform 1, *
```

Importato/Configurato manualmente: importato.

Configurazione di WebSphere Partner Gateway UI:

Composite : mimetype, mimeparameters, Constituent-idref, Constituent-excludeFromSignature, signatureTransform, encryptionTransform, Algorithm: questi valori vengono importati e memorizzati come attributi di canale, in **Amministrazione account > Connessioni > Connessioni partner**. Ricercare i canali e andare in **Attributi canale**. I valori restanti non vengono importati e non è possibile configurarli.

31.

Funzione
Elemento/Attributo

1.6.3.5.2 CanSend 0, * (8.4.10)

```
Encapsulation 0, *
- mimetype 1
- id 1
- mimeparameters  ImpliedConstituent 1
- idref 1
- excludeFromSignature Implied
- minOccurs Implied
- maxOccurs Implied
SignatureTransform 0, 1
Transform 1, *
EncryptionTransform 0, 1
Transform 1, *
```

Importato/Configurato manualmente: importato.

Configurazione di WebSphere Partner Gateway UI:

Encapsulation : mimetype, mimeparameters, Constituent-idref, Constituent-excludeFromSignature, signatureTransform, encryptionTransform, Algorithm: questi valori vengono importati e memorizzati come attributi di canale, in **Amministrazione account > Connessioni > Connessioni partner**. Ricercare i canali e andare in **Attributi canale**. I valori restanti non vengono importati e non è possibile configurarli.

32.

Funzione
Elemento/Attributo

1.6.3.5.2 CanSend 0, * (8.4.10)

```
1.9 Signature 0, 1 (8.7)
ds:Signature 1,3
SignedInfo 1
CanonicalizationMethod 0, 1
SignatureMethod 1
- AlgorithmReference 1, *
- URI FixedTransforms 1
Transform 1
- Algorithm Fixed
```

Importato/Configurato manualmente: non importato.

Configurazione di WebSphere Partner Gateway UI:

Impossibile configurarlo.

33.

Funzione
Elemento/Attributo

1.6.3.5.2 CanSend 0, * (8.4.10)

1.10 Comments 0, * (8.8)
- xml:lang

Importato/Configurato manualmente: non importato.

Configurazione di WebSphere Partner Gateway UI:

Impossibile configurarlo.

Attributi di connessione

La seguente tabella fornisce gli attributi oggetto di instradamento, che possono essere visualizzati nei canali business del messaggio sul package ebMS.

Fare clic su **Amministrazione account > Connessioni > Connessioni partner** e selezionare Origine e Destinazione. Se il canale è per il messaggio ebMS in entrata, fare clic su **Attributi** del lato origine, altrimenti se il canale è per il messaggio ebMS in uscita, fare clic su **Attributi** del lato destinazione. Scorrere sul pannello risultante e fare clic sulla cartella **Azione**.

Tabella 19. Attributi di connessione

Attributi XML di CPA	Valore predefinito	Valori possibili	Testo di visualizzazione in WebSphere Partner Gateway
isNonRepudiationRequired	False	True/false - associati a Sì/No	non-rifiuto richiesto
isNonRepudiationReceiptRequired	False	True/false - associati a Sì/No	Non-rifiuto di ricevuta
timeToAcknowledgeReceipt			Ora per riconoscere
Tentativi	3	Un numero	conteggio tentativi
MessageOrderSemantics	Non garantito	″Garantito″ ″Non garantito″	semantica ordine del messaggio
PersistDuration	P1D		continua durata
syncReplyMode	Nessuno	″mshSignalsOnly″ ″signalsOnly″ ″responseOnly″ ″signalsAndResponse″ ″none″ (Spostato alla fase 2)	modalità di risposta sincronizzata

Tabella 19. Attributi di connessione (Continua)

Attributi XML di CPA	Valore predefinito	Valori possibili	Testo di visualizzazione in WebSphere Partner Gateway
ackRequested	Per messaggio	″always″ - indica che il riconoscimento deve essere sempre richiesto. ″never″ - indica che il riconoscimento non essere mai richiesto. “perMessage” - implica che il riconoscimento può o non può essere richiesto, in base all’elemento di riconoscimento presente nel documento ebXML.	riconoscimento obbligatorio
ackSignatureRequested	Per messaggio	″always″ ″never″ ″perMessage″	firma di riconoscimento obbligatoria
duplicateElimination	Per messaggio	″always″ ″never″ ″perMessage″	Eliminazione duplicata
attore	″urn:oasis:names:tc:ebxml-msg:actor:nextMSH″	″urn:oasis:names:tc:ebxml-msg:actor:nextMSH″″urn:oasis:names:tc:ebxml-msg:actor:toPartyMSH″	attore
PartyRole	-	Ruolo in CPA	ruolo
intervallo tentativi	270	-	intervallo tentativi
NonRepudiationProtocol	-	http://www.w3.org/2000/09/xmldsig#	Protocollo basato sulla firma
SignatureAlgorithm	-	1. http://www.w3.org.2000/09/xmldsig#dsa-sha1 2. http://www.w3.org/2000/09/xmldsig#hmac-sha1 3. http://www.w3.org/2000/09/xmldsig#rsa-sha1	algoritmo firma
isEncryptionRequired	No	True/false - associati a Sì/No	EncryptionRequired
isCompressionRequired	No	True/false - associati a Sì/No	compressione obbligatoria
/Packaging/CompositeList /Encapsulation/Constituent: mimetype	-		Compress Mimeype
/tp:SenderDigitalEnvelope /tp:DigitalEnvelopeProtocol	-	SMIME XMLEncryption	EncryptionProtocol

Tabella 19. Attributi di connessione (Continua)

Attributi XML di CPA	Valore predefinito	Valori possibili	Testo di visualizzazione in WebSphere Partner Gateway
/tp:SenderDigitalEnvelope /EncryptionAlgorithm	-	3des-cbc, aes128-cbc, aes-256-cbc	algoritmo codifica
/tp:ReceiverDigitalEnvelope /tp:DigitalEnvelopeProtocol	-	SMIME XMLEncryption	EncryptionProtocol
/tp:ReceiverDigitalEnvelope /EncryptionAlgorithm	-	3des-cbc, aes128-cbc, aes-256-cbc	algoritmo codifica
/Packaging/CompositeList /Encapsulation tp:MimeType	-	text/xml application/pkcs7-mime	tipo Mime di codifica
/Packaging/CompositeList /Encapsulation- tp:mimeparameters	-		Parametro Mime di codifica
/Packaging/CompositeList /Encapsulation/Constituent: mimetype	-		Costituente codifica
/Packaging/CompositeList / Composite/ tp:mimeparameters	-		Parametro Mime del package
/Packaging/CompositeList / Composite /Constituent: mimetype	-		PackagingConstituent
/Packaging/CompositeList /Composite/Contituent /excludeFromSignature: mimetype	-		Escludi da firma
/Packaging/CompositeList / Composite/Contituent/ SignatureTransform	-	1. BASE64 2. ENVELOPED 3. XPATH 4. XPATH2 5. XSLT	Algoritmo di conversione firma
/Packaging/CompositeList /Composite/Contituent/ EncryptionTransform	-	1. BASE64 2. ENVELOPED 3. XPATH 4. XPATH2 5. XSLT	Algoritmo di conversione codifica

Limitazioni

Le seguenti sono le limitazioni dell'associazione di CPA a WebSphere Partner Gateway:

1. I certificati provenienti da CPA non vengono importati in WebSphere Partner Gateway. Vengono memorizzati nel file system e l'amministratore deve verificare manualmente tali certificati e caricarli su WebSphere Partner Gateway.
2. WebSphere Partner Gateway può indirizzare i flussi sincroni e asincroni da CPA, ma non più collegamenti aventi lo stesso valore azione.
3. Sono supportati solo ID DUNS a 9 caratteri numerici (non è supportato il modulo libero).

Mappatura delle intestazioni SOAP ebMS alle intestazioni di WebSphere Partner Gateway

La specifica ebMS 2.0 definisce un gruppo di intestazioni obbligatorie, che deve essere presente nel messaggio SOAP ebMS. La seguente tabella fornisce la mappatura tra alcune di queste intestazioni obbligatorie ebMS e le intestazioni di WebSphere Partner Gateway da cui sono utilizzati i valori.

Tabella 20. Intestazioni SOAP ebMS e le intestazioni corrispondenti di WebSphere Partner Gateway

Num. ser.	Nome intestazione nel messaggio SOAP ebMS	Nome intestazione corrispondente in WebSphere Partner Gateway
1	Da PartyId	"x-aux-sender-id" impostato dal sistema di backend
2	Dal ruolo	Attributo Ruolo sull'Origine degli attributi Definizione documento
3	Dal Tipo PartyId	L'utente non può configurarlo. Se PartyId è DUNS, il valore "type" sarà "urn:duns." Altrimenti, sarà "string."
4	A PartyId	"x-aux-receiver-id" impostato dal sistema di backend
5	Al ruolo	Attributo Ruolo sulla Destinazione degli attributi Definizione documento.
6	Al Tipo PartyId	L'utente non può configurarlo. Se PartyId è duns, il valore "type" sarà "urn:duns" o "string"
7	CPAId	Se CPA è presente nel database, WebSphere Partner Gateway utilizza l'ID CPA presente nel CPA. Altrimenti, l'utente può configurare l'attributo ID CPA presente sulla Destinazione degli Attributi Definizione documento. Se l'utente non ha configurato questo attributo e un CPA non è presente, WebSphere Partner Gateway crea un ID CPA in base agli ID del partner.
8	ID conversazione	"x-aux-process-instance-id" impostato dal sistema di backend. Se il sistema di backend non lo imposta, WebSphere Partner Gateway crea il proprio ID conversazione.
9	Servizio	Il valore Definizione documento sulla connessione Partner di destinazione. **Nota:** la Definizione documento e l'Attività coincidono nel flusso ebMS.
10	tipo di servizio	L'attributo Tipo di servizio sulla Destinazione degli attributi Definizione documento
11	Azione	Il valore Azione sulla connessione Partner di destinazione
12	IDMessaggio	"x-aux-msg-id" impostato dal sistema di backend. Se il sistema di backend non lo imposta, WebSphere Partner Gateway crea un proprio ID Messaggio.

Se una risposta sincrona ebMS viene inviata ad un documento di richiesta ebMS, il sistema di backend deve impostare l'intestazione "x-aux-request-msg-id" sul documento di risposta. Il valore di questa intestazione sarà l' ID messaggio del messaggio di richiesta. Inoltre, il documento di risposta deve trovarsi nella stessa conversazione del documento di richiesta. Ciò significa che "x-aux-process-instance-id" per la risposta deve coincidere con l'ID conversazione della richiesta.

l'ID conversazione e l'IDMessaggio del documento di richiesta sono state inviati al backend rispettivamente come "x-aux-process-instance-id" e "x-aux-msg-id".

Visualizzazione dei documenti ebMS

Informazioni su questa attività

Il Visualizzatore ebMS riporta le informazioni sui documenti ebMS. È possibile visualizzare i documenti non elaborati, gli eventi ed i dettagli di elaborazione dei documenti associati mediante determinati criteri di ricerca. Queste informazioni sono utili nel caso in cui si tenti di stabilire se un documento sia stato consegnato correttamente o determinare la causa di un problema.

Per avviare il Visualizzatore ebMS, procedere nel modo seguente:

1. Fare clic su **Visualizzatori > Visualizzatore ebMS**.
2. Selezionare i criteri di ricerca appropriati.
3. Fare clic su **Cerca**.

Nel Visualizzatore ebMS, i documenti sono organizzati in base all'ID conversazione. Ciò significa che tutti i documenti con lo stesso ID conversazione saranno raggruppati e possono essere visualizzati selezionando l'icona Ulteriori dettagli, posta a sinistra di ciascuna riga dell'ID conversazione. Quando si seleziona l'icona Ulteriori dettagli, viene visualizzata una nuova pagina in cui sono riportati tutti i messaggi di tale conversazione. Nella parte superiore della pagina, è presente un attributo definito ″Stato conversazione.″ Il valore di questo attributo è il successivo messaggio previsto in tale conversazione.

Richiesta dello stato di un messaggio ebMS

Informazioni su questa attività

Per richiedere lo stato di un messaggio ebMS, procedere nel modo seguente:

1. Una volta rilevato il documento ebMS di interesse, fare clic sull'icona **Visualizza dettagli**, posta accanto ad esso.
2. Fare clic su Richiedi stato. Quindi, viene visualizzato lo stato di tale documento.

Per aggiornare lo stato, fare clic su **Visualizza stato**.

Quando si esegue la configurazione per i documenti di richiesta stato e di risposta stato di ebMS, tenere conto dei seguenti fattori:

- È necessario creare solo la connessione di richiesta stato. La connessione di risposta stato utilizzerà la connessione di richiesta stato esistente.
- Per una connessione di richiesta stato dal partner interno ad un partner esterno, non viene utilizzata la destinazione di origine della connessione.
- Per una connessione di richiesta stato da un partner esterno ad un partner interno, la destinazione di origine della connessione viene utilizzata per inviare il documento di riposta stato di risposta al partner esterno.
- Se non dispone di un CPA, un utente deve abilitare le capacità B2B e creare un canale per il messaggio di richiesta stato di ebMS nel seguente modo:
  - Per il messaggio di richiesta dello stato di ebMS in entrata,

    La capacità B2B dell'origine deve essere:

    Package: N/A (N/A)
    Protocollo: ebMS(2.0)

Tipo documento: MSHService (2.0)
Attività: MSHService (2.0)
Azione: StatusRequest(N/A)

La capacità B2B della destinazione deve essere

Package: ebMS (2.0)
Protocollo: ebMS(2.0)
Tipo documento: MSHService (2.0)
Attività: MSHService (2.0)
Azione: StatusRequest(N/A)

– Per il messaggio di richiesta dello stato di ebMS in uscita

La capacità B2B dell'origine deve essere:

Package: ebMS (2.0)
Protocollo: ebMS(2.0)
Tipo documento: MSHService (2.0)
Attività: MSHService (2.0)
Azione: StatusRequest(N/A)

La capacità B2B della destinazione deve essere

Package: N/A (N/A)
Protocollo: ebMS(2.0)
Tipo documento: MSHService (2.0)
Attività: MSHService (2.0)
Azione: StatusRequest(N/A)

L'utente deve quindi attivare il canale ed impostare le destinazioni dalla pagina di connessione del partner.

Nota: queste informazioni sono valide per notifica ed errore ebMS. L'azione per questi canali cambierà in MessageError e Acknowledgment, rispettivamente.

Esecuzione del ping dei partner ebMS

Informazioni su questa attività

Dalla pagina Verifica connessione partner, è possibile eseguire il ping di partner ebMS. Ciò significa che è possibile inviare un messaggio di ping ad un partner, e, nel caso in cui un partner sia attivo ed è pronto per la ricezione, il partner risponde con un messaggio pong. Una volta caricato un CPA, viene creato il canale ping-pong.

Per fare in modo che il ping funzioni, le connessioni devono essere definite con il partner interessato. Per dettagli, consultare la sezione per eseguire il ping dei partner ebMS nella *Guida alla configurazione dell'hub di WebSphere Partner Gateway*.

Per eseguire il ping di un partner ebMS, procedere nel modo seguente:

1. Fare clic su **Strumenti** > **Verifica connessione partner**.
2. Per il **Comando**, selezionare **PING ebMS**.
3. Selezionare **Dal partner** e **Al partner**.
4. In alternativa, selezionare una **Destinazione** o inserire un **URL**.
5. Fare clic su **Verifica** per inviare un messaggio ping.

Per determinare lo stato del messaggio ping, fare clic su **Stato ping**. Lo stato per l'ultima richiesta ping viene quindi visualizzato sotto Risultati.

Nota: l'ultima richiesta ping può essere stata avviata dalla Verifica connessione partner o da un reinvio di Visualizzatore documenti di un documento Ping esistente.

Servizi Web

Un partner può richiamare un servizio Web ospitato dal partner interno. In modo analogo, il partner interno può richiamare un servizio Web ospitato da un partner. Il partner o il partner interno richiama il servizio Web tramite il server WebSphere Partner Gateway. WebSphere Partner Gateway funziona come un proxy, passando la richiesta del servizio Web al provider del servizio Web e restituendo la risposta in maniera sincrona dal provider al richiedente.

In questa sezione sono contenute le seguenti informazioni per impostare un servizio Web che sarà utilizzato da un partner o un partner interno:

- Identificazione dei partner per un servizio Web
- Impostazione di una definizione del documento per un servizio Web
- Aggiunta delle definizioni del documento alle capacità B2B del partner
- Restrizioni e limitazioni del supporto del servizio Web

Identificazione dei partner per un servizio Web

Quando Il servizio Web viene fornito dal partner interno per essere utilizzato dai partner; WebSphere Partner Gateway richiede l'identificazione dei partner interni ed esterni. WebSphere Partner Gateway release 6.1.1 e successive consente di creare più partner interno al di fuori di quello impostato come partner interno predefinito. Per sovrascrivere il partner interno predefinito e selezionare un partner interno, inviare gli altri parametri al destinatario WebSphere Partner Gateway, ad esempio **FromPartnerBusinessId** o **ToPartnerBusinessId** in base al flusso in uscita o in entrata rispettivamente. La condizione di errore è che se due diversi ID partner esterni sono forniti tramite l'autenticazione di base e l'URL, allora l'autenticazione di base ha la precedenza. Le diverse stringhe di query possibili per il flusso di uscita sono: `<Receiver-URL>?to=<business id>` e `<Receiver-URL?to=<business id>&from=<business id>`. Le diverse stringhe di query possibili per il flusso in entrata sono:`<Receiver-URL` e `Receiver-URL?to=business id`. Se in entrata, l'**autenticazione di base** è obbligatoria.

Creazione delle definizioni del documento

Per impostare la definizione del documento, si caricano i file WSDL (Web Service Definition Language) che definiscono il servizio Web, oppure si immettono le definizioni del documento manualmente mediante la Console comunità.

Caricamento dei file WSDL per un servizio Web

Informazioni su questa attività

La definizione per un servizio Web deve essere contenuta in un file WSDL primario, con estensione `.wsdl`, che potrebbe importare i file WSDL aggiuntivi mediante l'elemento di `importazione`. Se ci sono file importati, questi possono essere caricati con il file primario mediante uno dei seguenti metodi:

- Se il percorso del file o (HTTP) URL nell'attributo `posizione` di ciascun elemento di `importazione` è ricercabile dal server della Console comunità (non dalla macchina utente), il file principale può essere caricato direttamente e i file importati vengono caricati automaticamente.

- Se tutti i file importati e il file primario vengono compressi in un file zip, ognuno con un percorso zip corrispondente al percorso (se presente) nell'attributo della `posizione` di importazione, caricando il file compresso si caricano tutti i file primari contenuti e i file WSDL importati.

Ad esempio, si supponga che il file principale WSDL `helloworldRPC.wsdl` contenga il seguente elemento di importazione:

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

E si supponga che il file WSDL importato `bindingRPC.wsdl` contenga il seguente elemento di importazione:

Il file deve contenere quanto segue:

```
Name                    Path

helloworldRPC.wsdl

bindingRPC.wsdl

porttypeRPC.wsdl                port\
```

Quando una definizione del file WSDL di un servizio Web viene caricata, il WSDL originale viene salvato come Mappa di convalida. (I messaggi del servizio Web non vengono effettivamente convalidati per WSDL da WebSphere Partner Gateway). Questo viene chiamato WSDL *privato*.

Inoltre, un WSDL viene salvato con l'URL privato sostituito dall'URL di destinazione specificato nella pagina Carica/scarica package. Il WSDL pubblico viene fornito agli utenti del servizio Web che invocano il servizio Web sull'URL di destinazione (URL pubblico). Quindi WebSphere Partner Gateway instrada la richiesta del servizio Web ad una destinazione che indica l'indirizzo URL privato del provider del servizio Web. WebSphere Partner Gateway funziona come un proxy, inoltrando la richiesta a un URL del provider privato che è nascosto dall'utente del servizio Web.

Sia il WSDL pubblico che quello privato (compresi i file importati) possono essere scaricati dalla Console comunità dopo che il WSDL è stato caricato.

Caricamento dei file mediante la Console comunità: WebSphere Partner Gateway fornisce un modo per importare i file WSDL. Se un servizio Web viene definito in un file WSDL singolo, è possibile caricare il file WSDL direttamente. Se il servizio Web viene definito mediante più file WSDL (questo succede quando sono stati importati i file WSDL, in un file WSDL primario), vengono caricati in un archivio compresso.

Importante: Il file WSDL nell'archivio compresso devono essere in una directory specificata nell'elemento di importazione WSDL. Ad esempio, si supponga di disporre del seguente elemento di impostazione:

```
<import namespace="http://www.helloworld.com/wsdl/helloRPC.wsdl"
location="path1/bindingRPC.wsdl"/>
```

La struttura di directory all'interno dell'archivio compresso è: `path1/bindingRPC.wsdl`.

Ora, si consideri questo esempio:

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

Il file `bindingRPC.wsdl` si trova a livello root all'interno dell'archivio compresso.

Per caricare un singolo file WSDL o un archivio compresso, utilizzare la seguente procedura.

1. Fare clic su **Amministrazione hub** > **Configurazione hub** > **Definizione documento**.
2. Selezionare **Carica/Scarica package**.
3. Per **Package WSDL** fare clic su **Sì**.
4. Per **URL pubblico del servizio Web**, eseguire uno di seguenti passaggi:
   - Per un servizio Web fornito dal partner interno (che verrà richiamato da un partner), immettere l'URL pubblico del servizio Web. Ad esempio:

     `https://<target_host:port>/bcgreceiver/Receiver`

     L'URL è generalmente lo stesso della definizione HTTP di produzione definito in Destinazioni.
   - Per un servizio Web fornito da un partner (che sarà richiamato dal partner interno), inserire l'URL pubblico del partner con una stringa di query. Ad esempio:

     `https://<host_destinazione:porta>/bcgreceiver/Receiver?to=<ID_business_partner>`
5. Fare clic su **Sfoglia** e selezionare il file WSDL o l'archivio compresso.
6. Per **Salva nel database**, selezionare **No** se si desidera caricare il file in modalità di test. Quando si seleziona **No**, il file non viene installato nel sistema. Utilizzare i messaggi generati dal sistema visualizzati nella casella Messaggi per risolvere gli errori di aggiornamento. Selezionare **Sì** per caricare il file nel database del sistema.
7. Per **Sovrascrivi dati**, selezionare **Sì** per sostituire un file attualmente nel database. Selezionare **No** per aggiungere il file al database.
8. Fare clic su **Carica**. Il file WSDL viene installato nel sistema.

Convalida dei package utilizzando i file dello schema: Un insieme di schemi XML che descrivono i file XML che possono essere caricati mediante la console viene fornito su supporto di installazione di WebSphere Partner Gateway. I file caricati vengono convalidati rispetto agli schemi. I file dello schema sono un utile riferimento per la determinazione della causa di un errore quando un file non può essere caricato a causa di un XML non conforme. I file sono: `wsdl.xsd`, `wsdlhttp.xsd`, `ewsdlsoap.xsd`, che contengono lo schema che descrive il file di WSDL (Web Service Definition Language).

I file vengono posizionati in: `B2BIntegrate\packagingSchemas`

Creazione manuale della definizione del documento

Per inserire manualmente le equivalenti definizioni del documento, seguire le procedure di questa sezione. Inoltre, è necessario creare le voci Tipo di documento, Attività e Azione singolarmente in **Protocollo: servizio Web**, prestando particolarmente attenzione ai requisiti per l'Azione e la relativa relazione nei messaggi SOAP ricevuti.

Nei termini della gerarchia di Package/Protocollo/Tipo di documento/Attività/Azione delle definizioni documento, un servizio Web supportato è indicato come:

- **Package: Nessuno**
- **Protocollo: Servizio Web (1.0)**
- **Tipo di documento:** {*<Web_service_namespace>*:*<Web_service_name>*} (nome e codice), richiesto come univoco tra i tipi di documenti per il protocollo Servizio Web. In genere, è il nome e lo spazio dei nomi WSDL.
- **Attività:** un'attività per ciascuna operazione del servizio Web, con nome e codice:

  {*<operation_namespace>*}:*<operation_name>*
- **Azione**: un'azione per il messaggio di input per ciascuna operazione, con nome e codice:

  {*<namespace_of_identifying_xml_element = namespace_of_first_child_of_soap:body>*}:
  <name_of _identifying_xml_element = name_of_first_child_of_soap:body>

Le definizioni critiche sono Azioni perché WebSphere Partner Gateway utilizza lo spazio dei nomi e il nome per riconoscere un messaggio SOAP di richiesta del servizio Web in entrata ed instradarlo in maniera appropriata in base alla connessione del partner definita. Lo spazio dei nomi ed il nome del primo elemento XML child dell'elemento `soap:body` del messaggio SOAP devono corrispondere ad uno spazio dei nomi ed ad un nome di Azione definito nelle definizioni del documento di WebSphere Partner Gateway.

Ad esempio, se un messaggio SOAP di richiesta del servizio Web per un bind SOAP letterale del documento è:

```
<?xml versione="1.0" codifica="UTF-8"?>

<soapenv:Envelope xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/"
xmlns:xsd=
"http://www.w3.org/2001/XMLSchema" xmlns:xsi="http://www.w3.org/
2001/XMLSchema-instance">
 <soapenv:Body>
  <nameAndAddressElt xmlns="http://www.helloworld.com/xsd/helloDocLitSchema">
   <titleElt xmlns="">Mr</titleElt>
   <nameElt xmlns="">Joe Smith</nameElt>
   <addressElt xmlns="">
    <numberElt>123</numberElt>
    <streetElt>Elm St</streetElt>
    <cityElt>Peoria</cityElt>
   </addressElt>
  </nameAndAddressElt>
 </soapenv:Body>
</soapenv:Envelope>
```

WebSphere Partner Gateway cerca un'Azione del servizio Web definita con questo codice:

```
{http://www.helloworld.com/xsd/helloDocLitSchema}:nameAndAddressElt
```

Per un messaggio di richiesta SOAP di stile binding RPC, ad esempio:

```
<?xml versione="1.0" codifica="UTF-8"?>

<soapenv:Envelope xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/"
xmlns:xsd=
"http://www.w3.org/2001/XMLSchema" xmlns:xsi="http://www.w3.org/
2001/XMLSchema-instance">
 <soapenv:Body>
  <ns1:helloWorldRPC soapenv:encodingStyle="http://schemas.xmlsoap.org/soap/
encoding/ xmlns:ns1="http://www.helloworld.com/helloRPC">
```

```
   <name xsi:type="xsd:string">Joe Smith</name>
  </ns1:helloWorldRPC>
 </soapenv:Body>
</soapenv:Envelope>
```

WebSphere Partner Gateway ricerca un'azione del servizio Web definita con questo codice:

```
{http://www.helloworld.com/helloRPC}:helloWorldRPC
```

Per un binding RPC, lo spazio dei nomi e il nome del primo elemento child di `soap:body` di un messaggio di richiesta SOAP deve disporre di uno spazio dei nomi e di un nome dell'operazione del servizio Web applicabile.

Per un binding letterale del documento, lo spazio dei nomi e il nome del primo elemento child di `soap:body` di un messaggio di richiesta SOAP deve essere lo spazio dei nomi e il nome dell'attributo dell'elemento `XML` nell'elemento `parte` della `definizione del messaggio di input` per il servizio Web.

Creazione delle interazioni

Informazioni su questa attività

Per creare un'interazione per un servizio Web, utilizzare la stessa azione del tipo di documento del servizio Web per l'Origine e la Destinazione.

Per creare le interazioni, utilizzare la seguente procedura.

1. Fare clic su **Amministrazione hub** > **Configurazione hub** > **Definizione documento**.
2. Fare clic su **Crea interazione**.
3. In **Origine**, espandere **Package: Nessuno > Protocollo: Servizio Web > Tipo di documento: <** *document type*> **> Azione:** *<action>*.
4. Ripetere il precedente passaggio nella colonna **Destinazione**.
5. Selezionare **Pass Through** dall'elenco **Azione** in basso nella pagina. (**Pass Through** è l'unica opzione valida supportata in WebSphere Partner Gateway per un servizio Web).

Restrizioni e limitazioni del supporto del servizio Web

WebSphere Partner Gateway supporta i seguenti standard:

- WSDL 1.1
- SOAP 1.1
- WS-I Basic Profile v. 1.0 (che contiene restrizioni importanti sulla forma dei messaggi SOAP per il binding letterale del documento)

Nota:

- WebSphere Partner Gateway supporta parzialmente Basic Profile 1.0.
- I binding SOAP/HTTP sono supportati.
- Il rebinding non è supportato.
- Gli stili RPC codificato/RPC letterale e binding letterale del documento sono supportati (soggetti alle restrizioni in WS-I Basic Profile).

Consultare "Convalida busta Soap" a pagina 96 e "Deenveloping SOAP" a pagina 97.

documenti cXML

Il Gestore documenti di WebSphere Partner Gateway identifica un documento cXML grazie al nome dell'elemento root del documento XML, che è `cXML`, e la versione identificata da cXML DOCTYPE (DTD). Ad esempio, il seguente DOCTYPE è per cXML Versione 1.2.009:

```
<!DOCTYPE cXML SYSTEM "http://xml.cXML.org/schemas/cXML/1.2.009/cXML.dtd">
```

Gestore documenti effettua la convalida DTD sui documenti cXML; tuttavia, WebSphere Partner Gateway non fornisce DTD cXML. È possibile scaricarli da www.cxml.org, quindi caricarli in WebSphere Partner Gateway mediante il modulo Mappa di convalida nella Console comunità. Una volta caricato DTD, associarlo al tipo di documento cXML. Per ulteriori informazioni sull'associazione di DTD con il tipo di documento cXML, consultare la sezione "Associazione delle mappe alle definizioni di documento" a pagina 161.

Il Gestore documenti utilizza due attributi dell'elemento root cXML per la gestione del documento: l'ID payload e data e ora. Il cXML payloadID e data e ora vengono utilizzati come il numero ID del documento e la data e ora del documento. Entrambi sono visualizzabili nella Console comunità per la gestione del documento.

Gli elementi Da e A nell'intestazione cXML contengono l'elemento delle Credenziali che viene utilizzato per l'instradamento del documento e l'autenticazione. Il seguente esempio in basso vengono mostrati gli elementi Da e A come origine e destinazione del documento cXML.

Nota: in tutto il manuale, i numeri DUNS sono solo esempi.

```
<intestazione>
<Da>

            <Credential domain="AcmeUserId">
                <Identity>admin@acme.com</Identity>
            </Credential>
            <Credential domain="DUNS">
                <Identity>130313038</Identity>
            </Credential>
</Da
<A>
            <Credential domain="DUNS">
                <Identity>987654321</Identity>
            </Credential>
            <Credential domain="IBMUserId">
                <Identity>test@ibm.com</Identity>
            </Credential>
</A>
```

Se più di un elemento della credenziale viene utilizzato, il Gestore documenti utilizza il numero DUNS come identificativo di business per l'instradamento e l'autenticazione. Nel caso in cui non ci sia alcun numero fornito DUNS, viene utilizzata la prima Credenziale.

WebSphere Partner Gateway non utilizza le informazioni nell'elemento Mittente.

In una transazione sincrona, l'intestazione Da e A non viene utilizzata in un documento di risposta cXML. L'elemento di risposta viene inviato mediante la stessa connessione HTTP che viene stabilita dal documento di richiesta.

Tipi di documenti cXML

Un documento cXML può essere uno dei tre tipi: Richiesta, Risposta o Messaggio.

Richiesta

Ci sono molti tipi di richieste cXML. L'elemento `Richiesta` all'interno del documento cXML corrisponde al Tipo di documento di WebSphere Partner Gateway. Gli elementi tipici della richiesta sono:

- OrderRequest
- ProfileRequest
- PunchOutSetupRequest
- StatusUpdateRequest
- GetPendingRequest
- ConfirmationRequest
- ShipNoticeRequest

La seguente tabella riporta le relazioni tra gli elementi di un documento di richiesta cXML e le definizioni del documento all'interno di WebSphere Partner Gateway:

Elemento cXML
definizione del documento

cXML DOCTYPE
Protocollo

Versione DTD
Versione del protocollo

Richiesta (tipo) Ad esempio, OrderRequest
Tipo di documento

Risposta

Il partner di destinazione invia una risposta cXML per informare il partner di origine dei risultati della richiesta cXML. Poiché i risultati di alcune richieste potrebbero non disporre di dati, l'elemento `Risposta` può facoltativamente contenere un solo elemento `Stato`. Un elemento `Risposta` può contenere anche i dati a livello di applicazione. Durante un PunchOut, ad esempio, i dati a livello dell'applicazione sono contenuti in un elemento `PunchOutSetupResponse`. Gli elementi `Risposta` tipici sono:

- ProfileResponse
- PunchOutSetupResponse
- GetPendingResponse

La seguente tabella riporta le relazioni tra gli elementi di un documento di risposta cXML e le definizioni del documento all'interno di WebSphere Partner Gateway:

Elemento cXML
definizione del documento

cXML DOCTYPE
Protocollo

Versione DTD
Versione del protocollo

Risposta (tipo) Ad esempio, ProfileResponse
tipo di documento

Messaggio

Una messaggio cXML contiene le informazioni sul tipo di documento di WebSphere Partner Gateway nell'elemento `Message` cXML. Può contenere un elemento `Status` facoltativo identico a quello trovato nell'elemento `Response`. Può essere utilizzato nei messaggi che sono risposte ai messaggi di richiesta.

Il contenuto del messaggio è personale e definito dalle esigenze di business dell'utente. L'elemento direttamente al di sotto dell'elemento `<Message>` corrisponde al tipo di documenti creato in WebSphere Partner Gateway. Nel seguente esempio, SubscriptionChangeMessage è il tipo di documento:

```
<Message>
<SubscriptionChangeMessage type="new">
           <Subscription>
                <InternalID>1234</InternalID>
                <Name xml:lang="en-US">Q2 Prices</Name>
                <Changetime>1999-03-12T18:39:09-08:00</Changetime>
                <SupplierID domain="DUNS">942888711</SupplierID>
                <Format version="2.1">CIF</Format>
            </Subscription>
</SubscriptionChangeMessage>
</Message>
```

La seguente tabella mostra le relazioni tra gli elementi di un messaggio cXML e le definizioni del documento all'interno di WebSphere Partner Gateway:

Elemento cXML
definizione del documento

cXML DOCTYPE
Protocollo

Versione DTD
Versione del protocollo

Messaggio
Tipo di documento

Il modo più semplice per indicare la differenza tra un messaggio di sola andata e un documento Richiesta-Risposta è la presenza di un elemento `Message` invece di un elemento di richiesta o risposta.

Un messaggio può avere i seguenti attributi:

- `deploymentMode`, che indica se il messaggio se il messaggio è un documento di test o un documento di produzione. I valori consentiti sono produzione (predefinito) o verifica.
- `inReplyTo`, che specifica il messaggio cui questo risponde. Il contenuto dell'attributo `inReplyTo` è payloadID di un messaggio ricevuto precedentemente. Questo sarebbe utile per costruire una transazione in due modi con molti messaggi.

Intestazioni del tipo di contenuto e documenti allegati

Tutti i documenti cXML devono contenere Intestazione del tipo di contenuto. Per i documenti cXML senza allegati, vengono utilizzate le seguenti intestazioni del tipo di contenuto:

- Content-Type: text/xml
- Content-Type: application/xml

Il protocollo cXML supporta l'allegato dei file esterni mediante MIME. Ad esempio, gli acquirenti spesso devono chiarire gli ordini di acquisto con i memo, illustrazioni o fax di supporto. Una delle intestazioni del tipo di contenuto elencata in basso deve essere utilizzata nei documenti cXML che contengono gli allegati:

- Content-Type: multipart/related; boundary=<*something_unique*>
- Content-Type: multipart/mixed; boundary=<*something_unique*>

L'elemento `confine` è un testo unico che viene utilizzato per separare il corpo dalla parte payload del messaggio MIME. Per ulteriori informazioni, fare riferimento alla Guida utente cXML all'indirizzo www.cxml.org.

Interazioni cXML valide

WebSphere Partner Gateway supporta le seguenti interazioni della definizione del documento cXML:

- Dal partner esterno al partner interno: da None/cXML a None/cXML con Pass Through e convalida
- Dal partner interno al partner esterno:
  - Nessuno/cXML a Nessuno/cXML con Pass Through e convalida
  - Nessuno/XML a Nessuno/cXML con Pass Through, convalida e conversione

Creazione delle definizioni del documento

Informazioni su questa attività

Utilizzare il seguente processo per creare una nuova definizione del documento per un documento cXML.

Nota: è necessario verificare che la versione corretta di cXML sia stata definita prima di creare una definizione del documento cXML. Quella predefinita è la versione 1.2.009.

1. Fare clic su **Amministrazione hub** > **Configurazione hub** > **Definizione documento**.
2. Fare clic su **Crea definizione di documento**. La pagina Crea definizione di documento è stata visualizzata.
3. Selezionare **Tipo di documento** per il Tipo di documento.
4. Eseguire una delle attività riportate, in base al tipo di documento:
   - Per le richieste, inserire il tipo di richiesta (ad esempio, `OrderRequest`) nel campo **Nome**.
   - Per le risposte, se la Risposta non dispone di tag child diverse da `<Status>`, immettere `Response`. Altrimenti, immettere il nome della tag successiva rispetto a `<Status>`. Nel seguente esempio, immettere `Response` per il primo elemento Response e `Profile Response` per il secondo.

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

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

5. Inserire **1.0** per **Versione**.

   Il numero di versione è solo per riferimento. La versione di protocollo effettiva è derivata dalla versione DTD nel documento cXML.
6. Inserire una **Descrizione** facoltativa.
7. Selezionare **Sì** per **livello di documento**.
8. Selezionare **Abilitato** per **Stato**.
9. Selezionare **Sì** per tutti gli attributi **Visibilità**.
10. Fare clic sulla cartella **Package: Nessuno** per espandere le opzioni di selezione del package.
11. Selezionare **Protocollo: cXML (1.2.009): cXML**.
12. Fare clic su **Salva**.

Creazione delle interazioni

Informazioni su questa attività

Una volta creata la definizione del documento, impostare un'interazione per il documento cXML.

Per creare le interazioni, utilizzare la seguente procedura.

1. Fare clic su **Amministrazione hub** > **Configurazione hub** > **Definizione documento**.
2. Fare clic su **Crea interazione**.
3. Se il documento cXML è l'origine, in **Origine**, espandere **Package: Nessuno** e **Protocollo: cXML** e selezionare **Tipo documento:**<*document _flow*>. Se il documento cXML è la destinazione, espandere **Package: Nessuno** e **Protocollo: cXML** e selezionare **Tipo documento:** <*flusso_documento*> nella colonna **Destinazione**.
4. Espandere la colonna Origine o Destinazione per l'altra metà dell'interazione (il documento che verrà convertito in cXML o il documento che sarà convertito da cXML) ed espandere il package ed il protocollo e selezionare il tipo di documento.
5. Selezionare **Pass Through** dall'elenco **Azione** in basso nella pagina. (**Pass Through** è l'unica opzione valida supportata per i documenti cXML).

Elaborazione documento XML personalizzato

Questa sezione descrive il modo in cui è possibile configurare l'hub per instradare i documenti XML che non sono gestiti dagli altri protocolli di instradamento integrato.

XML personalizzato è un termine di WebSphere Partner Gateway che fa riferimento ai documenti XML che non sono gestiti da uno dei protocolli integrati.

Il modo in cui i documenti XML personalizzati sono stati identificati si basa su un processo di eliminazione. A seconda dell'ordine delle fasi di analisi per il protocollo del flusso di lavoro in entrata fisso, l'hub tenta di rilevare una corrispondenza tra i documenti XML e i protocolli standard prima che sia richiamata la fase di analisi del protocollo che gestisce il documento XML

personalizzato. L'handler XML personalizzato è richiamato per qualsiasi documento XML che non corrisponde ad uno dei tipi di documenti XML standard.

Per elaborare un documento XML personalizzato, il parser del protocollo deve estrarre le informazioni dal documento. La raccolta di formati XML, delle definizioni per il protocollo del documento e delle definizioni del tipo di documento fornisce il parser del protocollo XML personalizzato che contiene informazioni necessarie per il riconoscimento e l'elaborazione di un documento mediante la configurazione.

Da un livello alto, viene riportato il modo in cui il protocollo XML personalizzato funziona:

1. Il documento XML è stato analizzato per ottenere: valore del nome DTD del documento, lo spazio nomi della tag root e il nome della tag root.
2. In base agli identificativi ottenuti dalla prima fase, un gruppo di famiglie di documenti, che contiene i formati XML, è stato identificato come possibile corrispondenza per il documento. La sezione "Creazione di formati XML" a pagina 153 riporta il modo in cui creare le famiglie di documenti e i formati XML.
3. I possibili formati XML corrispondenti delle famiglie si applicano al documento per verificare se corrisponda al documento. In questa sezione, la corrispondenza viene descritta in seguito.
4. Quando un formato XML corrispondente è stato rilevato, esso consente di estrarre i dati dal documento che l'hub utilizza per elaborare il documento. La famiglia di documenti, a cui appartiene il formato XML corrispondente, determina il protocollo del documento utilizzato per l'instradamento. Il formato XML corrispondente è stato determinato con il tipo di documento, utilizzato per l'instradamento.

Mediante la pagina Gestisci protocolli XML, è possibile creare le famiglie di documenti associate ai protocolli del documento. Quindi, è possibile inserire le famiglie di formato con i formati XML, associati ai tipi di documenti.

Un formato XML comprende due tipologie di informazioni:

- Le espressioni XPath, che consentono di estrarre le informazioni dai documenti XML.
- I dati letterali che sono utilizzati come valore costante.

I formati XML sono stati utilizzati dal Gestore documenti per richiamare i valori che identificano esclusivamente un documento in entrata e le informazioni di accesso all'interno del documento richiesto per un corretto instradamento ed un'appropriata elaborazione.

L'impostazione di un instradamento XML personalizzato è un processo multifase. A tal fine, è necessario completare le seguenti attività:

1. Creare un protocollo che consente di instradare un gruppo di documenti correlati e associarlo ad uno o più package.
2. Creare un tipo di documento per il formato ed associarlo al protocollo creato di recente.
3. Creare una famiglia di documenti per gestire un gruppo di formati XML che corrisponde ai documenti da instradare con il protocollo.
4. Aggiungere i formati XML alla famiglia, che sono associati ad uno dei tipi di documenti per il protocollo della famiglia.

Quindi, creare le interazioni tra i nuovi tipi di documenti in modo da poter stabilire le connessioni.

Queste fasi vengono descritte nelle sezioni che seguono. È possibile trovare un esempio di queste fasi nella sezione "Impostazione dell'hub per i documenti XML personalizzati" a pagina 314.

Creazione di formati XML

I formati XML consentono di identificare ed estrarre i dati dai documenti XML personalizzati in modo da poterli elaborare. I formati XML sono presenti nelle famiglie di documenti. Una famiglia di documenti è una raccolta di formati XML relativi che condividono un nome DTD comune, una tag di elemento root o lo spazio nomi dell'elemento root. Quindi, esistono tre tipologie delle famiglie di documenti: famiglie DTD, famiglie Tag root e famiglie Spazio nomi.

Le famiglie di documenti hanno due ruoli:

- Possono determinare il modo in cui i documenti sono stati instradati. In runtime, quando un documento corrisponde ad un formato XML, la versione ed il protocollo di instradamento, associati alla famiglia di formati consentono di instradare un documento.
- Consentono l'organizzazione dei formati XML nel sistema. Durante la configurazione del sistema, è possibile organizzare i formati XML in base alle famiglie. Ad esempio, è possibile raggruppare i messaggi di acquisto in una famiglia definita Messaggi acquisti e, quindi, è possibile ricercare una famiglia di documenti per accedere ai formati presenti in una determinata famiglia.

Creazione di una famiglia di documenti

Informazioni su questa attività

Per raggruppare i formati XML relativi di una famiglia, è necessario creare prima una famiglia. Per creare una famiglia di documenti, procedere nel modo seguente:

1. Fare clic su **Amministrazione hub** > **Configurazione hub** > **Formati XML**.
2. Fare clic su **Crea una famiglia di documenti**.
3. Nella vista Nuova famiglia di documenti, inserire un **Nome famiglia**.

   Nota: è possibile che più famiglie abbiano lo stesso identificativo o nome. Il tipo di identificativo associato al nome costituisce una chiave famiglia esclusiva. Ad esempio, si supponga di voler instradare i messaggi SOAP mediante l'handler XML personalizzato. Se esistono diverse tipologie di messaggi SOAP, è possibile classificarli nelle famiglie con diversi nomi che hanno Envelope come identificativo della Tag root.
4. Selezionare un **Protocollo** dall'elenco dei protocolli disponibili del sistema. È necessario definire un protocollo personalizzato prima di definire la famiglia che lo utilizza. Una volta creata una famiglia, non è possibile modificare il protocollo per una famiglia, quindi pianificare tale attività.
5. Selezionare un'**Opzione File di grandi dimensioni**: Nessuno, Utilizza il processore file di grandi dimensioni o Utilizza il processore file di grandi dimensioni di conoscenza spazio nome.

   Nessuno indica che i formati XML della famiglia possono utilizzare le espressioni XPath versione 1.0, ma la dimensione dei file che è possibile elaborare sarà limitata da diversi fattori, inclusa la configurazione per la memoria del Gestore documenti, il carico di lavoro del Gestore documenti e la struttura dei documenti elaborati.

Utilizza il processore file di grandi dimensioni o **Utilizza il processore file di grandi dimensioni di conoscenza spazio nome** indica che la dimensione del file non rappresenta una limitazione ma si è limitati all'utilizzo di espressioni di percorso di elementi semplici nei formati XML che appartengono alla famiglia.

Utilizzare l'opzione File di grandi dimensioni se si scrive i formati XML che corrispondono a documenti di grande dimensione che non possono essere gestiti mediante il processore XPath completo. Se si seleziona l'opzione di conoscenza spazio nome, i percorsi dell'elemento includono i prefissi dello spazio nomi, quando vengono visualizzati in un documento.

6. Selezionare un documento **Tipo famiglia** dall'elenco: DTD, Tag root o Spazio nomi.
7. Inserire un **Identificativo famiglia** per il tipo di famiglia creata:

Tabella 21. Identificativi per i tipi di famiglia

Per questo tipo di famiglia	Inserire questo valore come identificativo
DTD	Il nome DTD
Tag root	La tag root dei messaggi presenti in tale famiglia **Nota:** se presente, omettere il prefisso dello spazio nomi.
Spazio nomi	Lo spazio nomi della tag root

In runtime, questo identificativo consente di selezionare una famiglia di formati XML, una delle quali potrebbe corrispondere al documento e viene utilizzata per estrarre le informazioni di elaborazione. Nel caso in cui esistano diverse famiglie che utilizzano lo stesso identificativo, i formati di tutte le famiglie saranno verificati a fronte del messaggio fino a quando non viene rilevata una corrispondenza.

8. Fare clic su **Salva** per salvare la nuova famiglia o fare clic su **Annulla** per interrompere la creazione di una famiglia di documenti o **Restituisci** per ritornare alla vista iniziale.

Rilevamento di una famiglia di documenti

Informazioni su questa attività

Per visualizzare una famiglia di documenti, è necessario rilevarla. Per individuare una famiglia di documenti, completare le seguenti attività:

1. Fare clic su **Amministrazione hub** > **Configurazione hub** > **Formati XML**.
2. Selezionare il protocollo della famiglia di documenti che si desidera visualizzare.
3. Inserire il nome della famiglia, se noto. Per effettuare una ricerca con caratteri jolly, è possibile utilizzare un asterisco (*)
4. Selezionare il tipo di famiglia: Qualsiasi tipo, DTD, Spazio nomi o Tag root.
5. Selezionare l'opzione File di grandi dimensioni: Nessuno, Utilizza il processore file di grandi dimensioni oppure Utilizza il processore file di grandi dimensioni di conoscenza spazio nome
6. Fare clic su **Cerca**. Tutte le famiglie di documenti, adatte ai criteri di ricerca, sono visualizzate al di sotto del pulsante Cerca.
7. Fare clic sull'icona **Visualizza dettagli**, posta accanto ad una famiglia di documenti per visualizzarne i dettagli.

Modifica di una famiglia di documenti
Informazioni su questa attività

Nella finestra di dettagli Famiglia di documenti, è possibile modificare le proprietà per una famiglia. A tal fine, completare le seguenti attività:

1. Per visualizzare una vista di modifica della Famiglia di documenti, fare clic sul pulsante a forma di matita nella vista dei dettagli della famiglia. Il protocollo non può essere modificato in questa vista. Si verifica tale situazione, poiché è possibile che siano presenti messaggi instradati mediante i formati della famiglia e si desidera rendere difficile il debug se il protocollo associato alla famiglia è stato modificato.
2. nella vista di modifica Famiglia di documenti, è possibile modificare il nome della famiglia, il tipo di famiglia e l'identificativo della famiglia.
3. Una volta apportate le modifiche, fare clic su **Salva** per salvarle. Fare clic su **Annulla** o selezionare il pulsante a forma di matita barrato per ritornare alla vista dei dettagli della famiglia senza salvare le eventuali modifiche apportate.

Aggiunta di un nuovo formato XML ad una famiglia
Informazioni su questa attività

Una volta creata una famiglia di documenti, è possibile aggiungere nuovi formati XML alla famiglia. A tal fine, completare le seguenti attività:

Nota: in questa sezione, di solito viene utilizzato il termine espressione XPath. Quando un formato XML utilizza l'opzione File di grandi dimensioni, questo termine deve indicare un'espressione di percorso Elemento, che è un semplice percorso dalla root di un documento ad un elemento che contiene un valore.

1. A partire dalla vista dei dettagli Famiglia di documenti, fare clic su **Crea il formato XML**. Viene visualizzata la vista di definizione del formato XML. Questa pagina è stata suddivisa in quattro sezioni nelle intestazioni **Definizione del tipo di documento**, **Criteri di definizione del tipo di documento**, **Attributi documento** e **Attributi definiti dall'utente**.
2. Completare la sezione **Definizione del tipo di documento**.

   Nella sezione Definizione del tipo di documento, è presente un elenco di selezione con i tipi di documenti, contenuti nel protocollo associato alla famiglia di documenti. In questo elenco, selezionare un **Tipo di documento**. Quando un documento corrisponde al formato XML, il protocollo associato alla famiglia di documenti ed il tipo di documento associato al formato consentono di instradare il documento.
3. Completare la sezione **Criteri di definizione del tipo di documento**.

   Le sezioni **Criteri di definizione del tipo di documento** e **Attributi documento** includono i campi in cui inserire i valori ed i percorsi di elementi se si utilizza l'opzione File di grandi dimensioni o immettere le espressioni XPath, gli spazi di nomi del prefisso ed i tipi di ritorno se non sono disponibili.

   Valore In questo campo, immettere un valore per l'identificativo del formato. È un campo obbligatorio.

   Percorso dell'elemento
   In questo campo, immettere un percorso dell'elemento. È un campo obbligatorio. Il percorso dell'elemento si applica solo ai formati che utilizzano l'opzione File di grandi dimensioni.

   Espressione XPath
   In questo campo, inserire una valida espressione XPath per il

documento che corrisponde al formato o ad un valore di stringa letterale, che è stato restituito come costante per ciascun documento. È un campo obbligatorio. Le espressioni XPath si applicano solo ai formati che non utilizzano l'opzione File di grandi dimensioni.

Campo Spazio nome del prefisso
In questo campo, inserire la definizione dell'ultimo prefisso dello spazio nomi, se presente, utilizzato nell'espressione XPath. È inserito nel formato prefisso=qualificatore spazio nomi. Ad esempio, se l'ultimo prefisso dello spazio nomi dell'espressione è SOAPENV ed il qualificatore è http://schemas.xmlsoap.org/soap/envelope/, è necessario inserire SOAPENV=http://schemas.xmlsoap.org/soap/envelope/ per il prefisso Spazio nomi. I formati che utilizzano l'opzione File di grandi dimensioni non hanno i campi Spazio nome del prefisso come parte della relativa definizione.

Tipo di ritorno
In questo campo, nell'elenco di selezione scegliere il nome della tag Costante, Testo o Elemento. Utilizzare Costante quando si desidera interpretare il campo Espressione XPath come una stringa letterale per tutti i documenti. Utilizzare Testo quando si desidera utilizzare il motore di valutazione XPath per stimare l'espressione nel contesto del documento. Utilizzare il nome della tag Elemento quando si desidera ottenere il nome dell'elemento per il primo elemento restituito dalla valutazione dell'espressione XPath. I formati che utilizzano l'opzione File di grandi dimensioni non includono il nome della tag Elemento come un tipo di ritorno.

Nella sezione Criteri di definizione del tipo di documento, inserire i valori e le espressioni XPath. I valori e i risultati di valutazione dell'espressione sono confrontati quando i documenti sono stati elaborati per determinare se un formato XML corrisponde ad un documento. Quando una corrispondenza è stata rilevata tra un documento ed un formato e quando gli identificativi di business di destinazione e di origine possono essere rilevati utilizzando il formato, il documento viene instradato mediante il protocollo ed il tipo di documento definiti nella sezione Definizione del tipo di documento. Per le informazioni dettagliate sui campi di questa sezione, consultare la Tabella 22 a pagina 157.

Tabella 22. Campi dei Criteri di definizione del tipo di documento

Campo	Richiesto/ Facoltativo	Azione
Identificativo del formato	Richiesto	Inserire l'espressione XPath o il percorso dell'elemento che definisce il percorso nel contenuto dei documenti XML che identificano esclusivamente il documento. Ad esempio, se la tag root appare come <PurchasingMessage type="Purchase Order"> per gli ordini di acquisto e appare come <PurchasingMessage type="Order Confirmation"> per le conferme, l'espressione XPath /PurchasingMessage/@type deve restituire il testo 'Purchase Order' per alcuni messaggi e 'Order Confirmation' per altri. I due formati XML, uno per gli ordini e un altro per le conferme, devono essere scritto ed il campo 'Valore' per gli ordini deve indicare 'Purchase Order' ed il campo 'Valore' per le conferme deve indicare 'Order Confirmation'. In runtime, il formato appropriato può essere individuato dal sistema poiché ricerca un formato in cui la valutazione di espressione fornisce un risultato che corrisponde al valore. Una volta rilevata la corrispondenza, il Tipo documento per l'instradamento, associato al formato, è stato utilizzato dal sistema.
Versione del formato	Richiesto	Inserire l'espressione XPath o il percorso dell'elemento che definisce la versione del formato. La versione del formato viene valutata in modo simile a quello utilizzato per l'identificativo del formato. Quando l'espressione per la versione corrisponde al valore di versione in un formato, il formato potrebbe essere utilizzato se anche l'identificativo corrisponde. Nel caso in cui sia presente solo una versione di un documento, è possibile inserire '1' per l'espressione con un tipo di ritorno Costante e '1' per il valore. Ciò indica che la versione corrisponde sempre e l'identificativo consente di stabilire un formato corrispondente.

4. Completare la sezione **Attributi documento**.

   Nella sezione **Attributi documento**, inserire i valori e le espressioni XPath nello stesso modo della sezione **Criteri di definizione del tipo di documento**. Per le informazioni dettagliate sui campi di questa sezione, consultare la Tabella 23.

Tabella 23. Campi Attributi documento

Campo	Richiesto/ Facoltativo	Azione
Identificativo di business di origine	Richiesto	Inserire l'espressione XPath o il percorso dell'elemento che definisce il percorso dell'ID di business di origine all'interno del documento XML. Consente di identificare il partner di origine per motivi di instradamento. Questi dati devono essere rilevati per il formato utilizzato.
Identificativo di business di destinazione	Richiesto	Inserire l'espressione XPath o il percorso dell'elemento che definisce il percorso dell'ID di business di destinazione all'interno del documento XML. Consente di identificare il partner di destinazione per motivi di instradamento. Questi dati devono essere rilevati per il formato utilizzato.

Tabella 23. Campi Attributi documento (Continua)

Campo	Richiesto/ Facoltativo	Azione
Identificativo documento	Facoltativo	Inserire l'espressione XPath o il percorso dell'elemento che definisce il percorso per il numero ID documento all'interno del documento XML. Questo valore sarà visualizzato nel visualizzatore del documento.
Data e ora documento	Facoltativo	Inserire l'espressione XPath o il percorso dell'elemento che definisce il percorso per la data e l'ora di creazione del documento all'interno del documento XML. Questo valore sarà visualizzato nel visualizzatore del documento.
Chiavi della verifica duplicati 1 - 5	Facoltativo	Inserire le espressioni XPath o i percorsi dell'elemento che definiscono i percorsi utilizzati per identificare se un documento sia univoco o un duplicato.
Indicatore sincrono	Facoltativo	Inserire un'espressione XPath o un percorso dell'elemento che viene valutato su *true* o *false*, indicando se questo tipo di documento richiede una risposta sincrona. È possibile inserire un'espressione XPath che utilizza il contenuto del documento per impostare il valore o immettere la stringa letterale true o false con un tipo di ritorno pari a Costante. L'attributo BCGDocumentConstants.BCG_GET_SYNC_RESPONSE sarà impostato in BDO durante l'elaborazione dell'analisi del canale se questo campo è stato impostato su true.
Elemento root di convalida	Facoltativo	Inserire l'espressione XPath che definisce il nodo root del contenuto (payload) di un messaggio sottoposto a enveloping all'interno del documento XML. WebSphere Partner Gateway convalida un documento che inizia con questo elemento. È necessario specificare un'azione che effettua la convalida. Questo campo non si applica ai formati che utilizzano l'opzione File di grandi dimensioni.
ID documento correlato	Facoltativo	Inserire l'espressione XPath o il percorso dell'elemento che fornisce l'identificativo del documento di un documento instradato in precedenza a cui è associato il documento corrente. Ad esempio, di solito Order Confirmation è relativo a Purchase Order. È possibile ottenere il valore identificativo del documento Purchase Order mediante un'espressione XPath (vedere sopra). Se Order Confirmation include l'identificativo Purchase Order, quindi è possibile reperirlo mediante l'espressione ID del documento relativo. Tale operazione associa i documenti nel visualizzatore del documento.
Campi di ricerca 1-10	Facoltativo	Inserire le espressioni XPath o i percorsi dell'elemento che definiscono il percorso sul contenuto del documento che si desidera utilizzare per personalizzare le ricerche all'interno del documento XML. Nel Visualizzatore documento, è possibile ricercare i documenti in base ai valori di questi campi.

5. Completare la sezione **Attributi definiti dall'utente**.

   Nella sezione **Attributi definiti dall'utente** è possibile aggiungere gli attributi definiti dall'utente personalizzati. Aggiungere un attributo inserendo il nome nel campo di immissione e selezionando **Aggiungi**. Quindi, definire questo

nuovo attributo come per gli altri attributi standard inserendo, nel modo appropriato, l'espressione XPath, il percorso dell'elemento, lo spazio nomi del prefisso e selezionando un tipo di ritorno per questo attributo

Una volta aggiunti gli attributi, sono utilizzati nello stesso modo in cui sono utilizzati gli attributi standard. Se si desidera rimuovere un attributo definito dall'utente da un formato, fare clic sulla X rossa, che viene visualizzata accanto al nome. Gli attributi definiti dall'utente sono destinati ad essere utilizzati dagli handler scritti dall'utente che elaborano il documento. I nomi di attributi e i relativi valori sono stati aggiunti al documento di business durante l'elaborazione del documento. Il codice dell'handler può accedere ad essi ottenendoli dal documento di business mediante i nomi definiti. Per ulteriori informazioni, consultare *WebSphere Partner Gateway Programmer Guide*.

6. Una volta inseriti i valori in questa vista, scorrere in basso e fare clic su **Salva** per salvare le modifiche apportate. Fare clic su **Annulla** o selezionare il pulsante a forma di matita barrata per annullare le modifiche apportate e ritornare alla vista di riepilogo della famiglia.

Creazione di una definizione del protocollo

Informazioni su questa attività

Le seguenti fasi descrivono come creare un formato di definizione del protocollo XML:

1. Fare clic su **Amministrazione hub > Configurazione hub > Definizione documento > Crea definizione di documento**.
2. Per il **Tipo di definizione di documento**, selezionare **Protocollo**.
3. Per il **Nome**, immettere un identificativo per la definizione del documento. Ad esempio, per un protocollo XML personalizzato, è possibile inserire XML personalizzato. Questo campo è obbligatorio.
4. Per la **Versione**, inserire un valore per la versione del protocollo. I valori Numerico o Stringa sono consentiti.
5. Inserire una descrizione facoltativa del protocollo.
6. Impostare **Livello di documento** su **No**, poiché viene definito un protocollo, invece di un tipo di documento (che sarà definito nella successiva sezione).
7. Impostare **Stato** in **Abilitato**.
8. Impostare **Visibilità** per questo protocollo. È probabile che si desidera renderlo visibile a tutti i partner.
9. Selezionare i package nei quali questo nuovo protocollo viene incluso. Ad esempio, se si desidera associare questo protocollo con i package AS, Nessuno e Integrazione di back-end, selezionare **Package: AS**, **Package: Nessuno**, **Package: Integrazione di back-end**.
10. Fare clic su **Salva**.

Creazione di una definizione di tipo di documento

Informazioni su questa attività

In seguito, utilizzare nuovamente la pagina Crea definizione di documento per creare un tipo di documento.

1. Fare clic su **Amministrazione hub > Configurazione hub > Definizione documento > Crea definizione di documento**.
2. Per il **Tipo di definizione di documento**, selezionare **Tipo documento**.

3. Per il **Nome**, immettere un identificativo per la definizione del documento. Ad esempio, è possibile inserire `Purchase order` come nome per il tipo di documento. Questo campo è obbligatorio.
4. Per la **Versione**, inserire un valore per la versione del tipo di documento. I valori Numerico o Stringa sono consentiti.
5. Inserire una descrizione facoltativa del tipo di documento.
6. Impostare il **Livello di documento** su **Sì** (poiché viene definito un oggetto di instradamento che corrisponde ad un documento corrente).
7. Impostare **Stato** in **Abilitato**.
8. Impostare **Visibilità** per questo flusso. È probabile che si desidera renderlo visibile a tutti i partner.
9. Fare clic sull'icona **Espandi** per espandere ciascun package selezionato al passo 9 a pagina 159. Espandere la cartella e selezionare il nome del protocollo creato nella precedente sezione (ad esempio, Protocollo: XML personalizzato.).
10. Fare clic su **Salva**.

Se sono stati utilizzati i valori di esempio, la pagina Gestisci le definizioni di documento contiene un tipo di documento di Purchase order e un protocollo di XML personalizzato nei package AS, Nessuno e Integrazione di backend.

Completamento della configurazione

Una volta stabilita la definizione del protocollo, sarà possibile sceglierla come protocollo di instradamento da utilizzare per una famiglia di documenti XML. Una volta aggiunti i tipi di documenti al protocollo, sarà possibile assegnarli alle definizioni del formato XML presenti nella famiglia di documenti. I messaggi che corrispondono ad un formato della famiglia saranno instradati mediante il protocollo associato alla famiglia e al tipo di documento associato al formato corrispondente.

Prima di poter definire qualsiasi canale che utilizza le nuove definizioni, è necessario abilitare le interazioni tra i nuovi protocolli e i tipi di documenti e gli altri protocolli ed i tipi di documenti. È anche necessario abilitare le capacità B2B dei partner per consentire loro di inviare e ricevere documenti mediante il nuovo protocollo ed i tipi di documenti.

Utilizzo delle mappe di convalida

WebSphere Partner Gateway utilizza le mappe di convalida per convalidare la struttura di alcuni documenti. Se si desidera associare una mappa di convalida con un documento, prima accertarsi che la mappa sia valida per WebSphere Partner Gateway, come descritto in "Aggiunta mappe di convalida". Per gestire le mappe di convalida, consultare *Hub administration tasks Chapter of WebSphere Partner Gateway Administrator Guide*.

Aggiunta mappe di convalida

Informazioni su questa attività

Un'azione può avere una mappa di convalida associata per verificare che il partner di destinazione o il sistema di back-end possa analizzare il documento. Si noti che una mappa di convalida convalida solo la *struttura* del documento. Non convalida i contenuti del messaggio.

Nota: una volta associata una mappa di convalida ad una definizione del documento, non è possibile separarli.

Per aggiungere una nuova mappa di convalida all'hub, utilizzare la seguente procedura.

1. Salvare il file della mappa di convalida nell'hub o nella posizione da cui WebSphere Partner Gateway può leggere i file.
2. Fare clic su **Amministrazione hub > configurazione hub > Mappe > Mappe di convalida**.
3. Fare clic su **Crea**.
4. Digitare una descrizione della mappa di convalida.
5. Passare al file di schema da utilizzare per convalidare i documenti, quindi fare clic su **Apri**.
6. Fare clic su **Salva**.

Associazione delle mappe alle definizioni di documento

Informazioni su questa attività

Per associare una mappa di convalida ad una definizione del documento, utilizzare la seguente procedura.

1. Fare clic su **Amministrazione hub > configurazione hub > Mappe > Mappe di convalida**.
2. Fare clic sull'icona **Visualizza dettagli**, posta accanto alla mappa di convalida che si desidera associare alla definizione del documento.
3. Fare clic sull'icona **Espandi** accanto a un package per espanderlo singolarmente al livello appropriato (ad esempio **Azione** per un documento RosettaNet).
4. Selezionare la definizione del documento che si desidera associare alla mappa di convalida.
5. Fare clic su **Salva**.

Utilizzo delle associazioni di conversione

Informazioni su questa attività

WebSphere Partner Gateway utilizza le associazioni di conversione per convertire i documenti da un modulo all'altro, ad esempio, per convertire il documento XML in EDI.

Di seguito, vengono riportati i passi per l'utilizzo delle associazioni di conversione:

1. Accedere alla console di gestione di WebSphere Partner Gateway.
2. Fare clic su **Procedure guidate**.
3. Nella procedura guidata di importazione EIF, **sfogliare** e specificare il percorso del file .EIF.
4. Fare clic su **Importa**.
5. Nella pagina Riepilogo importazione, fare clic su **Avanti**.
6. Nel pannello Review Transformation Maps e Modify Interactions da creare, selezionare l'associazione di conversione, aggiungere un'interazione e selezionare l'azione per l'interazione creata.
7. Fare clic su **Fine**.

Visualizzazione di documenti

Informazioni su questa attività

Il Visualizzatore documenti riporta le informazioni sui documenti che costituiscono un tipo di documento. È possibile visualizzare i documenti non elaborati, gli eventi ed i dettagli di elaborazione dei documenti associati mediante determinati criteri di ricerca. Queste informazioni sono utili nel caso in cui si tenti di stabilire se un documento sia stato consegnato correttamente o determinare la causa di un problema.

Per visualizzare il Visualizzatore documenti, completare le seguenti attività:

1. Fare clic su **Visualizzatori > Visualizzatore documenti**.
2. Selezionare i criteri di ricerca appropriati.
3. Fare clic su **Cerca**.

Per le informazioni sull'utilizzo del Visualizzatore documenti, consultare il manuale *WebSphere Partner Gateway Administrator Guide*.

Configurazione della registrazione di non rifiuto

È possibile configurare la registrazione di non rifiuto dei messaggi utilizzando gli attributi del package, del protocollo o del flusso di documenti utilizzati per l'instradamento dei documenti. L'attributo viene denominato Non-Repudation Required e può avere un valore uguale a Sì o No. La definizione dell'attributo viene definita a livello dell'oggetto di instradamento e può essere sovrascritta modificandola a livello delle capacità B2B o a livello della connessione.

Configurazione memorizzazione messaggio

È possibile configurare la memorizzazione messaggio gli attributi del package, del protocollo o del flusso di documenti utilizzati per l'instradamento dei documenti. L'attributo viene denominato Message Store Required e può avere un valore uguale a Sì o No. La definizione dell'attributo viene definita a livello dell'oggetto di instradamento e può essere sovrascritta modificandola a livello delle capacità B2B o a livello della connessione.

Capitolo 10. Configurazione dei flussi di documenti EDI

In questo capitolo viene descritto il modo in cui configurare le definizioni del documento e le interazioni per gli scambi EDI standard. In questo capitolo sono incluse le descrizioni di ricezione e conversione dei documenti ROD (record-oriented-data). In questo capitolo, vengono descritti i seguenti argomenti:

È, inoltre, possibile disporre di uno scambio EDI trasmesso senza deenveloping o conversione. I passaggi per la creazione delle interazioni per questo tipo di scambio vengono rappresentati in "Documenti EDI con azione Pass Through" a pagina 105.

Nota: è necessario utilizzare sempre la stessa istanza del browser con cui si accede alla Console comunità per apportare modifiche alla configurazione di WebSphere Partner Gateway. L'utilizzo simultaneo di più istanze del browser può causare l'eliminazione delle modifiche di configurazione.

Panoramica su EDI

EDI è un metodo di trasmissione delle informazioni aziendali tramite una rete tra associati aziendali che concordano nel seguire gli standard industriali e nazionali approvati nella conversione e scambio delle informazioni. WebSphere Partner Gateway fornisce la funzione di deenveloping, la conversione e l'operazione di enveloping per i seguenti standard EDI:

- X12, uno standard EDI comune approvato da American National Standards Institute
- UN/EDIFACT (United Nations Electronic Data Interchange for Administration Commerce and Support)
- UCS (Uniform Communication Standard)

Nelle sezioni successive viene fornita una panoramica di scambi EDI che sono conformi agli standard X12, EDIFACT e UCS e delle transazioni e dei gruppi contenuti negli scambi. Inoltre, viene descritto il modo in cui vengono convertiti i documenti XML e ROD e gli scambi EDI.

Struttura di scambio EDI

Uno scambio EDI contiene una o più transazioni di business. Negli standard X12 e correlati, una transazione viene denominata *set di transazioni*. Negli standard EDIFACT e correlati, una transazione viene denominata *messaggio*. In genere, questo documento utilizza il termine *transazione* o *transazione di business* per fare riferimento ad una serie di transazioni X12 o UCS o ad un messaggio EDIFACT.

Gli scambi EDI sono composti di *segmenti* che contengono *elementi dati*. Gli elementi dati rappresentano elementi, quali il nome, la quantità, la data o l'ora. Un segmento è un gruppo di elementi dati correlati. I segmenti vengono identificati da un nome o una tag, che appare all'inizio del segmento. (Gli elementi dati non vengono identificati dal nome, ma sono delimitati da caratteri di separazione speciali riservati a questo scopo).

In alcuni casi, è utile distinguere i segmenti in dettagli o di dati in una transazione da altri segmenti utilizzati a scopo amministrativo. I segmenti amministrativi vengono denominati *segmenti di controllo* in X12 e *segmenti di servizio* in EDIFACT. I segmenti della *busta* che delimitano i confini di uno scambio EDI sono un esempio di questi segmenti di controllo e di servizio.

Gli scambi EDI possono contenere tre livelli di segmenti. Su ciascun livello, c'è un segmento di intestazione all'inizio ed un segmento dell'elemento di coda alla fine.

Uno scambio dispone sempre di un segmento di intestazione dello scambio all'inizio e uno di coda alla fine.

Uno scambio può contenere uno o più gruppi. Un gruppo, a sua volta, contiene una o più transazioni correlate. Il livello di gruppo è facoltativo in EDIFACT ma è obbligatorio negli standard X12 e correlati. Quando i gruppi sono presenti, c'è un'intestazione del gruppo ed un segmento dell'elemento di coda del gruppo per ciascun gruppo.

Un gruppo (o uno scambio, dove i gruppi non sono presenti) contiene una o più transazioni. Ciascuna transazione ha un'intestazione dell'insieme di transazioni ed un elemento di coda dell'insieme di transazioni.

Una transazione rappresenta un documento di business, come ad esempio un ordine di acquisto. Il contenuto del documento di business è rappresentato dai segmenti di dettaglio tra il segmento di intestazione dell'insieme di transazioni e il segmento dell'elemento di coda dell'insieme di transazioni.

Per ogni standard EDI viene fornito un metodo per la visualizzazione dei dati in uno scambio. Nella seguente tabella vengono elencati i segmenti per ciascuno dei tre standard EDI supportati.

Tabella 24. Segmenti per standard EDI supportati

Segmento standard	X12	UCS	EDIFACT
Avvio scambio	ISA	BG	UNB
Fine scambio	IEA	EG	UNZ
Avvio gruppo	GS	GS	UNG
Fine gruppo	GE	GE	UNE
Avvio transazione	ST	ST	UNH

Tabella 24. Segmenti per standard EDI supportati (Continua)

Segmento standard	X12	UCS	EDIFACT
Fine transazione	SE	SE	UNT

In Figura 22 viene mostrato un esempio di uno scambio X12 e i segmenti che costituiscono lo scambio.

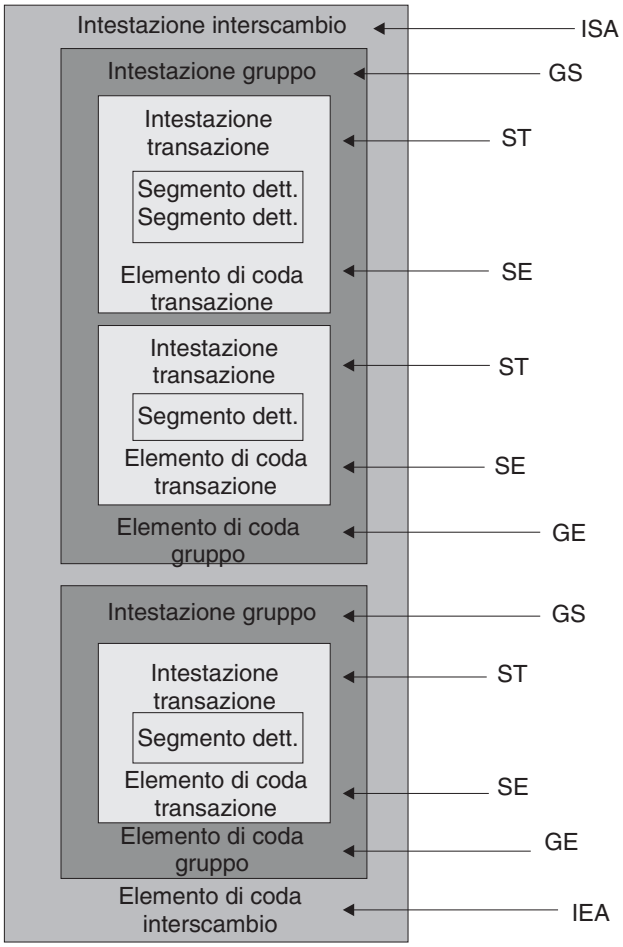


Figura 22. Una busta dello scambio

Mappe

Lo specialista della mappa del client Data Interchange Services crea mappe di conversione che descrivono come modificare un documento di un formato in un altro documento di un formato differente. È possibile, ad esempio, disporre di una mappa di conversione che modifica una transazione X12 in un messaggio EDIFACT. È possibile anche convertire una transazione EDI in un documento XML o in un documento dati ROD (record-oriented data).

Le mappe possono essere create utilizzando DIS o WTX Design Studio. DIS viene utilizzato per creare mappe per la conversione WDI, mentre WTX Design Studio viene utilizzato per la conversione WTX. Le mappe create utilizzando DIS non possono essere migrate per la conversione WTX, ma possono essere scritte nuovamente. In base all'azione, il motore di conversione verrà selezionato se entrambe sono operative.

Per creare qualsiasi mappa viene richiesta la definizione dei documenti di origine e destinazione. Le definizioni dei documenti di origine per EDI vengono fornite da WDI stesso, ma per ROD e XML è necessario crearle utilizzando il client DIS. Per fare in modo che questo standard venga utilizzato dal codice di runtime, è necessario compilarlo. Nelle versioni precedenti, le mappe di conversione sono richieste per lo standard, ma questa versione consente di eseguire la compilazione senza utilizzare la mappa di conversione. Lo standard eif per EDI viene importato, ma per ROD viene creato utilizzando il client DIS. In caso di XML DTD/XSD viene importato nel database di sviluppo. Per EDI, nella console di gestione passare alle procedure guidate EDI. Verranno visualizzati i formati / standard dei dati disponibili nel file EIF. È possibile importarli tutti in una sola volta o sceglierne uno o più da importare. Su una selezione corretta la stringa di controllo standard verrà importata nel database di runtime.

La mappa di conversione può anche creare più documenti da un singolo documento. Questo tipo di mappa crea l'utilizzo di un *concatenamento di mappe*, che produce più output da una singola transazione. Nel concatenamento di mappe, una volta che un documento di origine è stato convertito correttamente in un documento di destinazione, si utilizza di nuovo una mappa successiva per convertire il documento di origine per produrre un altro documento di destinazione. Ciò può ripetersi tutte le volte che si rivela necessario produrre quanti documenti si desidera.

Oltre alle mappe di conversione, è possibile utilizzare le mappe di riconoscimento funzionale e le mappe di convalida. Le mappe di riconoscimento funzionale forniscono istruzioni su come produrre un riconoscimento funzionale, che notifica al mittente di un documento EDI che il documento è arrivato. Molte mappe di riconoscimento funzionale standard EDI vengono installate quando si installa WebSphere Partner Gateway. Per un elenco di queste mappe, vedere "Impostazione dei riconoscimenti" a pagina 208.

Quando l'hub di invio prevede un riconoscimento funzionale che non si verifica nel tempo previsto per il riconoscimento, il documento originale viene inviato nuovamente. Il numero di tentativi e l'intervallo tentativi sono configurabili. Questa funzione non viene attivata per impostazione predefinita. È necessario impostare manualmente il valore nelle proprietà EDI. Se Ora per riconoscere è impostato su Sì, i valori devono essere impostati per l'intervallo e il conteggio tentativi. Gli eventi di tentativi vengono registrati per scopi di monitoraggio. Se il numero di tentativi è stato esaurito senza FA, l'evento appropriato verrà registrato per scopi di monitoraggio.

Le mappe di riconoscimento funzionale possono essere create dallo specialista della mappatura del client Data Interchange Services. WebSphere Partner Gateway genera un riconoscimento funzionale quando viene convalidata una transazione EDI e quando tale transazione dispone di una mappa di riconoscimento funzionale associata. Il documento di origine deve essere un documento EDI.

WebSphere Partner Gateway fornisce un livello standard di convalida sul documento EDI. Se un riconoscimento funzionale viene generato, i risultati della convalida di un documento EDI vengono salvati. Le mappe di convalida vengono create per fornire una convalida aggiuntiva su un documento EDI. La creazione di un riconoscimento funzionale utilizza la mappa di riconoscimento funzionale e i risultati della convalida del documento EDI. La mappa di riconoscimento funzionale contiene comandi di mappatura che indicano come utilizzare i risultati di convalida per creare un riconoscimento funzionale specifico. Se un documento

viene accettato per la conversione dal processo di convalida, si utilizza la mappa di conversione dei dati appropriati per convertire il documento di origine.

Panoramica dei documenti XML e ROD

Lo specialista della mappatura del client Data Interchange Services può creare definizioni del documento per documenti XML e ROD, quindi creare le mappe di conversione che modificano un tipo di documento in un altro.

documenti XML

I documenti XML vengono definiti da una definizione DTD XML o da uno schema XML. Lo specialista della mappatura del client Data Interchange Services crea una mappa di conversione basata sulla definizione DTD o sullo schema che descrive come convertire il documento XML in un altro formato. Un documento XML può essere convertito in un altro documento XML, un documento ROD o una transazione EDI.

documenti ROD

Il termine ROD si riferisce ai documenti conformi ad un formato del proprietario. Lo specialista della mappatura del client Data Interchange Services definisce una definizione del documento ROD, che si riferisce ai dati di strutture aziendali in un documento. Una volta definita una definizione di un documento, lo specialista della mappatura può creare una mappa per convertire il documento ROD in un altro documento ROD, un documento XML o una transazione EDI.

Splitter e più documenti

I documenti XML o ROD possono inserire l'hub come documento singolo o come gruppo di documenti nello stesso file. È possibile che più documenti siano stati inseriti nello stesso file quando, ad esempio, un lavoro pianificato sul partner o sul partner interno carica periodicamente i documenti da inviare. Se più documenti XML o ROD arrivano in un solo file, il Destinatario chiama l'handler splitter associato (XMLSplitterHander o RODSplitterHandler) per dividere il gruppo di documenti. (Gli handler splitter vengono configurati quando si crea una destinazione). Per informazioni, consultare la sezione " Preelaborazione" a pagina 72). I documenti vengono, quindi, reintrodotti nel Gestore documenti in modo che vengano elaborati singolarmente.

Nota: gli ID mittente e destinatario devono essere parte della definizione di documento ROD associata alla mappa di conversione. Le informazioni necessarie per stabilire il tipo di documento ed i valori del dizionario devono essere presenti anche nella definizione del documento. Assicurarsi che lo specialista della mappatura del client Data Interchange Services sia a conoscenza dei requisiti, quando si crea la mappa di conversione.

Inoltre, è possibile inviare più scambi EDI in un singolo file. Se arrivano più scambi EDI in un file, il Destinatario richiama EDISplitterHandler per separare la serie di scambi. Gli scambi vengono reintrodotti nel Gestore documenti per essere elaborati singolarmente.

Nota: la separazione viene eseguita sullo scambio, non sulle singole transazioni all'interno dello scambio. Le transazioni all'interno dello scambio vengono sottoposte a deenveloping.

Panoramica della creazione dei tipi di documenti e impostazione di attributi

Una definizione del documento è costituita almeno da un package, protocollo e da un tipo documento. Le definizioni del documento specificano le tipologie di documenti che saranno elaborate da WebSphere Partner Gateway.

Il termine impacchettamento indica la logica richiesta per impacchettare un documento secondo una specifica, come ad esempio, AS2. Un flusso di protocollo è la logica richiesta per elaborare un documento che aderisce ad un certo protocollo, come ad esempio, EDI-X12. Un tipo di documento descrive come deve essere il documento.

Le seguenti sezioni descrivono brevemente le fasi generali per impostare un flusso del documento tra il partner interno ed un partner esterno. Inoltre, in queste sezioni vengono descritti i punti in cui è possibile impostare gli attributi.

Fase 1: Verificare che la definizione del documento sia disponibile

Informazioni su questa attività

Prima di poter inviare o ricevere un documento, è necessario definire una definizione del documento per il documento. WebSphere Partner Gateway fornisce diverse definizioni predefinite del documento, incluse quelle che rappresentano i riconoscimenti funzionali. Al momento dell'importazione delle mappa di conversione per le conversioni EDI o per i documenti XML o ROD, le definizioni del documento associate sono visualizzate nella pagina Definizioni documento. Allo stesso modo, se si importa una mappa di riconoscimento funzionale che non è stata già definita, la definizione del documento per il riconoscimento viene visualizzata nella pagina Definizioni documento. È anche possibile creare le proprie definizioni del documento.

Per stabilire la definizione del documento, è possibile modificare determinati attributi. Gli attributi consentono di effettuare varie funzioni di elaborazione e le funzioni di instradamento, come, ad esempio la convalida, la verifica della codifica e il conteggio tentativi. Gli attributi impostati sul livello della definizione del documento forniscono un'impostazione globale per il package, protocollo o tipo di documento associato. Gli attributi disponibili variano, in base alla definizione del documento. Gli attributi per le definizioni del documento EDI presentano diversi attributi rispetto alle definizioni del documento RosettaNet.

Ad esempio, se viene specificato un valore per **Consenti una richiesta TA1** al livello del tipo documento ISA, l'impostazione si applica a tutti i documenti ISA. Se successivamente si imposta **Consenti una richiesta TA1** al livello delle capacità B2B per un partner o un partner interno, tale impostazione sovrascrive quella impostata al livello della definizione del documento.

Per gli attributi, che è possibile impostare su più livelli della definizione del documento, i valori impostati al livello del tipo del documento ha la priorità su quelli impostati al livello del protocollo e gli attributi impostati al livello del protocollo hanno la precedenza su quelli impostati al livello del package. Ad esempio, se un profilo busta viene specificato al livello del protocollo &X44TA1, ma è stato specificato un diverso profilo busta al livello del tipo documento TA1, viene utilizzato il profilo busta specificato al livello del tipo documento TA1.

Prima di poter creare le interazioni, è necessario che il tipo documento sia elencato nella pagina Gestisci le definizioni di documento.

Fase 2: Creare le interazioni

Informazioni su questa attività

Quindi, impostare le interazioni, che sono modelli per creare le connessioni del partner. Le interazioni trasmettono il modo in cui il documento entra, l'elaborazione eseguita sul documento e il modo in cui quest'ultimo viene inviato dall'hub.

Per alcuni protocolli, sono necessari solo due flussi, uno per descrivere il documento ricevuto nell'hub (dal partner o partner interno) e l'altro che descrive il documento inviato dall'hub (al partner o partner interno). Se, tuttavia, l'hub invia o riceve uno scambio EDI che verrà sottoposto a deenveloping in singole transazioni o in cui sono richiesti i riconoscimenti, verranno create effettivamente più interazioni. Ad esempio, se si riceve uno scambio EDI all'hub, l'interazione descrive il modo in cui lo scambio è stato inviato all'hub e il modo in cui viene elaborato. Inoltre, si avrà un'interazione per ciascuna transazione all'interno dell'hub che descrive il modo in cui viene elaborata la transazione. Per gli scambi EDI che lasciano l'hub, l'interazione descrive il modo in cui la busta dello scambio viene inviata al destinatario.

Fase 3: Creare i profili del partner, le destinazioni e le capacità B2B

Informazioni su questa attività

Si procede quindi alla creazione dei profili del partner per il partner interno e per i partner esterni. Si definiscono le destinazioni (che determinano dove saranno inviati i documenti) e le capacità B2B, che specificano i documenti che il partner interno o un partner è in grado di inviare e ricevere. La pagina Capacità B2B elenca tutti i tipi di documenti definiti.

È possibile impostare attributi sul livello delle capacità B2B. Gli attributi impostati su questo livello sovrascrivono quelli impostati al livello della definizione del documento. Ad esempio, se si imposta **Consenti una richiesta TA1** su **No** al livello della definizione del documento per i documenti ISA, impostarlo su **Sì** al livello delle capacità B2B, viene utilizzato il valore **Sì**. L'impostazione di un attributo al livello B2B consente di personalizzare l'attributo per un determinato partner.

Se il profilo busta è stato impostato al livello del protocollo o del tipo documento (nella pagina Gestisci le definizioni di documento) e poi viene impostato su un valore diverso nella pagina Capacità B2B, viene utilizzato l'ultimo valore.

Prima di poter stabilire le connessioni tra loro, è necessario che i profili e le capacità B2B del partner interno e dei partner esterni siano definiti.

Fase 4: Attivare le connessioni

Informazioni su questa attività

Attivare, infine, le connessioni tra il partner interno ed i partner esterni. Le connessioni disponibili si basano sulle capacità B2B dei partner e delle interazioni create. Le interazioni dipendono dalle definizioni del documento disponibili.

Per alcuni scambi, viene richiesta una sola connessione. Ad esempio, se un partner invia un documento binario ad un'applicazione di back-end del partner interno, risulta necessaria solo una connessione. Tuttavia, per lo scambio di scambi EDI in cui lo scambio è sottoposto a deenveloping e le singole transazioni vengono convertite, vengono stabilite più connessioni.

Nota: per gli scambi EDI passati come tali, è richiesta una sola connessione.

È possibile impostare attributi sul livello della connessione. Gli attributi impostati su questo livello sostituiscono quelli impostati sul livello degli attributi B2B. Ad esempio, se si imposta **Consenti una richiesta TA1** su **Sì** a livello delle capacità B2B, ma poi si imposta su **No** a livello di connessione, il valore utilizzato è **No**. L'impostazione di un valore per un attributo al livello della connessione consente di personalizzare ulteriormente l'attributo, in base ai requisiti di instradamento dei partner e delle applicazioni richiamate.

Panoramica sui flussi possibili

In questa sezione, viene fornita una breve panoramica dei tipi di conversione che WebSphere Partner Gateway può eseguire. I dettagli di queste conversioni e ciò che è necessario per configurarle vengono descritti in "Definizione degli scambi del documento" a pagina 194.

flusso da EDI a EDI

WebSphere Partner Gateway può accettare uno scambio EDI da un partner o dal partner interno, convertirlo in una tipologia diversa dello scambio EDI (ad esempio, da EDI-X12 a EDIFACT) ed inviare il documento al partner interno o ad un qualsiasi partner. I passaggi seguenti hanno luogo quando uno scambio EDI viene convertito in un altro scambio EDI:

1. Lo scambio EDI ricevuto sull'hub viene sottoposto a deenveloping.
2. Le singole transazioni in uno scambio EDI vengono convertite nel formato EDI del partecipante.
3. Le transazioni EDI convertite vengono sottoposte a enveloping ed inviate al destinatario.

In Figura 23 viene mostrato uno scambio X12 che consiste di tre transazioni da sottoporre a deenveloping. Le transazioni sono convertite in formato EDIFACT e sono quindi sottoposte a enveloping ed inviate al partner.

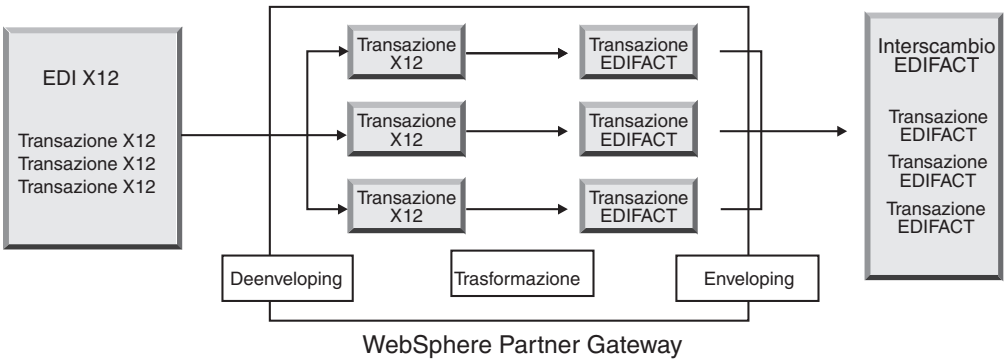


Figura 23. Flusso da scambio EDI a scambio EDI

Ciascuna delle transazioni ha una mappa di conversione associata che specifica come viene convertita la transazione. La transazione può essere convertita in una transazione singola oppure , se è stato il concatenamento di mappe per la creazione della mappa, più transazioni. Se il batch dell'Enveloper è attivo, le transazioni che arrivano nell'hub in una busta lasciano l'hub in una busta. Tuttavia, se sono presenti interruzioni di busta (ad esempio, valori diversi per gli attributi EDI o un profilo di busta diverso) o se il batch è stato disattivato, le transazioni lasciano l'hub in buste diverse. Consultare la sezione "Enveloper" a pagina 182 per una descrizione generale dell'Enveloper (che è il componente che raccoglie un gruppo di transazioni da inviare ad un partner, lo include in una busta e lo invia). Per ulteriori informazioni sul batch, consultare la sezione "Modalità batch" a pagina 182.

La transazione potrebbe anche avere una mappa di convalida ad essa associata.

Flusso da EDI a XML o ROD

WebSphere Partner Gateway può accettare uno scambio EDI da un partner o dal partner interno, eseguire il deenveloping dello scambio e convertire le transazioni EDI risultanti in documenti XML o ROD.

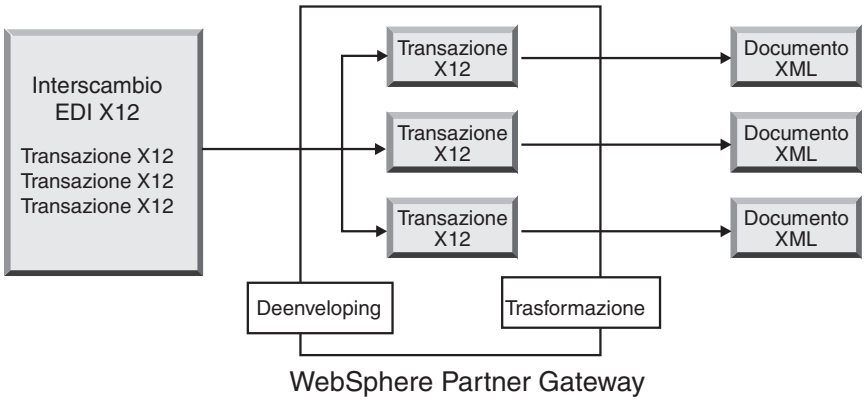


Figura 24. Flusso dallo scambio EDI ai documenti XML

La transazione può essere convertita in un singolo documento oppure se è stato utilizzato il concatenamento della mappa, più documenti.

Flusso da XML o ROD a EDI

WebSphere Partner Gateway può ricevere i documenti XML o ROD da un partner o dal partner interno, convertire i documenti in transazioni EDI, eseguire l'enveloping delle transazioni ed inviarle al partner o al partner interno.

La Figura 25 a pagina 172 mostra i documenti XML che sono stati convertiti in transazioni X12 e quindi sottoposti a enveloping.

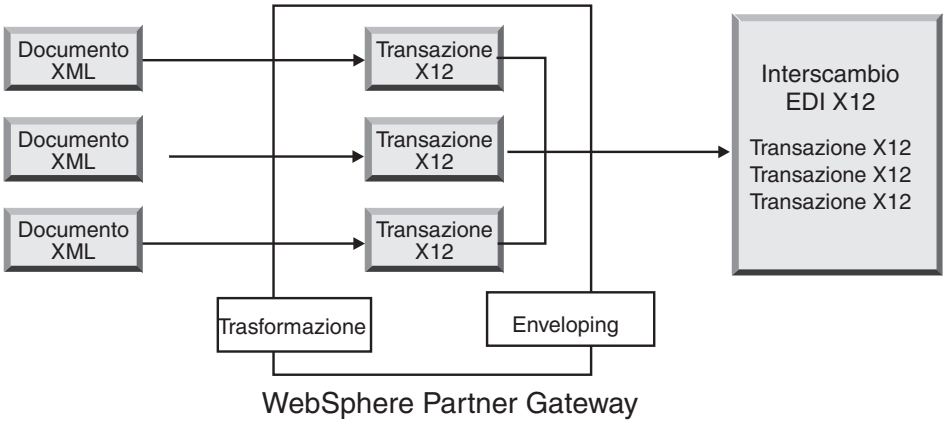


Figura 25. Flusso dal documento XML allo scambio EDI

Un documento può essere convertito in più transazioni (se è stato utilizzato il concatenamento di mappe per creare la mappa) e le transazioni sottoposte a enveloping in scambi differenti. In Figura 26 viene mostrato un documento XML convertito in tre transazioni X12. Due delle transazioni vengono sottoposte a enveloping insieme. Una di esse viene inserita in una busta separata.

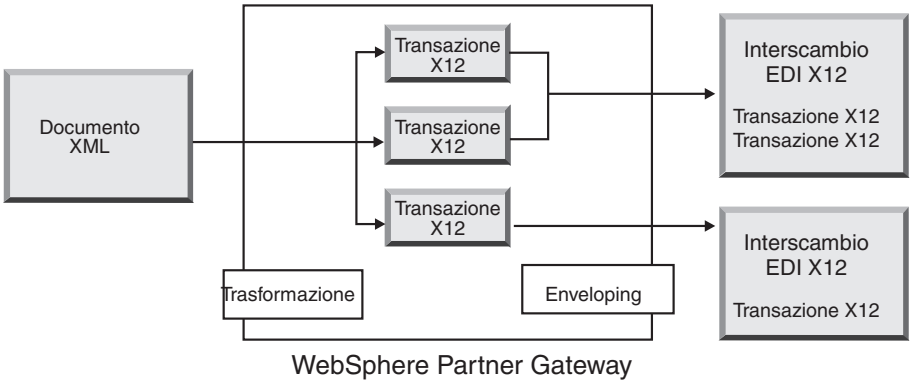


Figura 26. Flusso di documenti XML in più transazioni EDI

Flusso da più documenti XML o ROD allo scambio EDI

WebSphere Partner Gateway può ricevere un file, costituito da uno o più documenti XML o ROD da un partner o dal partner interno, convertire il documento o i documenti nelle transazioni EDI, eseguire l'enveloping delle transazioni EDI in più buste ed inviarli al partner o al partner interno.

Ciascun documento può essere convertito in una singola transazione o se è stato utilizzato il concatenamento della mappa, più transazioni.

Notes:

1. I documenti inviati in un file devono essere dello stesso tipo, sia che si tratti di documenti XML che di documenti ROD, ma non entrambi.
2. I documenti ROD devono essere dello stesso tipo.

Figura 27 a pagina 173 illustra una serie di documenti XML da separare in documenti XML singoli. I documenti XML vengono convertiti in transazioni X12 e le transazioni vengono sottoposte a enveloping.

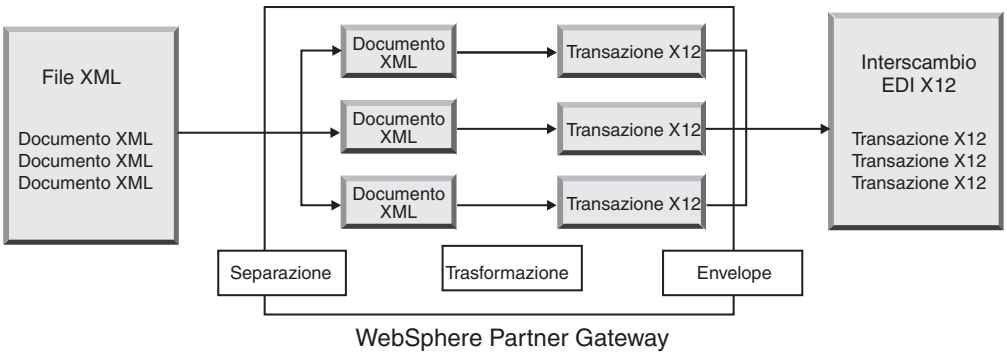


Figura 27. Flusso di più documenti XML in scambio EDI

Nella Figura 27, i documenti vengono divisi (mediante l'handler splitter XML) e le transazioni convertite vengono sottoposte a enveloping insieme. L'handler splitter XML deve includere l'opzione BCG_BATCHDOCS impostata su on (valore predefinito) affinché si verifichi questo scenario. Se BCG_BATCHDOCS è stato impostato su on ed è attivo il modo batch dell'Enveloper, queste transazioni possono essere sottoposte a enveloping nella stessa busta EDI. L'attributo per il modo batch dell'Enveloper viene descritto nella sezione "Modalità batch" a pagina 182.

Flusso da XML a ROD o da ROD a XML

WebSphere Partner Gateway può ricevere un documento XML o ROD da un partner o dal partner interno, convertire il documento in un'altra tipologia (da XML a ROD o da ROD a XML), quindi inviare il documento al partner o al partner interno.

La Figura 28 mostra una serie di documenti XML convertiti in documenti ROD.

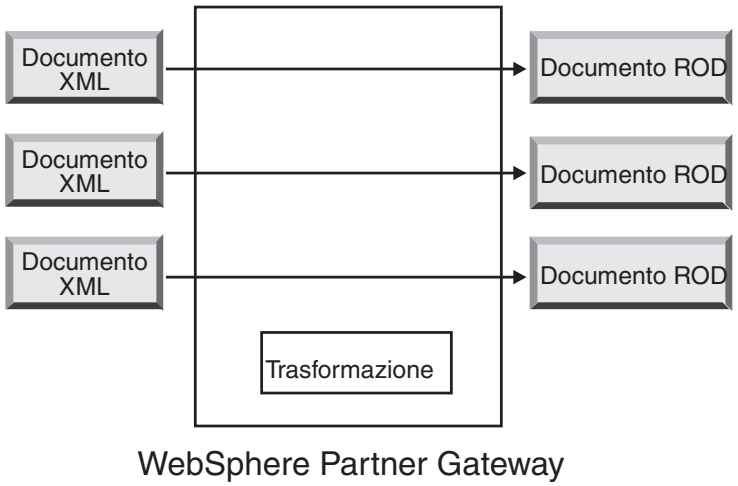


Figura 28. Flusso di documenti XML in documenti ROD

Il documento può essere convertito in un singolo documento oppure se è stato utilizzato il concatenamento delle mappe, in più documenti.

Flusso da XML a XML o da ROD a ROD

WebSphere Partner Gateway può ricevere un documento XML o ROD da un partner o dal partner interno, convertirlo in un documento della stessa tipologia (da XML a XML o da ROD a ROD) ed inviare quindi il documento al partner o al partner interno.

La Figura 29 mostra i documenti XML, convertiti in documenti XML di un formato diverso.

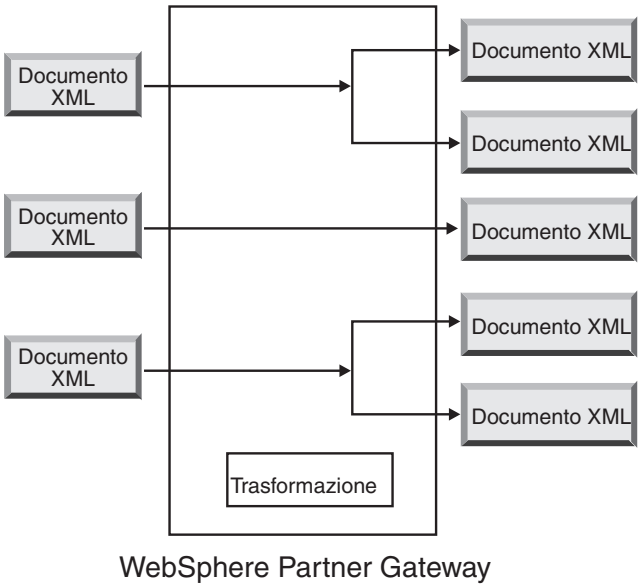


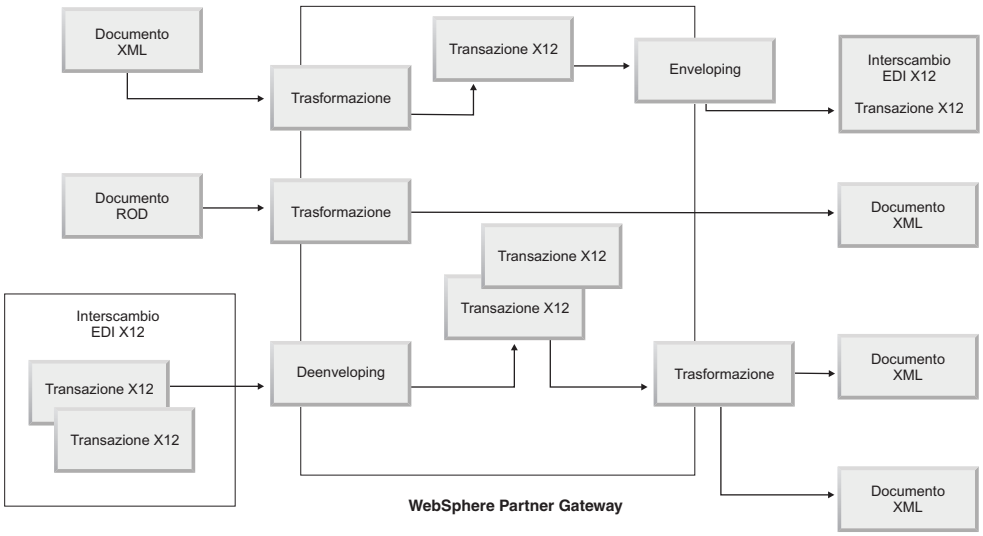
Figura 29. Flusso di documenti XML in documenti XML

Il documento può essere convertito in un singolo documento oppure se è stato utilizzato il concatenamento delle mappe, in più documenti.

Flusso da qualsiasi formato a qualsiasi formato

WTX consente di effettuare conversioni da qualsiasi formato a qualsiasi formato. WTX design studio viene utilizzato per creare mappe. I vari flussi sono: da ROD a qualsiasi, da XML a qualsiasi e da EDI a qualsiasi. Ovunque richiesto configurare lo splitter per suddividere i documenti. Nel caso in cui ROD è il documento di origine, devono essere anche impostate le informazioni di instradamento. Il formato XML fornisce le informazioni di instradamento necessarie se XML è il documento di origine. Le azioni differenti per i flussi differenti sono:

- Da ROD a qualsiasi - Conversione WTX
- Da XML a qualsiasi - Conversione WTX
- Da EDI a qualsiasi - Deenveloping-EDI se si desidera eseguire il deenveloping dello scambio nelle transazioni. Quindi le azioni di Reenveloper EDI e di conversione WTX vengono utilizzate per il reenveloping delle transazioni e per la conversione delle stesse dal formato EDI - a qualsiasi. Convalida EDI se le transazioni devono essere convalidate. Utilizzare Convalida scambio EDI se si desidera convalidare lo scambio senza eseguire il deenveloping.



Panoramica sui motori di conversione

WebSphere Partner Gateway supporta due motori di conversione differenti - WDI nativo e WTX.

WDI nativo - Le mappe di conversione vengono create nel client DIS per il WDI nativo. Le varie azioni fornite da WebSphere Partner Gateway per l'integrazione con WDI sono: Deenveloping EDI, Conversione CEDI, Convalida EDI, Reenveloping EDI, Enveloping EDI, Conversione ROD e Conversione XML. Non esiste alcuna configurazione separata richiesta per l'integrazione poiché si tratta di WDI nativo.

WTX - Le mappe di conversione vengono create utilizzando WTX Design Studio. Le varie azioni fornite da WebSphere Partner Gateway per l'integrazione con WTX sono Conversione WTX, Convalida scambio EDI, Deenveloping EDI, Convalida EDI, Reenveloping EDI e Enveloping EDI. RMI e nativo sono due approcci per WTX. RMI è consigliato nel caso in cui WTX non sia installato nella stessa macchina come WebSphere Partner Gateway. Le fasi per richiamare WTX in modalità remota sono le seguenti:

1. Nella directory DTXHome, aprire il file rmiserver.properties e modificare le proprietà. Ad esempio, è possibile impostare il numero della porta.
2. Dalla directory DTXHome, eseguire startrmiserver.bat.
3. Nelle proprietà della Console comune, fornire il nome host (dove il server RMI è in esecuzione) e il numero della porta. Impostare l'opzione del server RMI su Sì.
4. Fornire l'ubicazione fisica della mappa.

Per un approccio nativo, impostare il percorso di sistema come directory Home WTX. Inoltre, impostare la proprietà su No per rmiuseserver.

Transazioni busta da backend

Quando si utilizza WTX in casi asincroni, l'applicazione di backend utilizza le transazioni EDI generate da WTX e le invia a WebSphere Partner Gateway per l'enveloping con lo standard package di backend. Le intestazioni di backend predefinite vengono utilizzate per fornire dettagli di una transazione

(x-aux-senderid, x-aux-receiverid, x-aux-protocol, x-aux-protocol-version, x-aux-process-type, x-aux-process-version e BCG_DOCSYNTAX). Le intestazioni package di backend conterranno le informazioni sul Protocollo/Dizionario-EDI (X12v4R1) e le informazioni sulla transazione del processo (850) per le intestazioni specificate precedentemente. Fare riferimento alla sezione relativa all'azione di enveloping WTX.

Modalità di elaborazione degli scambi EDI

Uno scambio EDI ricevuto sull'hub è, di solito, sottoposto a deenveloping e le singole transazioni elaborate. Spesso, le transazioni EDI (come ad esempio X12 850 o EDIFACT ORDERS, che rappresenta un ordine di acquisto) vengono convertite in un formato che può essere compreso da un'applicazione di back-end. Inoltre, un riconoscimento funzionale viene spesso inviato al partner per indicare la ricezione dello scambio. Lo scambio degli scambi EDI, quindi, richiede più azioni (Deenveloping EDI, Conversione EDI, Convalida EDI, Enveloping EDI, Scambio convalida EDI, Rienveloping EDI, Conversione WTX e Busta WTX). Se, ad esempio, lo scambio contiene due transazioni e non viene richiesto alcun riconoscimento, WebSphere Partner Gateway effettua le seguenti azioni:

1. Esegue il deenveloping dello scambio

   WebSphere Partner Gateway estrae le informazioni sullo scambio dall'intestazione della busta e i segmenti dell'elemento di coda ai livelli di scambio, gruppo e transazione. Le informazioni possono includere:

   - Al livello dello scambio, gli identificativi di business dei partner che inviano e ricevono, l'indicatore di utilizzo, che specifica se lo scambio indica un ambiente di produzione o di test e la data e l'ora di preparazione dello scambio
   - Al livello del gruppo, gli identificativi dell'applicazione del mittente e del destinatario e la data e l'ora in cui è stato preparato il gruppo
   - Al livello della transazione, il tipo di transazione (come, ad esempio, X12 850 o EDIFACT ORDERS)
   - Se è richiesta la convalida per singole transazioni, viene eseguito il deenveloping dell'EDI. Dopo l'esecuzione della convalida, viene eseguito l'enveloping delle transazioni convalidate e queste vengono inviate al motore di conversione (WDI o WTX per l'elaborazione) o alla destinazione in base all'azione.
2. Converte la prima transazione secondo la mappa associata.
3. Converte la seconda transazione secondo la mappa associata.
4. Consegna i documenti convertiti all'applicazione di back-end.

In modo analogo, quando l'hub invia un documento o dei documenti creati nell'applicazione di back-end del partner interno, i documenti vengono convertiti in transazioni EDI standard. Le transazioni EDI risultanti vengono sottoposte a enveloping prima di essere inviate al partner. Come nel caso di ricezione di uno scambio EDI, vengono richieste più azioni per creare, eseguire l'enveloping ed inviare uno scambio EDI.

Le transazioni, i gruppi e gli scambi vengono identificati dai numeri di controllo. WebSphere Partner Gateway imposta questi numeri quando si verifica uno scambio. Si possono personalizzare i numeri di controllo, come descritto in "Numeri di controllo" a pagina 191.

La seguente illustrazione offre un quadro di insieme del modo in cui uno scambio EDI, impacchettato come AS, viene inviato da un partner, con l'eventuale obiettivo

di distribuire due documenti XML convertiti a due diverse destinazioni sul sistema di back-end del partner interno. In questo esempio, le transazioni 850 vengono convertite in ordini di acquisto che possono essere elaborati da un'applicazione di back-end. Le transazioni 890 vengono convertite in ordini di spedizione di magazzino che possono essere elaborati dall'applicazione di back-end.

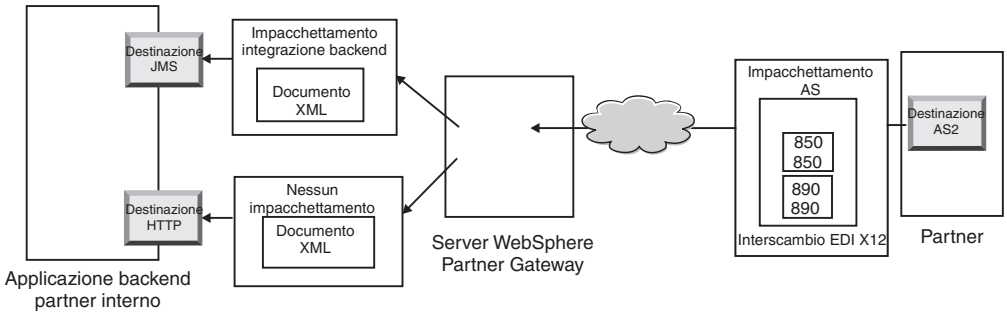


Figura 30. Flusso generale da un partner al partner interno

Anziché una connessione dal partner al partner interno, questo scambio richiede tre connessioni:

- Una dal partner all'hub per eseguire il deenveloping dello scambio. Poiché questa è una fase intermedia (viene eseguito il deenveloping dello scambio ma non viene recapitato al partner), il lato destinazione della connessione partner è N/A (non applicabile).

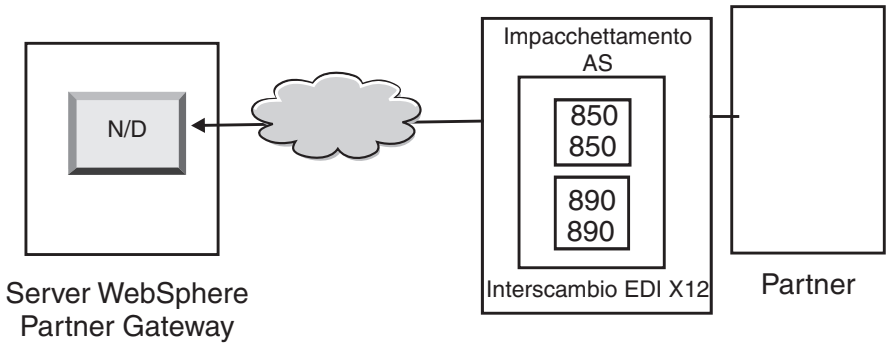


Figura 31. Connessione di deenveloping

- Una per la prima transazione da convertire e distribuire alla destinazione JMS del partner interno e una per la seconda transazione da convertire e inviare alla destinazione HTTP del partner interno.

  Per le transazioni, l'impacchettamento di origine non è applicabile, poiché le transazioni sono arrivate nello scambio di origine che era stato sottoposto a deenveloping dal sistema. Quindi, l'origine delle transazioni deve disporre dell'**Impacchettamento: N/A** specificato nella connessione del partner.

  Per la transazione convertita in XML e che passa all'applicazione di back-end mediante JMS, la destinazione sulla connessione del partner di questa transazione deve essere specificata come destinazione JMS del partner interno. Per la transazione convertita in XML e che passa all'applicazione di back-end mediante HTTP, la destinazione sulla connessione del partner di questa transazione deve essere specificata come una destinazione HTTP.

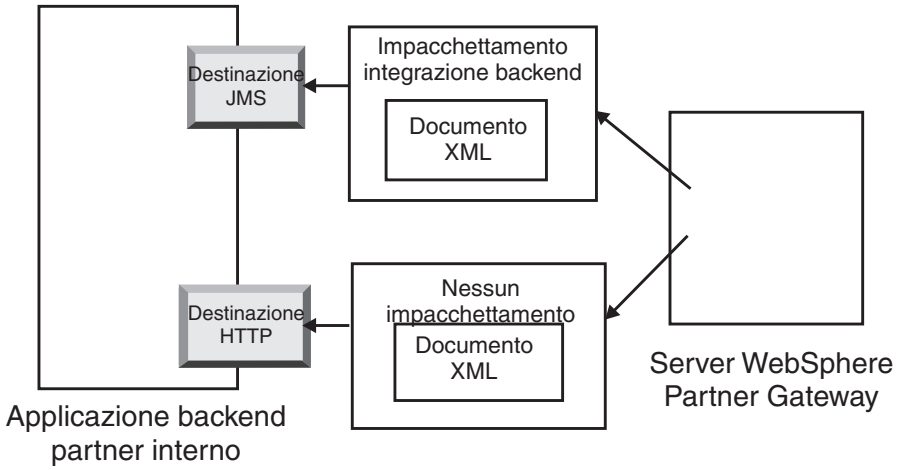


Figura 32. Connessioni per singole transazioni

È possibile utilizzare il visualizzatore documenti per visionare lo scambio e le singole transazioni, che, nei termini del visualizzatore documenti, sono gli *elementi child* dello scambio. Utilizzando il visualizzatore di documenti, è possibile visualizzare gli elementi child associati allo scambio di origine o di destinazione ed è possibile visualizzare gli eventi associati. Il Visualizzatore documenti è descritto nella sezione "Viewing Events and Documents" del manuale *WebSphere Partner Gateway Administrator Guide*.

Se il mittente richiede riconoscimenti, sono necessarie connessioni aggiuntive:

- Una per ciascun riconoscimento inviato nuovamente al partner. I riconoscimenti funzionali sono stati creati dal sistema, e, quindi, l'origine della connessione del partner deve specificare **Impacchettamento: N/A**. I riconoscimenti funzionali vengono sottoposti a enveloping prima di essere distribuiti e, quindi, per la destinazione della connessione del partner deve essere specificato **Impacchettamento: N/A**. L'Enveloper raccoglie questi riconoscimenti secondo la pianificazione impostata. Per le informazioni sull'impostazione della pianificazione, consultare la sezione "Enveloper" a pagina 182.
- Una per eseguire l'enveloping dei riconoscimenti prima che vengano inviati di nuovo al partner. La busta viene creata dal sistema e, pertanto, l'origine della connessione del partner deve specificare **Impacchettamento: N/A**. La destinazione della connessione del partner deve avere la destinazione impostata sulla destinazione del partner e, in tal caso, con **Package: AS specificato**. È possibile utilizzare una busta predefinita per lo standard EDI oppure è possibile utilizzare delle buste personalizzate. Per le informazioni sulla personalizzazione delle buste, consultare la sezione " Profili busta" a pagina 184.

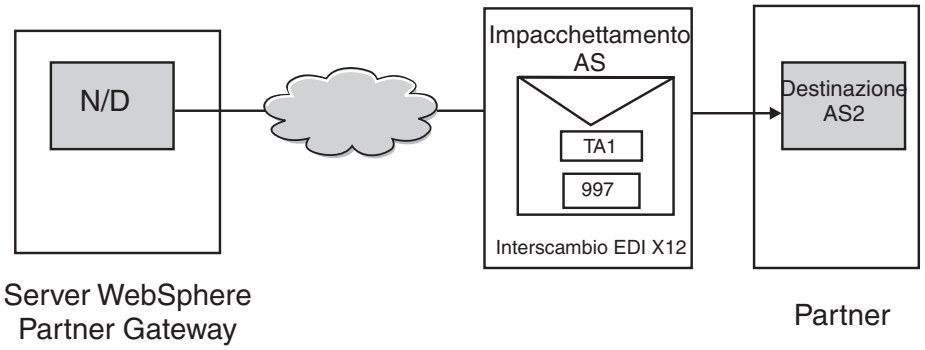


Figura 33. Enveloping ed invio di riconoscimenti al creatore

Conversione sincrona

WTX fornisce la possibilità di convertire un formato qualsiasi in un formato qualsiasi utilizzando una singola mappa. Viene fornita un'opzione per effettuare direttamente chiamate all'API WTX per la conversione. La conversione convalidata e di cui è stato eseguito il deenveloping viene inviata a WTX per l'elaborazione dopo l'enveloping.

Nota: per i diversi formati EDI disponibili, consultare l'argomento "Panoramica su EDI" a pagina 163.

Un output - l'attributo di instradamento determina se il documento di output deve essere reintrodotto nel flusso di lavoro o se deve essere inviato direttamente al flusso di lavoro in uscita per l'elaborazione.

Più output - basati sull'indicatore di instradamento, quello child verrà inviato direttamente al flusso di lavoro in uscita o reinstradato nel flusso di lavoro in entrata fisso per fare in modo che passi attraverso un nuovo canale.

Conversione asincrona

Quando un partner interno invia un messaggio al partner esterno in modalità asincrona, il partner esterno può utilizzare WESB/WMB o WTX per la conversione. La configurazione non è necessaria poiché WTX è considerato una destinazione JMS. WTX invia il documento dopo l'elaborazione al backend e non esiste un ritorno del flusso di informazioni a WebSphere Partner Gateway. Il documento EDI verrà contrassegnato per essere inviato dopo la riuscita del recapito al gateway JMS.

Modalità di elaborazione di documenti XML o ROD

Un documento XML o ROD viene ricevuto sull'hub come singolo documento o come gruppo nello stesso file. Quando un gruppo di documenti nello stesso file viene ricevuto sull'hub, WebSphere Gateway esegue le seguenti azioni:

1. Separa la serie di documenti in documenti singoli.
2. Converte ogni documento secondo la mappa associata.
3. Se i documenti vengono convertiti in transazioni EDI, impacchetta le transazioni e le consegna all'applicazione di back-end. Se i documenti vengono convertiti in documenti XML o ROD, vengono consegnati convertiti all'applicazione di back-end.

Se il documento XML o ROD arriva come singolo documento, WebSphere Partner Gateway esegue le seguenti azioni:

1. Converte il documento secondo la mappa associata.
2. Se il documento viene convertito in una transazione EDI, impacchetta la transazione e la consegna all'applicazione di back-end. Se il documento viene convertito in un documento XML o ROD, il documento viene consegnato all'applicazione di back-end.

In modo analogo, quando l'hub invia un documento o dei documenti creati nell'applicazione di back-end del partner interno, i documenti vengono convertiti in documenti XML o ROD o in transazioni EDI. Per le transazioni EDI, le transazioni vengono sottoposte a enveloping prima di essere inviate al partner. Come nel caso di ricezione di uno scambio EDI, sono richieste più azioni per convertire il documento o i documenti, eseguire l'enveloping delle transazioni risultanti ed inviare lo scambio EDI.

Integrazione Enveloping WTX e mappa Polimorfica

In WebSphere Partner Gateway, la struttura ad albero del tipo di metadati è definita. E' possibile configurare e fornire informazioni sul tipo di dati in ciascuna scheda. Di solito, le seguenti proprietà sono previste per essere configurate. I valori e i nomi di proprietà sono sensibili alle maiuscole e alle minuscole. Solo i valori booleani non sono sensibili alle maiuscole e alle minuscole.

Tabella 25. Proprietà della struttura ad albero del tipo di metadati

Nome proprietà	Valore proprietà	Descrizione
BCG_DOCSYNTAX	EDI_INTERCHANGE EDI_TRANSACTION XML ROD	EDI_INTERCHANGE deve essere impostato se l'output è uno scambio EDI di cui è stato eseguito l'enveloping. EDI_TRANSACTION deve essere impostato se l'output è una conversione EDI e di cui non è stato eseguito l'enveloping. XML e ROD deve essere impostato di conseguenza per l'output XML e ROD.
BCG_REENVELOPE	true/false	Se il valore è true e BCG_DOCSYNTAX è EDI_INTERCHANGE verrà eseguito il Deenveloping della busta EDI. Dopo aver eseguito il Deenveloping ogni transazione creata verrà considerata come un documento singolo per operazioni future.
BCG_REROUTE	true/false	Se il valore è true, il documento verrà reinstradato. Se il valore false e l'output è singolo, il BDO esistente verrà aggiornato con il nuovo file e inviato.
ProtocolName	Come appropriato	Il nome del protocollo del documento di output. Obbligatorio nel caso in cui ReRoute è impostato su true. Questo verrà utilizzato per acquisire il canale per il documento reinstradato.

Tabella 25. Proprietà della struttura ad albero del tipo di metadati (Continua)

Nome proprietà	Valore proprietà	Descrizione
ProtocolVersion	Come appropriato	La versione del protocollo del documento di output. Obbligatorio nel caso in cui ReRoute è impostato su true. Questo verrà utilizzato per acquisire il canale per il documento reinstradato.
ProcessCode	Come appropriato	Il codice del processo del documento di output. Obbligatorio nel caso in cui ReRoute è impostato su true. Questo verrà utilizzato per acquisire il canale per il documento reinstradato.
ProcessVersion	Come appropriato	La versione del processo del documento di output. Obbligatorio nel caso in cui ReRoute è impostato su true. Questo verrà utilizzato per acquisire il canale per il documento reinstradato.
SegmentCountElementName	SE01/UNT01	Se l'output è EDI_TRANSACTION è necessario specificare questo attributo. Questo attributo deve essere impostato in base al tipo di enveloping desiderato.
SegmentCount	Come appropriato	Se l'output è EDI_TRANSACTION è necessario specificare questo attributo. Questo attributo conterrà le informazioni sul numero di segmenti nella transazione.

Se la destinazione è EDI dopo conversione, è necessario eseguire l'enveloping prima di inviarlo ai partner esterni. Il documento di output convertito può avere qualsiasi combinazione di formati. Questo dipende dagli elementi codificati nel numero di scheda della scheda dei metadati. Questo conterrà le proprietà di altri dettagli della scheda. Il creatore della mappa codificherà la scheda. Gli attributi differenti che vengono considerati sono ReRoute, ReEnvelope e DocSyntax. ReRoute e ReEnvelope possono avere i valori True o False, mentre DocSyntax può avere qualsiasi valore immesso dall'utente. Solo se il valore per DocSyntax è ediInchg, verrà considerato per il deenveloping. Quanto segue contiene le spiegazioni relative al risultato possibile della combinazione differente dei valori di ReRoute e ReEnvelope. Si presume che docSyntax sia impostato su EDI_INTERCHANGE:

- ReRoute = True, ReEnvelope = False: il documento viene elaborato in modo simile a qualsiasi altro documento (XML o ROD).
- ReRoute = False, ReEnvelope = False: il documento viene elaborato in modo simile a qualsiasi altro documento (XML o ROD).
- Reroute = True, ReEnvelope = True: per prima cosa viene eseguito il Deenveloping del documento. Per ognuna delle transazioni secondarie, viene creato un bdo secondario. Il dizionario e il documento vengono impostati come protocollo e processo. Ogni ChildBDO (Transazione) viene reinstradato con il package N/A. Deve essere presente un canale appropriato. Il profilo dell'enveloper può essere configurato negli attributi di destinazione di questo canale. E' necessario creare un canale separato per il passaggio della busta.
- Reroute = False, Reenvelope = True: per prima cosa viene eseguito il Deenveloping del documento. Se la singola transazione viene creata come output, il documento di business viene aggiornato con il file di transazione come ubicazione e inviato. Se vengono create molte transazioni come output, i BDO

secondari vengono creati senza essere reinstradati e inviati. L'attributo di destinazione di questo canale è previsto per essere configurato in modo appropriato per il profilo dell'enveloper. Deve essere presente un canale per il passaggio dell'enveloper.

Impostazione dell'ambiente EDI

Come menzionato nella sezione precedente, è possibile specificare molti attributi che riguardano lo scambio di scambi EDI. Ad esempio, è possibile modificare i profili busta forniti dal prodotto, definire specifiche buste da utilizzare per determinate connessioni, impostare i numeri di controllo assegnati alle varie parti di uno scambio ed impostare i profili di connessione in modo tale che lo stesso scambio possa essere distribuito in un modo diverso. Queste attività vengono descritte in questa sezione.

Enveloper

L'Enveloper è il componente che raccoglie un gruppo di transazioni da inviare ad un partner, lo raccoglie in una busta e lo invia. Pianificare l'Enveloper (o accettare la pianificazione predefinita) per segnalare a WebSphere Partner Gateway il momento in cui si desidera che l'Enveloper cerchi le transazioni che sono in attesa per l'invio. È anche possibile aggiornare i valori predefiniti per il tempo di blocco, il periodo di accodamento e la modalità di batch.

Nota: la configurazione di Enveloper è facoltativa. Se nessun valore è stato modificato per l'Enveloper, vengono utilizzati i valori predefiniti forniti dal prodotto.

Blocco

Ogni istanza di Gestore documenti ha il proprio Enveloper. Se si dispone di due Gestori documenti installati sul sistema, si dispone di due Enveloper. Di conseguenza, è possibile, per due (o più) istanze di Enveloper di tentare di eseguire il polling delle transazioni in attesa di essere sottoposte a enveloping. Per assicurarsi che venga eseguito il polling di una determinata transazione da esattamente un Enveloper, vengono utilizzati i blocchi. I blocchi assicurano che se sono coinvolti più Enveloper, solo uno esegue il polling ed elabora una determinata transazione. Gli Enveloper eseguono il polling contemporaneamente, ma lavorano su transazioni diverse.

Sul blocco è impostato un intervallo di tempo limite. Il valore predefinito per un'istanza dell'Enveloper per il blocco è di 250 secondi.

Se Enveloper deve attendere il blocco, viene posizionato in una coda. Il tempo massimo di accodamento (periodo di tempo di attesa di Enveloper) è pari a 740 secondi.

In genere, non è necessario modificare i valori predefiniti per il blocco.

Modalità batch

Più documenti che arrivano in un file vengono divisi, in base all'handler splitter configurato per quel tipo di documento. (La configurazione degli handler splitter, che è parte della definizione delle destinazioni, è descritta nella sezione " Modifica dei punti di configurazione" a pagina 72.) Uno degli attributi dell'handler splitter è BCG_BATCHDOCS. Quando BCG_BATCHDOCS è stato impostato su on (valore predefinito) lo splitter aggiunge gli ID di batch ai documenti una volta divisi.

L'Enveloper dispone di un attributo per la modalità batch, correlato all'attributo BCG_BATCHDOCS. Se gli ID di batch sono stati assegnati ai singoli documenti e se si accetta il valore predefinito (on) per la modalità batch, l'Enveloper assicura che tutti i documenti che arrivano nello stesso file siano elaborati prima di eseguire l'enveloping ed inviarli, per garantire che le transazioni siano sottoposte a enveloping insieme. Ad esempio, si supponga che cinque documenti XML arrivino nello stesso file. I documenti XML devono essere convertiti in transazioni EDI e consegnati allo stesso destinatario. Dopo che solo tre documenti sono stati convertiti, l'Enveloper inizia il polling pianificato per le transazioni. Se si seleziona la modalità batch, l'Enveloper non elabora (operazione di enveloping) le tre transazioni pronte. Al contrario, attende finché non termina l'elaborazione delle cinque transazioni prima di eseguire l'enveloping ed inviarle. Le transazioni vengono messe nella stessa busta, a meno che lo standard EDI applicabile non lo impedisca.

Modifica dei valori predefiniti

Informazioni su questa attività

Per modificare i valori predefiniti per l'Enveloper, effettuare i passi di seguito riportati:

1. Fare clic su **Amministrazione hub > Configurazione hub > EDI > Enveloper**.
2. Fare clic sull'icona **Modifica**.
3. Immettere nuovi valori per **Tempo max blocco (secondi)** e **Durata accodamento massima (secondi)** se si desidera più o meno tempo assegnato a questi attributi.

   Nota: in genere, non è necessario modificare i valori predefiniti.
4. Se si desidera disattivare la modalità batch, deselezionare **Utilizza modalità batch**.
5. Se si desidera modificare la frequenza con cui Enveloper controlla le transazioni in attesa di essere inviate, eseguire uno dei seguenti gruppi di attività:
   - Per utilizzare la pianificazione basata sull'intervallo (che è il valore predefinito) ma modificare la quantità di tempo, immettere un nuovo orario accanto a **Intervallo**. Se, ad esempio, si modifica il valore in 30 secondi, Enveloper controllerà i documenti, li imbusterà e li invierà al destinatario.
   - Per utilizzare la pianificazione basata sul calendario, eseguire le seguenti attività:
     a. Fare clic su **Pianificazione basata sul calendario**.
     b. Scegliere il tipo di pianificazione (**Pianificazione giornaliera**, **Pianificazione settimanale** o **Pianificazione personalizzata**).
        - Se si seleziona **Pianificazione giornaliera**, selezionare il giorno (le ore e i minuti) quando Enveloper controlla i documenti.
        - Se si seleziona **Pianificazione settimanale**, selezionare uno o più giorni della settimana oltre all'ora del giorno.
        - Se si seleziona **Pianificazione personalizzata**, selezionare l'ora del giorno e scegliere **Intervallo** o **Giorni selettivi** per la settimana e il mese. Con **Intervallo**, si specifica la data di inizio e quella di fine. (È possibile, ad esempio, fare clic su **Lun** e **Ven**, se si desidera che Enveloper controlli i documenti ad una certa ora solo settimanalmente). Con **Giorni selettivi**, si scelgono i giorni specifici della settimana e del mese.
6. Fare clic su **Salva**.

Profili busta

Un profilo busta stabilisce i valori posizionati in elementi specifici della busta. Assegnare il profilo busta alle transazioni EDI nell'attributo **Profilo busta** della definizione del documento. WebSphere Partner Gateway fornisce un profilo busta per ogni standard supportato (X12, EDIFACT o UCS). È possibile utilizzare queste buste predefinite direttamente, modificarle o copiarle in nuovi profili della busta. Le fasi per modificare o creare un profilo busta sono descritte nella sezione "Modifica dei valori predefiniti" a pagina 185.

I profili Busta hanno un campo per ogni elemento nello standard della busta. I profili forniscono dati letterali e costanti per la creazione dei segmenti di intestazione e dell'elemento di coda per gli insiemi di transazioni, i messaggi, i gruppi funzionali e gli scambi. Sono forniti solo i valori che devono essere inseriti e per i quali non viene fornito alcun valore da un'altra origine.

I nomi di campo vengono designati per semplificare il riferimento incrociato. Ad esempio, il campo UNB03 è il terzo elemento dati nel segmento UNB.

Come descritto nella sezione " Attributi busta", gli attributi impostati ovunque hanno la precedenza sui valori impostati nel profilo busta. Alcuni attributi possono essere sovrascritti nelle mappe o negli attributi relativi alla definizione del documento.

Attributi busta

Durante il processo di configurazione, gli attributi busta possono essere impostati in diversi punti e possono essere impostati anche nella mappa di conversione associata ai documenti. Ad esempio, lo specialista della mappatura del client Data Interchange Services può specificare la proprietà CtlNumFlag quando si definisce una mappa. Inoltre, questa proprietà può essere impostata anche come parte del profilo busta (nel campo **Numeri di controllo per ID transazione**). Gli attributi impostati nella mappa di conversione possono sostituire i valori correlati impostati sulla Console comunità. Ad esempio, se CtlNumFlag è impostato nella mappa della conversione come **N** (no) e viene immesso un valore **S** (sì) nel campo **Numeri di controllo per ID della transazione**, il valore **N** è quello utilizzato.

Gli altri profili busta possono essere impostati al livello del protocollo (nella pagina Gestisci le definizioni di documento o nella pagina Capacità B2B associata ad un partner) oppure possono essere impostati come parte della connessione. L'ordine di precedenza viene riportato nel seguente elenco:

1. Le proprietà impostate nella mappa di conversione hanno la precedenza sugli attributi impostati nella Console comunità.
2. Gli attributi impostati sul livello della connessione hanno la precedenza sugli attributi impostati sul livello delle capacità B2B.
3. Gli attributi impostati al livello delle capacità B2B hanno la priorità su quelli impostati al livello della definizione del documento.
4. Gli attributi impostati ovunque (nella mappa di conversione o al livello della connessione, delle capacità B2Bo della definizione del documento) hanno la priorità sui valori impostati nel profilo busta.

Per un elenco delle proprietà della mappa di conversione e gli attributi del Gestore comunità associati, consultare la sezione "Proprietà del client Data Interchange Services" a pagina 424.

Modifica dei valori predefiniti

Informazioni su questa attività

La sezione " Attributi del profilo di busta" a pagina 413 fornisce una tabella che mostra i valori predefiniti utilizzati per ogni attributo standard EDI, se non si immette un valore nel profilo o se non si crea il profilo. Verificare che i profili della busta utilizzati forniscano elementi obbligatori non forniti dal sistema al runtime.

Per impostare un profilo della busta, eseguire i questi passaggi:

1. Fare clic su **Amministrazione hub > Configurazione hub > EDI > Profilo busta**.
2. Eseguire uno dei seguenti gruppi di passaggi:
   - Creare una busta
     a. Fare clic su **Crea**.
     b. Inserire un nome per il profilo busta. Si tratta del nome che apparirà nell'elenco dei profili busta.
     c. In alternativa, inserire una **Descrizione** del profilo.
     d. Fare clic su **Standard EDI** a cui appartiene la busta. Se, ad esempio, si scambiano documenti conformi allo standard EDI-X12, selezionare **X12**.
   - Modificare una busta
     a. Selezionare uno dei profili busta esistenti facendo clic sull'icona **Visualizza i dettagli** accanto al nome del profilo.
     b. Fare clic sull'icona **Modifica**.
3. Il pulsante **Generale** viene scelto per impostazione predefinita. Si può immettere un valore per qualsiasi campo tranne che per ENVTYPE, che è già riempito con lo standard scelto nel passaggio 2d.

   Si possono aggiungere valori per i seguenti campi:
   - **Lunghezza numero di controllo dello scambio**, per indicare come molti caratteri devono essere utilizzati quando viene assegnato un numero di controllo ad uno scambio all'interno della busta.
   - **Lunghezza numero di controllo del gruppo**, per indicare come molti caratteri devono essere utilizzati quando viene assegnato un numero di controllo ad un gruppo all'interno della busta.
   - **Lunghezza numero di controllo della transazione**, per indicare come molti caratteri devono essere utilizzati quando viene assegnato un numero di controllo ad una transazione all'interno della busta.
   - **Numero max di transazioni**, per indicare il numero massimo di transazioni consentite in questa busta.
   - **Numeri di controllo per ID transazione**, per indicare se si desidera utilizzare l'ID transazione (come parte della chiave) quando i numeri della serie vengono ricercati nel database. Quindi, serie separate di numeri di controllo vengono utilizzate per ciascun ID della transazione.

   I campi per il profilo busta Generale sono gli stessi in tutti e tre gli standard, tranne che per EDIFACT che ha un campo aggiuntivo: **Crea gruppi per EDI**.

   Se si sono apportate modifiche alla pagina Generale, fare clic su **Salva**.
4. Per specificare i valori per lo scambio, fare clic su **Scambio**. Nella pagina vengono visualizzati nuovi campi. I campi variano in base allo standard EDI. Si noti che alcuni valori sono già riempiti o lo saranno in fase di runtime.
   - Per lo standard EDI-X12, è possibile modificare i seguenti campi:

- **ISA01: Qualificatore informazioni autorizzazione**, ovvero il codice per il tipo di informazioni in ISA02.
- **ISA02: Informazioni autorizzazione**, le cui informazioni sono utilizzate per identificare o autorizzare ulteriormente il mittente dei dati di scambio.
- **ISA03: Qualificatore informazioni di sicurezza**, ovvero un codice per il tipo di informazioni in ISA04. I valori possibili sono:

  00 ISA04 non è significativo

  01 ISA04 contiene una password
- **ISA04: Informazioni sulla sicurezza**, ovvero informazioni sulla sicurezza per il mittente o i dati di scambio. il codice in ISA03 definisce il tipo di informazioni.
- **ISA11: ID standard di scambio**, ovvero un codice per l'agenzia che controlla lo scambio. I valori appropriati sono: **U** (comunità US EDI di ASC X12), **TDCC** e **UCS**.

  Nota: questo attributo viene utilizzato per le versioni da X12 a 4010. In X12 4020, viene utilizzato l'elemento ISA11 per il separatore di ripetizione.
- **ISA12: ID versione scambio**, ovvero il numero di versione della sintassi utilizzata nei segmenti di scambio e di controllo del gruppo funzionale.
- **ISA14: riconoscimento richiesto**, ovvero il codice del mittente per richiedere un riconoscimento. I valori possibili sono:

  0 Non richiedere riconoscimento

  1 Richiedi un riconoscimento per la ricezione ed il riconoscimento dei segmenti ISA e IEA
- **ISA15: Indicatore di prova**, ovvero un'indicazione che lo scambio è per prova o produzione. I valori possibili sono:

  T Per dati di prova

  P Per dati di produzione

- Per lo standard UCS, è possibile modificare i seguenti campi:
  - **BG01: ID comunicazioni**, ovvero l'identificazione dell'azienda di trasmissione.
  - **BG02: Password comunicazioni**, che indica una password assegnata dal destinatario, viene utilizzata come concordata dai partner.
- Per lo standard EDIFACT, è possibile modificare i seguenti campi:
  - **UNB0101: ID sintassi**, ovvero l'identificativo dell'agenzia che controlla la sintassi utilizzata. L'agenzia di controllo è UNO. Il livello è A o B.
  - **UNB0102: Versione sintassi**, ovvero il numero di versione della sintassi utilizzata dall'ID sintassi.
  - **UNB0601: Riferimento/password destinatari**, che indica una password assegnata dal destinatario, viene utilizzata come concordata dai partner.
  - **UNB0602: Qualificatore riferimento/password destinatari**, che indica un qualificatore per la password del destinatario, viene utilizzata come concordata dai partner.
  - **UNB07: Riferimento applicazione**, ovvero l'identificativo del mittente dell'area funzionale cui sono correlati i messaggi di scambio.
  - **UNB08: Priorità**, che indica il codice del mittente per elaborare la priorità, come concordata con il partner. Il codice A è la massima priorità.

- **UNB09: Richiesta di riconoscimento**, ovvero il codice del mittente per la richiesta di un riconoscimento.
- **UNB10: ID accordo comunicazioni**, che indica il nome o il codice per il tipo di accordo utilizzato per questo scambio, come concordato con il partner.
- **UNB11: Indicatore di prova (Indicatore di utilizzo)**, ovvero un indicatore del fatto che lo scambio è per prova. 1 indica uno scambio di prova.

Se si sono apportate modifiche alla pagina Scambio, fare clic su **Salva**.

5. Per specificare i valori dei gruppi nello scambio, fare clic su **Gruppo**. Viene visualizzato un nuovo insieme di campi. I campi variano in base allo standard EDI.

   I campi visualizzati in questa pagina definiscono il mittente e il destinatario del gruppo.

   - Per gli standard EDI-X12 e UCS, è possibile immettere valori nei seguenti campi:
     - **GS01: ID gruppo funzionale**, ovvero un identificativo del tipo di transazione impostata nel gruppo.
     - **GS02: Mittente applicazione**, ovvero il nome o il codice per un reparto specifico nell'azienda del mittente.
     - **GS03: Destinatario dell'applicazione**, ovvero il nome o il codice per il reparto specifico dell'azienda del destinatario che deve ricevere il gruppo.
     - **GS07: Agenzia gruppo**, ovvero il codice utilizzato con GS08 per identificare l'agenzia che controlla lo standard.
     - **GS08: Versione gruppo**, ovvero il codice della versione, release e produzione dello standard.
   - Per lo standard EDIFACT, è possibile immettere valori nei seguenti campi:
     - **UNG01: ID gruppo funzione**, ovvero un identificativo del tipo di messaggi nel gruppo.
     - **UNG0201: ID mittente applicazione**, ovvero il nome o il codice per un reparto specifico dell'azienda del mittente.
     - **UNG0202: Qualificatore ID mittente applicazione**, ovvero il qualificatore per il codice dell'ID del mittente. Fare riferimento alla directory dell'elemento di dati per un elenco dei qualificatori del codice.
     - **UNG0301: ID destinatario dell'applicazione**, ovvero il nome o il codice per il reparto specifico nell'azienda del destinatario che deve ricevere il gruppo.
     - **UNG0302: Qualificatore ID destinatario applicazione**, ovvero il qualificatore per il codice ID del destinatario. Fare riferimento alla directory dell'elemento di dati per un elenco dei qualificatori del codice.
     - **UNG06: Agenzia di controllo**, il codice che identifica l'agenzia che controlla il tipo di messaggio nel gruppo funzionale.
     - **UNG0701: Versione messaggio**, ovvero il numero di versione per il tipo di messaggio.
     - **UNG0702: Release messaggio**, ovvero il numero di release all'interno del numero di versione per il tipo di messaggio.
     - **UNG0703: Associazione assegnata**, ovvero il codice, assegnato dall'associazione responsabile, che identifica ulteriormente il tipo di messaggio.
     - **UNG08: Password applicazione**, ovvero la password assegnata dal reparto specifico nell'azienda del destinatario.

Se si sono apportate modifiche alla pagina Gruppo, fare clic su **Salva**.

6. Per specificare valori per la transazione in un gruppo, fare clic su **Transazione** o, nel caso di EDIFACT, su **Messaggio**. Viene visualizzato un nuovo insieme di campi. I campi variano in base allo standard EDI.
   - Per lo standard EDI-X12 o USC, è possibile immettere un valore per **ST03: Stringa ID convenzione implementazione**.
   - Per lo standard EDIFACT, è possibile immettere un valore nei seguenti campi:
     - **UNH0201: Tipo di messaggio**, ovvero il codice assegnato dall'agenzia di controllo per identificare il tipo di messaggio.
     - **UNH0202: versione messaggio**, ovvero il numero di versione per il tipo di messaggio.
     - **UNH0203: Release messaggio**, ovvero il numero di release all'interno del numero di versione per il tipo di messaggio.
     - **UNH0204: Agenzia di controllo**, ovvero il codice per l'agenzia che controlla il tipo di messaggio.
     - **UNH0205: Codice associazione assegnato**, ovvero il codice, assegnato dal responsabile dell'associazione, che identifica ulteriormente il tipo di messaggio.
     - **UNH03: Riferimento accesso comune**, ovvero la chiave relativa a tutti i trasferimenti successivi di dati ad un file comune. I partner possono accettare l'utilizzo di una chiave, costituita dai componenti, ma non è possibile utilizzare separatori dell'elemento secondario.

   Se sono state apportate eventuali modifiche alla pagina Transazione, fare clic su **Salva**.
7. Fare clic su **Salva**.
8. Ripetere i passi da 2 a pagina 185 a 7 per altri eventuali profili busta da definire o modificare.

Una volta definito un profilo busta, esso viene visualizzato nell'elenco Profili busta. Nell'elenco, è possibile selezionare il profilo e si fa clic sull'icona **Dove utilizzato** per stabilire le connessioni mediante il profilo.

Profili di connessione

Si utilizzano profili della connessione con transazioni sottoposte a deenveloping e scambi EDI create da Enveloper. Per le transazioni, il profilo della connessione determina il modo in cui la transazione viene elaborata una volta sottoposta a deenveloping. Per gli scambi, il profilo della connessione stabilisce come viene consegnato lo scambio.

Utilizzare la finestra Profilo connessione per creare un nuovo profilo o per modificare le informazioni di un profilo esistente. Il nome di ciascun profilo definito correntemente e la sua descrizione, se ne esiste una, sono visualizzati nell'elenco dei profili di connessione. Per ulteriori informazioni sui Profili di connessione, consultare la *Guida alla configurazione dell'hub di WebSphere Partner Gateway*.

Transazioni

Quando uno scambio EDI va a finire in WebSphere Partner Gateway, la prima azione server, di solito, per eseguire l'operazione di deenveloping dello scambio in singole transazioni. Quando vengono create le transazioni, l'azione di deenveloping imposta l'**indicatore utilizzo scambio** e le informazioni sul gruppo (**Identificativo mittente applicazione di gruppo**, **Identificativo destinatario**

applicazione di gruppo e **Password applicazione gruppo**) nei metadati della transazione. Ogni transazione viene quindi elaborata di nuovo da WebSphere Partner Gateway in un flusso di lavoro personalizzato.

Si supponga di disporre di due transazioni dello stesso tipo (ad esempio, 850) che necessitano di essere gestite in modo differente, a seconda del gruppo in cui erano o in base ai valori degli indicatori di utilizzo dello scambio). Se l'**Indicatore di utilizzo** è Produzione (**P**), ad esempio, è possibile stabilire di utilizzare una mappa (A) e se l'**Indicatore di utilizzo** è Prova (**T**), utilizzare una seconda mappa (B). Due connessioni simili vengono richieste per questa transazione, con l'unica differenza che una connessione utilizza la mappa A e l'altra connessione utilizza la mappa B.

Poiché le transazioni sono le stesse (hanno lo stesso partner di origine e di destinazione, package, protocollo e tipo documento), il Gestore documenti necessita di un modo per stabilire la connessione da utilizzare. Mediante la corrispondenza della connessione con l'attributo del profilo della connessione, si impostano i metadati della transazione. In questo esempio, se si creano due profili di connessione, - uno (CPProduction) con **Tipo di utilizzo EDI** impostato su **P** e l'altro (CPTest) con il **Tipo di utilizzo EDI** impostato su **T**, il Gestore documenti trova la corrispondenza con la transazione che dispone dell'indicatore di utilizzo P con il profilo CPProduction. Sa, quindi, utilizzare la mappa A per convertire la transazione.

L'esempio in questa sezione ha utilizzato l 'attributo **Indicatore di utilizzo scambio**, ma può anche utilizzare gli attributi **Identificativo applicazione mittente gruppo**, **Identificativo applicazione destinatario gruppo** e **password applicazione gruppo** come fattore distintivo per una transazione.

Scambi

Per gli scambi, utilizzare l'attributo **Qualificatore profilo connessione 1**.

Si supponga, ad esempio, di essere al centro di una migrazione della società dall'utilizzo di una VAN (nessun impacchettamento) o di Internet (impacchettamento AS2). Si desidera transazioni 840 (Richiesta di quotazione) per utilizzare VAN e transazioni 850 (Ordine di acquisto) per utilizzare Internet. Impostare due connessioni del partner, entrambe con lo stesso scambio di origine ma con diverse destinazioni (una con nessun impacchettamento e l'altra con impacchettamento AS2). I profili connessione consentono di fare distinzione tra le due connessioni.

La configurazione del profilo della connessione per gli scambi coinvolge molti passaggi. Si tratta di passaggi da eseguire per creare due profili connessioni per l'esempio:

1. Creare due connessioni per le transazioni. Impostare l'attributo **Qualificatore profilo di connessione 1** sulla parte "A" di entrambe le connessioni. Il valore dovrebbe essere pieno di significato (ad esempio, ConNone e ConAS2).
2. Definire due profili di connessione (ad esempio, CPNone e CPAS2), ciascuno con il valore **Qualifier1** impostato in modo da corrispondere agli attributi **Profilo di connessione Qualifier1** impostati al passo 1 (ConNone e ConAS2).
3. Creare due connessioni per lo scambio. Ciascuna connessione ha uno stesso impacchettamento di origine (N/A), ma un differente impacchettamento di destinazione (Nessuno e AS2). La connessione del partner con il profilo di connessione CPNone avrà la destinazione impostata sulla destinazione Script FTP che può collegarsi a VAN. La connessione del partner con il profilo di connessione CPAS2 avrà l'impacchettamento di destinazione impostato su AS.

4. Associare il profilo di connessione appropriato a ognuno.

L'Enveloper utilizza l'attributo **Qualificatore profilo connessione 1** sulla parte ″A″ della connessione del partner come un punto di interruzione della busta. Pertanto, le transazioni con valori diversi per l'attributo **Qualificatore profilo di connessione 1** verranno sottoposte a enveloping in buste diverse. Quando si impostano valori diversi per le transazioni, l'Enveloper non imbusterà mai le transazioni 840 e 850 nello stesso scambio.

Quando Gestore documenti cerca la connessione, vengono trovate le due possibili connessioni, ma si utilizza quella con profilo corrispondente.

Impostazione di profili connessione

Informazioni su questa attività

L'impostazione di profili connessione è facoltativa. Se non è necessario disporre di più connessioni per ciascuna tipologia di documento che sarà trasmessa per un partner, ignorare questa sezione.

Per impostare un profilo di connessione:

1. Fare clic su **Amministrazione hub > Configurazione hub > EDI > Profili di connessione**.
2. Fare clic su **Crea profilo connessione**.
3. Nella pagina Dettagli del profilo connessione, immettere un nome richiesto per questo profilo connessione.
4. Inserire una descrizione facoltativa del profilo.

   Il nome e la descrizione (se si immette una descrizione) appariranno nella pagina dell'elenco dei profili connessione.
5. Facoltativamente, immettere un valore per **Qualificatore 1** per indicare il valore che determina la connessione da utilizzare per uno scambio EDI. Consultare l'argomento " Scambi" a pagina 189 per un esempio sull'utilizzo di **Qualificatore 1**.
6. Facoltativamente, immettere un valore per **Tipo di utilizzo EDI** per indicare se si tratta di una verifica, produzione o di uno scambio di informazioni. Consultare l'argomento " Transazioni" a pagina 188 per un esempio sull'utilizzo di **Tipo di utilizzo EDI**.
7. Facoltativamente, immettere un valore per **ID mittente applicazione** per indicare l'applicazione o il reparto della società associato al mittente del gruppo.
8. Facoltativamente, immettere un valore per **ID destinatario applicazione** per indicare l'applicazione o il reparto della società associato al destinatario del gruppo.
9. Facoltativamente, immettere un valore per la **Password** se richiesta tra il mittente e il destinatario dell'applicazione.
10. Fare clic su **Salva**.

Per le transazioni che si desidera inserire in determinate buste di scambio, è possibile specificare il valore di attributo **Qualificatore profilo connessione 1** che corrisponde al profilo di connessione con lo stesso valore dell'attributo **Qualificatore 1**. L'attributo **Qualificatore profilo connessione 1** può essere impostato al livello del protocollo di una definizione del documento (ad esempio, è possibile modificare gli attributi del protocollo X12V5R1 nella pagina Gestisci le definizioni di documento per indicare il profilo di connessione da utilizzare

facendo clic sul valore di attributo **Qualificatore profilo connessione 1** corrispondente). Quindi, quando si attiva la connessione dello scambio, associare il profilo di connessione facendo clic sul pulsante **Profilo di connessione** e selezionare il profilo dall'elenco.

Numeri di controllo

Enveloper utilizza numeri di controllo per fornire una numerazione univoca per scambi, gruppi e transazioni in una busta. I numeri di controllo sono stabiliti per il partner interno e per i partner esterni. Quando si verifica lo scambio dei documenti, i numeri di controllo sono stati anche creati per la *coppia* dei partner.

Per ciascun partner che dispone delle Capacità B2B EDI, è presente un gruppo di valori di inizializzazione per i numeri di controllo. Tali valori sono utilizzati alla prima creazione ed invio dello scambio EDI tra una coppia di partner. I valori di inizializzazione sono validi al partner a cui viene inviato lo scambio. Una volta inviato un documento da un partner all'altro, gli ultimi numeri utilizzati possono esser visualizzati nella pagina Numeri di controllo correnti. È possibile che siano presenti diverse voci per una determinata coppia del partner se **Numeri di controllo per Id transazione** è stato impostato su **S**. Quando una voce esiste, essa consente di creare nuovi numeri di controllo.

Come parte della inizializzazione del numero di controllo, è possibile utilizzare maschere per modificare la creazione del numero di controllo normale da parte di Enveloper. Le maschere vengono utilizzate per basare il numero di controllo sia per lo scambio che per il numero di controllo del gruppo. Segue la descrizione della maschera. Sostituire *n* nella maschera di modifica con il numero di byte che si desidera utilizzare per creare il valore del numero di controllo. Per le descrizioni dei codici disponibili, consultare Tabella 26.

Tabella 26. Maschere del numero di controllo

Codice	Numero di controllo	Descrizione
G	Transazione	Il numero di controllo della transazione è lo stesso del numero di controllo della transazione. Si consente una sola transazione per gruppo.
G*n*	Transazione	*n* byte vengono utilizzati dal numero di controllo del gruppo. Il resto del numero di controllo della transazione viene riempito con gli zero nella dimensione massima. Si consente una sola transazione per gruppo.
C	Gruppo, Transazione	I byte restanti nel gruppo o nel campo del numero di controllo della transazione consentono di gestire un numero di controllo per questo partner.
V	Gruppo, Transazione	Si utilizza un valore di incremento cosicché il primo gruppo o transazione ha un valore pari a 1, il secondo pari a 2, e così via.
V*n*	Transazione	Si utilizza un valore di incremento pari a *n* byte in modo che la prima transazione abbia un valore di 1, la seconda un valore pari a 2 e così via.

Tabella 26. Maschere del numero di controllo (Continua)

Codice	Numero di controllo	Descrizione
G*n*C	Transazione	*n* byte vengono presi dal numero di controllo del gruppo e i restanti byte nel campo del numero di controllo della transazione vengono utilizzati per mantenere un numero di controllo. Il numero di posizioni a sinistra stabilisce il valore massimo del numero di controllo. Ad esempio, G5C lascia quattro posizioni; di conseguenza il valore massimo è 9999. Il numero numero di controllo va dal valore massimo fino a 1.
G*n*V	Transazione	*n* byte vengono utilizzati dal numero di controllo del gruppo. Per i byte restanti nel campo del numero di controllo della transazione, si utilizza un valore di incremento cosicché la prima transazione ha un valore pari a 1, la seconda un valore pari a 2, e così via.
G*n*V*m*	Transazione	*n* byte vengono utilizzati dal numero di controllo del gruppo. Per i byte restanti, fino a *m* byte nel campo del numero di controllo della transazione, si utilizza un valore di incremento cosicché la prima transazione ha un valore pari a 1, la seconda un valore pari a 2, e così via.
I	Gruppo, Transazione	Il numero di controllo del gruppo o della transazione deve essere lo stesso del numero di controllo scambio. Solo un gruppo è consentito per lo scambio e solo una transazione è consentita per il gruppo o scambio.
I*n*	Gruppo, Transazione	*n* byte vengono utilizzati dal numero di controllo della transazione. Il resto del numero di controllo del gruppo o della transazione viene riempito con gli zero fino alla dimensione massima. Solo un gruppo è consentito per ogni scambio e solo una transazione è consentita per ogni gruppo.
I*n*C	Gruppo, Transazione	*n* byte vengono utilizzati dal numero di controllo della transazione. I restanti byte nel campo del numero di controllo della transazione o del gruppo vengono utilizzati per mantenere un numero di controllo. Il numero di posizioni a sinistra stabilisce il valore massimo del numero di controllo. Ad esempio, I5C lascia quattro posizioni; di conseguenza, il valore massimo è 9999. Il numero numero di controllo va dal valore massimo fino a 1.
I*n*V	Gruppo, Transazione	*n* byte vengono utilizzati dal numero di controllo della transazione. Per i byte restanti nel campo del numero di controllo del gruppo o della transazione, si utilizza un valore di incremento cosicché il primo gruppo o transazione ha un valore pari a 1, il secondo un valore pari a 2, e così via.
I*n*V*m*	Transazione	*n* byte vengono utilizzati dal numero di controllo della transazione. Per i byte restanti, fino a *m* byte nel campo del numero di controllo della transazione, si utilizza un valore di incremento cosicché la prima transazione ha un valore pari a 1, la seconda un valore pari a 2, e così via.

Tabella 26. Maschere del numero di controllo (Continua)

Codice	Numero di controllo	Descrizione
I*n*G*m*	Transazione	*n* byte vengono presi dal numero di controllo scambio e un massimo di *m* byte dal numero di controllo del gruppo. Se *n* più *m* è maggiore di 9, solo 9 - *n* byte vengono presi dal numero di controllo del gruppo. Ad esempio, se si utilizza I4G6, 4 byte vengono presi dallo scambio
I*n*G*m*C	Transazione	*n* byte vengono presi dal numero di controllo scambio e *m* byte dal numero di controllo del gruppo. I restanti byte nel campo del numero di controllo della transazione vengono utilizzati per mantenere un numero di controllo. Il numero di posizioni a sinistra stabilisce il valore massimo del numero di controllo. Ad esempio, I2G4C lascia tre posizioni; di conseguenza il valore massimo è 999. Il numero numero di controllo va dal valore massimo fino a 1.
I*n*G*m*V	Transazione	*n* byte vengono presi dal numero di controllo scambio e *m* byte dal numero di controllo del gruppo. Per i byte restanti nel campo del numero di controllo della transazione, si utilizza un valore di incremento cosicché la prima transazione ha un valore pari a 1, la seconda un valore pari a 2, e così via.
I*n*G*m*V*o*	Transazione	*n* byte vengono presi dal numero di controllo scambio e *m* byte dal numero di controllo del gruppo. Per i byte restanti, fino a *0* byte nel campo del numero di controllo della transazione, si utilizza un valore di incremento cosicché la prima transazione ha un valore pari a 1, la seconda un valore pari a 2, e così via.

Inizializzazione numero di controllo

Informazioni su questa attività

Per configurare numeri di controllo che Enveloper utilizzerà, eseguire questi passaggi:

1. Fare clic su **Ammin hub > Configurazione hub > EDI > Inizializzazione numero di controllo**.
2. Inserire un nome del partner e fare clic su **Cerca** oppure fare clic su **Cerca** senza inserire un nome per visualizzare tutti i partner. Se **Compatibile EDI** resta selezionato, limitare la ricerca ai partner che hanno capacità B2B del documento EDI. Se si rimuove il segno di spunta, vengono ricercati tutti i partner.
3. Fare clic sull'icona **Visualizza dettagli**, posta accanto al partner.
4. Le assegnazioni del numero di controllo correnti del partner (se presenti) sono state elencate nella pagina Dettagli della configurazione del numero di controllo. Fare clic sull'icona **Modifica** per modificare i valori.
5. Immettere o modificare il valore accanto a **Scambio** per indicare il numero che si desidera utilizzare per inizializzare la generazione del numero di controllo per gli scambi.
6. Immettere o modificare il valore accanto a **Gruppo** per indicare il numero che si desidera utilizzare per inizializzare la generazione del numero di controllo

per gli scambi. In alternativa, è possibile fare clic su **Maschera** ed immettere una maschera da utilizzare invece che il valore fisso.

7. Immettere o modificare il valore accanto a **Transazione** per indicare il numero che si desidera utilizzare per inizializzare la generazione del numero di controllo per le transazioni. In alternativa, è possibile fare clic su **Maschera** ed immettere una maschera da utilizzare invece che il valore fisso.
8. Fare clic su **Salva**.

Numeri di controllo correnti

Per una determinata coppia del partner che contiene già i dati nella tabella di controllo, è possibile modificare la creazione del numero di controllo. È possibile:

- Ripristinare la generazione del numero di controllo per la coppia ad uno stato iniziale.
- Modificare il numero di scambio, gruppo o transazione (oppure una qualunque combinazione di questi numeri) e salvarla con un nuovo valore.

Nota: il ripristino della generazione del numero di controllo o la modifica di un gruppo o di una maschera dovrebbe essere eseguito con attenzione, in modo che i problemi legati ai numeri fuori dalla sequenza o quelli legati al numero di controllo duplicato non si verifichino. Si potrebbe voler eseguire queste azioni durante una fase di verifica, se un partner richiede nello specifico numeri di controllo differenti

Per stabilire i partner che hanno i numeri di controllo assegnati (e per stabilire i numeri), utilizzare la funzione Numeri di controllo correnti.

1. Fare clic su **Amministrazione hub > Configurazione hub > EDI > Numeri di controllo correnti**.
2. Effettuare una delle seguenti attività:
   - Se si desidera visualizzare lo stato corrente di tutti i partner, lasciare **Qualsiasi partner** selezionato negli elenchi del partner e fare clic su **Visualizza stato corrente**.
   - Se si desidera visualizzare lo stato dei partner selezionati, effettuare la seguente procedura:
     a. Inserire il nome dei partner di origine e di destinazione e fare clic su **Cerca**. Se si desidera limitare i risultati di ricerca solo a determinati partner che trasmettono i documenti EDI, lasciare **Trova compatibile EDI** selezionato.
     b. Negli elenchi risultanti, selezionare uno o più partner da ciascun elenco e fare clic su **Visualizza stato corrente**.

Definizione degli scambi del documento

È possibile definire gli scambi del documento manualmente o mediante le procedure guidate. Se si desidera definire le connessioni mediante procedure guidate, consultare la sezione “Definizione degli scambi del documento mediante procedure guidate” a pagina 195. Se si desidera effettuare tale attività manualmente o modificare manualmente le connessioni, consultare la sezione “Definizione manuale degli scambi del documento” a pagina 197.

Definizione degli scambi del documento mediante procedure guidate

WebSphere Partner Gateway 6.1 include due procedure guidate per stabilire gli scambi del documento. Esse sono la Procedura guidata di importazione EIF e la Procedura guidata di connessione EDI.

La Procedura guidata di importazione EIF assiste l'utente durante le fasi richieste per importare le mappe contenute all'interno dei file EIF, visualizza i dettagli delle mappe caricate, associa tali mappe agli Oggetti di instradamento corretti e crea le interazioni logiche. Al termine della procedura guidata, le nuove mappe sono state caricate ed eventuali interazioni necessarie sono state create nel sistema. Quindi, è necessario utilizzare la Procedura guidata di connessione EDI per creare le connessioni mediante le mappe caricate di recente.

Nota: per evitare confusione, soltanto un utente può utilizzare una procedura guidata di importazione EIF alla volta.

La Procedura guidata di connessione EDI può essere utilizzata in seguito alla procedura guidata EIF e assiste l'utente durante le fasi richieste per configurare un'interazione EDI (invio o ricezione di un documento EDI). Al termine della procedura guidata, i partner selezionati sono stati configurati per l'interazione EDI. Include l'abilitazione delle capacità B2B, la creazione di valide interazioni, la creazione di connessioni del partner e l'assegnazione di attributi EDI necessari. La Procedura guidata di connessione crea connessioni del partner consigliate in base agli input. L'intero elenco delle possibili connessioni create viene riportato di seguito:

- De-Enveloper per i messaggi base
- Conversione
- Enveloper per i messaggi base
- Creazione TA1
- Creazione FA
- Enveloper per TA1 e/o FA
- De-Enveloper per TA1 e/o FA

Entrambe queste procedure guidate sono state posizionate nella scheda Procedure guidate della console.

Importazione delle mappe mediante la Procedura guidata di importazione EIF

Informazioni su questa attività

Per importare le mappe mediante la Procedura guidata di importazione EIF, completare la seguente procedura:

1. Avviare la Console di WebSphere Partner Gateway.
2. Fare clic su **Procedure guidate**.
3. Fare clic sulla **Procedura guidata di importazione EIF**.
4. Inserire il nome del file che si desidera importare oppure fare clic su **Sfoglia** per rilevarlo.

   Nota: durante l'importazione di un file EIF che contiene più mappe, verificare che i nomi della mappa contenuti nel file siano univoci. Se più mappe sono

state caricate nello stesso file EIF con lo stesso nome della mappa, l'ultima mappa corrispondente sovrascrive le precedenti mappe corrispondenti nel database.

5. Fare clic su **Importa**.
6. Viene visualizzato un elenco delle mappe, importate correttamente. Fare clic su **Fine** per accettare i valori predefiniti o fare clic su **Avanti** per visualizzarli o modificarli.
7. Se è stato selezionato **Avanti**, è necessario quindi esaminare le mappe di conversione e modificare le eventuali interazioni. Selezionare una mappa di conversione. Se esiste un'interazione, viene visualizzata come sola lettura. Per aggiungere un'interazione, fare clic su **Aggiungi un'interazione**.
8. Nella finestra Aggiungi un'interazione, selezionare un'interazione e fare clic su **Aggiungi questa interazione** per aggiungere un'interazione all'elenco.
9. Una volta esaminate le mappe di conversione, fare clic su **Avanti** per verificare le mappe di convalida.
10. Esaminare le mappe di convalida importate. Se sono corrette, fare clic su **Fine**. Se si desidera visualizzare le mappe FA, fare clic su **Avanti**.
11. Verificare le mappe RF importate e fare clic su **Fine** e viene visualizzata una finestra finale che mostra le mappe importate correttamente oltre alle interazioni create .

Impostazione delle connessioni mediante la Procedura guidata di connessione EDI

Informazioni su questa attività

Prima di impostare le connessioni mediante la Procedura guidata di connessione EDI, è necessario creare:

- Il partner interno
- Almeno un partner esterno
- Un ID di business per ciascun partner. In questa procedura guidata, un ID di business EDI è stato definito come un identificativo di business in figura a mano libera che ha il formato *qq-xxxxxxxxx*, dove *qq* indica il qualificatore di scambio EDI a 2 cifre e *xxxxxxxxx* indica l'identificativo dello scambio EDI a 9 cifre.
- Destinazioni e destinazioni predefinite
- Profili busta

È possibile che siano richieste ulteriori fasi di configurazione prima che i flussi EDI possano essere eseguiti correttamente. Di seguito sono riportati gli esempi:

- Configurare i formati XML (se si inviano o si ricevono XML)
- Configurare i destinatari con splitter ROD (se si ricevono ROD)
- Configurare ulteriori Attributi di connessione per AS o AS2 (se si utilizza l'impacchettamento AS)

Per creare le Connessioni mediante la Procedura guidata di connessione EDI, completare la seguente procedura:

1. Avviare la Console di WebSphere Partner Gateway.
2. Fare clic su **Procedure guidate**.
3. Fare clic sulla **Procedura guidata di connessione EDI**.
4. Fare clic sul tipo di attività da configurare (**Invia un documento EDI ad un partner EDI** o **Ricevi un documento EDI da un partner EDI**), quindi fare clic su **Avanti**.

5. A seconda della selezione di **Ricevi un documento EDI da un partner EDI** o **Invia un documento EDI ad un partner EDI**, inserire il partner di origine o di destinazione e fare clic su **Cerca**.
6. Selezionare un partner di origine o di destinazione nell'elenco a discesa e fare clic su **Avanti**.
7. Selezionare le proprietà generali per il partner di destinazione o di origine. Se la Sintassi è EDI, è anche necessario specificare le proprietà EDI. Alla selezione di tutte le proprietà desiderate, fare clic su **Avanti**.

   Nota:

   a. Le proprietà TA1 e RF sono visibili solo se l'origine è un partner esterno. Il tempo richiesto RF è visibile solo se la destinazione è un partner esterno.
   b. La Procedura guidata di connessione EDI contiene un elenco di valori comuni utilizzati come valori di delimitatore EDI. Se si desidera utilizzare un valore che non è presente nell'elenco fornito, una volta completata la procedura guidata, è necessario modificare l'attributo di connessione. È possibile modificare gli attributi di connessione facendo clic su **Amministrazione account > Connessioni**.
   c. È necessario specificare una Destinazione per ciascuna modalità operativa. Ciò significa che non è possibile selezionare l'opzione vuota ("Nessuna destinazione selezionata"). L'applicazione di questa ulteriore configurazione di Connessione non influenza negativamente la maggior parte dei documenti che effettua attività di invio o ricezione. Se è necessario rimuovere la specifica di destinazione dalla connessione, è possibile effettuare questa operazione dopo aver completato la procedura guidata facendo clic su **Amministrazione account > Connessioni**.
8. Selezionare la **Mappa di convalida**, l'**Azione** e la **Mappa di conversione** di origine o destinazione per il partner di origine o destinazione. Le descrizioni della mappa sono visualizzate una volta selezionata una mappa. Il package è vuoto per evitare confusione nei casi in cui EDI utilizza il package AS. Una volta selezionate le voci, fare clic su **Avanti**.
9. Verificare le connessioni consigliate, fare clic su **Attributi**, **Azioni** o **Destinazioni** per verificare tali impostazioni.

   Nota: le connessioni che già esistono e non sono state create diventano inattive. Tali connessioni hanno anche un'icona Esiste, posta accanto e non hanno la casella Crea. Se le connessioni già esistono, non sono sovrascritte da questa procedura guidata. In tal caso, viene visualizzato un avviso che descrive tale situazione.
   Se le connessioni devono essere modificate, fare clic su **Indietro**. Una volta soddisfatte le connessioni elencate, fare clic su **Fine**. Se è necessario modificarle, fare clic su **Indietro**. Viene visualizzata una finestra che mostra le connessioni create correttamente.

Definizione manuale degli scambi del documento

La Procedura guidata di importazione EIF e la Procedura guidata di connessione EDI possono definire gli scambi di documento (per ulteriori informazioni su queste procedure guidate, consultare la sezione "Definizione degli scambi del documento mediante procedure guidate" a pagina 195. Tuttavia, è possibile definire manualmente i documenti. In questa sezione, viene fornita una panoramica di alto livello delle attività necessarie per stabilire lo scambio dei documenti per scambi EDI che si inseriscono nell'hub, documenti o transazioni convertite sull'hub e per scambi EDI inviati dall'hub. I passaggi descritti nelle sezioni successive sono generali e applicabili solo all'importazione delle mappe e alla configurazione delle

interazioni. Le fasi generali per abilitare le capacità B2B per i partner (per tutti i tipi di scambi del documento) sono descritte nella sezione "Impostazione delle capacità B2B" a pagina 26. I passaggi generali per la gestione delle connessioni (per tutti i tipi di scambi dei documenti) vengono descritti in Capitolo 12, "Gestione connessioni", a pagina 237. Se si desidera visualizzare un esempio completo di uno scambio EDI dall'importazione delle mappe fino alla gestione delle connessioni, fare riferimento a Capitolo 19, "Esempi EDI", a pagina 319. Nell'appendice sono inclusi questi esempi specifici:

- " Esempio da EDI a ROD" a pagina 319
- " Esempio da EDI a XML" a pagina 333
- " Esempio da ROD a EDI" a pagina 345
- " Esempio da XML a EDI" a pagina 338

Importazione manuale di mappe

Informazioni su questa attività

Le mappe di conversione per documenti EDI, XML o ROD (record-oriented-data) possono essere create con il programma del client Data Interchange Services. Il client Data Interchange Services è un programma utilizzato per creare e mantenere definizioni di documenti di schema XML, definizioni di documenti DTD XML, standard EDI, definizioni documenti ROD e mappe.

Le mappe WTX vengono create utilizzando WTX Design Studio e importate in WebSphere Partner Gateway.

Il client Data Interchange Services è un programma installato separatamente incluso sui supporti WebSphere Partner Gateway ma che di solito risiede su un altro computer. Lo specialista della mappatura del client Data Interchange Services crea una mappa che specifica come gli elementi in un solo documento vengono spostati in elementi in altro documento differente. Oltre ad avere le istruzioni che illustrano come convertire un documento da un formato all'altro, Data Interchange Services deve anche conoscere il layout, o il formato del documento di origine e di destinazione. In Data Interchange Services il layout di un documento è la *definizione del documento*.

Durante l'importazione di una mappa di conversione in WebSphere Partner Gateway, le definizioni del documento create in Data Interchange Services sono visualizzate come definizioni del documento (package, protocollo e tipo di documento) nelle pagine Mappa di conversione e Gestisci le definizioni di documento.

Se, ad esempio, si converte un documento XML in una transazione X12, si importa la mappa che definisce le definizioni del documento della transazione XML e X12 e la conversione che ha luogo.

Ci sono due metodi per ricevere i file di mappatura da Data Interchange Services. Se il client Data Interchange Services ha una connessione diretta al database WebSphere Partner Gateway, lo specialista della mappatura di Data Interchange Services può esportare il file direttamente nel database. Uno scenario più simile è quello in cui si riceveranno i file via e-mail o come trasferimento FTP. Se i file vengono trasferiti tramite FTP, si noti che devono essere in formato binario.

Se si verifica un errore durante l'esportazione di una mappa dal client Data Interchange Services, è possibile visualizzare il nome della mappa nella Console comunità. La mappa non può essere utilizzata per convertire i documenti. Sarà

necessario avvertire lo specialista della mappatura del client Data Interchange Services del problema di esportazione e richiedergli di esportare nuovamente la mappa prima che possa essere utilizzata per convertire i documenti.

Per importare una mappa, eseguire questi passaggi:

1. Aprire la finestra dei comandi.
2. Immettere il seguente comando o script:
   - In un sistema UNIX:

     `<DirProdotto>/bin/bcgDISImport.sh <control_string_map>`
   - In un sistema Windows:

     `<DirProdotto>\bin\bcgDISImport.bat <control_string_map>`

     dove <*database_user_ID*> e <*password*> corrispondono ai valori utilizzati al momento dell'installazione del database come parte dell'installazione di WebSphere Partner Gateway. <*control_string_map*> è il percorso completo del file di stringa del controllo mappa esportato dal Data Interchange Services.
3. Per le mappe di conversione, verificare che la definizione del documento sia stata importata.
   a. Fare clic su **Amministrazione hub > Configurazione hub > Mappe > Mappe di conversione**.
   b. Nella pagina Mappe di conversione, fare clic sull'icona **Visualizza dettagli** accanto alla mappa da Data Interchange Services. Le definizioni del documento per l'origine e la destinazione sono state visualizzate, indicando il formato in cui il documento sarà ricevuto sull'hub e il formato in cui sarà distribuito dall'hub.
   c. Fare clic su **Amministrazione hub > Configurazione hub> Definizione documento**.
   d. Espandere i package ed i protocolli associati alle definizioni del documento nella pagina Mappe di conversione per verificare che i tipi di documenti siano visualizzati nella pagina Gestisci le definizioni di documento.

È possibile utilizzare le mappe di convalida insieme alle mappe di conversione per aggiungere una convalida degli standard EDI aggiuntiva ai processi di conversione che comprendono gli standard EDI. Le mappe di convalida forniscono un controllo completo sulla convalida di un documento EDI.

Si noti che le mappe di conversione e di convalida esportate dal client Data Interchange Services o importate con l'utilità bcgDISImport non possono essere scaricate dalla Console comunità di WebSphere Partner Gateway. Lo specialista della mappatura del client Data Interchange Services gestisce queste mappe collegandole al database di WebSphere Partner Gateway mediante il client Data Interchange Services.

Importazione di mappe WTX

Informazioni su questa attività

Le mappe WTX create utilizzando WTX Design Studio devono essere importate in WebSphere Partner Gateway, in modo che possano essere associate a specifiche connessioni partecipanti. E' necessario creare manualmente un DFD. I DFD creati vengono esportati da WTX Design Studio nel formato di una mappa compilata per il sistema operativo nativo. Per importare una mappa in WebSphere Partner gateway, passare a hubadmin > Mappe > mappe di conversione e fare clic su Crea. La mappa importata verrà memorizzata in un file system comune in una cartella specifica destinata alle mappe WTX (common/maps).

Importazione di EIF standard WDI
Informazioni su questa attività

Al fine di eseguire la convalida di transazioni EDI in WebSphere Partner Gateway, il modulo compilato dello standard EDI deve essere disponibile in WebSphere Partner Gateway. Per creare questa stringa di controllo standard compilata, effettuare le seguenti operazioni:

1. Scaricare lo standard EDI dal sito Web di supporto WDI.
2. Creare una mappa di conversione dati e selezionare la transazione EDI che si desidera convalidare in WebSphere Partner Gateway. Ad esempio, se si desidera convalidare la transazione 810 di X12V4R1, creare una mappa di conversione dati da X12V4R1-810 a X12V4R1-810.
3. Eseguire la mappatura solo un segmento obbligatorio e compilare la mappa di conversione.
4. Esportare la stringa di controllo della mappa di conversione dati nel database del gestore documenti. Questa operazione esporterà anche lo standard compilato nel database del gestore documenti, che può essere utilizzato per la convalida.

Nota: in alternativa, esistono alcuni EIF di esempio forniti che includono solo la stringa di controllo standard compilata.

Impostazione di un flusso da EDI a EDI
Informazioni su questa attività

In questa sezione, vengono descritte le interazioni necessarie a ricevere uno scambio EDI, eseguire il deenveloping dello scambio, convertire una transazione da un formato EDI ad un altro, eseguire l'enveloping della transazione e consegnarla.

1. Verificare che una definizione del documento sia presente per lo scambio EDI ricevuto sull'hub. Una volta sottoposto a deenveloping lo scambio, la busta di origine non continua ad essere elaborata. In altre parole, non c'è un punto di consegna. Pertanto, si utilizza **N/A** per il package sull'interazione di destinazione.
   a. Fare clic su **Amministrazione hub > Configurazione hub> Definizione documento**.
   b. Verificare se una definizione del documento già esiste. Ad esempio, se un partner invia uno scambio EDI nell'impacchettamento AS, nel protocollo EDI-X12, e nel tipo documento ISA, la definizione è già disponibile. Allo stesso modo, una definizione del documento N/A/EDI-X12/ISA già esiste.
   c. Immettere un valore (o selezionarlo dall'elenco) per un attributo da associare al profilo. Ad esempio, se si desidera specificare che è necessario eliminare la busta se sono rilevati errori con una delle transazioni, fare clic sull'icona **Modifica i valori dell'attributo** posta accanto alle **Definizioni documento**. Nella riga **Elimina busta in caso di errori**, selezionare **Sì** dall'elenco.
   d. Se una definizione del documento non esiste, crearne una selezionando il Package, Protocollo ed il Tipo documento.
2. Creare un'interazione per lo scambio.
   a. Fare clic su **Amministrazione hub > Configurazione hub> Definizioni documento**.
   b. Selezionare **Crea interazione**.

c. Selezionare le definizioni del documento di origine e di destinazione. Tranne che per l'impacchettamento (che sarà **N/A** per la destinazione), le definizioni del documento saranno uguali.

d. Selezionare **Deenveloping di EDI** dall'elenco Azione.

3. Importare la mappa di conversione che fornisce le definizioni del documento delle transazioni EDI e che descrive come la transazione viene convertita da un formato EDI all'altro. Fare riferimento a " Importazione manuale di mappe" a pagina 198.

   Se lo scambio contiene più di una transazione, ripetere questo passaggio per ciascuna transazione.

4. Se si desidera modificare gli attributi delle definizioni del documento associate alla mappa, eseguire questi passaggi:

   a. Fare clic su **Amministrazione hub > Configurazione hub> Definizione documento**.

   b. Fare clic sull'icona **Modifica valori dell'attributo** accanto al protocollo. Per i protocolli EDI, viene visualizzato un elenco di attributi che è possibile impostare.

   c. Immettere un valore (o selezionarne uno dall'elenco) per un attributo da associare al protocollo.

   d. Fare clic sull'icona **Modifica i valori dell'attributo**, posta accanto alla definizione del documento. In genere, viene visualizzato un piccolo elenco di attributi rispetto a quelli associati al protocollo.

   e. Inserire un valore (o selezionare il valore dall'elenco) per qualsiasi attributo che si desidera associare al tipo di documento. Ad esempio, è possibile modificare la **mappa di convalida** associata al tipo di documento.

      Verificare che sia stato selezionato un profilo busta per la transazione.

5. Creare un'interazione per la mappa importata.

   a. Fare clic su **Amministrazione hub > Configurazione hub> Definizioni documento**.

   b. Fare clic su **Crea interazione**.

   c. In **Origine**, selezionare il tipo di documento associato alla transazione. Espandere il package ed il protocollo e selezionare il tipo di documento. Di solito, è **N/A** (poiché la transazione non è stata creata da un partner), il protocollo è stato definito nella mappa (ad esempio, **X12V4R1**) ed il documento EDI corrente è stato definito nella mappa (ad esempio, **850**).

   d. In **Destinazione**, selezionare la definizione del documento per il documento convertito. Espandere il package ed il protocollo e selezionare il tipo di documento. Poiché la transazione sarà sottoposta a enveloping (e quindi non sarà distribuita direttamente ad un partner), l'impacchettamento sarà nuovamente **N/A**.

   e. Nell'elenco delle mappe di conversione, selezionare la mappa che definisce come convertire questo documento.

   f. Dall'elenco Azioni, selezionare **Convalida EDI e conversione EDI** per il WDI nativo. In caso di WTX, selezionare **Convalida EDI e Conversione WTX**.

6. Verificare che una definizione del documento sia presente per lo scambio EDI inviato dall'hub ed impostare gli attributi che si desidera associare allo scambio.

   a. Fare clic su **Amministrazione hub > Configurazione hub> Definizione documento**.

b. Verificare se una definizione del documento già esiste. Il package di origine sarà N/A, con il protocollo ed il tipo di documento che corrisponde al protocollo e al tipo di documento utilizzati per distribuire lo scambio. Se, ad esempio, lo scambio verrà consegnato come AS/EDI-X12/ISA, l'origine sarà N/A/EDI-X12/ISA.

c. Modificare gli attributi che vengono applicati allo scambio consegnato.

d. Se una definizione del documento non esiste, crearne una selezionando il Package, Protocollo ed il Tipo documento.

7. Creare un'interazione per lo scambio EDI che è stato inviato dall'hub una volta convertita la transazione.

   a. Fare clic su **Amministrazione hub > Configurazione hub> Definizioni documento**.

   b. Fare clic su **Crea interazione**.

   c. Selezionare i documenti di origine e di destinazione. Tranne che per l'impacchettamento (che sarà **N/A** per il documento di origine), le definizioni del documento saranno uguali.

   d. Selezionare **Pass Through** dall'elenco **Azione**.

Per aggiungere un riconoscimento al flusso, consultare "Impostazione dei riconoscimenti" a pagina 208.

Una volta impostate le interazioni, creare le capacità B2B per i partner.

- Per il partner di origine, abilitare tre definizioni del documento (in **Imposta origine**)--una per il tipo di documento di origine, una per la transazione EDI ed una per la busta.
- Per il partner di destinazione, abilitare tre definizioni del documento (in **Imposta destinazione**), una per il tipo di documento sottoposto a deenveloping, una per la transazione EDI convertita ed una per la busta EDI.

Le fasi dettagliate per la creazione delle capacità B2B sono descritte nella sezione "Impostazione delle capacità B2B" a pagina 26.

Una volta impostate le capacità B2B per i partner, creare le connessioni. Sono necessarie tre connessioni:

- Una per la busta dal partner di origine all'hub.
- Una per la transazione EDI di origine alla transazione EDI di destinazione.
- Una per la busta dall'hub al partner di destinazione.

Le fasi dettagliate per la creazione delle connessioni sono descritte nella sezione Capitolo 12, "Gestione connessioni", a pagina 237.

Impostazione di un flusso da EDI a XML o ROD

Informazioni su questa attività

In questa sezione, vengono descritte le interazioni necessarie a ricevere uno scambio EDI, eseguire il deenveloping dello scambio, convertire una transazione da un formato EDI in un documento XML o ROD e consegnarlo.

Nota: per un esempio completo del flusso EDI in XML, vedere " Esempio da EDI a XML" a pagina 333. Per un esempio completo del flusso EDI in ROD, vedere " Esempio da EDI a ROD" a pagina 319.

1. Verificare che una definizione del documento sia presente per lo scambio EDI ricevuto sull'hub. Si ricordi che dopo che lo scambio viene sottoposto a

deenveloping, la busta non continua ad essere elaborata. In altre parole, non c'è un punto di consegna. Pertanto, si utilizza **N/A** per il package sull'interazione di destinazione.

a. Fare clic su **Amministrazione hub > Configurazione hub> Definizione documento**.
b. Verificare se una definizione del documento già esiste. Ad esempio, se un partner invia uno scambio EDI nell'impacchettamento AS, nel protocollo EDI-X12, e nel tipo documento ISA, la definizione è già disponibile. Allo stesso modo, una definizione del documento N/A/EDI-X12/ISA già esiste.
c. Se una definizione del documento non esiste, creare una nuova.

2. Creare un'interazione per lo scambio EDI ricevuto sull'hub.
   a. Fare clic su **Amministrazione hub > Configurazione hub> Definizioni documento**.
   b. Selezionare **Crea interazione**.
   c. Selezionare i documenti di origine e di destinazione. Tranne che per l'impacchettamento (che sarà **N/A** per la destinazione), le definizioni del documento saranno uguali.
   d. Selezionare **Deenveloping di EDI** dall'elenco Azione.
3. Importare la mappa di conversione che fornisce le definizioni del documento della transazione EDI e il documento XML e ROD e che descrive come la transazione viene convertita in un documento XML o ROD. Fare riferimento a " Importazione manuale di mappe" a pagina 198.

   Se lo scambio contiene più di una transazione, ripetere questo passaggio per ciascuna transazione.
4. Creare un'interazione per la mappa importata.
   a. Fare clic su **Amministrazione hub > Configurazione hub> Definizioni documento**.
   b. Fare clic su **Crea interazione**.
   c. In **Origine**, selezionare il tipo di documento associato alla transazione. Espandere il package ed il protocollo e selezionare il tipo di documento. Di solito, è **N/A** (poiché la transazione non è stata creata da un partner), il protocollo è stato definito nella mappa (ad esempio, **X12V4R1**) ed il documento EDI corrente è stato definito nella mappa (ad esempio, **850**).
   d. In **Destinazione**, selezionare la definizione del documento per il documento convertito (XML o ROD). Espandere il package ed il protocollo e selezionare il tipo di documento.
   e. Nell'elenco delle mappe di conversione, selezionare la mappa che definisce come convertire questo documento.
   f. Dall'elenco Azioni, selezionare **Convalida EDI e conversione EDI** se di tratta di WDI nativo. In caso di WTX, selezionare **Convalida EDI e Conversione WTX**.

Per aggiungere un riconoscimento al flusso, consultare "Impostazione dei riconoscimenti" a pagina 208.

Una volta impostate le interazioni, creare le capacità B2B per i partner.

- Per il partner di origine, abilitare due definizioni di documenti (in **Imposta origine**)--una per la busta e una per la transazione EDI.
- Per il partner di destinazione, abilitare due definizioni di documenti (in **Imposta destinazione**)--una per la busta EDI e una per il documento XML o ROD.

Le fasi dettagliate per la creazione delle capacità B2B sono descritte nella sezione “Impostazione delle capacità B2B” a pagina 26.

Una volta impostate le capacità B2B per i partner, creare le connessioni. Sono necessarie due connessioni:

- Una per la busta dal partner di origine all'hub.
- Una per la transazione EDI di origine al documento XML o ROD.

Le fasi dettagliate per la creazione delle connessioni sono descritte nella sezione Capitolo 12, “Gestione connessioni”, a pagina 237.

Impostazione di un flusso da XML o ROD a EDI

Informazioni su questa attività

In questa sezione, vengono descritte le interazioni necessarie per ricevere un documento XML o ROD, convertirlo in una transazione EDI, eseguire l'enveloping della transazione e consegnarla.

Nota: per un esempio completo del flusso XML o in ROD, vedere “ Esempio da XML a EDI” a pagina 338. Per un esempio completo del flusso ROD in EDI, vedere “ Esempio da ROD a EDI” a pagina 345.

1. Importare la mappa di conversione che fornisce le definizioni del documento XML o ROD e della transazione EDI e che descrive come il documento venga convertito in una transazione EDI. Fare riferimento a “ Importazione manuale di mappe” a pagina 198.
2. Creare un'interazione per la mappa importata.
   a. Fare clic su **Amministrazione hub > Configurazione hub> Definizioni documento**.
   b. Fare clic su **Crea interazione**.
   c. In **Origine**, selezionare la definizione del documento associata al documento XML o ROD. Espandere il package ed il protocollo e selezionare il tipo di documento.
   d. In **Destinazione**, selezionare il tipo di documento associato alla transazione EDI. Espandere il package ed il protocollo e selezionare il tipo di documento. Poiché la transazione non verrà recapitata direttamente (verrà sottoposta a enveloping prima di essere recapitata), per il package verrà indicato **N/A**.
   e. Nell'elenco delle mappe di conversione, selezionare la mappa che definisce come convertire questo documento.
   f. Dall'elenco Azioni, selezionare **Convalida EDI e conversione EDI** o **Convalida EDI e conversione ROD** per il WDI nativo. In caso di WTX, selezionare **Conversione WTX**.
3. Verificare che una definizione del documento sia presente per lo scambio EDI inviato dall'hub ed impostare gli attributi che si desidera associare allo scambio.
   a. Fare clic su **Amministrazione hub > Configurazione hub> Definizione documento**.
   b. Verificare se una definizione del documento già esiste. Per il package per il documento di origine dovrebbe essere indicato **N/A** (essendo lo scambio inviato dall'hub).
   c. Modificare gli attributi che vengono applicati allo scambio consegnato.
   d. Se una definizione del documento non esiste, crearne una selezionando il Package, Protocollo ed il Tipo documento.

4. Creare un'interazione per lo scambio EDI che viene inviato dall'hub dopo che il documento è stato convertito.
   a. Fare clic su **Amministrazione hub > Configurazione hub> Definizioni documento**.
   b. Fare clic su **Crea interazione**.
   c. Selezionare i documenti di origine e di destinazione. I documenti di origine e di destinazione hanno diversi tipi di impacchettamento (il documento di origine ha l'impacchettamento N/A), ma il protocollo (ad esempio, EDI-X12) ed il tipo di documento (ad esempio, ISA) devono essere uguali.
   d. Selezionare **Pass Through** nell'elenco Azione.

Una volta impostate le interazioni, creare le capacità B2B per i partner.

- Per il partner di origine, il numeri delle definizioni di documenti da dover impostare (in **Imposta origine**) varia a seconda del tipo di documento.
  – Ad esempio, per un documento XML in cui il tipo di documento è ICGPO e la transazione EDI convertita è MX12V3R1, abilitare tre definizioni di documenti (in **Imposta origine**)--una per il documento XML (ICGPO), una per la transazione EDI (MX12V3R1) ed una per la busta inviata dall'hub.
  – Per gli altri documenti XML e ROD, abilitare due definizioni di documenti (in **Imposta origine**)--una per il documento XML o ROD ed una per la busta inviata dall'hub.
- Per il partner di destinazione, abilitare due definizioni di documenti (in **Imposta destinazione**)--una per la transazione EDI ed una per la busta EDI ricevuta. Per la transazione EDI, fare clic sull'icona **Modifica valori dell'attributo** accanto al protocollo, quindi specificare un profilo di busta. È inoltre possibile specificare altri attributi.

Le fasi dettagliate per la creazione delle capacità B2B sono descritte nella sezione "Impostazione delle capacità B2B" a pagina 26.

Una volta impostate le capacità B2B per i partner, creare le connessioni. Sono necessarie due connessioni:

- Una per il documento XML o ROD di origine alla transazione EDI.
- Una per la busta dall'hub al partner.

Le fasi dettagliate per la creazione delle connessioni sono descritte nella sezione Capitolo 12, "Gestione connessioni", a pagina 237.

Impostazione del flusso di più documenti XML o ROD in un file in EDI

Informazioni su questa attività

In questa sezione vengono descritte le interazioni per ricevere più documenti XML o ROD in un file, convertire i documenti in transazioni EDI, eseguire l'enveloping delle transazioni e consegnare lo scambio EDI.

1. Importare la mappa di conversione che fornisce le definizioni del documento dei documenti XML o ROD e delle transazioni EDI e che descrive la conversione. Fare riferimento a " Importazione manuale di mappe" a pagina 198.
2. Creare un'interazione per documenti di origine e di destinazione.
   a. Fare clic su **Amministrazione hub > Configurazione hub> Definizioni documento**.
   b. Fare clic su **Crea interazione**.

c. Per il WDI nativo, selezionare i documenti di origine e destinazione e selezionare **Conversione XML e Convalida EDI** o **Conversione ROD e Convalida EDI** dall'elenco Azioni. Per WTX, selezionare **Conversione WTX** e **Convalida EDI**.

3. Ripetere il passaggio 2 a pagina 205 per il documento di origine e ciascun documento di destinazione dalla mappa di conversione.
4. Verificare che una definizione del documento sia presente per lo scambio EDI inviato dall'hub ed impostare gli attributi che si desidera associare allo scambio.
   a. Fare clic su **Amministrazione hub > Configurazione hub> Definizione documento**.
   b. Verificare se una definizione del documento già esiste. L'origine sarà N/A, con il protocollo ed il tipo di documento che corrisponde al protocollo ed al tipo di documento utilizzati per distribuire lo scambio. Se, ad esempio, lo scambio verrà consegnato come AS/EDI-X12/ISA, l'origine sarà N/A/EDI-X12/ISA.
   c. Modificare gli attributi che vengono applicati allo scambio consegnato.
   d. Se una definizione del documento non esiste, crearne una selezionando il Package, Protocollo ed il Tipo documento.
5. Creare un'interazione per lo scambio EDI che è stato inviato dall'hub una volta convertita la transazione.
   a. Fare clic su **Amministrazione hub > Configurazione hub> Definizioni documento**.
   b. Fare clic su **Crea interazione**.
   c. Selezionare i documenti di origine e di destinazione. I documenti di origine e di destinazione hanno diversi tipi di impacchettamento (il documento di origine ha l'impacchettamento N/A), ma il protocollo (ad esempio, EDI-X12) ed il tipo di documento (ad esempio, ISA) devono essere uguali.
   d. Selezionare **Pass Through** nell'elenco Azione.

Una volta impostate le interazioni, creare le capacità B2B per i partner.

- Per il partner di origine, il numeri delle definizioni di documenti da dover impostare (in **Imposta origine**) varia a seconda del tipo di documento.
  - Ad esempio, per un documento XML in cui il tipo di documento è ICGPO e la transazione EDI convertita è MX12V3R1, abilitare tre definizioni di documenti (in **Imposta origine**)--una per il documento XML (ICGPO), una per la transazione EDI (MX12V3R1) ed una per la busta inviata dall'hub.
  - Per gli altri documenti XML e ROD, abilitare due definizioni di documenti (in **Imposta origine**)--una per il documento XML o ROD ed una per la busta inviata dall'hub.

Le fasi dettagliate per la creazione delle capacità B2B sono descritte nella sezione "Impostazione delle capacità B2B" a pagina 26.

Una volta impostate le capacità B2B per i partner, creare le connessioni. Sono necessari varie connessioni:

- Una per ciascun documento XML o ROD convertito in una transazione EDI.
- Una per la busta dall'hub al partner.

Le fasi dettagliate per la creazione delle connessioni sono descritte nella sezione Capitolo 12, "Gestione connessioni", a pagina 237.

Impostazione di un flusso di documenti da XML a ROD o da ROD a XML

Informazioni su questa attività

In questa sezione, vengono descritte le interazioni necessarie per ricevere un documento XML o ROD, convertirlo in un altro tipo di documento (XML in ROD o ROD in XML) e consegnarlo.

1. Importare la mappa di conversione che fornisce le definizioni dei documenti XML o ROD e che descrive in che modo i documenti vengono convertiti. Fare riferimento a " Importazione manuale di mappe" a pagina 198.
2. Fare clic su **Ammin hub > Configurazione hub > Mappe > Mappe di conversione**, quindi fare clic sull'icona **Visualizza dettagli** accanto alla mappa importata.
3. Creare un'interazione per la mappa importata.
   a. Fare clic su **Amministrazione hub > Configurazione hub> Definizioni documento**.
   b. Fare clic su **Crea interazione**.
4. Selezionare i documenti di origine e destinazione e selezionare **Conversione WTX** per WTX. o **Conversione ROD e Convalida EDI** dall'elenco Azioni.

Una volta impostate le interazioni, creare le capacità B2B per i partner.

- Per il partner di origine, abilitare le definizioni di documenti (in **Imposta origine**) per il documento XML o ROD.
- Per il partner di destinazione, abilitare le definizioni di documenti (in **Imposta destinazione**) per il documento XML o ROD.

Le fasi dettagliate per la creazione delle capacità B2B sono descritte nella sezione "Impostazione delle capacità B2B" a pagina 26.

Una volta impostate le capacità B2B per i partner, creare le connessioni. È necessaria una connessione - per il flusso da XML a ROD o da ROD a XML. Le fasi dettagliate per la creazione delle connessioni sono descritte nella sezione Capitolo 12, "Gestione connessioni", a pagina 237.

Impostazione di un flusso da XML a XML o da ROD a ROD

Informazioni su questa attività

In questa sezione, vengono descritte le interazioni necessarie per ricevere un documento XML o ROD, convertirlo in un documento dello stesso tipo (XML in XML o ROD in ROD) e consegnarlo.

1. Importare la mappa di conversione che fornisce le definizioni dei documenti XML o ROD e che descrive in che modo i documenti vengono convertiti. Fare riferimento a " Importazione manuale di mappe" a pagina 198.
2. Fare clic su **Ammin hub > Configurazione hub > Mappe > Mappe di conversione**, quindi fare clic sull'icona **Visualizza dettagli** accanto alla mappa importata.
3. Creare un'interazione per la mappa importata.
   a. Fare clic su **Amministrazione hub > Configurazione hub> Definizioni documento**.
   b. Fare clic su **Crea interazione**.
   c. Selezionare i documenti di origine e di destinazione.

d. Per il WDI nativo, selezionare **Conversione XML e Convalida EDI** o **Conversione ROD e Convalida EDI** dall'elenco Azioni. Per WTX, selezionare **Conversione WTX** e **Convalida scambio EDI**.

Una volta impostate le interazioni, creare le capacità B2B per i partner.

- Per il partner di origine, abilitare una definizione di documento (in **Imposta origine**) per il documento XML o ROD.
- Per il partner di destinazione, abilitare una definizione di documento (in **Imposta destinazione**) per il documento XML o ROD.

Le fasi dettagliate per la creazione delle capacità B2B sono descritte nella sezione "Impostazione delle capacità B2B" a pagina 26.

Una volta impostate le capacità B2B per i partner, creare le connessioni. È necessaria una connessione - per il flusso da XML a XML o da ROD a ROD. Le fasi dettagliate per la creazione delle connessioni sono descritte nella sezione Capitolo 12, "Gestione connessioni", a pagina 237.

Impostazione dei riconoscimenti

In questa sezione, viene descritto come impostare le interazioni per inviare riconoscimenti della ricezione dello scambio o della transazione a chi ha originato il documento.

Riconoscimenti funzionali

Le mappe di riconoscimento funzionale consentono di fornire la creazione dei riconoscimenti funzionali durante la risposta ai documenti EDI ricevuti da un partner. WebSphere Partner Gateway fornisce un insieme di mappe di riconoscimento funzionale che producono i riconoscimenti funzionali EDI comunemente utilizzati. Lo specialista della mappatura può anche creare riconoscimenti funzionali e mappe di convalida, in cui queste mappe dovrebbero essere caricate in WebSphere Partner Gateway.

Nota: una mappa di riconoscimento funzionale deve essere creata quando viene richiesto un riconoscimento funzionale personalizzato.

Oltre alle mappe di riconoscimento funzionale fornite con WebSphere Partner Gateway, vengono forniti il protocollo &FUNC_ACK_METADATA_DICTIONARY e &FUNC_ACK_META associata. Vengono elencati in **Package: Nessuno** nella pagina Definizioni documento. &FUNC_ACK_META è la definizione del documento di origine per tutte le mappe di riconoscimento funzionale. Questa mappa fornisce la struttura di un riconoscimento funzionale. Un riconoscimento funzionale passa ai partner e la mappa del riconoscimento funzionale indica al sistema il modo in cui creare il riconoscimento. Il nome della definizione del documento di origine non può essere modificato. Lo specialista della mappatura del client Data Interchange Services non può creare una mappa di riconoscimento funzionale senza questa definizione del documento nel database.

La definizione del documento di destinazione in una mappa di riconoscimento funzionale descrive il layout del riconoscimento funzionale. Deve essere una definizione di documento EDI con un nome 997, 999, o CONTRL.

Le seguenti mappe di riconoscimento funzionale sono state installate con WebSphere Partner Gateway e sono visualizzate nella pagina Definizioni documento di **Package: N/A**:

Tabella 27. Mappe di riconoscimento funzionale fornite dal prodotto

Protocollo	Tipo di documento	Descrizione
&DTCTL21	CONTRL	Riconoscimento funzionale CONTRL – UN/EDIFACT versione 2 release 1 (D94B)
&DTCTL	CONTRL	Riconoscimento funzionale CONTRL – UN/EDIFACT prima del D94B
&DT99933	999	Riconoscimento funzionale 999 – UCS versione 3 release 3
&DT99737	997	Riconoscimento funzionale 997 – X12 versione 3 release 7
&DT99735	997	Riconoscimento funzionale 997 – X12 versione 3 release 5
&DT99724	997	Riconoscimento funzionale 997 – X12 versione 2 release 4

Inoltre, il protocollo &X44TA1 (con un tipo di documento TA1 associato) è stato elencato in **Package: N/A**. Questa mappa consente di creare TA1. TA1 è un riconoscimento funzionale generato per gli scambi X12 in entrata.

Anche il protocollo &WDIEVAL (con X12ENV associato) viene fornito sotto **Package: N/A**.

Al pari delle transazioni EDI, i riconoscimenti funzionali sono sempre inseriti in uno scambio prima di essere consegnati.

Riconoscimenti TA1

TA1 è un segmento EDI che fornisce un riconoscimento funzionale dello scambio X12. Riconosce la ricezione e la correttezza sintattica di una coppia intestazione/elemento di coda X12 (ISA e IEA) di uno scambio. Il mittente può richiedere un TA1 dal destinatario impostando l'elemento 14 di ISA Interchange Control Header su **1**. Il numero di controllo dello scambio di un TA1 corrisponde ad uno scambio X12 trasmesso in precedenza con lo stesso numero di controllo per completare il processo di riconoscimento.

Al pari delle transazioni EDI e dei riconoscimenti, i TA1 sono sempre inseriti in uno scambio prima di essere consegnati.

Aggiunta di un riconoscimento al tipo di documento

Informazioni su questa attività

Per aggiungere un riconoscimento ad un flusso, eseguire i passi indicati:

1. Se la mappa di riconoscimento funzionale non è fornita da WebSphere Partner Gateway, importare la mappa dal client Data Interchange Services. Fare riferimento a " Importazione manuale di mappe" a pagina 198.
2. Associare la mappa RF ad una definizione del documento:
   a. Fare clic su **Amministrazione hub > Configurazione hub > Mappe > Mappe RF EDI**.
   b. Fare clic sull'icona **Visualizza dettagli** accanto alla mappa.
   c. Fare clic sull'icona **Espandi** accanto al package per espandere fino al livello appropriato (ad esempio, espandere le cartelle **Package** e **Protocollo**, quindi selezionare la transazione).

d. Fare clic su **Salva**.

3. Creare un'interazione per la mappa importata.
   a. Fare clic su **Amministrazione hub > Configurazione hub> Definizione documento**.
   b. Fare clic su **Crea interazione**.
   c. In **Origine**, selezionare il tipo di documento associato al riconoscimento funzionale. Espandere il package ed il protocollo e selezionare il tipo di documento.
   d. In **Destinazione**, selezionare gli stessi valori.
   e. Nell'elenco Azione, selezionare **Pass Through**.
4. Verificare che una definizione del documento sia presente per lo scambio EDI inviato dall'hub ed impostare gli attributi che si desidera associare allo scambio.
   a. Fare clic su **Amministrazione hub > Configurazione hub> Definizione documento**.
   b. Verificare se una definizione del documento già esiste. L'origine sarà N/A, con il protocollo ed il tipo di documento che corrisponde al protocollo ed al tipo di documento utilizzati per distribuire lo scambio. Se, ad esempio, lo scambio verrà consegnato come AS/EDI-X12/ISA, l'origine sarà N/A/EDI-X12/ISA.
   c. Modificare gli attributi che vengono applicati allo scambio consegnato.
   d. Se una definizione del documento non esiste, crearne una selezionando il Package, Protocollo ed il Tipo documento.
5. Creare un'interazione per lo scambio EDI che viene inviato dall'hub dopo che il documento è stato convertito.
   a. Fare clic su **Amministrazione hub > Configurazione hub> Definizioni documento**.
   b. Fare clic su **Crea interazione**.
   c. Selezionare i documenti di origine e di destinazione.
   d. Selezionare **Pass Through** dall'elenco **Azione**.

Risultati

Una volta impostate le interazioni, creare le capacità B2B per i partner. Il partner di destinazione di una trasmissione del riconoscimento funzionale è il partner di origine del documento EDI originale.

- Per il partner di origine, abilitare le definizioni di documenti (in **Imposta origine**) per il riconoscimento funzionale. Abilitare anche una definizione del documento per la busta inviata dall'hub.
- Per il partner di destinazione, abilitare una definizione del documento (in **Imposta destinazione**) per il riconoscimento funzionale. Inoltre, abilitare una definizione del documento per la busta EDI ricevuta.

  Per il riconoscimento funzionale, fare clic sull'icona **Modifica valori dell'attributo** accanto al protocollo, quindi specificare un profilo di busta.

Le fasi dettagliate per la creazione delle capacità B2B sono descritte nella sezione "Impostazione delle capacità B2B" a pagina 26.

Una volta impostate le capacità B2B per i partner, creare le connessioni. Sono necessarie due connessioni:

- Una per il riconoscimento funzionale.

- Una per la busta dall'hub al partner.

Le fasi dettagliate per la creazione delle connessioni sono descritte nella sezione Capitolo 12, "Gestione connessioni", a pagina 237.

Visualizzazione di transazioni e scambi EDI

Informazioni su questa attività

Come menzionato precedentemente in questo capitolo, il Visualizzatore documenti viene utilizzato per visualizzare informazioni sugli scambi e sulle transazioni EDI che costituiscono un flusso di documenti. È possibile visualizzare i documenti non elaborati, gli eventi ed i dettagli di elaborazione dei documenti associati mediante determinati criteri di ricerca. Queste informazioni sono utili se si prova a determinare se uno scambio EDI è stato recapitato correttamente o determinare l'eventuale causa del problema.

Per visualizzare il Visualizzatore documenti, completare le seguenti attività:

1. Fare clic su **Visualizzatori > Visualizzatore documenti**.
2. Selezionare i criteri di ricerca appropriati.
3. Fare clic su **Cerca**.

Per le informazioni sull'utilizzo del Visualizzatore documenti, consultare il manuale *WebSphere Partner Gateway Administrator Guide*.

Capitolo 11. Creazione delle destinazioni

Una volta creati i partner, definire le destinazioni per i partner. Le destinazioni definiscono i punti di entrata nel sistema del partner.

In questo capitolo vengono riportate le seguenti sezioni:

Nota: è necessario utilizzare sempre la stessa istanza del browser con cui si accede alla Console comunità per apportare modifiche alla configurazione di WebSphere Partner Gateway. L'utilizzo simultaneo di più istanze del browser può causare l'eliminazione delle modifiche di configurazione.

Panoramica delle destinazioni

WebSphere Partner Gateway utilizza le destinazioni per instradare i documenti nella corretta destinazione. Il destinatario può essere un partner esterno o il partner interno.
Il protocollo di trasporto in uscita determina le informazioni utilizzate durante la

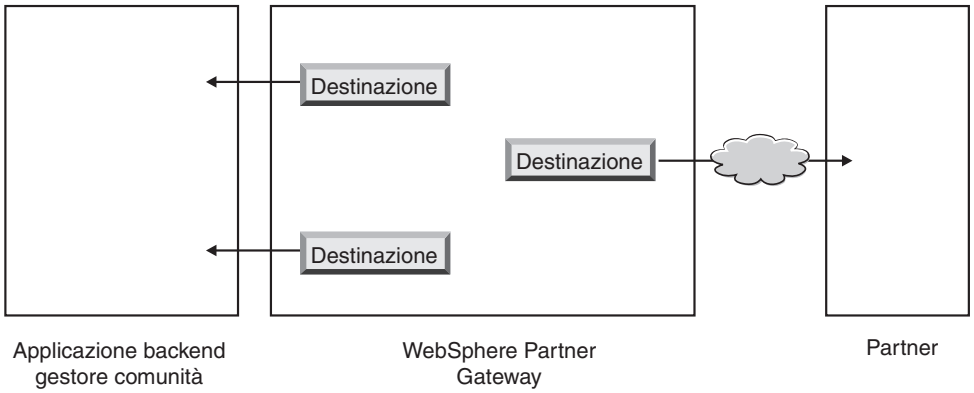


Figura 34. Destinazioni al partner interno e ai partner esterni

configurazione della destinazione.

I seguenti trasporti sono stati supportati (per impostazione predefinita) per le destinazioni del partner:

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

  Nota: è possibile definire una destinazione SMTP solo per i partner esterni (non per il partner interno).
- SFTP
- Directory file
- Script FTP

È inoltre possibile specificare un trasporto definito dall'utente, che è possibile caricare durante la creazione della destinazione.

In qualità di amministratore hub, è possibile impostare le destinazioni per i partner o i partner sono in grado di effettuare questa attività in modo autonomo. In questo capitolo, viene riportato il modo in cui eseguire l'attività per i partner. Per gestire le destinazioni, consultare *Hub Administration tasks Chapter of Administrator Guide*.

Impostazione dei valori globali di trasporto

Informazioni su questa attività

Impostare gli attributi globali di trasporto validi per tutte le destinazioni Script FTP. Se non sono definite le destinazioni Script FTP, questa sezione non è valida.

Il trasporto Script FTP utilizza un meccanismo di blocco che impedisce a più istanze di Script FTP di accedere alla stessa destinazione simultaneamente. I valori predefiniti vengono forniti per esprimere, ad esempio, per quanto tempo l'istanza del gateway ottiene il blocco e quante volte può tentare di recuperarlo, se il blocco è in uso. È anche possibile utilizzare questi valori predefiniti o modificarli.

1. Fare clic su **Amministrazione account > Profili**.
2. Fare clic su **Destinazioni**.
3. Selezionare gli **Attributi globali di trasporto** nella pagina Dettagli della destinazione.

   Se si è aggiornato **Tempo max di blocco (secondi)** o **Tempo max di accodamento (secondi)** quando sono stati specificati i valori di trasporto globale durante la creazione delle destinazioni, questi valori aggiornati si riflettono qui.
4. Se i valori predefiniti sono appropriati per la configurazione, fare clic su **Annulla**. Altrimenti, continuare con gli altri passaggi descritti in questa sezione.
5. Fare clic sull'icona **Modifica** accanto a **Trasporto script FTP**.
6. Per modificare uno o più valori, immettere il nuovo o i nuovi valori. È possibile modificare:

- **Conteggio tentativi blocco**, che indica quante volte viene eseguita la destinazione per ottenere un blocco se il blocco è attualmente in uso. Il valore predefinito è 3.
- **Intervallo tentativi del blocco (secondi)**, che indica il tempo tra un tentativo e l'altro per ottenere il blocco. Il valore predefinito è 260 secondi.
- **Tempo max di blocco (secondi)**, che indica la durata di tempo in cui la destinazione può gestire il blocco. Il valore predefinito è 240 secondi (a meno che non venga modificato quando si creano destinazioni).
- **Tempo max di accodamento (secondi)**, che indica per quanto tempo la destinazione attenderà in una coda per ottenere il blocco. Il valore predefinito è 740 secondi (a meno che non venga modificato quando si creano le destinazioni).

7. Fare clic su **Salva**

Configurazione di un proxy di inoltro

Informazioni su questa attività

Per il trasporto HTTP, è possibile impostare un supporto proxy, in modo che i documenti vengano inviati mediante un server proxy configurato. Con WebSphere Partner Gateway, è possibile impostare i seguenti tipi di supporto:

- Supporto proxy su HTTP
- Supporto proxy su HTTP con autenticazione
- Supporto proxy su SOCKS

Nota: WebSphere Partner Gateway si collega al server Proxy solo sulla porta HTTP.

Una volta impostato un proxy di inoltro, è possibile renderlo globale per il trasporto contrassegnandolo come destinazione predefinita (ad esempio, tutte le destinazioni HTTP utilizzano il proxy di inoltro).

Per impostare un proxy di inoltro, attenersi alla seguente procedura:

1. Fare clic su **Amministrazione account > Profili > Partner**.
2. Fare clic su **Destinazioni**.
3. Fare clic su **Supporto proxy di inoltro**.
4. Nella pagina Elenco proxy di inoltro, fare clic su **Crea**.
5. Digitare un nome per il proxy.
6. Facoltativamente, immettere una descrizione del proxy.
7. Selezionare il tipo di trasporto dall'elenco.

   Nota: i trasporti disponibili sono HTTP e HTTPS.
8. Immettere le informazioni di seguito riportate. Immettere l'host proxy e la porta proxy*o* l'host proxy dei sock e la porta proxy dei sock.
   - Per **host proxy**, immettere il server proxy da utilizzare (ad esempio: http://proxy.abc.com).
   - Per **Porta proxy**, immettere il numero della porta.
   - Se il server proxy richiede un nome utente e una password, specificarli nei campi **Nome utente** e **Password**.
   - Per **Host proxy SOCKS**, immettere il server proxy SOCKS da utilizzare.
   - Per **Porta proxy SOCKS**, immettere il numero della porta.

9. Selezionare la casella se si desidera che questo proxy sia quello predefinito (che può essere utilizzato da un partner che ha specificato il supporto per il proxy).
10. Fare clic su **Salva**.

Nota: la tecnica di tunneling HTTP viene utilizzata nel proxy di inoltro, ma non esiste alcun supporto per il proxy di inoltro sicuro. Il tunnel HTTP viene creato con il server proxy. E' necessario verificare la connettività prima di inviare qualsiasi tipo di dati (HTTP o HTTPS) al partner finale. I dati sono codificati SSL. La porta utilizzata per il proxy di inoltro deve essere la porta 80 HTTP. Si tratta di una passthru dell'handshake SSL tra WebSphere Partner Gateway e il Partner.

Impostazione di una destinazione HTTP

Informazioni su questa attività

Impostare una destinazione HTTP in modo tale che i documenti possano essere inviati dall'hub all'indirizzo IP dei partner. Una volta impostata una destinazione HTTP, è possibile specificare che i documenti siano inviati mediante un server proxy configurato.

Per avviare il processo di creazione di un destinazione HTTP, utilizzare la seguente procedura.

1. Fare clic su **Amministrazione account > Profili**.
2. Inserire i criteri di ricerca e fare clic su **Cerca** oppure fare clic su **Cerca** senza inserire i criteri di ricerca per visualizzare un elenco di tutti i partner.
3. Fare clic sull'icona **Visualizza dettagli** per visualizzare il profilo del partner.
4. Fare clic su **Destinazioni**.
5. Fare clic su **Crea**.

Dettagli della destinazione

Informazioni su questa attività

Dalla pagina **Elenco destinazioni**, effettuare le seguenti operazioni:

1. Inserire un nome per identificare la destinazione. È un campo obbligatorio. Si tratta del nome visualizzato nell'elenco delle destinazioni.
2. In alternativa, indicare lo stato della destinazione. **Abilitato** è il valore predefinito. Una destinazione abilitata può inviare i documenti. Una destinazione disabilitata non può inviare i documenti.
3. In alternativa, indicare se la destinazione sia In linea o Non in linea. Il valore predefinito è **In linea**.
4. In alternativa, immettere una destinazione della destinazione.

Configurazione della destinazione

Informazioni su questa attività

Nella sezione **Configurazione della destinazione** della pagina, effettuare la seguente procedura:

1. Facoltativamente, selezionare un server proxy da utilizzare. L'**elenco Proxy di inoltro** include i server proxy creati, compreso il server proxy predefinito. Il valore predefinito per questo campo è **Usa proxy inoltro predefinito**. Se si desidera che il partner selezionato utilizzi un diverso server proxy, selezionare

tale server dall'elenco. Se non si desidera utilizzare questa funzione con il partner selezionato, scegliere **Non usare proxy di inoltro**.

2. Nel campo **Indirizzo**, inserire l'URI in cui il documento viene recapitato. Questo campo è obbligatorio.

   Il formato è: http://*<nome_server>*:*<porta_facoltativa>*/*<percorso>*

   Un esempio di questo formato è:

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

   Nota: se si specifica l'indirizzo IPv6, fornire il formato numerico, non il nome della macchina o il nome dell'host.

   Gli esempi degli indirizzi IPv6 includono:

   ```
   http://[FEDC:BA98:7654:3210:FEDC:BA98:7654:3210]:80/index.html
   http://[1080:0:0:0:8:800:200C:417A]/index.html
   http://[3ffe:2a00:100:7031::1]
   http://[1080::8:800:200C:417A]/foo
   http://[::192.9.5.5]/ipng
   http://[::FFFF:129.144.52.38]:80/index.html
   http://[2010:836B:4179::836B:4179]
   ```

   Durante l'impostazione di una destinazione da utilizzare per un servizio Web, specificare l'indirizzo URL privato, fornito dal provider del servizio Web. Indica il punto in cui WebSphere Partner Gateway richiama il servizio Web quando agisce come proxy per il provider del servizio Web.

3. Facoltativamente, inserire un nome utente e una password, se richiesti per accedere al server HTTP.
4. Nel campo **Conteggio tentativi**, inserire il numero di volte in base al quale la destinazione tenta di inviare un documento prima di restituire un errore. Il valore predefinito è 3.
5. Nel campo **Intervallo tentativi**, inserire il tempo di attesa della destinazione prima di inviare nuovamente il documento. Il valore predefinito è 300 secondi.
6. Nel campo **Numero di thread**, inserire il numero di documenti che possono essere elaborati simultaneamente. Il valore predefinito è 3.
7. Nel campo **Convalida IP client**, selezionare **Sì** se si desidera convalidare l'indirizzo IP del mittente prima che il documento venga elaborato. Altrimenti, selezionare **No**. Il valore predefinito è **No**.
8. Nel campo **Accoda automaticamente**, selezionare **Sì** se si desidera porre la destinazione fuori linea (automaticamente) se un errore di recapito sta per verificarsi poiché il numero di tentativi è stato esaurito. Altrimenti, selezionare **No**. Il valore predefinito è **No**.

   Durante la sezione di **Accoda automaticamente**, tutti i documenti restano in coda fino a quando la destinazione non ritorna manualmente in linea.
9. Nel campo **Scadenza connessione**, inserire il numero di secondi in cui un socket rimane aperto senza traffico. Il valore predefinito è 120 secondi.
10. Se si desidera configurare la fase di Preelaborazione o Postelaborazione per la destinazione, consultare la sezione "Configurazione degli handler" a pagina 232. Altrimenti, fare clic su **Salva**.

Impostazione di una destinazione HTTPS

Informazioni su questa attività

Impostare una destinazione HTTPS in modo tale che i documenti possano essere inviati dall'hub all'indirizzo IP dei partner. Quando una destinazione HTTPS è stata impostata, è anche possibile specificare i documenti da inviare mediante un server proxy configurato.

Per creare le destinazioni HTTPS, effettuare la seguente procedura.

1. Fare clic su **Amministrazione account > Profili > Partner**.
2. Inserire i criteri di ricerca e fare clic su **Cerca** oppure fare clic su **Cerca** senza inserire i criteri di ricerca per visualizzare un elenco di tutti i partner.
3. Fare clic sull'icona **Visualizza dettagli** per visualizzare il profilo del partner.
4. Fare clic su **Destinazioni**.
5. Fare clic su **Crea**.

Dettagli della destinazione

Informazioni su questa attività

Nella pagina Dettagli della destinazione, effettuare la seguente procedura:

1. Inserire un nome per identificare la destinazione. È un campo obbligatorio.
2. In alternativa, indicare lo stato della destinazione. **Abilitato** è il valore predefinito. Una destinazione abilitata può inviare i documenti. Una destinazione disabilitata non può inviare i documenti.
3. In alternativa, indicare se la destinazione sia In linea o Non in linea. Il valore predefinito è **In linea**.
4. In alternativa, immettere una destinazione della destinazione.
5. Selezionare **HTTPS/1.0** o **HTTPS/1.1** dall'elenco **Trasporto** .

Configurazione della destinazione

Informazioni su questa attività

Nella sezione **Configurazione della destinazione** della pagina, effettuare la seguente procedura:

1. Facoltativamente, selezionare un server proxy da utilizzare. L'**elenco Proxy di inoltro** include i server proxy creati, compreso il server proxy predefinito. Il valore predefinito per questo campo è **Usa proxy inoltro predefinito**. Se si desidera che il partner selezionato utilizzi un diverso server proxy, selezionare tale server dall'elenco. Se non si desidera utilizzare questa funzione con il partner selezionato, scegliere **Non usare proxy di inoltro**.
2. Nel campo **Indirizzo**, inserire l'URI in cui il documento viene recapitato. Questo campo è obbligatorio.

   Il formato è: https://*<nome_server>:<porta_facoltativa>/<percorso>*

   Ad esempio:

   ```
   https://unaltroserver.ibm.com:57443/bcgreceiver/Receiver
   ```

   Nota: se si specifica l'indirizzo IPv6, fornire il formato numerico, non il nome della macchina o il nome dell'host.

   Gli esempi degli indirizzi IPv6 includono:

```
https://[FEDC:BA98:7654:3210:FEDC:BA98:7654:3210]:80/index.html
https://[1080:0:0:0:8:800:200C:417A]/index.html
https://[3ffe:2a00:100:7031::1]
https://[1080::8:800:200C:417A]/foo
https://[::192.9.5.5]/ipng
https://[::FFFF:129.144.52.38]:80/index.html
https://[2010:836B:4179::836B:4179]
```

3. Facoltativamente, inserire un nome utente e una password, se richiesti per accedere al server HTTP protetto.
4. Nel campo **Conteggio tentativi**, inserire il numero di volte in base al quale la destinazione tenta di inviare un documento prima di restituire un errore. Il valore predefinito è 3.
5. Nel campo **Intervallo tentativi**, inserire il tempo di attesa della destinazione prima di inviare nuovamente il documento. Il valore predefinito è 300 secondi.
6. Nel campo **Numero di thread**, inserire il numero di documenti che possono essere elaborati simultaneamente. Il valore predefinito è 3.
7. Nel campo **Convalida IP client**, selezionare **Sì** se si desidera convalidare l'indirizzo IP del mittente prima che il documento venga elaborato. Altrimenti, selezionare **No**. Il valore predefinito è **No**.
8. Nel campo **Convalida Cert SSL client**, selezionare **Sì** se si desidera che il certificato digitale del partner di invio sia convalidato con l'ID di business associato al documento. Il valore predefinito è **No**.
9. Nel campo **Accoda automaticamente**, selezionare **Sì** se si desidera porre la destinazione fuori linea (automaticamente) se un errore di recapito sta per verificarsi poiché il numero di tentativi è stato esaurito. Altrimenti, selezionare **No**. Il valore predefinito è **No**.

   Durante la sezione di **Accoda automaticamente**, tutti i documenti restano in coda fino a quando la destinazione non ritorna manualmente in linea.
10. Nel campo **Scadenza connessione**, inserire il numero di secondi in cui un socket rimane aperto senza traffico. Il valore predefinito è 120 secondi.
11. Se si desidera configurare la fase di Preelaborazione o Postelaborazione per la destinazione, consultare la sezione "Configurazione degli handler" a pagina 232. Altrimenti, fare clic su **Salva**.

Impostazione di una destinazione FTP

Informazioni su questa attività

Per creare una destinazione FTP, effettuare la seguente procedura.

1. Fare clic su **Amministrazione account > Profili > Partner**.
2. Inserire i criteri di ricerca e fare clic su **Cerca** oppure fare clic su **Cerca** senza inserire i criteri di ricerca per visualizzare un elenco di tutti i partner.
3. Fare clic sull'icona **Visualizza dettagli** per visualizzare il profilo del partner.
4. Fare clic su **Destinazioni**.
5. Fare clic su **Crea**.

Nota: la modalità passiva FTP non è supportata. Per il supporto passivo, consultare "Impostazione di una destinazione Script FTP" a pagina 228.

Dettagli della destinazione

Informazioni su questa attività

Nella pagina Dettagli della destinazione, effettuare la seguente procedura:

1. Inserire un nome per identificare la destinazione. Questo è un campo obbligatorio.
2. In alternativa, indicare lo stato della destinazione. **Abilitato** è il valore predefinito. Una destinazione abilitata può inviare i documenti. Una destinazione disabilitata non può inviare i documenti.
3. In alternativa, indicare se la destinazione sia In linea o Non in linea. Il valore predefinito è **In linea**.
4. In alternativa, immettere una destinazione della destinazione.

Configurazione della destinazione

Informazioni su questa attività

Nella sezione **Configurazione della destinazione** della pagina, effettuare la seguente procedura:

1. Nel campo **Indirizzo**, inserire l'URI in cui il documento viene recapitato. Questo campo è obbligatorio.

   Il formato è: ftp://<*nome_server_ftp*>:<*nport*>

   Ad esempio:

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

   Se non si inserisce un numero di porta, viene utilizzata la porta FTP standard.

   Nota: se si specifica l'indirizzo IPv6, fornire il formato numerico, non il nome della macchina o il nome dell'host.

   Gli esempi degli indirizzi IPv6 includono:

   ```
   ftp://[FEDC:BA98:7654:3210:FEDC:BA98:7654:3210]:21
   ftp://[1080:0:0:0:8:800:200C:417A]:21
   ftp://[3ffe:2a00:100:7031::1]:21
   ftp://[1080::8:800:200C:417A]:21
   ftp://[::192.9.5.5]:21
   ftp://[::FFFF:129.144.52.38]:21
   ftp://[2010:836B:4179::836B:4179]:21
   ```
2. Facoltativamente, inserire un nome utente e una password, se richiesti per accedere al server FTP.
3. Nel campo **Conteggio tentativi**, inserire il numero di volte in base al quale la destinazione tenta di inviare un documento prima di restituire un errore. Il valore predefinito è 3.
4. Nel campo **Intervallo tentativi**, inserire il tempo di attesa della destinazione prima di inviare nuovamente il documento. Il valore predefinito è 300 secondi.
5. Nel campo **Numero di thread**, inserire il numero di documenti che possono essere elaborati simultaneamente. Il valore predefinito è 3.
6. Nel campo **Convalida IP client**, selezionare **Sì** se si desidera convalidare l'indirizzo IP del mittente prima che il documento venga elaborato. Altrimenti, selezionare **No**. Il valore predefinito è **No**.
7. Nel campo **Accoda automaticamente**, selezionare **Sì** se si desidera porre la destinazione fuori linea (automaticamente) se un errore di recapito sta per verificarsi poiché il numero di tentativi è stato esaurito. Altrimenti, selezionare **No**. Il valore predefinito è **No**.

   Durante la sezione di **Accoda automaticamente**, tutti i documenti restano in coda fino a quando la destinazione non ritorna manualmente in linea.
8. Nel campo **Scadenza connessione**, inserire il numero di secondi in cui un socket rimane aperto senza traffico. Il valore predefinito è 120 secondi.

9. Nel campo **Usa Nome file univoco**, lasciare la casella selezionata se si desidera che il documento disponga del nome di origine quando viene inviato a destinazione. Altrimenti, deselezionare la casella di spunta; in tal caso, WebSphere Partner Gateway assegnerà un nome al file.
10. Se si desidera configurare la fase di Preelaborazione o Postelaborazione per la destinazione, consultare la sezione "Configurazione degli handler" a pagina 232. Altrimenti, fare clic su **Salva**.

Impostazione di una destinazione SMTP

Informazioni su questa attività

Per creare una destinazione SMTP, effettuare la seguente procedura.

1. Fare clic su **Amministrazione account > Profili > Partner**.
2. Inserire i criteri di ricerca e fare clic su **Cerca** oppure fare clic su **Cerca** senza inserire i criteri di ricerca per visualizzare un elenco di tutti i partner.
3. Fare clic sull'icona **Visualizza dettagli** per visualizzare il profilo del partner.
4. Fare clic su **Destinazioni**.
5. Fare clic su **Crea**.

Dettagli della destinazione

Informazioni su questa attività

Dalla pagina Elenco destinazioni, effettuare le seguenti operazioni:

1. Inserire un nome per identificare la destinazione. È un campo obbligatorio.
2. In alternativa, indicare lo stato della destinazione. **Abilitato** è il valore predefinito. Una destinazione abilitata può inviare i documenti. Una destinazione disabilitata non può inviare i documenti.
3. In alternativa, indicare se la destinazione sia In linea o Non in linea. Il valore predefinito è **In linea**.
4. In alternativa, immettere una destinazione della destinazione.

Configurazione della destinazione

Informazioni su questa attività

Nella sezione **Configurazione della destinazione** della pagina, effettuare la seguente procedura:

1. Nel campo **Indirizzo**, inserire l'URI in cui il documento viene recapitato. Questo campo è obbligatorio.

   Il formato è: mailto:<*utente@nome_server*>

   Ad esempio:

   ```
   mailto:admin@anotherserver.ibm.com
   ```
2. Facoltativamente, inserire un nome utente e una password, se richiesti per accedere al server SMTP.
3. Nel campo **Conteggio tentativi**, inserire il numero di volte in base al quale la destinazione tenta di inviare un documento prima di restituire un errore. Il valore predefinito è 3.
4. Nel campo **Intervallo tentativi**, inserire il tempo di attesa della destinazione prima di inviare nuovamente il documento. Il valore predefinito è 300 secondi.

5. Nel campo **Numero di thread**, inserire il numero di documenti che possono essere elaborati simultaneamente. Il valore predefinito è 3.
6. Nel campo **Convalida IP client**, selezionare **Sì** se si desidera convalidare l'indirizzo IP del mittente prima che il documento venga elaborato. Altrimenti, selezionare **No**. Il valore predefinito è **No**.
7. Nel campo **Accoda automaticamente**, selezionare **Sì** se si desidera porre la destinazione fuori linea (automaticamente) se un errore di recapito sta per verificarsi poiché il numero di tentativi è stato esaurito. Altrimenti, selezionare **No**. Il valore predefinito è **No**.

   Durante la sezione di **Accoda automaticamente**, tutti i documenti restano in coda fino a quando la destinazione non ritorna manualmente in linea.
8. Nel campo **Autenticazione necessaria**, indicare se un nome utente e password vengono forniti nel documento. Il valore predefinito è **No**.
9. Se si desidera configurare la fase di Preelaborazione o Postelaborazione per la destinazione, consultare la sezione "Configurazione degli handler" a pagina 232. Altrimenti, fare clic su **Salva**.

Impostazione di una destinazione JMS

Informazioni su questa attività

Per creare le destinazioni JMS, effettuare la seguente procedura.

1. Fare clic su **Amministrazione account > Profili > Partner**.
2. Inserire i criteri di ricerca e fare clic su **Cerca** oppure fare clic su **Cerca** senza inserire i criteri di ricerca per visualizzare un elenco di tutti i partner.
3. Fare clic sull'icona **Visualizza dettagli** per visualizzare il profilo del partner.
4. Fare clic su **Destinazioni**.
5. Fare clic su **Crea**.

Nota: per informazioni sulla configurazione delle librerie di runtime in modo che WebSphere Partner Gateway possa rilevare i file jar di WebSphere MQ requisiti, consultare "Configurazione delle librerie di runtime" a pagina 40.

Dettagli della destinazione

Informazioni su questa attività

Dalla pagina Elenco destinazioni, effettuare le seguenti operazioni:

1. Inserire un nome per identificare la destinazione. È un campo obbligatorio.
2. In alternativa, indicare lo stato della destinazione. **Abilitato** è il valore predefinito. Una destinazione abilitata può inviare i documenti. Una destinazione disabilitata non può inviare i documenti.
3. In alternativa, indicare se la destinazione sia In linea o Non in linea. Il valore predefinito è **In linea**.
4. In alternativa, immettere una destinazione della destinazione.

Configurazione della destinazione

Informazioni su questa attività

Nella sezione **Configurazione della destinazione** della pagina, effettuare la seguente procedura:

1. Nel campo **Indirizzo**, inserire l'URL in cui il documento viene consegnato. Questo campo è obbligatorio.

   Per WebSphere MQ JMS, il formato dell'URL di destinazione è il seguente:

   `file:///<percorso_collegamento_JNDI_MQ_definito_dall'utente>`

   Ad esempio:

   `file:///opt/JNDI-Directory nel caso di UNIX e`
   `file://c:/temp/ nel caso di Windows.`

   La directory contiene il file ".bindings" per JNDI basato sul file. Questo file indica a WebSphere Partner Gateway il modo in cui instradare il documento nella destinazione prevista.

   - Per una destinazione JMS interna (ossia, la destinazione al sistema di back-end), è necessario che corrisponda al valore inserito (il percorso del file system al file bindings) durante la configurazione di WebSphere Partner Gateway per JMS (fase 5 a pagina 38). Inoltre, è possibile specificare la cartella secondaria per il contesto JMS come parte dell'URL del provider JMS.

     Ad esempio, senza il contesto JMS, immettere `c:/temp/JMS`. Con il contesto JMS, immettere `c:/temp/JMS/JMS`.
   - Per le destinazioni del partner, il partner fornisce probabilmente il file ".bindings".

   Questo campo è obbligatorio.
2. Facoltativamente, inserire un nome utente e una password, se richiesti per accedere alla coda JMS.
3. Nel campo **Conteggio tentativi**, inserire il numero di volte in base al quale la destinazione tenta di inviare un documento prima di restituire un errore. Il valore predefinito è 3.
4. Nel campo **Intervallo tentativi**, inserire il tempo di attesa della destinazione prima di inviare nuovamente il documento. Il valore predefinito è 300 secondi.
5. Nel campo **Numero di thread**, inserire il numero di documenti che possono essere elaborati simultaneamente. Il valore predefinito è 3.
6. Nel campo **Convalida IP client**, selezionare **Sì** se si desidera convalidare l'indirizzo IP del mittente prima che il documento venga elaborato. Altrimenti, selezionare **No**. Il valore predefinito è **No**.
7. Nel campo **Accoda automaticamente**, selezionare **Sì** se si desidera porre la destinazione fuori linea (automaticamente) se un errore di recapito sta per verificarsi poiché il numero di tentativi è stato esaurito. Altrimenti, selezionare **No**. Il valore predefinito è **No**.

   Durante la sezione di **Accoda automaticamente**, tutti i documenti restano in coda fino a quando la destinazione non ritorna manualmente in linea.
8. Nel campo **Autenticazione necessaria**, indicare se un nome utente e password vengono forniti nel documento. Il valore predefinito è **No**.
9. Nel campo **Nome factory JMS**, inserire il nome della classe Java che il provider JMS utilizza per collegarsi alla coda JMS. Questo campo è obbligatorio.

   Per le destinazioni JMS interne, questo nome deve corrispondere a quello specificato con il comando `define qcf` al momento della creazione del file bindings (fase 4 a pagina 39).

   Se viene immessa la cartella secondaria per il contesto JMS al passo 1, immettere solo il nome factory qui (ad esempio, `Hub`). Se non è stata immessa la cartella secondaria per il contesto JMS nel campo **Indirizzo**, specificare tale cartella prima del nome factory (ad esempio `JMS/Hub`).

10. Nel campo **Classe di messaggi JMS**, inserire la classe di messaggi. Le scelte sono tutte le classi di messaggi JMS, come TextMessage o BytesMessage. Questo campo è obbligatorio.
11. Nel campo **Tipo di messaggio JMS**, inserire il tipo di messaggio. Questo è un campo facoltativo.
12. Nel campo **Package URL del provider**, inserire il nome delle classi (o file JAR) che Java utilizza per comprendere l'URL del contesto JMS. Questo campo è facoltativo. Se un valore non è stato specificato, viene utilizzato il percorso del file system del file bindings.
13. Nel campo **Nome coda JMS**, inserire il nome della coda JMS in cui i documenti vengono inviati. Questo campo è obbligatorio.

    Per le destinazioni JMS interne, questo nome deve corrispondere a quello specificato con il comando `define q` al momento della creazione del file bindings (fase 4 a pagina 39).

    Se viene immessa la cartella secondaria per il contesto JMS al passo 1 a pagina 223, immettere solo il nome della coda qui (ad esempio `outQ`). Se non è stata immessa la cartella secondaria per il contesto JMS nell'URL del provider JMS, specificare tale cartella prima del nome factory (ad esempio `JMS/outQ`).
14. Nel campo **Nome factory JNDI JMS**, inserire il nome della factory utilizzato per collegarsi al servizio nome. Questo campo è obbligatorio. Il valore di com.sun.jndi.fscontext.RefFSContextFactory è l'unico probabilmente utilizzato, se si imposta la configurazione JMS per WebSphere MQ come descritto in "Configurazione dell'hub per il protocollo di trasporto JMS" a pagina 37.
15. Se si desidera configurare la fase di Preelaborazione o Postelaborazione per la destinazione, consultare la sezione "Configurazione degli handler" a pagina 232. Altrimenti, fare clic su **Salva**.

Impostazione di una destinazione file-directory

Informazioni su questa attività

Per creare le destinazioni file-directory, effettuare la seguente procedura.

1. Fare clic su **Amministrazione account > Profili > Partner**.
2. Inserire i criteri di ricerca e fare clic su **Cerca** oppure fare clic su **Cerca** senza inserire i criteri di ricerca per visualizzare un elenco di tutti i partner.
3. Fare clic sull'icona **Visualizza dettagli** per visualizzare il profilo del partner.
4. Fare clic su **Destinazioni**.
5. Fare clic su **Crea**.

Dettagli della destinazione

Informazioni su questa attività

Dalla pagina Elenco destinazioni, effettuare le seguenti operazioni:

1. Inserire un nome per identificare la destinazione. È un campo obbligatorio.
2. In alternativa, indicare lo stato della destinazione. **Abilitato** è il valore predefinito. Una destinazione abilitata può inviare i documenti. Una destinazione disabilitata non può inviare i documenti.
3. In alternativa, indicare se la destinazione sia In linea o Non in linea. Il valore predefinito è **In linea**.
4. In alternativa, immettere una destinazione della destinazione.

Configurazione della destinazione

Informazioni su questa attività

Nella sezione **Configurazione della destinazione** della pagina, effettuare la seguente procedura:

1. Nel campo **Indirizzo**, inserire l'URI in cui il documento viene recapitato. Questo campo è obbligatorio.

   Il formato per i sistemi UNIX e Windows in cui la directory file si trova sulla stessa unità su cui è stato installato WebSphere Partner Gateway è: file://<*path_to_target_directory*>

   Ad esempio:

   ```
   file://localfiledir
   ```

   in cui *localfiledir* è una directory della directory root.

   Per i sistemi Windows in cui la directory file si trova su un'unità diversa rispetto a WebSphere Partner Gateway, il formato è: file://<*drive_letter*>:/<*path*>
2. Nel campo **Conteggio tentativi**, inserire il numero di volte in base al quale la destinazione tenta di inviare un documento prima di restituire un errore. Il valore predefinito è 3.
3. Nel campo **Intervallo tentativi**, inserire il tempo di attesa della destinazione prima di inviare nuovamente il documento. Il valore predefinito è 300 secondi.
4. Nel campo **Numero di thread**, inserire il numero di documenti che devono essere elaborati simultaneamente. Il valore predefinito è 3.
5. Nel campo **Convalida IP client**, selezionare **Sì** se si desidera convalidare l'indirizzo IP del mittente prima che il documento venga elaborato. Altrimenti, selezionare **No**. Il valore predefinito è **No**.
6. Nel campo **Accoda automaticamente**, selezionare **Sì** se si desidera porre la destinazione fuori linea (automaticamente) se un errore di recapito sta per verificarsi poiché il numero di tentativi è stato esaurito. Altrimenti, selezionare **No**. Il valore predefinito è **No**.

   Durante la sezione di **Accoda automaticamente**, tutti i documenti restano in coda fino a quando la destinazione non ritorna manualmente in linea.
7. Nel campo **Usa Nome file univoco**, lasciare la casella selezionata se si desidera che il documento disponga del nome di origine quando viene inviato a destinazione. Altrimenti, deselezionare la casella di spunta; in tal caso, WebSphere Partner Gateway assegnerà un nome al file.
8. Se si desidera configurare la fase di Preelaborazione o Postelaborazione per la destinazione, consultare la sezione "Configurazione degli handler" a pagina 232. Altrimenti, fare clic su **Salva**.

Impostazione di una destinazione FTPS

Informazioni su questa attività

Per creare le destinazioni FTPS, effettuare la seguente procedura.

1. Fare clic su **Amministrazione account > Profili > Partner**.
2. Inserire i criteri di ricerca e fare clic su **Cerca** oppure fare clic su **Cerca** senza inserire i criteri di ricerca per visualizzare un elenco di tutti i partner.
3. Fare clic sull'icona **Visualizza dettagli** per visualizzare il profilo del partner.
4. Fare clic su **Destinazioni**.
5. Fare clic su **Crea**.

Nota: la modalità passiva FTPS non è supportata. Per il supporto passivo, consultare "Impostazione di una destinazione Script FTP" a pagina 228.

Dettagli della destinazione

Informazioni su questa attività

Dalla pagina Elenco destinazioni, effettuare le seguenti operazioni:

1. Inserire un nome per identificare la destinazione. È un campo obbligatorio.
2. In alternativa, indicare lo stato della destinazione. **Abilitato** è il valore predefinito. Una destinazione abilitata può inviare i documenti. Una destinazione disabilitata non può inviare i documenti.
3. In alternativa, indicare se la destinazione sia In linea o Non in linea. Il valore predefinito è **In linea**.
4. In alternativa, immettere una destinazione della destinazione.

Configurazione della destinazione

Informazioni su questa attività

Nella sezione **Configurazione della destinazione** della pagina, effettuare la seguente procedura:

1. Nel campo **Indirizzo**, inserire l'URI in cui il documento viene recapitato. Questo campo è obbligatorio.

   Il formato è: ftp://<*nome_server_ftp*>:<*nport*>

   Ad esempio:

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

   Se non si inserisce un numero di porta, viene utilizzata la porta FTP standard.
2. Facoltativamente, inserire un nome utente e una password, se richiesti per accedere al server FTP.
3. Nel campo **Conteggio tentativi**, inserire il numero di volte in base al quale la destinazione tenta di inviare un documento prima di restituire un errore. Il valore predefinito è 3.
4. Nel campo **Intervallo tentativi**, inserire il tempo di attesa della destinazione prima di inviare nuovamente il documento. Il valore predefinito è 300 secondi.
5. Nel campo **Numero di thread**, inserire il numero di documenti che devono essere elaborati simultaneamente. Il valore predefinito è 3.
6. Nel campo **Convalida IP client**, selezionare **Sì** se si desidera convalidare l'indirizzo IP del mittente prima che il documento venga elaborato. Altrimenti, selezionare **No**. Il valore predefinito è **No**.
7. Nel campo **Accoda automaticamente**, selezionare **Sì** se si desidera porre la destinazione fuori linea (automaticamente) se un errore di recapito sta per verificarsi poiché il numero di tentativi è stato esaurito. Altrimenti, selezionare **No**. Il valore predefinito è **No**.

   Durante la sezione di **Accoda automaticamente**, tutti i documenti restano in coda fino a quando la destinazione non ritorna manualmente in linea.
8. Nel campo **Scadenza connessione**, inserire il numero di secondi in cui un socket rimane aperto senza traffico. Il valore predefinito è 120 secondi.
9. Nel campo **Usa Nome file univoco**, lasciare la casella selezionata se si desidera che il documento disponga del nome di origine quando viene inviato a destinazione. Altrimenti, deselezionare la casella di spunta; in tal caso, WebSphere Partner Gateway assegnerà un nome al file.

10. Se si desidera configurare la fase di Preelaborazione o Postelaborazione per la destinazione, consultare la sezione “Configurazione degli handler” a pagina 232. Altrimenti, fare clic su **Salva**.

Impostazione di una destinazione SFTP

Informazioni su questa attività

Si imposta una destinazione SFTP in modo tale che i documenti possano essere inviati dall'hub all'indirizzo IP dei partner. L'adattatore si collega al server SFTP e invia il documento al server SFTP. I dati del documento vengono forniti all'adattatore come un flusso.

Per creare le destinazioni SFTP, utilizzare la seguente procedura.

1. Fare clic su **Amministrazione account > Profili > Partner**.
2. Inserire i criteri di ricerca e fare clic su **Cerca** oppure fare clic su **Cerca** senza inserire i criteri di ricerca per visualizzare un elenco di tutti i partner.
3. Fare clic sull'icona **Visualizza dettagli** per visualizzare il profilo del partner.
4. Fare clic su **Destinazioni**.
5. Fare clic su **Crea**.

Dettagli della destinazione

Informazioni su questa attività

Nella pagina Dettagli della destinazione, completare la seguente procedura:

1. Inserire un nome per identificare la destinazione. Questo è un campo obbligatorio.
2. In alternativa, indicare lo stato della destinazione. **Abilitato** è il valore predefinito. Una destinazione abilitata può inviare i documenti. Una destinazione disabilitata non può inviare i documenti.
3. In alternativa, indicare se la destinazione sia In linea o Non in linea. Il valore predefinito è **In linea**.
4. In alternativa, immettere una destinazione della destinazione.
5. Selezionare **SFTP** dall'elenco **Trasporto**.

Configurazione della destinazione

Informazioni su questa attività

Nella sezione **Configurazione della destinazione** della pagina, effettuare la seguente procedura:

1. Immettere **IP host SFTP / Nome host**. Accetta un massimo di 100 caratteri. È anche possibile immettere indirizzi IP, IPv4 e IPv6.
2. Immettere il **Numero porta**. Il valore minimo è 1 e il massimo è 65535. Il valore predefinito è 22.
3. Immettere la **Directory di output**. Accetta un massimo di 100 caratteri. Può contenere i caratteri in base alla locale.
4. Nel campo **Tipo di autenticazione**, selezionare l'autenticazione chiave pubblica o nome utente/password.
5. Immettere il **Nome utente** e la **Password** per nome utente/password. Se il tipo di autenticazione è autenticazione chiave pubblica, è necessario utilizzare il **File**

di chiavi private (chiavi) e la **Passphrase** (certificati configurati nella console). **File di chiavi private** è il percorso del file di chiavi private in formato OpenSSH.

6. La chiave privata deve essere salvata in un file e il percorso deve essere impostato. Sono supportati i certificati X.509, ma se l'adattatore della risorsa richiede la chiave privata in formato OpenSSH, utilizzare il formato OpenSSH.
7. **Codifica EIS** è la codifica del server FTP. Utilizzare questo valore per impostare la codifica per la connessione di controllo del server FTP.
8. Immettere la configurazione dell'handler e fare clic su **Salva** per salvare i dettagli di configurazione.

Impostazione di una destinazione Script FTP

Una destinazione Script FTP viene eseguita in base alla pianificazione impostata. Il comportamento di una destinazione Script FTP è regolata da uno script di comandi FTP.

Nota: se il database non è attivo e l'utente blocco è impostato su ″sì″, la destinazione Script FTP potrebbe non funzionare in quanto non riceverà il blocco dal database

Creazione dello script FTP

Informazioni su questa attività

Per utilizzare una destinazione Script FTP, creare un file che include tutti i comandi FTP richiesti, che possono essere accettati dal server FTP.

1. Creare uno script per le destinazioni, per indicare le azioni che si desidera eseguire. Di seguito è riportato un esempio di script di connessione al server FTP specificato (con nome e password specificati), passando alla directory specificata sul server.

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

   I segnaposto (ad esempio, %BCGSERVERIP%) sono stati sostituiti quando la destinazione è stata inserita nel servizio dai valori immessi al momento della creazione di una determinata istanza di una destinazione Script FTP, come riportato nella seguente tabella:

Tabella 28. Modalità in cui i parametri di script sono associati alle voci del campo di destinazione Script FTP

Parametro dello script	Voce del campo di destinazione Script FTP
%BCGSERVERIP%	IP server
%BCGUSERID%	ID utente
%BCGPASSWORD%	Password
%BCGOPTIONx%	Opzione*x*, in **Attributi definiti dall'utente**

   È possibile gestire al massimo 10 opzioni definite dall'utente.

2. Salvare il file.

Comandi script FTP

È possibile utilizzare i seguenti comandi durante la creazione dello script:

- ascii, binario, passivo, epsv

  Questi comandi non vengono inviati al server FTP. Modificano la modalità di trasferimento (ascii, binario o passivo) al server FTP.

- cd

  Questo comando passa alla directory specificata.

- delete

  Questo comando rimuove un file dal server FTP.

- mkdir

  Questo comando rimuove una directory dal server FTP.

- mput

  Questo comando utilizza un singolo argomento, che specifica uno o più file da trasferire al sistema remoto. Questo argomento può contenere i caratteri globali standard per identificare più file ('*' e '?').

- mputren

  Per questo comando sono validi tre argomenti, <source>, <temporary> e <target>, dove un asterisco (*) rappresenta il nome file corrente in fase di elaborazione.

  source Il nome del file in fase di memorizzazione sul server FTP. Il valore previsto è un asterisco (*).

  temporary
  Il nome del file temporaneo da utilizzare quando si memorizza l'<origine> sul server FTP.

  destinazione
  Il nome file da utilizzare per la ridenominazione di quello <temporaneo>. Dopo la ridenominazione di questo file, il file temporaneo non esisterà più.

  Esempi:

  `mputren * *.tmp *`
  Quest'esempio memorizza il file corrente sul server FTP con l'estensione .tmp. Dopo la memorizzazione del file sul server, il server verrà ridenominato, assumendo nuovamente il nome originario.

  `mputren * *.tmp *.ready`
  Quest'esempio memorizza il file corrente sul server FTP con l'estensione .tmp. Dopo la memorizzazione del file sul server, il server verrà ridenominato, assumendo nuovamente il nome originario, con l'estensione .ready.

  `mputren * *.tmp /complete/*`
  Quest'esempio memorizza il file corrente sul server FTP con l'estensione .tmp. Dopo la memorizzazione del file sul server, il server verrà ridenominato, assumendo nuovamente il nome originario, ma esisterà nella directory /complete. Il file temporaneo *.tmp non esisterà più.

  `mputren * *.tmp /complete/*.final`
  Quest'esempio memorizza il file corrente sul server FTP con l'estensione .tmp. Dopo la memorizzazione del file sul server, il server verrà

ridenominato, assumendo nuovamente il nome originario, ma esisterà nella directory /complete con un'estensione .final. Il file temporaneo *.tmp non esisterà più.

- open

  Questo comando utilizza tre parametri - l'indirizzo IP del server FTP, il nome utente e una password. Tali parametri consentono di mappare le variabili %BCGSERVERIP%, %BCGUSERID% e %BCGPASSWORD%.

  Pertanto, la prima riga dello script di destinazione Script FTP deve essere:

  ```
  open %BCGSERVERIP% %BCGUSERID% %BCGPASSWORD%
  ```

- quit

  Questo comando termina una connessione esistente ad un server FTP.

- quote

  Questo comando indica che tutto ciò che segue QUOTE deve essere inviato al sistema remoto come comando. In tal modo, si inviano i comandi ad un server FTP remoto che potrebbe non essere definito nel protocollo FTP standard.

- rmdir

  Questo comando rimuove una directory dal server FTP.

- site

  Questo comando può essere utilizzato per inviare comandi specifici del sito al sistema remoto. Il sistema remoto stabilisce se il contenuto di questo comando è valido.

Destinazioni Script FTP

Informazioni su questa attività

Se le destinazioni Script FTP saranno utilizzate, effettuare le seguenti attività:

Per creare le destinazioni Script FTP, effettuare la seguente procedura.

1. Fare clic su **Amministrazione account > Profili > Partner**.
2. Inserire i criteri di ricerca e fare clic su **Cerca** oppure fare clic su **Cerca** senza inserire i criteri di ricerca per visualizzare un elenco di tutti i partner.
3. Fare clic sull'icona **Visualizza dettagli** per visualizzare il profilo del partner.
4. Fare clic su **Destinazioni**.
5. Fare clic su **Crea**.

Dettagli della destinazione

Informazioni su questa attività

Dalla pagina Elenco destinazioni, effettuare le seguenti operazioni:

1. Inserire un nome per identificare la destinazione. È un campo obbligatorio.
2. In alternativa, indicare lo stato della destinazione. **Abilitato** è il valore predefinito. Una destinazione abilitata può inviare i documenti. Una destinazione disabilitata non può inviare i documenti.
3. In alternativa, indicare se la destinazione sia In linea o Non in linea. Il valore predefinito è **In linea**.
4. In alternativa, immettere una destinazione della destinazione.

Configurazione della destinazione

Informazioni su questa attività

Nella sezione **Configurazione della destinazione** della pagina, effettuare la seguente procedura:

1. Immettere l'indirizzo IP del server FTP a cui si inviano i documenti. Il valore immesso sostituisce %BCGSERVERIP% quando si esegue lo script FTP.

   Nota: se si specifica l'indirizzo IPv6, fornire il formato numerico, non il nome della macchina o il nome dell'host.

   Gli esempi degli indirizzi IPv6 includono:

   ```
   FEDC:BA98:7654:3210:FEDC:BA98:7654:3210
   1080:0:0:0:8:800:200C:417A
   3ffe:2a00:100:7031::1
   1080::8:800:200C:417A
   ::192.9.5.5
   ::FFFF:129.144.52.38
   2010:836B:4179::836B:4179
   ```

2. Inserire l'ID utente e la password necessari per accedere al server FTP. I valori immessi sostituiscono %BCGUSERID% e %BCGPASSWORD% quando si esegue lo script FTP.
3. Se la destinazione è in modalità protetta, fare clic su **Sì** per **Modalità FTPS**. Altrimenti, utilizzare il valore predefinito di **No**.
4. Caricare il file di script seguendo questi passi:
   a. Fare clic su **Carica file di script**.
   b. Immettere il nome del file che contiene lo script per l'elaborazione dei documenti oppure utilizzare **Sfoglia** per navigare nel file.
   c. Selezionare il **Tipo di codifica del file script**.
   d. Fare clic su **Carica file** per caricare il file di script nella casella di testo **File di script al momento caricato**.
   e. Se il file di script è quello che si desidera utilizzare, fare clic su **Salva**.
   f. Fare clic su **Chiudi finestra**.
5. Nel campo **Conteggio tentativi**, inserire il numero di volte in base al quale la destinazione tenta di inviare un documento prima di restituire un errore. Il valore predefinito è 3.
6. Nel campo **Intervallo tentativi**, inserire il tempo di attesa della destinazione prima di inviare nuovamente il documento. Il valore predefinito è 300 secondi.
7. Nel campo **Scadenza connessione**, inserire il numero di secondi in cui un socket rimane aperto senza traffico. Il valore predefinito è 120 secondi.
8. Nel campo **Utente blocco**, indicare se la destinazione richiede un blocco, in modo tale che nessuna altra istanza di una destinazione Script FTP possa ottenere l'accesso alla stessa directory del server FTP contemporaneamente.

Nota: i valori di **Attributi globali script FTP** sono già riempiti e non è possibile modificarli in questa pagina. Per modificare questi valori, si utilizza la pagina Attributi globali di trasporto, come descritto in "Impostazione dei valori globali di trasporto" a pagina 214.

Attributi definiti dall'utente

Informazioni su questa attività

Se si desidera specificare attributi aggiuntivi, eseguire questi passaggi. Il valore immesso per l'opzione sostituisce %BCGOPTION*x*% quando si esegue lo script FTP (dove *x* corrisponde al numero dell'opzione).

1. Fare clic su **Nuovo**.
2. Immettere un valore accanto a **Opzione 1**
3. Se si dispone di attributi aggiuntivi da specificare, fare di nuovo clic su **Nuovo** ed immettere in valore.
4. Ripetere il passaggio 3 per tutti gli attributi che si desidera definire.

Si supponga, ad esempio che lo script FTP sia come segue:

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

%BCGOPTION% in questo caso dovrebbe essere della directory.

Pianificazione

Informazioni su questa attività

Nella sezione Pianifica della pagina, eseguire questi passaggi:

1. Specificare se si desidera la pianificazione basata sul calendario o quella basata sull'intervallo.
   - Se è stato selezionato **Pianificazione basata sull'intervallo**, selezionare il numero di secondi che devono intercorrere prima di eseguire il polling della destinazione (o accettare il valore predefinito).
   - Se si seleziona **Pianificazione basata sul calendario**, scegliere il tipo di pianificazione (**Pianificazione giornaliera**, **Pianificazione settimanale** o **Pianificazione personalizzata**).
     - Se è stata selezionata **Pianificazione giornaliera**, immettere l'ora in cui si desidera eseguire il polling della destinazione.
     - Se si seleziona **Pianificazione settimanale**, selezionare uno o più giorni della settimana oltre all'ora del giorno.
     - Se si seleziona **Pianificazione personalizzata**, selezionare l'ora del giorno e scegliere **Intervallo** o **Giorni selettivi** per la settimana e il mese. Con **Intervallo**, si specifica la data di inizio e quella di fine. (Ad esempio, fare clic su **Lun** e **Ven** se si desidera effettuare il polling del gateway ad una certa ora solo settimanalmente). Con **Giorni selettivi**, si scelgono i giorni specifici della settimana e del mese.
2. Se si desidera configurare la fase di Preelaborazione o Postelaborazione per la destinazione, consultare la sezione "Configurazione degli handler". Altrimenti, fare clic su **Salva**.

Configurazione degli handler

Informazioni su questa attività

E' possibile modificare i due punti di elaborazione per una destinazione--Preelaborazione e Postelaborazione.

Per impostazione predefinita, non viene fornito alcun handler per la fase Preelaborazione o Postelaborazione e, di conseguenza, nessun handler viene elencato nell'**Elenco disponibile**. Se è stato caricato un handler, è possibile selezionarlo e spostarlo nell'**Elenco configurato**.

Per applicare un handler scritto dall'utente per questi punti di configurazione, è necessario caricare prima l'handler. Fare riferimento al manuale *Guida alla configurazione dell'hub* per la procedura di caricamento dell'handler. Quindi procedere nel modo seguente:

1. Selezionare **preelaborazione** o **postelaborazione** dall'elenco **Handler del punto di configurazione**.
2. Selezionare un handler nell'**Elenco disponibile** e fare clic su **Aggiungi**.
3. Se si desidera modificare gli attributi dell'handler, selezionarlo nell'**Elenco configurato** e fare clic su **Configura**. Viene visualizzato l'elenco di attributi che è possibile modificare. Apportare le modifiche necessarie e fare clic su **Imposta valori**.
4. Fare clic su **Salva**.

È possibile modificare ulteriormente l'**Elenco configurato** come segue:

- Rimuovere un handler selezionandolo nell'**Elenco configurato** e facendo clic su **Rimuovi**. L'handler viene spostato nell'**Elenco disponibile**.
- Disporre nuovamente l'ordine in base al quale l'handler viene elaborato selezionandolo e facendo clic su **Sposta su** o **Sposta giù**.

Impostazione di una destinazione per un trasporto definito dall'utente

Informazioni su questa attività

Se si desidera caricare un trasporto definito dall'utente, procedere nel modo seguente.

1. Fare clic su **Amministrazione account > Profili > Partner**.
2. Fare clic su **Destinazioni**.
3. Fare clic su **Gestisci tipi di trasporti**.
4. Inserire il nome di un file XML che definisce il trasporto (o utilizzare **Sfoglia** per navigare nel file).
5. Utilizzare il valore predefinito **Sì** per **Salva nel database**. Selezionare **No** se si desidera controllare questo trasporto prima di inserirlo nella produzione.
6. Specificare se questo file deve sostituire un file con lo stesso nome già presente nel database.
7. Fare clic su **Carica**.

   Nota: nella pagina Gestisci tipi di trasporto, è anche possibile eliminare un tipo di trasporto definito dall'utente. È impossibile eliminare un trasporto fornito da WebSphere Partner Gateway. Inoltre, non è possibile eliminare un trasporto definito dall'utente una volta utilizzato per creare una destinazione.
8. Fare clic su **Crea**
9. Inserire un nome per identificare la destinazione. È un campo obbligatorio.
10. In alternativa, indicare lo stato della destinazione. **Abilitato** è il valore predefinito. Una destinazione abilitata può inviare i documenti. Una destinazione disabilitata non può inviare i documenti.
11. In alternativa, indicare se la destinazione sia In linea o Non in linea. Il valore predefinito è **In linea**.

12. In alternativa, immettere una destinazione della destinazione.
13. Completare i campi (che saranno univoci per ciascun trasporto definito dall'utente) e fare quindi clic su **Salva**.

Impostazione di una destinazione SFTP

Informazioni su questa attività

Si imposta una destinazione SFTP in modo tale che i documenti possano essere inviati dall'hub all'indirizzo IP dei partner. L'adattatore si collega al server SFTP e invia il documento al server SFTP. I dati del documento vengono forniti all'adattatore come un flusso.

Per creare le destinazioni SFTP, utilizzare la seguente procedura.

1. Fare clic su **Amministrazione account > Profili > Partner**.
2. Inserire i criteri di ricerca e fare clic su **Cerca** oppure fare clic su **Cerca** senza inserire i criteri di ricerca per visualizzare un elenco di tutti i partner.
3. Fare clic sull'icona **Visualizza dettagli** per visualizzare il profilo del partner.
4. Fare clic su **Destinazioni**.
5. Fare clic su **Crea**.

Dettagli della destinazione

Informazioni su questa attività

Nella pagina Dettagli della destinazione, completare la seguente procedura:

1. Inserire un nome per identificare la destinazione. Questo è un campo obbligatorio.
2. In alternativa, indicare lo stato della destinazione. **Abilitato** è il valore predefinito. Una destinazione abilitata può inviare i documenti. Una destinazione disabilitata non può inviare i documenti.
3. In alternativa, indicare se la destinazione sia In linea o Non in linea. Il valore predefinito è **In linea**.
4. In alternativa, immettere una destinazione della destinazione.
5. Selezionare **SFTP** dall'elenco **Trasporto**.

Configurazione della destinazione

Informazioni su questa attività

Nella sezione **Configurazione della destinazione** della pagina, effettuare la seguente procedura:

1. Immettere **IP host SFTP / Nome host**. Accetta un massimo di 100 caratteri. È anche possibile immettere indirizzi IP, IPv4 e IPv6.
2. Immettere il **Numero porta**. Il valore minimo è 1 e il massimo è 65535. Il valore predefinito è 22.
3. Immettere la **Directory di output**. Accetta un massimo di 100 caratteri. Può contenere i caratteri in base alla locale.
4. Nel campo **Tipo di autenticazione**, selezionare l'autenticazione chiave pubblica o nome utente/password.
5. Immettere il **Nome utente** e la **Password** per nome utente/password. Se il tipo di autenticazione è autenticazione chiave pubblica, è necessario utilizzare il **File**

di chiavi private (chiavi) e la **Passphrase** (certificati configurati nella console). **File di chiavi private** è il percorso del file di chiavi private in formato OpenSSH.

6. La chiave privata deve essere salvata in un file e il percorso deve essere impostato. Sono supportati i certificati X.509, ma se l'adattatore della risorsa richiede la chiave privata in formato OpenSSH, utilizzare il formato OpenSSH.
7. **Codifica EIS** è la codifica del server FTP. Utilizzare questo valore per impostare la codifica per la connessione di controllo del server FTP.
8. Immettere la configurazione dell'handler e fare clic su **Salva** per salvare i dettagli di configurazione.

Specifica di una destinazione predefinita

Informazioni su questa attività

Una volta create le destinazioni per il partner interno o un partner, selezionare una delle destinazioni come destinazione predefinita.

1. Fare clic su **Amministrazione account > Profili > Partner**.
2. Inserire i criteri di ricerca e fare clic su **Cerca** oppure fare clic su **Cerca** senza inserire i criteri di ricerca per visualizzare un elenco di tutti i partner.
3. Fare clic sull'icona **Visualizza dettagli** per visualizzare il profilo del partner.
4. Fare clic su **Destinazioni**.
5. Fare clic su **Visualizza destinazioni predefinite**.

   Viene visualizzato un elenco delle destinazioni definito per il partner.
6. Nell'elenco **Produzione**, selezionare la destinazione predefinita per questo partner. È anche possibile impostare le destinazioni predefinite per le altre tipologie di destinazioni, come ad esempio **Verifica**.
7. Fare clic su **Salva**.

Capitolo 12. Gestione connessioni

Una volta create le capacità B2B dei partner, si stabiliscono le connessioni tra il partner interno ed i partner esterni. In questo capitolo vengono riportate le seguenti sezioni:

- "Panoramica sulle connessioni"
- "Attivazione delle connessioni del partner"
- "Specifica e modifica di attributi" a pagina 238

Nota: è necessario utilizzare sempre la stessa istanza del browser con cui si accede alla Console comunità per apportare modifiche alla configurazione di WebSphere Partner Gateway. L'utilizzo simultaneo di più istanze del browser può causare l'eliminazione delle modifiche di configurazione.

Panoramica sulle connessioni

Impostare una connessione tra i partner per ciascuna tipologia di documento che sarà scambiata. Ad esempio, è possibile disporre di più connessioni dal partner interno allo stesso partner, poiché l'impacchettamento, il protocollo, il tipo di documento, l'azione o la mappa potrebbero essere diversi.

Durante l'attivazione delle connessioni, è possibile specificare gli attributi per il partner di origine o di destinazione. Eventuali attributi impostati al livello della connessione hanno la priorità sugli attributi impostati al livello delle capacità B2B (per un determinato partner) o al livello della definizione del documento.

Per i documenti EDI, XML e ROD, si dispone di più connessioni per ciascuno scambio, se lo scambio coinvolge l'operazione di enveloping e la conversione. Si possono definire connessioni per questi tipi di documenti selezionandole da un insieme di profili associati alla connessione. Fare riferimento a "Profili di connessione" a pagina 188 per i dettagli.

Configurazione di più partner interni

WebSphere Partner Gateway non presenta alcuna limitazione sul numero di partner interni. È necessario configurare il partner interno predefinito per fornire la compatibilità con le versioni precedenti per il servizio Web e i documenti binari che fluiscono nelle funzioni di supporto FTPScript. Per ulteriori informazioni sulla configurazione dei servizi Web e del documento binario per più partner interni, consultare i tipi di documento Configurazione capitolo.

Attivazione delle connessioni del partner

Informazioni su questa attività

Le connessioni del partner contengono le informazioni necessarie per lo scambio appropriato di ciascun tipo di documento. Un documento non può essere instradato a meno che non esista una connessione tra il partner interno ed uno dei suoi partner esterni.

Il sistema crea automaticamente le connessioni tra il partner interno ed esterno in base alle capacità B2B e alle interazioni.

Ricercare queste connessioni e attivarle.

Quando si seleziona un'Origine e una Destinazione, accertarsi che l'origine sia univoca.

Attenersi alla seguente procedura per effettuare la ricerca di base per le connessioni e quindi attivarle.

1. Fare clic su **Amministrazione account > Connessioni**. Viene visualizzata la pagina Gestisci connessioni.
2. In **Origine**, selezionare un'origine. Ad esempio, se si imposta uno scambio creato dal partner interno, selezionare il partner interno.
3. In **Destinazione**, selezionare una destinazione. Ad esempio, se si imposta uno scambio che sarà ricevuto da un partner, selezionare tale partner.

   Nota: quando si crea una nuova connessione, il valore di Origine e quello di Destinazione devono essere univoci.
4. Fare clic su **Cerca** per cercare i collegamenti che corrispondono al criterio.

   Nota: è, inoltre, possibile utilizzare la pagina di Ricerca avanzata, se si desidera inserire il criterio di ricerca più dettagliato.
5. Per attivare una connessione, fare clic su **Attiva**. La pagina Gestisci connessioni viene visualizzata di nuovo, questa volta con la connessione evidenziata in verde. Questa pagina visualizza il package, il protocollo ed il tipo di documento per l'origine e la destinazione. Vengono forniti anche i pulsanti ed è possibile fare clic per visualizzare e modificare lo stato della connessione del partner e i parametri.
6. Per specificare gli attributi per l'origine e la destinazione o per selezionare un profilo connessione, consultare la sezione "Specifica e modifica di attributi".

Se il PIP è un PIP a due azioni, attivare la connessione in entrambe le direzioni per supportare la seconda azione del PIP. A tal fine, l'origine e la destinazione della seconda azione sono l'opposto dell'origine e della destinazione della prima azione.

Per i documenti EDI, XML o ROD per cui è stata definita più di un'interazione, assicurarsi di attivare tutte le connessioni associate alle interazioni.

Specifica e modifica di attributi

Informazioni su questa attività

Quando si attiva la connessione, è possibile impostare gli attributi o modificare quelli definiti. Per specificare o modificare gli attributi per questa connessione:

1. Fare clic su **Attributi** per visualizzare o modificare i valori degli attributi.

   Ad esempio, supporre che il partner interno stia inviando un documento incluso come Nessuno ad un partner. Il partner riceverà il documento incluso come AS. È possibile che al partner interno sia stato assegnato più di un ID di business. Per indicare a WebSphere Partner Gateway l'ID da utilizzare:
   a. Fare clic su **Attributi** sul lato Origine della connessione.
   b. Quando la pagina Attributi di connessione viene visualizzata, espandere la cartella **Nessuno**.
   c. Selezionare nell'elenco **Aggiornamento** l'ID AS che si desidera inviare al partner.

d. Fare clic su **Salva**.

Nota: se, in precedenza, è stato specificato un ID AS (nella pagina Capacità B2B, ad esempio), il valore immesso sostituirà quello precedente.

un altro esempio per impostare gli attributi è immettere un valore per l'indirizzo MDN durante la ricezione dei documenti inclusi come AS da un partner. L'indirizzo specifica dove viene consegnato MDN.

2. Fare clic su **Azioni**, se si desidera visualizzare o modificare un'azione o una mappa di conversione associata a questa connessione. Qualsiasi valore modificato qui sostituisce altri valori impostati per l'azione o la mappa.
3. Fare clic su **Destinazioni** se si desidera visualizzare o modificare la destinazione di origine o quella di destinazione.
4. Se si preme il pulsante **Aggiungi profilo connessione** e si visualizza l'elenco **Profili attivi**, è possibile associare questa connessione ad un profilo del partecipante definito in precedenza.

Gli attributi impostati al livello della connessione hanno la priorità su quelli impostati al livello del protocollo o del tipo documento.

Capitolo 13. Abilitazione della sicurezza per gli scambi del documento

Mediante WebSphere Partner Gateway, è possibile installare e utilizzare diversi tipi di certificati per proteggere le transazioni in entrata e quelle in uscita. Questo capitolo include le seguenti sezioni:

I certificati ed i protocolli di sicurezza forniscono i seguenti vantaggi di protezione in WebSphere Partner Gateway:

- La verifica come a chi viene inviato il documento
- La verifica che il documento non è stato alterato in transito
- La protezione da parte di altri utenti di visualizzare il contenuto del documento
- La verifica che la persona che invia il documento è autorizzata a eseguire tale operazione.

Nota: è necessario utilizzare sempre la stessa istanza del browser con cui si accede alla Console comunità per apportare modifiche alla configurazione di WebSphere Partner Gateway. L'utilizzo simultaneo di più istanze del browser può causare l'eliminazione delle modifiche di configurazione.

Panoramica della protezione

Meccanismi di protezione e protocolli utilizzati in WebSphere Partner Gateway

A seconda del protocollo di business, WebSphere Partner Gateway utilizza i certificati per consentire a questi meccanismi di proteggere gli scambi del documento:

Codifica e decodifica

La codifica è un metodo per modificare i dati in modo tale che i dati sono illeggibili fino a quando vengono decodificati. WebSphere Partner Gateway utilizza un sistema di crittografia definito anche codifica della chiave

pubblica per proteggere la comunicazione tra i partner e l'hub. I diversi protocolli di business come AS2 o RosettaNet includono i requisiti per la codifica. SSL utilizza anche la codifica. In questo capitolo, se non diversamente indicato, l'utilizzo del termine *codifica* si applica ai protocolli di business.

La decodifica è un metodo per decodificare i dati codificati in modo da renderli leggibili. La decodifica viene eseguita sui documenti in entrata.

Firma digitale e Verifica della firma digitale
La firma digitale è il meccanismo per verificare chi ha inviato il documento e che il documento non è stato alterato in transito. È anche utile durante la verifica di non-rifiuto. Non-rifiuto significa che un partner non può negare di aver originato ed inviato un messaggio. Verifica anche che il partner non può negare di aver ricevuto un messaggio.

Nota: le informazioni di non rifiuto sono ottenute dai parametri della connessione partner. I parametri della connessione partner sono ottenuti dopo una ricerca con esito positivo della connessione partner. Per impostazione predefinita, il non rifiuto è impostato su "Sì"; questo significa che, se per qualche ragione le informazioni non sono disponibili dalla connessione partner, il documento verrà inserito nella memoria di non rifiuto.

SSL SSL è un protocollo generalmente utilizzato per la gestione della sicurezza in Internet. SSL fornisce le connessioni protette abilitando due applicazioni collegate ad una connessione di rete per verificare che ognuna sia attendibile e mediante la codifica dei dati per verificare la riservatezza dei dati. La codifica è indipendente dalla tipologia dei dati. SSL è utilizzato sui trasporti come HTTP e FTP.

Autenticazione di base
Quando tutti i messaggi in entrata vengono inviati su HTTP o HTTPS, il destinatario può autenticare il partner di invio con le credenziali di autenticazione di base. L'ID utente e la password vengono passate nell'intestazione HTTP. Poiché anche la password viene inviata, l'autenticazione di base dovrebbe essere utilizzata con SSL/TLS per assicurare che le intestazioni siano codificate. L'autenticazione viene fornita utilizzando ID/username:password o Username:password nel formato codificato Base64. Il valore nell'intestazione HTTP viene considerato solo se **Abilita autenticazione di base** viene impostato su true. Selezionare Autenticazione di base nella pagina Dettagli destinatario della console per impostarla su True.

Se l'autenticazione non riesce, la risposta di autenticazione non riuscita viene restituita al mittente. Altrimenti, il documento viene inviato per un'ulteriore elaborazione. In caso di autenticazione client SSL, viene identificato l'ID di business del partner di invio. Quando il documento è ricevuto, il destinatario verifica se il certificato è associato a un altro partner, altrimenti il documento genera un errore se non c'è corrispondenza. Per la compatibilità con le versioni precedenti, durante l'invio di un messaggio SOAP con autenticazione di base, impostare al destinatario l'indicatore **Abilita autenticazione di base** su "No". A meno che l'autenticazione del documento non riesca nel destinatario, è possibile visualizzare il documento nel programma di visualizzazione del documento. L'autenticazione di base viene supportata per i seguenti documenti:

- Documenti EDI/XML

- Documenti AS2 con payload binario/EDI/XML
- Richiesta servizio Web
- Messaggio Rosettanet
- Messaggio ebMS

La sicurezza può trovarsi sul protocollo di business o di trasporto. L'autenticazione di utente nel destinatario supporta i documenti binari dai partner esterni su HTTP. Il partner di invio viene identificato utilizzando le credenziali di autenticazione di base o utilizzando le credenziali di autenticazione client SSL.

Certificati e meccanismi di protezione

I certificati costituiscono la base di tutti e tre metodi alla sicurezza: codifica, firme digitali e SSL. Questi metodi sono abilitati in WebSphere Partner Gateway. L'utilizzo di un certificato consente i documenti protetti durante la trasmissione.

Ogni partner ha uno o più certificati per inviare o ricevere i documenti con WebSphere Partner Gateway e WebSphere Partner Gateway rappresentato dall'operatore hub dispone di uno o più certificati per inviare o ricevere i documenti con il partner.

Nota: gli stessi certificati utilizzati per un partner o l'operatore hub sono validi a tutti i documenti. I certificati non variano in base al tipo di documento.

Certificati e codifica

Un certificato contiene la parte della chiave pubblica di una coppia di chiave privata/pubblica in modo matematico. La chiave pubblica "blocca" o codifica un documento prima che sia inviato ed effettua tale operazione in modo tale che solo la chiave privata può quindi "sbloccare" o decodificare un documento una volta inviato. Una chiave pubblica ha questo nome perché la si condivide con i partner da cui si ricevono documenti codificati, mentre ci si riserva l'utilizzo della chiave privata in modo da poterli decodificare. Un certificato contiene la chiave pubblica e la collega ad un Nome oggetto, che è il nome per l'End-Entity cui appartiene il certificato.

I certificati sono creati dal partner e sono firmati automaticamente dal partner o emessi da CA. Un certificato emesso da CA è un certificato richiesto da un partner mediante CSR (Certificate Signing Request) e ricevuto da CA (certifying authority). Un certificato emesso da CA viene firmato da CA e non dal partner. Ciascun partner ha almeno un certificato da utilizzare durante l'invio o la ricezione dei documenti.

La codifica del documento di business si applica se lo standard di business supporta la codifica. Non tutti gli standard supportano la codifica. Per gli standard che supportano la codifica ogni standard ha diversi metodi per applicare la codifica. WebSphere Partner Gateway comprende le differenze tra gli standard e il modo in cui applicare la codifica.

Se WebSphere Partner Gateway invia un documento ad un partner, il certificato dei partner consente di codificare il documento. In questo metodo solo il partner può leggere il contenuto decodificando il documento con la propria chiave privata. Il certificato utilizzato sarà il certificato di codifica caricato in WebSphere Partner Gateway per tale partner.

Se sta inviando un documento a WebSphere Partner Gateway, il partner utilizza il certificato dell'Operatore hub per codificare il documento. In questo metodo solo

l'Operatore hub che ha la chiave privata può leggere il contenuto decodificando il documento. La chiave privata utilizzata è quella caricata per l'Operatore hub nell'opzione Carica PKCS12. Nota: il certificato dell'Operatore hub deve essere fornito al partner dall'amministratore.

Notes:

1. WebSphere Partner Gateway supporta gli algoritmi RC2 e TripleDES. Non supporta l'algoritmo RC5. Se si utilizza un algoritmo RC5 nella prima release, passare ad uno di quelli supportati.
2. WebSphere Partner Gateway supporta anche i seguenti algoritmi:
   - AES, TripleDES e RC2: per i documenti ebMS inviati e ricevuti.
   - TripleDES e RC2: per i documenti RNIF.
   - DES: per ebMS, ma si consiglia l'utilizzo di algoritmi più efficaci come RC2, TripleDES o AES.

   È possibile impostare questi algoritmi nella console di WebSphere Partner Gateway in Gestione sistema > Gestione DocMgr > Vista Sicurezza o con l'API SecurityService in Uscite utente. Per informazioni sulle proprietà di protezione, consultare il manuale *WebSphere Partner Gateway Administrator Guide*. Per informazioni su SecurityService, consultare il manuale *WebSphere Partner Gateway Programmer Guide*.

Procedura di base

Per ricevere un documento codificato, è necessario completare la seguente procedura di base. Per la procedura completa, consultare la sezione "Utilizzo dei certificati per abilitare la codifica e la decodifica" a pagina 252.

1. Ottenere una coppia di chiave pubblica/privata generandola o ricevendone una da CA.
2. Caricare la chiave privata sul server WebSphere Partner Gateway in Operatore hub (la chiave può essere utilizzata per tutti i partner interni) o Partner interno (la chiave può essere utilizzata solo dal partner interno specifico), in modo che il server possa decodificare i documenti in entrata.
3. Fornire il certificato pubblico al partner commerciale in modo tale che il partner possa caricare il certificato nel server del partner e tale partner possa codificare i documenti prima di inviarli.

Una volta completata questa procedura, questo partner, mediante il certificato, può inviare i documenti codificati solo nel modo in cui è possibile decodificarli. Per inviare i documenti codificati dai partner, è necessario invertire questa procedura, caricando i certificati e utilizzando questi certificati per codificare i documenti da inviare.

Certificati e firma digitale

WebSphere Partner Gateway supporta la firma digitale come richiesto dai protocolli B2B. Utilizzare i certificati per la firma allo stesso modo in cui sono utilizzati i certificati di codifica escluso quello invertito. È necessario creare il certificato per inviare un documento con una firma digitale ai partner e non viceversa.

Le firme digitali consentono di verificare il mittente corrente del documento e di stabilire che il documento non è stato alterato in transito. Sono validi solo se lo standard di business supporta le firme digitali. Non tutti gli standard supportano le firme digitali. Per gli standard che supportano le firme digitali, ogni standard ha

diversi metodi per applicare le firme digitali. WebSphere Partner Gateway comprende le differenze tra gli standard e il modo in cui applicare le firme digitali.

Se WebSphere Partner Gateway sta inviando un documento ad un partner, per firmare il documento viene utilizzata la chiave privata Operatori hub caricata nell'opzione Carica PKCS12. Il partner utilizza il certificato dell'Operatore hub per verificare che WebSphere Partner Gateway sia quello che ha firmato il documento. Se la chiave privata dell'Operatore hub non è stata utilizzata per firmare il documento, il certificato dell'Operatore hub di cui dispone il partner non sarà in grado di verificare le firme. Nota: il certificato dell'Operatore hub deve essere fornito al partner dall'amministratore.

Se un partner sta inviando un documento a WebSphere Partner Gateway, WebSphere Partner Gateway utilizza il certificato Firma digitale del partner per verificare che il partner sia quello che ha firmato il documento. Se la chiave privata del partner non è stata utilizzata per firmare il documento, il certificato che WebSphere Partner Gateway ha per il partner non sarà in grado di verificare la firma.

Procedura di base:

Per inviare un documento con firma digitale, è necessario completare la seguente procedura di base. Per la procedura completa, consultare la sezione "Utilizzo dei certificati per abilitare la firma digitale" a pagina 257.

1. Ottenere una coppia di chiave pubblica/privata generandola o ricevendone una da CA.
2. Caricare la chiave privata sul server WebSphere Partner Gateway in Operatore hub in modo tale che il server può firmare i documenti inviati.
3. Fornire il certificato pubblico al partner commerciale in modo tale che il partner possa caricare il certificato nel server del partner e tale partner possa verificare i documenti ricevuti.

Al termine della procedura, mediante la chiave privata, è possibile inviare i documenti con firma digitale in modo tale che il partner rileva che non è possibile inviarne altri. Per ricevere allo stesso modo i documenti firmati dai partner, è necessario invertire questa procedura, caricando i certificati e utilizzandoli per accertarne l'origine.

Certificati e SSL/TLS

Durante l'invio di documenti, è possibile utilizzare SSL per codificare i documenti in modo tale che solo il destinatario possa leggere questi documenti, quindi verificando la riservatezza dei dati.

All'interno di SSL vi è la nota di *client* e *server*. Un client si connette ad un server per inviare un documento al server. Quando il client si connette al server, il server invia al client un certificato da utilizzare durante la codifica del documento. Questo certificato del server fa parte anche dell'autenticazione del server, significa che il server utilizza il certificato per autenticarlo sui client. A volte, il server richiede anche un certificato dal client. Viene definito Autenticazione client e viene utilizzato dal server per verificare che il client viene definito sul server.

Quando WebSphere Partner Gateway invia un documento ad un partner, WebSphere Partner Gateway è il client ed il partner è il server (indicando, il documento inviato al server del partner).

Nota: il server del partner è la destinazione definita in WebSphere Partner Gateway per questo partner.

Quando il partner invia un documento a WebSphere Partner Gateway, il partner è il client e WebSphere Partner Gateway è il server.

Nota: indica il destinatario definito in WebSphere Partner Gateway.

Quando un partner invia un documento a WebSphere Partner Gateway utilizzando SSL, l'identità effettiva del partner non è nota. Se l'Autenticazione client viene utilizzata, l'identità del partner non è ancora nota. Tuttavia, è noto solo che questo partner è ritenuto attendibile per l'invio di documenti a WebSphere Partner Gateway. WebSphere Partner Gateway ha anche un'ulteriore funzione per identificare il partner dal certificato Autenticazione client fornito dal partner.

Se WebSphere Partner Gateway invia un documento ad un partner, il certificato del partner consente di codificare il documento. Quindi, solo tale partner può leggere il contenuto decodificando il documento con la propria chiave privata del partner. Come parte di SSL durante il runtime, il partner invia in modo dinamico il certificato da utilizzare per la codifica a WebSphere Partner Gateway. WebSphere Partner Gateway verifica che il certificato sia valido creando e convalidando il percorso di certificazione utilizzando i certificati caricati come certificati Root/Intermedio sotto l'Operatore hub.

Si tratta della seconda parte facoltativa di SSL definita Autenticazione client per convalidare il mittente in cui il partner richiede un certificato da WebSphere Partner Gateway. WebSphere Partner Gateway invia il certificato Autenticazione client caricato in Operatore hub. Nota: il certificato dell'Operatore hub per l'Autenticazione client deve essere fornito al partner dall'amministratore. Se il certificato Autenticazione client è autofirmato, il certificato autofirmato deve essere fornito al partner. Se il certificato Autenticazione client è emesso da una CA, potrebbe essere necessario fornire il certificato CA al partner, se il partner non ha già il certificato CA.

Se un *partner* invia un documento a WebSphere Partner Gateway utilizzando SSL, il certificato di WebSphere Partner Gateway consente di codificare il documento. Quindi, solo WebSphere Partner Gateway può leggere il contenuto decodificando il documento con la propria chiave privata. Come parte di SSL durante il runtime, WebSphere Partner Gateway invia in modo dinamico il certificato da utilizzare per la codifica al partner. Il partner verifica che il certificato sia valido confrontandolo con l certificato che l'Amministratore ha fornito in precedenza al partner. Si tratta della seconda parte facoltativa di SSL definita Autenticazione client per convalidare il mittente in cui WebSphere Partner Gateway richiede un certificato dal partner. Il partner invia il certificato Autenticazione client a WebSphere Partner Gateway e questo certificato sarà verificato con il certificato che il partner ha fornito in precedenza all'amministratore.

Nota: per ricevere il documento dai partner mediante SSL, WebSphere Partner Gateway utilizza le funzioni di WebSphere Application Server sottostanti. Quindi, i certificati utilizzati durante il runtime non sono stati caricati mediante la console di WebSphere Partner Gateway ma sono invece caricati nel truststore e nel keystore di WebSphere Application Server.

Mediante l'Autenticazione client, esiste un'identificazione aggiuntiva del partner che WebSphere Partner Gateway effettua al di fuori del trasporto SSL. Il certificato Autenticazione client fornito dal partner sarà passato a WebSphere Partner

Gateway che lo confronterà con il certificato caricato per il client SSL del partner in modo tale che il partner possa essere identificato.

Una connessione SSL basata su HTTP è sempre avviata dal client mediante un URL che inizia con https:// invece di http://. Una connessione SSL comincia con un handshake. Durante questa fase, le applicazioni scambiano i certificati, si accordano sugli algoritmi di codifica da utilizzare e creano le chiavi di codifica utilizzate per il promemoria della sessione.

Procedure di base

Per *inviare* un documento mediante SSL, è necessario completare la seguente procedura di base. Per la procedura completa, consultare la sezione "Utilizzo di certificati per abilitare SSL" a pagina 261.

1. Ottenere un certificato dal partner e caricarlo nel truststore di WebSphere Application Server.
2. Per l'Autenticazione client sul partner ottenere una coppia di chiave pubblica/privata creandola o ricevendone una da CA.
3. Caricare la chiave privata e il certificato pubblico nel keystore di WebSphere Application Server.
4. Fornire il certificato pubblico al partner commerciale in modo tale che il partner possa caricare il certificato nel server del partner e tale partner possa verificare la ricezione del certificato Autenticazione client durante la comunicazione di runtime SSL.

Per *ricevere* un documento mediante SSL, è necessario completare la seguente procedura di base. Per la procedura completa, consultare la sezione "Utilizzo di certificati per abilitare SSL" a pagina 261.

1. Ottenere una coppia di chiave pubblica/privata generandola o ricevendone una da CA.
2. Caricare la chiave privata e il certificato pubblico nel keystore di WebSphere Application Server.
3. Fornire il certificato pubblico al partner commerciale in modo tale che il partner possa caricare il certificato nel server del partner e tale partner possa verificare la ricezione del certificato Server durante la comunicazione di runtime SSL.
4. Per l'Autenticazione client ottenere un certificato dal partner e caricarlo nel truststore di WebSphere Application Server. Sarà utilizzato durante la comunicazione di runtime SSL.
5. Per identificare il partner dal certificato Autenticazione client nella console di WebSphere Partner Gateway, caricare il certificato dei partner sotto l'Autenticazione client del partner.

Memorizzazione dei certificati nei keystore e truststore

WebSphere Partner Gateway dispone di due metodi per memorizzare i certificati. Per i documenti inviati da un partner a WebSphere Partner Gateway mediante SSL, i certificati sono memorizzati nel keystore e nel truststore di WebSphere Application Server. I truststore consentono di memorizzare i certificati attendibili che a loro volta consentono di convalidare la ricezione di un certificato da un partner. I keystore consentono di memorizzare la chiave privata e pubblica dell'Operatore hub di WebSphere Partner Gateway. I certificati utilizzati per la protezione del documento di business sono memorizzati caricandoli mediante la console di WebSphere Partner Gateway. Questa sezione descrive il keystore ed il truststore utilizzati con WebSphere Application Server. Durante l'installazione di

WebSphere Partner Gateway, un keystore ed un truststore sono stati creati per WebSphere Application Server su cui sono installati la console ed il destinatario.

- Un keystore è un file che contiene le chiavi pubbliche e private.
- Un truststore è un file database di chiave che contiene le chiavi pubbliche per i certificati CA e quelli autofirmati dei partner. La chiave pubblica viene memorizzata come certificato del firmatario. Per il CA commerciale, viene aggiunto un CA root. Poiché il file truststore non contiene la chiave privata, il file del truststore può essere più accessibile pubblicamente rispetto al file del keystore.
- iKeyman viene utilizzato per gestire il keystore ed il truststore. Questa utilità è descritta nelle sezioni che ne richiedono l'utilizzo.

  Nota: la console di gestione di WebSphere Application Server può essere utilizzata anche per gestire i certificati, i keystore e i truststore per il Destinatario e la Console. Consultare l'articolo ″Protezione delle applicazioni e del relativo ambiente″ nel centro informazioni di WebSphere Application Server per informazioni dettagliate su come gestire i certificati ed i keystore utilizzando la console di gestione di WebSphere Application Server.

Per impostazione predefinita, un keystore ed un truststore vengono creati nella directory *<DirProdotto>*/common/security/keystore. I nomi sono:

- bcgSecurity.jks
- bcgSecurityTrust.jks

Modifica della password predefinita

La password predefinita per accedere alle memorie è WebAS. WebSphere Application Server è configurato per utilizzare queste memorie. È possibile utilizzare l'utilità iKeyman per modificare la password. In alternativa, è possibile utilizzare il comando keytool per modificare la password del file keystore. In UNIX, il comando sarà il seguente:

```
/<WAS_Installation_Dir>/java/bin/keytool
 -storepasswd -new $NEW_PASSWORD$ -keystore $KEYSTORE_LOCATION$
 -storepass $CURRENT_PASSWORD$ -storetype JKS
```

In Windows, utilizzare il comando precedente utilizzando però barre rovesciate e nomi di unità.

Se le password keystore vengono modificate, ciascuna configurazione dell'istanza WebSphere Application Server deve essere modificata allo stesso modo. Questo può essere effettuato mediante: bcgChgPassword.jacl. Per l'istanza della Console, navigare nella seguente directory:

```
/<DirProdotto>/bin
```

ed inviare il seguente comando:

```
./bcgwsadmin.sh -f /<DirProdotto>/scripts/
bcgChgPassword.jacl -conntype NONE
```

Ripetere questo comando per le istanze di WebSphere Application Server del Destinatario e del Gestore documenti.

Nota: per le installazioni Windows, utilizzare bcgwsadmin.bat invece di ./bcgwsadmin.sh.

Viene richiesta una nuova password.

Sostituzione e certificato scaduto

Se un certificato nel truststore è scaduto, è necessario aggiungerne uno nuovo per sostituirlo mediante questa procedura:

1. Avviare iKeyman, se non è già in esecuzione.
2. Aprire il file truststore.
3. Digitare la password e fare clic su **OK**.
4. Selezionare **Certificati del firmatario** dal menu.
5. Fare clic su **Aggiungi**.
6. Fare clic su **Tipo di dati** e selezionare un tipo di dati, come i dati codificati Base64 ASCII.

   Questo tipo di dati deve corrispondere ai tipi di dati del certificato di importazione.
7. Digitare un nome di file del certificato e la posizione per il certificato digitale CA root o fare clic su **Sfoglia** per selezionare il nome e la posizione.
8. Fare clic su **OK**.
9. Digitare un'etichetta per il certificato di importazione.
10. Fare clic su **OK**.

Utilizzo delle catene di certificati

Una catena di certificati è costituita da un certificato del partner e da qualsiasi certificato utilizzato per autenticare il certificato del partner. Ad esempio, se un CA consente di creare il certificato del partner, tale CA potrebbe essere stato certificato da un altro CA. La catena di trust inizia sull'autorità di certificazione CA *root* (aggancio trust). Il certificato digitale dell'autorità di certificazione root è autofirmato; vale a dire, l'autorità di certificazione utilizza la propria chiave privata per firmare il certificato digitale. Tutti i certificati tra il trust anchor e il certificato del partner (il certificato di destinazione) sono certificati *intermedi*.

Per tutti i certificati inviati dall'Autorità di certificazione, tutti i certificati nella catena devono essere aggiunti. Ad esempio, in una catena di certificati in cui A (l'aggancio trust) è l'emittente di B e B è l'emittente di C (certificato di destinazione), i certificati A e B devono essere caricati come certificati CA.

WebSphere Partner Gateway considera tutti i certificati autofirmati come agganci trust. Il certificato autofirmato può essere un'autori di certificazione (CA) o un certificato autofirmato creato dal partner.

Per SSL in entrata, tutti i certificati root (trust anchor) e i certificati intermedi sono conservati nel truststore di WebSphere Application Server come descritto in precedenza. Per tutti i certificati dei partner, i relativi certificati root (trust anchor) e certificati intermedi sono caricati in Operatore hub.

Utilizzo di certificati principali e secondari

È possibile creare più di un certificato di un tipo particolare ed indicare uno come certificato principale e l'altro come certificato secondario. Se il certificato principale scade o non è in grado di essere utilizzato, WebSphere Partner Gateway passa al certificato secondario.

Nota: questa funzione può essere utilizzata per passare dal vecchio certificato ad un nuovo certificato senza arrestare il server.
Si specifica, sulla Console Comunità, il certificato principale e quello secondario.

La capacità di fornire certificati principali e secondari è disponibile per i seguenti certificati:

- Certificato di codifica di un partner
- Firma del certificato dell'operatore hub
- Certificato del Client SSL dell'operatore hub

Modifica dell'intensità della codifica

JRE (Java Runtime Environment) fornito con WebSphere Partner Gateway applica le limitazioni sugli algoritmi di codifica e i livelli massimi di codifica consentiti. Ad esempio, i criteri di limitazione specificano i limiti di lunghezza consentiti, e come risultato, il livello delle chiavi di codifica. Queste limitazioni vengono specificate in file denominati *file criteri di protezione di legislazione*. La lunghezza massima consentita è di 2048 byte.

Se si desidera supportare certificati con una dimensione della chiave maggiore di 2048 byte, utilizzare la versione illimitata dei file di criteri di protezione di legislazione. Si può desiderare di utilizzare criteri più forti, illimitati installando nuovi file di criteri di protezione in una directory secondaria del JRE installato.

Inoltre, sono presenti le limitazioni di codifica sugli algoritmi della chiave simmetrica, come ad esempio 3DES. Se è necessario un algoritmo di chiave simmetrica forte, la sostituzione dei file dei criteri di giurisdizione rimuove anche le limitazioni per le chiavi simmetriche. Ad esempio, se si sta utilizzando l'algoritmo AES, sono obbligatori i file delle politiche di crittografia senza limitazioni. Fare riferimento al link http://www.ibm.com/developerworks/java/jdk/security/50 per i dettagli.

Tuttavia, a causa di limitazioni del controllo di importazione, i file delle politiche di giurisdizione distribuiti con IBM SDK per Java 5 Development Kit consentono l'utilizzo di una crittografia **efficace** ma limitata. La seguente tabella fornisce le dimensioni massime delle chiavi, consentite da questa versione **efficace** dei file delle politiche di giurisdizione:

Tabella 29. La dimensione massima delle chiavi degli algoritmi efficaci utilizzati nei file delle politiche di giurisdizione

Algoritmo	Dimensione massima della chiave
DES	64
DESede	112 (effettivo) o 168 (effettivo)
RC2	128
RSA	2048
* (tutti gli altri)	128

Istruzioni di installazione per i sistemi operativi Windows, Linux e AIX

Per installare i file dei criteri di giurisdizione non limitati in WebSphere Partner Gateway, seguire le operazioni riportate di seguito:

1. Scaricare i file dei criteri di giurisdizione illimitati dal link **IBM SDK Policy files** presso il seguente sito Web: http://www.ibm.com/developerworks/java/jdk/security/50/.
2. Decomprimere il file scaricato in una cartella temporanea
3. Copiare local_policy.jar e US_export_policy.jar dalla cartella temporanea.

4. Arrestare tutti i server ospitati dall'istanza di WebSphere Application Server di cui si sta eseguendo la configurazione.
5. Passare alla cartella *<DirInstallazioneWAS>*\java\jre\lib\security.
6. Rinominare i file local_policy.jar e US_export_policy.jar esistenti come local_policy.jar.bak e US_export_policy.jar.bak
7. Incollare i file jar copiati al passo 3 a pagina 250 nella cartella *<DirInstallazioneWAS>*\was\java\jre\lib\security.
8. Riavviare i server ospitati dall'istanza di WebSphere Application Server di cui si è appena eseguita la riconfigurazione.

Questi passi sono validi per tutte le installazioni di WebSphere Application Server in cui sono installate delle applicazioni WebSphere Partner Gateway.

Istruzioni di installazione per i sistemi operativi HP-UX e Solaris

Per le piattaforme HP-UX e Solaris, sono applicabili le seguenti istruzioni:

1. Scaricare i file dei criteri di giurisdizione illimitati dal link **IBM SDK Policy files** presso il seguente sito Web: http://www.ibm.com/developerworks/java/jdk/security/50/.
2. Decomprimere il file scaricato in una cartella temporanea.
3. Arrestare tutti i server ospitati dall'istanza di WebSphere Application Server di cui si sta eseguendo la configurazione.
4. Passare alla cartella *<DirInstallazioneWAS>*\java\jre\lib\security.
5. Rinominare i file local_policy.jar e US_export_policy.jar esistenti come local_policy.jar.bak e US_export_policy.jar.bak
6. Copiare local_policy.jar e US_export_policy.jar dalla cartella temporanea a *<DirInstallazioneWAS>*\java\jre\lib\security.
7. Riavviare i server ospitati dall'istanza di WebSphere Application Server di cui si è appena eseguita la riconfigurazione.

Questi passi sono validi per tutte le installazioni di WebSphere Application Server in cui sono installate delle applicazioni WebSphere Partner Gateway.

Configurazione di SSL con Autenticazione client

Se si invieranno dei documenti utilizzando un protocollo di trasporto con SSL con Autenticazione client, è necessario apportare un'ulteriore modifica per il provider JSSE utilizzato. Per ulteriori informazioni, consultare il Capitolo 14, "Troubleshooting "SSL handshake fails due to no certificate received," nel manuale *WebSphere Partner Gateway Administrator Guide*.

Scadenza dei certificati

Solo i certificati utilizzati per la codifica, la firma digitale e SSL sono disabilitati quando scadono. Questi certificati devono essere certificati end-entity e non certificati di CA. I certificati di CA non vengono disabilitati quando scadono.

Se i certificati di tipo root o intermedio scadono tra i riavvii del server, essi non verranno inclusi nell'elenco dei certificati attendibili. Questo significa che se la creazione del percorso dei certificati ha esito negativo perché non è stato trovato il certificato CA, è possibile che il certificato CA sia scaduto. Se un certificato root o intermedio è scaduto durante il runtime, la creazione del percorso dei certificati avrà esito negativo ed il corrispondente certificato end-entity non verrà utilizzato nella transazione di business. È possibile controllare il periodo di validità e lo stato

del certificato utilizzando la vista Elenco certificati nella console di WebSphere Partner Gateway. La data di validità dei certificati scaduti viene visualizzata in rosso in questa vista.

Se un certificato CA è scaduto, è possibile ottenere un nuovo certificato dalla CA che lo ha emesso. Caricare il nuovo certificato CA utilizzando la console di WebSphere Partner Gateway. Per informazioni sul caricamento di certificati, consultare "Utilizzo dei certificati per abilitare la codifica e la decodifica", "Utilizzo dei certificati per abilitare la firma digitale" a pagina 257 e "Utilizzo di certificati per abilitare SSL" a pagina 261.

Utilizzo dei certificati per abilitare la codifica e la decodifica

Questa sezione descrive la codifica e la decodifica dei certificati.

Creazione e installazione di certificati di decodifica in entrata

Questo certificato viene utilizzato dall'hub per decodificare i file codificati ricevuti dai partner. L'hub utilizza la chiave privata per decodificare i documenti. La codifica viene utilizzata per impedire a tutti tranne che al mittente e al destinatario previsto di visualizzare i documenti in transito.

Osservare la seguente limitazione importante sulla ricezione dei messaggi AS2 codificati dai partner. Se un partner invia un messaggio AS2 codificato e utilizza il certificato errato, la decodifica ha esito negativo. Nessun MDN viene restituito al partner per indicare l'errore. Affinché il partner riceva MDN in questa situazione, creare una connessione al partner con la seguente definizione del documento:

- Package: **AS** Al package: **Nessuno**
- Protocollo: **Binario**Al protocollo: **Binario**
- Tipo di documento: **Binarop**al tipo di documento: **Binario**

La connessione creata deve essere da AS a Nessuno, cioé, deve creare una connessione attivando la capacità AS B2B su un partner e la capacità Nessuno B2B sull'altro. Verificare che il gateway di origine sul lato AS sia un gateway SMTP (in caso di AS1), gateway HTTP (in caso di AS2) o un gateway FTP (in caso di AS3), configurato sull'indirizzo MDN. Quindi, l'errore di decodifica MDN viene inviato di nuovo su questa connessione AS a Nessuno binario.

Fase 1: ottenere un certificato

Informazioni su questa attività

Creazione di un certificato autofirmato: Se si intende utilizzare la decodifica, completare la seguente procedura.

1. Avviare l'utilità iKeyman.
2. Utilizzare iKeyman per generare un certificato autofirmato e una coppia di chiavi.
3. Utilizzare iKeyman per estrarre in un file il certificato che contiene la chiave pubblica.
4. Distribuire il certificato ai partner. Questi sono necessari per importare il file nel prodotto B2B per uso come certificato di codifica. Consigliare loro di utilizzarlo quando desiderano inviare i file codificati al partner interno. Se il certificato è un CA firmato, fornire anche il certificato CA.
5. Utilizzare iKeyman per salvare il certificato autofirmato e la coppia di chiavi private nella forma di un file PKCS12.

6. Passare a **Profilo** > **{Operatore hub/Partner interno}** > **certificati** > **crea nuovo certificato.**
7. Nell'elenco a discesa **A quale partner appartiene questo certificato**, selezionare il partner da associare al certificato appena caricato.
8. Fare clic su **Cerca** per trovare partner specifici o un sottoinsieme di partner.
9. Fare clic su **Sfoglia** accanto a **Posizione certificato** per caricare il certificato.
10. Fare clic su **Avanti**.
11. In Fornisci dettagli certificato, immettere le seguenti informazioni di certificato: **Certificato foglia**, **Certificato CA root** O **Certificato CA intermedio**.
12. Associare questo certificato a **Decodifica**.
13. Nell'**Utilizzo certificato**, selezionare **Primario** o **Secondario**.
14. Selezionare **abilitato** o **disabilitato** nello **Stato** in base a se si desidera abilitare o disabilitare il Certificato dopo il caricamento
15. Selezionare la **Modalità operativa**.
16. Fare clic su **Fine** per salvare le modifiche e chiudere la procedura guidata.

Utilizzo di un certificato firmato da un'Autorità di certificazione: Se si utilizza un certificato firmato da un CA, attenersi alla seguente procedura:

1. Avviare l'utilità iKeyman.
2. Utilizzare iKeyman per generare una richiesta di certificato e una coppia di chiavi per il Destinatario.
3. Inoltrare un CSR (Certificate Signing Request) a CA.
4. Quando si riceve il certificato firmato da CA, utilizzare iKeyman per posizionare il certificato firmato nel keystore.

Fase 2: distribuire il certificato
Informazioni su questa attività

Distribuire il certificato CA di firma a tutti i partner.

Installazione dei certificati di codifica in uscita

Il certificato di codifica in uscita viene utilizzato quando l'hub invia i documenti codificati ai partner. WebSphere Partner Gateway codifica i documenti con le chiavi pubbliche dei partner ed i partner decodificano i documenti con le relative chiavi private.

Il partner può avere più certificati di codifica. Uno è quello principale, che è quello predefinito. L'altro è quello secondario, che viene utilizzato se il certificato principale scade.

Fase 1: ottenere un certificato del partner
Informazioni su questa attività

Ottenere il certificato di codifica del partner. Il certificato deve essere nel formato X.509 DER. Si noti che WebSphere Partner Gateway supporta solo certificati X5.09.

Fase 2: installare il certificato del partner
Informazioni su questa attività

Installare il certificato mediante la Console comunità nel profilo del partner completando la seguente procedura:

1. Passare a **Profilo** > **Partner esterno** > **certificati**> **Carica certificato**.
2. Nella pagina **Seleziona partner, Posizione file, Password** della procedura guidata, immettere i seguenti valori:
   - **A quale partner appartiene questo certificato**: Selezionare il partner da associare al certificato appena caricato. Fare clic su Cerca per trovare un partner specifico o un sottoinsieme di partner. Se il partner è un Operatore hub o un Partner interno, immettere la posizione del certificato, la posizione della chiave privata e la password (OPPURE) Fornire il truststore o il keystore con la password. Per il Partner esterno, immettere la posizione del certificato (OPPURE) fornire la posizione del truststore che contiene la catena di certificato.
   - **Posizione certificato**: Fare clic su **Sfoglia** per selezionare la posizione del pubblico certificato.
3. Fare clic su **Avanti** per andare alla pagina **Dettagli certificato** della procedura guidata.
4. Nella pagina **Dettagli certificato** della procedura guidata, immettere i seguenti dettagli del certificato:
   - **Nome certificato foglia** - Il nome del certificato foglia. Il nome del campo dipende da se si tratta di Certificato foglia, Certificato CA root o Certificato CA intermedio.
   - **Descrizione** - La descrizione del Certificato foglia.
   - **Tipo certificato** - Associare questo certificato alla Codifica.
   - **Utilizzo certificato** - Associare un utilizzo per il certificato. I valori sono Primario e Secondario.
   - **Modalità operativa** - Immettere la modalità dell'operazione.
   - **Stato** - Selezionare abilitato o disabilitato in base a se si desidera abilitare o disabilitare un certificato dopo il caricamento. Il pulsante Avanti è abilitato solo se è abilitato il certificato.
   - **Imposta gestione** - È possibile associare un certificato ad un insieme esistente o creare un nuovo insieme. Se il certificato è un certificato secondario, questo può essere associato ad un insieme esistente. È possibile associare il certificato a qualunque insieme per un partner interno con la codifica del tipo o per un partner esterno con SSL del tipo (Autorizzazione client in entrata) o Firma (Verifica).
5. Fare clic su **Avanti** per andare alla pagina Insieme della procedura guidata. Se il certificato è primario, non è necessario creare insiemi e associare il certificato ad un insieme e alla connessione partecipante. Se si è selezionata la casella di spunta **Crea nuovo insieme**, allora verrà aperta la pagina **Crea nuovo insieme** della procedura guidata- Altrimenti, si apre la pagina **Aggiungi ad esistente** della procedura guidata. Se il file contiene una chiave privata del partner interno o il certificato pubblico del partner esterno utilizzato per SSL / Firma digitale, allora è possibile fare clic su **Fine**.
6. Nella pagina **Crea nuovo insieme** della procedura guidata, immettere i dettagli del nuovo insieme. Per i certificati primari, non è necessario creare gli insiemi e associarne un certificato. Inserire i seguenti valori:
   - **Nome insieme** - Il nome dell'insieme.
   - **Descrizione** - La descrizione dell'insieme.
   - **Stato** - Selezionare abilitato o disabilitato. Se è disabilitato, il pulsante **Avanti** non verrà abilitato.
   - **Esegui impostazioni predefinite** - Selezionare questa casella di spunta se si desidera che questo insieme sia il predefinito.

7. Nella pagina **Aggiungi all'insieme esistente** della procedura guidata, selezionare gli insiemi a cui aggiungere il certificato. Inserire i seguenti valori:
   - **Selezionare dall'elenco di Insiemi disponibili per il tipo di certificato selezionato** - Dall'elenco, selezionare insiemi a cui aggiungere il certificato.
   - **Rendi impostazioni predefinite**: selezionare questa casella di spunta se si desidera che questo insieme sia quello predefinito.
8. Da **Crea nuovo insieme** o **Aggiungi a insieme esistente**, fare clic su **Avanti** per andare alla pagina **Impostazioni predefinite** della procedura guidata. Il pulsante **Avanti** viene abilitato solo se lo stato dell'insieme è abilitato.
9. Selezionare **abilitato** o **disabilitato** nello **Stato** in base a se si desidera abilitare o disabilitare il Certificato dopo il caricamento.

   Nota: Se si è selezionata la casella di spunta **Rendi insieme predefinito** nella pagina precedente (Crea nuovo insieme o Aggiungi ad insieme esistente), allora è necessario associare l'insieme ad una modalità operativa. Questo visualizza utilizzi di certificato rispetto alle modalità operative. La codifica verrà disabilitata per i partner interni. Il client SSL e la Firma digitale verranno disabilitati per i partner esterni.
10. Fare clic su **Avanti** per andare alla pagina Configurazione della procedura guidata. Se viene fatto clic su **Fine** e vi sono delle root mancanti o certificati CA intermedi, verrà richiesto il caricamento. Se viene fatto clic su ″Sì″ nella finestra di richiesta, si aprirà la prima pagina della procedura guidata. Fare clic su **Annulla** se si desidera eseguire il caricamento in un momento successivo.
11. Nella pagina di configurazione della procedura guidata, immettere i seguenti valori:

    Nota: La pagina Configurazione visualizza un elenco di utilizzi di certificato rispetto alle modalità operative. Il nome insieme corrente è pre-popolato per tutti, ma è possibile reimpostarlo.
    - **Dal partner** - Questo campo verrà pre-popolato con il valore del partner interno.
    - **Al partner** - Questo elenco a discesa viene pre-popolato con l'elenco di tutti i i partner esterni. È possibile selezionare il valore ″Tutti″ per includere tutti i partner esterni.
    - **Dal package** - Dall'elenco a discesa, selezionare gli oggetti Definizioni flusso documento del package del partner interno.
    - **Al package** - Dall'elenco a discesa, selezionare gli oggetti Definizioni flusso documento del package del partner esterno.
12. Fare clic su **Aggiungi altre connessioni** se si desidera associare l'insieme ad altre connessioni partecipanti.
13. Fare clic su **Aggiungi certificato secondario** per aggiungere un certificato secondario all'insieme corrente.
14. Fare clic su **Fine** per caricare il certificato. In caso ci siano root mancanti o certificati CA intermedi, verrà richiesto il caricamento. Se viene fatto clic su ″Sì″ nella finestra di richiesta, si aprirà la prima pagina della procedura guidata. Fare clic su **Annulla** nella finestra di richiesta se si desidera eseguire il caricamento in un momento successivo.

Ripetere questa fase se il partner ha un secondo certificato di codifica.

Fase 3: installare i certificati emessi da CA
Informazioni su questa attività

Se il certificato è stato firmato da CA e il certificato root CA e gli altri certificati che fanno parte della catena di certificati non sono ancora installati nel profilo Operatore hub, installare i certificati seguendo questa procedura:

Nota: non è necessario effettuare questa fase se il certificato emesso da CA è già stato installato.

1. Passare a **Profilo**> **<Operatore hub> utente**> **certificati** > **crea nuovo certificato.**
2. Nell'elenco a discesa **A quale partner appartiene questo certificato**, selezionare il partner da associare al certificato appena caricato.
3. Fare clic su **Cerca** per trovare partner specifici o un sottoinsieme di partner.
4. Fare clic su **Sfoglia** accanto a **Posizione Truststore (o) Keystore**.
5. Per il Certificato ed il Truststore, immettere la **Password**.
6. Per il Truststore, immettere il **Tipo keystore** fare clic su **Avanti**.
7. Nella pagina **Seleziona certificato end-entity da caricare** della procedura guidata, selezionare un certificato da caricare.

   Nota: Quando si caricano i certificati utilizzando un truststore che ha più di un certificato, **Seleziona l'elenco di certificati CA root ed intermedi da caricare** viene popolato con tutti i certificati. È inoltre possibile caricare più certificati.
8. Fare clic su **Fine**.

Fase 4: abilitare la codifica
Informazioni su questa attività

Abilitare la codifica al livello del package (livello più alto), partner o connessione (livello più basso). L'impostazione sostituisce le altre al livello di connessione. Il riepilogo di connessioni informa se un attributo necessario è mancante.

Ad esempio, per alterare gli attributi di una connessione del partner, fare clic su **Amministrazione account > Connessioni** e quindi selezionare i partner. Fare clic su **Attributi** e quindi modificare l'attributo (ad esempio, **AS codificato**).

Quando viene visualizzato il messaggio di errore `Non è stato trovato alcun certificato di codifica valido`, non sono validi né il primo né il secondo certificato. I certificati potrebbero essere scaduti o potrebbero essere stati revocati. Se i certificati sono scaduti o sono stati revocati, l'evento corrispondente (`Certificato revocato o scaduto`) è visibile anche nel Visualizzatore eventi. Si noti che questi due eventi potrebbero essere separati da altri eventi.

Per visualizzare il Visualizzatore eventi completare quanto segue:

1. Fare clic su **Visualizzatori > Visualizzatore eventi**.
2. Selezionare i criteri di ricerca appropriati.
3. Fare clic su **Cerca**.

Consultare il manuale *WebSphere Partner Gateway Administrator Guide* per le informazioni sull'utilizzo del Visualizzatore eventi.

Utilizzo dei certificati per abilitare la firma digitale

Creazione di un certificato di firma in uscita

Il Gestore documenti utilizza questo certificato quando invia i documenti firmati, in uscita ai partner. Lo stesso certificato e la chiave vengono utilizzati per tutte le porte e i protocolli.

È possibile disporre di più un certificato di firma digitale. Uno è quello principale, che è quello predefinito. L'altro è quello secondario, che viene utilizzato se il certificato principale scade.

Creazione di un certificato autofirmato

Informazioni su questa attività

Se si utilizza il certificato autofirmato, attenersi alla seguente procedura.

1. Avviare l'utilità iKeyman.
2. Utilizzare iKeyman per generare un certificato autofirmato e una coppia di chiavi.
3. Utilizzare iKeyman per estrarre in un file il certificato che contiene la chiave pubblica.
4. Distribuire il certificato ai partner. Il metodo preferito per la distribuzione è l'invio del certificato in un file compresso e protetto da password, via e-mail. I partner devono richiamare e richiedere la password per il file compresso.
5. Utilizzare iKeyman per esportare il certificato autofirmato e la coppia di chiavi private nella forma di un file PKCS12.

Installazione certificato autofirmato in uscita

Informazioni su questa attività

1. Passare a **Profilo** > {**Operatore hub/Partner interno**} > **certificati**> **Carica certificato**.
2. Nella pagina **Seleziona partner, Posizione file, Password** della procedura guidata, immettere i seguenti valori:
   - **A quale partner appartiene questo certificato**: Selezionare il partner da associare al certificato appena caricato. Fare clic su Cerca per trovare un partner specifico o un sottoinsieme di partner. Se il partner è un Operatore hub o un Partner interno, immettere la posizione del certificato, la posizione della chiave privata e la password (OPPURE) Fornire il truststore o il keystore con la password. Per il Partner esterno, immettere la posizione del certificato (OPPURE) fornire la posizione del truststore che contiene la catena di certificato.
   - **Chiave privata:** Fare clic su **Sfoglia** per selezionare la chiave privata del certificato.
   - **Password:** Se il certificato dispone di una password, immettere il valore.
   - **Posizione truststore (o) keystore:** Fare clic su **Sfoglia** per selezionare la posizione keystore. Keystore è una raccolta di chiavi private con i certificati root attendibili e CA.
   - **Password:** Immettere la password per la posizione keystore.
   - **Tipo:** Selezionare il tipo di Truststore (o) Keystore. I valori disponibili nell'elenco a discesa sono: JKS, JCEKS, e PKCS12.

   .

3. Fare clic su **Avanti** per andare alla pagina **Dettagli certificato** della procedura guidata. La pagina **Seleziona end-entity e certificati CA** della procedura guidata si apre quando si caricano i certificati tramite un truststore che ha più di un certificato. Viene visualizzato l'elenco di certificati disponibili nel truststore.
4. Nella pagina **Seleziona certificato end-entity e certificato CA** della procedura guidata, immettere i seguenti valori:
   - **Il keystore contiene più di un certificato end-entity. Selezionare il certificato da caricare?** - L'elenco a discesa ha un elenco di tutti i certificati end-entity. Selezionare il certificato da caricare.
   - **Password** - Se il keystore dispone di una password, selezionare questa casella di spunta ed immettere la password nella casella di testo.
   - **Selezionare l'elenco di certificati root e CA intermedi da caricare**- Dal riquadro dell'elenco, selezionare i certificati root e CA intermedi da caricare.
5. Fare clic su **Avanti** per andare alla pagina **Dettagli certificato** della procedura guidata.
6. Nella pagina **Dettagli certificato** della procedura guidata, immettere i seguenti dettagli del certificato:
   - **Nome certificato foglia** - Il nome del certificato foglia. Il nome del campo dipende da se si tratta di Certificato foglia, Certificato CA root o Certificato CA intermedio.
   - **Descrizione** - La descrizione del Certificato foglia.
   - **Tipo certificato** - Associare questo certificato alla Codifica.
   - **Utilizzo certificato** - Associare un utilizzo per il certificato. I valori sono Primario e Secondario.
   - **Modalità operativa** - Immettere la modalità dell'operazione.
   - **Stato** - Selezionare abilitato o disabilitato in base a se si desidera abilitare o disabilitare un certificato dopo il caricamento. Il pulsante Avanti è abilitato solo se è abilitato il certificato.
   - **Imposta gestione** - È possibile associare un certificato ad un insieme esistente o creare un nuovo insieme. Se il certificato è un certificato secondario, questo può essere associato ad un insieme esistente. È possibile associare il certificato a qualunque insieme per un partner interno con la codifica del tipo o per un partner esterno con SSL del tipo (Autorizzazione client in entrata) o Firma (Verifica).

     Nota: Per l'operatore hub, non ci sarà un'altra gestione di insieme. I certificati verranno associato all'insieme predefinito creato.
7. Fare clic su **Avanti** per andare alla pagina Insieme della procedura guidata. Se il certificato è primario, non è necessario creare insiemi e associare il certificato ad un insieme e alla connessione partecipante. Se si è selezionata la casella di spunta **Crea nuovo insieme**, allora verrà aperta la pagina **Crea nuovo insieme** della procedura guidata- Altrimenti, si apre la pagina **Aggiungi ad esistente** della procedura guidata. Se il file contiene una chiave privata del partner interno o il certificato pubblico del partner esterno utilizzato per SSL / Firma digitale, allora è possibile fare clic su **Fine**.
8. Nella pagina **Crea nuovo insieme** della procedura guidata, immettere i dettagli del nuovo insieme. Per i certificati primari, non è necessario creare gli insiemi e associarne un certificato. Inserire i seguenti valori:
   - **Nome insieme** - Il nome dell'insieme.
   - **Descrizione** - La descrizione dell'insieme.

- **Stato** - Selezionare abilitato o disabilitato. Se è disabilitato, il pulsante **Avanti** non verrà abilitato.
- **Esegui impostazioni predefinite** - Selezionare questa casella di spunta se si desidera che questo insieme sia il predefinito.

9. Nella pagina **Aggiungi all'insieme esistente** della procedura guidata, selezionare gli insiemi a cui aggiungere il certificato. Inserire i seguenti valori:
   - **Selezionare dall'elenco di Insiemi disponibili per il tipo di certificato selezionato** - Dall'elenco, selezionare insiemi a cui aggiungere il certificato.
   - **Rendi impostazioni predefinite**: selezionare questa casella di spunta se si desidera che questo insieme sia quello predefinito.
10. Da **Crea nuovo insieme** o **Aggiungi a insieme esistente**, fare clic su **Avanti** per andare alla pagina **Impostazioni predefinite** della procedura guidata. Il pulsante **Avanti** viene abilitato solo se lo stato dell'insieme è abilitato.
11. Selezionare **abilitato** o **disabilitato** nello **Stato** in base a se si desidera abilitare o disabilitare il Certificato dopo il caricamento.

    Nota: Se si è selezionata la casella di spunta **Rendi insieme predefinito** nella pagina precedente (Crea nuovo insieme o Aggiungi ad insieme esistente), allora è necessario associare l'insieme ad una modalità operativa. Questo visualizza utilizzi di certificato rispetto alle modalità operative. La codifica verrà disabilitata per i partner interni. Il client SSL e la Firma digitale verranno disabilitati per i partner esterni.
12. Fare clic su **Avanti** per andare alla pagina Configurazione della procedura guidata. Se viene fatto clic su **Fine** e vi sono delle root mancanti o certificati CA intermedi, verrà richiesto il caricamento. Se viene fatto clic su ″Sì″ nella finestra di richiesta, si aprirà la prima pagina della procedura guidata. Fare clic su **Annulla** se si desidera eseguire il caricamento in un momento successivo.
13. Nella pagina di configurazione della procedura guidata, immettere i seguenti valori:

    Nota: La pagina Configurazione visualizza un elenco di utilizzi di certificato rispetto alle modalità operative. Il nome insieme corrente è pre-popolato per tutti, ma è possibile reimpostarlo.
    - **Dal partner** - Questo campo verrà pre-popolato con il valore del partner interno.
    - **Al partner** - Questo elenco a discesa viene pre-popolato con l'elenco di tutti i i partner esterni. È possibile selezionare il valore ″Tutti″ per includere tutti i partner esterni.
    - **Dal package**: dall'elenco a discesa, selezionare il package Oggetti delle definizioni del flusso di documenti del partner interno.
    - **Al package**: dall'elenco, selezionare il package Oggetti delle definizioni del flusso di documenti del partner esterno.
14. Fare clic su **Aggiungi altre connessioni** se si desidera associare l'insieme ad altre connessioni partecipanti.
15. Fare clic su **Aggiungi certificato secondario** per aggiungere un certificato secondario all'insieme corrente.
16. Fare clic su **Fine** per caricare il certificato. In caso ci siano root mancanti o certificati CA intermedi, verrà richiesto il caricamento. Se viene fatto clic su ″Sì″ nella finestra di richiesta, si aprirà la prima pagina della procedura guidata. Fare clic su **Annulla** nella finestra di richiesta se si desidera eseguire il caricamento in un momento successivo.

Se si stanno caricando i certificati principali e secondari per l'autenticazione del client SSL e la firma digitale e si sta caricando i certificati principali come due voci a parte, verificare che i certificati secondari corrispondenti siano caricati come due voci diverse.

Reperimento di un certificato firmato da CA
Informazioni su questa attività

Se si utilizza un certificato firmato da un CA, attenersi alla seguente procedura:

1. Avviare l'utilità iKeyman.
2. Utilizzare iKeyman per generare una richiesta di certificato e una coppia di chiavi per il Destinatario.
3. Inoltrare un CSR (Certificate Signing Request) a CA.
4. Quando si riceve il certificato firmato da CA, utilizzare iKeyman per posizionare il certificato firmato nel keystore.
5. Distribuire il certificato CA di firma a tutti i partner.

Installazione di un certificato di verifica della firma digitale in entrata

Informazioni su questa attività

Il Gestore documenti utilizza il certificato firmato del partner per verificare la firma del mittente durante la ricezione dei documenti. I partner inviano i relativi certificati di firma autofirmati in formato X.509 DER. Quindi, installare i certificati dei partner mediante la Console comunità nel rispettivo profilo del partner.

Per installare il certificato, attenersi alla seguente procedura.

1. Ricevere il certificato di firma X.509 del partner in formato DER.
2. Passare a **Profilo**> **Partner esterno**> **Certificati** > **Carica certificato**.
3. Fare clic su **Cerca** per trovare partner specifici o un sottoinsieme di partner.
4. Fare clic su **Sfoglia** accanto a **Posizione certificato** per caricare il certificato.
5. Fare clic su **Avanti** per andare alla pagina **Dettagli certificato** della procedura guidata.
6. Associare questo certificato a **Verifica della firma digitale**.
7. Selezionare **abilitato** o **disabilitato** nello **Stato** in base a se si desidera abilitare o disabilitare il Certificato dopo il caricamento.
8. Selezionare la **Modalità operativa**. Se si è un operatore hub, non si dispone dell'opzione di selezionare la **Modalità operativa**.
9. Fare clic su **Fine** per salvare le modifiche e chiudere la procedura guidata.
10. Se il certificato viene firmato da un CA e il certificato CA root e qualsiasi altro certificato parte della catena di certificati non viene installato nel profilo Operatore hub, installarlo. Questo riguarda solo Truststore/Keystore.
    a. Fare clic su **Amministratore hub> Profilo partner hub> Certificati** per visualizzare la pagina Elenco certificati.

       Accertarsi di essersi registrato nella Console comunità come Operatore hub e installare il certificato nel proprio profilo.
    b. Fare clic su **Carica certificato**.
    c. Selezionare **Root e Intermedio**.
    d. Immettere una descrizione del certificato (necessario).
    e. Modificare lo stato in **Abilitato**.

f. Fare clic su **Sfoglia** e navigare nella directory nella quale è stato salvato il certificato.

g. Selezionare il certificato e fare clic su **Apri**.

h. Fare clic su **Carica** e fare clic su **Salva**.

Nota: non è necessario effettuare il passaggio precedente, se il certificato CA è già installato.

11. Abilitare la firma al livello del package (livello più elevato), partner o connessione (livello più basso). L'impostazione sostituisce le altre al livello di connessione. Il riepilogo di connessioni informa se un attributo necessario è mancante.

    Ad esempio, per alterare gli attributi di una connessione del partner, fare clic su **Amministrazione account > Connessioni** e quindi selezionare i partner. Fare clic su **Attributi** e quindi modificare l'attributo (ad esempio, **AS firmato**).

Utilizzo di certificati per abilitare SSL

Nelle sezioni successive viene descritto il modo in cui creare ed installare certificati SSL per essere utilizzati con WebSphere Partner Gateway. È inclusa anche una panoramica del processo handshake SSL. Se la comunità non utilizza SSL, né l'utente né i partner necessitano di un certificato SSL in entrata o in uscita.

Handshake SSL

Informazioni su questa attività

Una connessione SSL comincia con un handshake.

Quando un client (il partner o il partner interno) avvia uno scambio di messaggi, si verificano le seguenti operazioni:

1. Il client invia un messaggio di benvenuto al client in cui vengono elencate le capacità di codifica del client (ordinate secondo l'ordine di preferenza del client), come ad esempio la versione di SSL, il package di crittografia supportato dal client e i metodi di compressione dei dati supportati dal client. Il messaggio contiene anche un numero casuale di 28 byte.
2. Il server risponde con un messaggio di benvenuto del server che contiene il metodo di codifica (package di crittografia) e il metodo di compressione di dati selezionati dal server, l'ID sessione ed un altro numero casuale.

   Nota: il client e i server devono supportare almeno un package di crittografia, o altrimenti l'handshake non riesce. Il server, in genere, sceglie il package di crittografia più comune e valido.
3. Il server invia il certificato digitale.

   In questo passo si verifica l'autenticazione del server.
4. Il server invia un messaggio di richiesta di un certificato digitale. Nel messaggio di richiesta di un certificato digitale, il server invia un elenco di tipi di certificato digitale supportati e i nomi distinti di autorità di certificazione accettabili.
5. Il server invia un messaggio di benvenuto del server ed attende la risposta del client.
6. Dopo la ricezione del messaggio di benvenuto del server, il client verifica la validità del certificato digitale del server e verifica che i parametri di benvenuti siano accettabili.

7. Se il server ha richiesto un certificato digitale del client, il client invia un certificato digitale o se non è disponibile alcun certificato digitale appropriato, il client invia un avviso ″nessun certificato digitale″. Questo avviso è solo un avviso, ma l'applicazione del server può compromettere la sessione, se l'autenticazione è obbligatoria.
8. Il client invia un messaggio ″scambio chiave del client″. Questo messaggio contiene il segreto premaster, un numero casuale di 46 byte utilizzato nella generazione delle chiavi di codifica simmetriche e le chiavi MAC (Message Authentication Code), codificate con la chiave pubblica del server.
9. Se il client ha inviato un certificato digitale al server, il client invia un messaggio ″verifica certificato digitale″ firmato con la chiave privata del client. Verificando la firma di questo messaggio, il server può verificare esplicitamente la proprietà del certificato digitale del client.

   Nota: un processo aggiuntivo per verificare il certificato digitale del server non è necessario. Se il server non dispone della chiave privata che appartiene al certificato digitale, non è in grado di decodificare il segreto premaster e creare le chiavi corrette per l'algoritmo di codifica simmetrico e l'handshake non riesce.
10. Il client utilizza una serie di operazioni di codifica per convertire il segreto premaster in segreto master da cui deriva tutto il materiale delle chiavi necessario per la codifica e l'autenticazione del messaggio. Il client quindi invia un messaggio ″modifica spec. codifica″ per far sì che il server passi al package di crittografia appena negoziato. Il messaggio successivo inviato dal client (il messaggio di chiusura) è il primo messaggio codificato con questo metodo e chiavi di codifica.
11. Il server risponde con messaggi propri ″modifica spec. codifica″ e ″terminato″.

L'autenticazione del client richiede i passi 4 a pagina 261, 7 e 9.

L'handshake SSL termina e i dati dell'applicazione codificati possono essere inviati.

Configurazione di certificati SSL in entrata

Questa sezione descrive il modo in cui configurare l'autenticazione del server e del client per le richieste di connessione in entrata dai partner.

Una richiesta in entrata è quando il partner invia un documento a WebSphere Partner Gateway. Se la comunità non utilizza SSL, non è necessario un certificato SSL in entrata o in uscita.

Nota: per FTPS in entrata, WebSphere Partner Gateway utilizza un server FTP fornito dal cliente, quindi la configurazione SSL in entrata è valida per il server FTP specifico che il cliente utilizza.

Fase 1: Ottenere un certificato SSL

Informazioni su questa attività

WebSphere Application Server utilizza il certificato SSL quando riceve le richieste di connessione dai partner mediante SSL. Indica il certificato che il destinatario presenta per identificare l'hub al partner. Questo certificato del server può essere autofirmato, o può essere firmato da un CA. Nella maggior parte dei casi si utilizza un certificato CA per aumentare la sicurezza. È possibile utilizzare un certificato autofirmato in un ambiente di test. Utilizzare iKeyman o la console di gestione di WebSphere Application Server per generare un certificato ed una

coppia di chiavi. Consultare la documentazione disponibile da IBM per ulteriori informazioni sull'utilizzo di iKeyman o della console di gestione di WebSphere Application Server.

Una volta creati il certificato e la coppia di chiavi, utilizzare il certificato per il traffico SSL in entrata per tutti i partner. Se si dispone di più Destinatari e Console, copiare il keystore che ne risulta in ogni istanza. Se il certificato viene generato utilizzando la console di gestione di WebSphere Application Server, la chiave ed il certificato possono essere importati in un altro keystore in un altro server utilizzando la console di gestione di WebSphere Application Server. Se il certificato è autofirmato, fornire questo certificato ai partner. Per ottenere questo certificato, utilizzare iKeyman per estrarre il certificato pubblico in un file.

Creazione di un certificato autofirmato: Se si utilizzano i certificati del server autofirmato, attenersi alla seguente procedura.

1. Avviare l'utilità iKeyman, che si trova in */<dir_installazione_WAS>*/bin. Se questa è la prima volta che si utilizza iKeyman, eliminare il certificato "fittizio" che si trova nel keystore.
2. Aprire il keystore di Destinatario o Console utilizzando iKeyman ed utilizzare iKeyman per generare un certificato autofirmato ed una coppia di chiavi per il keystore di Destinatario o Console.
3. Utilizzare iKeyman per estrarre in un file il certificato che contiene la chiave pubblica.

   Salvare il keystore in un file JKS, PKCS12 o JCEKS.
4. Distribuire il certificato ai partner. Il metodo preferito per la distribuzione è l'invio del certificato in un file compresso e protetto da password, via e-mail. I partner devono richiamare e richiedere la password per il file compresso.
5. Utilizzando la console di gestione di WebSphere Application Server, impostare il nuovo certificato nella Configurazione SSL e nelle impostazioni per destinatario e console. È possibile eseguire questa operazione selezionando l'alias del nuovo certificato nel keystore nella Configurazione per ciascun nodo o server.

Reperimento di un certificato creato da CA: Se si utilizza un certificato firmato da un'autorità di certificazione, attenersi alla seguente procedura.

1. Avviare l'utilità iKeyman, che si trova nella directory */<dir_installazione_WAS>*/bin.
2. Utilizzare iKeyman per generare una richiesta di certificato e una coppia di chiavi per il Destinatario.
3. Inoltrare un CSR (Certificate Signing Request) a CA.
4. Quando si riceve il certificato firmato da CA, utilizzare iKeyman per posizionare il certificato firmato nel keystore.
5. Distribuire il certificato CA a tutti i partner, se richiesto.
6. Utilizzando la console di gestione di WebSphere Application Server, impostare il nuovo certificato nella Configurazione SSL e nelle impostazioni per destinatario e console. È possibile eseguire questa operazione selezionando l'alias del nuovo certificato nel keystore nella Configurazione per ciascun nodo o server.

   Nota: la console di gestione di WebSphere Application Server può essere utilizzata anche per completare i passi precedenti.

Fase 2: Autenticare i client
Informazioni su questa attività

Se si desidera autenticare i partner che inviano i documenti, effettuare la seguente procedura di questa sezione.

Installazione del certificato del client:
Informazioni su questa attività

Per l'autenticazione client, attenersi alla seguente procedura:

1. Ottenere il certificato del partner.
2. Se il certificato è autofirmato, installare il certificato nel truststore utilizzando iKeyman o la console di gestione di WebSphere Application Server.
3. Se il certificato è rilasciato da una CA, aggiungere i certificati CA correlati nel truststore correlato utilizzando iKeyman oppure la console di gestione di WebSphere Application Server.

Nota: quando si aggiungono più partner alla comunità hub, è possibile utilizzare iKeyman o la console di gestione di WebSphere Application Server per aggiungere i loro certificati al truststore. Se un partner abbandona la comunità, è possibile utilizzare iKeyman o la console di gestione di WebSphere Application Server per rimuovere i certificati del partner dal truststore.

Impostazione dell'autenticazione del client:
Informazioni su questa attività

Dopo l'installazione del certificato o dei certificati, configurare WebSphere Application Server per utilizzare l'autenticazione client eseguendo lo script dell'utilità bcgClientAuth.jacl.

1. Passare alla seguente directory: /<*DirProdotto*>/bin
2. Per attivare l'autenticazione client, chiamare lo script come segue:

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

   Nota: per disattivare l'autenticazione client, chiamare lo script come segue:

```
./bcgwsadmin.sh -f /<DirProdotto>/receiver/scripts/bcgClientAuth.jacl
  -conntype NONE clear
```

È necessario riavviare il server bcgreceiver per rendere effettive queste modifiche. È anche possibile abilitare l'Autenticazione client utilizzando la console di gestione di WebSphere Application Server. Un valore di ″Supportato″ significa che il server richiederà il certificato client ma, se il certificato client non è disponibile, può ancora essere stabilito l'handshake SSL. Un valore di ″Obbligatorio″ significa che il certificato client deve essere inviato. In caso contrario, l'handshake SSL avrà esito negativo.

Convalida del certificato del client:
Informazioni su questa attività

C'è una funzione aggiuntiva che può essere utilizzata con l'autenticazione client SSL. Questa funzione viene abilitata mediante la Console comunità. Per HTTPS, WebSphere Partner Gateway verifica i certificati rispetto agli ID di business nei documenti in entrata. Per utilizzare tale funzione, creare il profilo del partner, importare il certificato del client e indicarlo come SSL.

1. Importare il certificato del client.

a. Fare clic su **Amministrazione account > Profili > Partner** e ricercare il profilo del partner.
b. Fare clic su **Certificati**.
c. Fare clic su **Carica certificato**
d. Fare clic su **Sfoglia** e navigare nella directory nella quale è stato salvato il certificato.
e. Selezionare **Client SSL** come tipo di certificato.
f. Immettere una descrizione del certificato (necessario).
g. Modificare lo stato in **Abilitato**.
h. Se si desidera selezionare una modalità operativa diversa dalla **Produzione** (valore predefinito), selezionarla dall'elenco.
i. Fare clic su **Fine**.

2. Aggiornare la destinazione del client.
   a. Fare clic su **Amministrazione account > Profili > Partner** e ricercare il profilo del partner.
   b. Fare clic su **Destinazioni**.
   c. Selezionare la destinazione HTTPS creata in precedenza. Se non è stata ancora creata la destinazione HTTPS, consultare la sezione "Impostazione di una destinazione HTTPS" a pagina 218.
   d. Per modificare la destinazione, fare clic sull'icona **Modifica**.
   e. Selezionare **Sì** per **Convalida certificato SSL client**.
   f. Fare clic su **Salva**.

Configurazione di keystore e TrustStore distinti per destinatario e console

Per impostazione predefinita, WebSphere Partner Gateway Versione 6.1 utilizza il keystore e il truststore comuni per il destinatario e la console. Tuttavia, è possibile configurare keystore e truststore distinti per il destinatario e la console nell'installazione in in modalità distribuita.

Per configurare il keystore e il truststore, creare ed impostare un keystore e un truststore distinti per destinatario e console. Inoltre, creare le configurazioni SSL distinte. Le configurazioni SSL possono essere a livello di cluster o a livello di server. L'impostazione della configurazione SSL a livello di cluster è più facile in quanto la configurazione sarà poi applicabile a tutti i server compresi in tale cluster, e non sarà necessario configurare ciascun server separatamente.

Impostazione della configurazione SSL a livello di cluster: Durante l'impostazione della configurazione SSL con nuovi keystore e truststore a livello di cluster, non vi deve essere alcuna configurazione impostata a livello di server. Se vi è una configurazione SSL impostata a livello di server, la configurazione SSL a livello di cluster non verrà utilizzata; verrà invece utilizzata quella impostata per il server.

Seguire tali passi per impostare la configurazione SSL per bcgconsoleCluster:

1. Creare un keystore per il cluster della console. Il keystore deve essere creato in ambito cluster bcgconsole passando a **Sicurezza > Gestione chiavi e certificati SSL > Keystore e certificati**.
2. Creare un truststore per il cluster della console. Il truststore deve essere creato in ambito cluster bcgconsole passando a **Sicurezza > Gestione chiavi e certificati SSL > Keystore e certificati**.

3. Creare una configurazione SSL per il cluster della console in ambito cluster console passando a **Sicurezza > Gestione chiavi e certificati SSL > Configurazioni SSL**. Impostare il keystore e il truststore creati nei passi precedenti. Aggiornare gli alias dei certificati nell'elenco relativo facendo clic su **Acquisisci alias certificato** e selezionare l'alias da utilizzare per l'autenticazione del server. Impostare il gestore sicuro su **IbmPKIX**.
4. Impostare questa configurazione SSL in bcgconsoleCluster sovrascrivendo la configurazione SSL ereditata. Aggiornare gli alias dei certificati facendo clic su **Aggiorna alias certificato** e selezionare l'alias da utilizzare per l'autenticazione al server.
5. Riavviare bcgconsoleCluster.

Seguire tali passi per impostare la configurazione SSL per bcgreceiverCluster:

1. Creare un keystore per il cluster del destinatario. Il keystore deve essere creato in ambito cluster bcgreceiver passando a **Sicurezza > Gestione chiavi e certificati SSL > Keystore e certificati**.
2. Creare un truststore per il cluster del destinatario. Il truststore deve essere creato in ambito cluster bcgconsole passando a **Sicurezza > Gestione chiavi e certificati SSL > Keystore e certificati**.
3. Creare una configurazione SSL per il cluster destinatario in ambito cluster destinatario passando a **Sicurezza > Gestione chiavi e certificati SSL > Configurazioni SSL** e impostare il keystore e il truststore creati nelle fasi precedenti. Acquisire gli alias dei certificati facendo clic su **Acquisisci alias certificato** e selezionare l'alias da utilizzare per l'autenticazione al server. Impostare il gestore sicuro su **IbmPKIX**.
4. Impostare questa configurazione SSL in bcgreceiverCluster sovrascrivendo la configurazione SSL ereditata. Aggiornare gli alias dei certificati facendo clic su **Aggiorna alias certificato** e selezionare l'alias da utilizzare per l'autenticazione al server.
5. Riavviare il bcgreceiverCluster.

Per ulteriori informazioni sulle operazioni con keystore, truststore, configurazione SSL, e le configurazioni dell'endpoint, fare riferimento alla sezione *Protezione delle applicazioni e del relativo ambiente della documentazione di WebSphere Application Server.*.

Impostazione di NodeDefaultTrustStore in NodeDefaultSSLSetting in modalità distribuita: Questa impostazione deve essere eseguita per la modalità distribuita semplice. Ma, ciò vale anche per la modalità distribuita completa se il keystore e il truststore devono essere utilizzati per il destinatario e per la console. Se un nodo è federato in una cella, i certificati firmatario dal nodo vengono aggiunti a CellDefaultTrustStore. Per impostazione predefinita, NodeDefaultSSLSetting fa riferimento a CellDefaultTrustStore come truststore. Per il destinatario e la console di WebSphere Partner Gateway, non si consiglia l'utilizzo dei certificati firmatario da altri nodi. Per utilizzare un truststore dedicato per i nodi in cui è installato WebSphere Partner Gateway, NodeDefaultTrustStore può essere impostato in NodeDefaultSSLSettings come truststore.

Per eseguire tale modifica eseguire le seguenti operazioni:

1. Nella console di gestione di WebSphere Application Server, passare a **Sicurezza > Certificato SSL e gestione chiavi > Gestisci configurazioni di sicurezza endpoint > <nome_nodo> > Configurazioni SSL > NodeDefaultSSLSettings**.
2. Nel campo Nome memoria sicura, selezionare **NodeDefaultTrustStore**.

Nota: Assicurarsi che NodeDefaultTrustStore sia configurato per il truststore che si desidera utilizzare; ad esempio, bcgSecurityTrust.jks.

3. Fare clic su **Applica**.
4. Sulla seguente pagina della console, fare clic su **Salva** per aggiornare le modifiche sulla configurazione principale.
5. Riavviare i server su tale nodo.

Nota: Per la modalità distribuita completamente, le suddette modifiche devono essere effettuate per tutti i nodi contenenti i server bcgreceiver e bcgconsole. Per la modalità distribuita semplice, tali modifiche devono essere effettuate per tutti i nodi che contengono bcgserver.

Aggiunta dei certificati firmatario a trust.p12 se NodeDefaultTrustStore è impostato per il nodo che contiene i server di WebSphere Partner Gateway: Al momento, NodeDefaultTrustStore fa riferimento a trust.p12. Se NodeDefaultTrustStore è impostato per il nodo che contiene i server di WebSphere Partner Gateway, bcgSecurityTrust.jks non verrà utilizzato. I certificati firmatario da bcgSecurityTrust.jks devono essere aggiunti a trust.p12 come richiesto.

Configurazione dei certificati SSL in uscita

Una richiesta in uscita è quando WebSphere Partner Gateway invia un documento ad un partner. Se la comunità non utilizza SSL, non è necessario un certificato SSL in entrata o in uscita.

Fase 1: Autenticare il server

Informazioni su questa attività

Quando SSL consente di inviare i documenti in uscita ai partner, WebSphere Partner Gateway richiede un certificato del server dai partner. Lo stesso certificato CA può essere utilizzato per più partner. Il certificato deve essere nel formato X.509 DER.

Nota: è possibile convertire il formato con l'utilità iKeyman. Seguire queste procedure per utilizzare iKeyman per convertire il formato:

1. Avviare iKeyman.
2. Creare un nuovo keystore vuoto oppure aprire un keystore esistente.
3. Nel contenuto del database della chiave, selezionare **Autore firma certificati**.
4. Aggiungere il certificato ARM utilizzando l'opzione **Aggiungi**.
5. Estrarre lo stesso certificato come dati DER binari utilizzando l'opzione **Estrai**.
6. Chiudere iKeyman.

Installare il certificato autofirmato del partner nel profilo Operatore hub. Se il certificato viene firmato da un CA e il certificato CA root e qualsiasi altro certificato parte della catena di certificati non viene installato nel profilo Operatore hub, installarlo.

1. Utilizzare **Amministrazione account > Profili > Certificati** per visualizzare la pagina Elenco certificati.

   Accertarsi di essersi registrati nella Console comunità come Operatore hub o Partner interno.
2. Fare clic su **Carica PKCS12**.

Nota: il file PKCS12 che sta per essere caricato dovrebbe contenere solo una chiave privata e il certificato associato. È anche possibile caricare il certificato e la chiave privata con formattazione PKCS#8 separatamente.

3. Selezionare **Client SSL** come tipo di certificato.
4. Immettere una descrizione del certificato (necessario).
5. Modificare lo stato in **Abilitato**.
6. Fare clic su **Sfoglia** e navigare nella directory nella quale è stato salvato il certificato.
7. Selezionare il certificato e fare clic su **Apri**.
8. Immettere la password.
9. Se si desidera selezionare una modalità operativa diversa dalla **Produzione** (valore predefinito), selezionarla dall'elenco.
10. Se ci fossero due certificati SSL, indicare quello principale e quello secondario selezionando **Principale** o **Secondario** dall'elenco **Utilizzo certificato**.
11. Fare clic su **Carica** e fare clic su **Salva**.

Nota: non è necessario effettuare i passaggi precedenti se il certificato CA è già installato.

Fase 2: Autenticare i client

Informazioni su questa attività

Se l'autenticazione del client SSL è obbligatoria, il partner, a sua volta, richiederà un certificato dall'hub. Utilizzare la Console comunità per importare il certificato in WebSphere Partner Gateway. È possibile modificare le informazioni mediante iKeyman. Se il certificato è autofirmato, è necessario che sia fornito al partner. Se si tratta di un certificato firmato da CA, il certificato root CA deve essere fornito ai partner, in modo tale che possano aggiungerlo ai relativi certificati attendibili.

È possibile disporre di più un certificato SSL. Uno è quello principale, che è quello predefinito. L'altro è quello secondario, che viene utilizzato se il certificato principale scade.

Utilizzo di un certificato autofirmato:
Informazioni su questa attività

Se si utilizza il certificato autofirmato, attenersi alla seguente procedura.

1. Avviare l'utilità iKeyman.
2. Utilizzare iKeyman per generare un certificato autofirmato e una coppia di chiavi.
3. Utilizzare iKeyman per estrarre in un file il certificato che contiene la chiave pubblica.
4. Distribuire il certificato ai partner. Il metodo preferito per la distribuzione è l'invio del certificato in un file compresso e protetto da password, via e-mail. I partner devono richiamare e richiedere la password per il file compresso.
5. Utilizzare iKeyman per esportare il certificato autofirmato e la coppia di chiavi private nella forma di un file PKCS12.
6. Installare il certificato autofirmato e la chiave mediante la Console comunità.
   a. Utilizzare **Amministrazione account > Profili > Certificati** per visualizzare la pagina Elenco certificati.

      Accertarsi di essersi registrati nella Console comunità come Operatore hub.
   b. Fare clic su **Carica PKCS12**.

Nota: il file PKCS12 che sta per essere caricato dovrebbe contenere solo una chiave privata e il certificato associato. È anche possibile caricare il certificato e la chiave privata con formattazione PKCS#8 separatamente.

c. Selezionare **Client SSL** come tipo di certificato.

d. Immettere una descrizione del certificato (necessario).

e. Modificare lo stato in **Abilitato**.

f. Fare clic su **Sfoglia** e navigare nella directory nella quale è stato salvato il certificato.

g. Selezionare il certificato e fare clic su **Apri**.

h. Immettere la password.

i. Se si desidera selezionare una modalità operativa diversa dalla **Produzione** (valore predefinito), selezionarla dall'elenco.

j. Se ci fossero due certificati SSL, indicare quello principale e quello secondario selezionando **Principale** o **Secondario** dall'elenco **Utilizzo certificato**.

k. Fare clic su **Carica** e fare clic su **Salva**.

Se si stanno caricando i certificati principali e secondari per l'autenticazione del client SSL e la firma digitale e si sta caricando i certificati principali come due voci a parte, verificare che i certificati secondari corrispondenti siano caricati come due voci diverse.

Utilizzo di un certificato firmato da un'Autorità di certificazione: Informazioni su questa attività

Se si utilizza un certificato firmato da un CA, attenersi alla seguente procedura:

1. Utilizzare iKeyman per generare una richiesta di certificato e una coppia di chiavi per il Destinatario.
2. Inoltrare un CSR (Certificate Signing Request) a CA.
3. Quando si riceve il certificato firmato da CA, utilizzare iKeyman per posizionare il certificato firmato nel keystore.
4. Distribuire il certificato CA di firma a tutti i partner.

Aggiunta di un CRL (Certificate Revocation List)

WebSphere Partner Gateway include una funzione CRL (Certificate Revocation List). Il CRL, emesso da CA (Certificate Authority), identifica i partner che hanno revocato i certificati prima della data di scadenza pianificata. Ai partner con i certificati revocati verrà negato l'accesso a WebSphere Partner Gateway.

Ogni certificato revocato viene identificato in un CRL dal numero seriale del certificato. Il Gestore documenti scansiona il CRL ogni 60 secondi e rifiuta un certificato se viene contenuto nell'elenco CRL. Tuttavia, è possibile configurare l'intervallo di tempo in cui viene effettuata la scansione della directory CRL. L'intervallo di tempo viene specificato per la proprietà di configurazione bcg.rosettanet.encrypt.CertDbRefreshInterval.

Per impostazione predefinita, i CRL sono memorizzati nella seguente posizione: /<*directory_dati_condivisi*>/security/crl. WebSphere Partner Gateway utilizza l'impostazione bcg.CRLDir in Console > Gestione sistema > Gestione DocMgr > Sicurezza per identificare l'ubicazione della directory CRL.

Inserire i CRL nella directory CRL.

Configurazione di DRL DP

Informazioni su questa attività

Configurare DRL DP modificando le impostazioni di Java Virtual Machine, ovvero, impostare il valore di Dcom.ibm.security.enableCRLDP = True.

Questa operazione deve essere eseguita per il server bcgdocmgr in modalità distribuita completa. Per bcgserver in caso di modalità distribuita semplice e modalità semplice.

I passi sono i seguenti:

1. Collegarsi alla console di gestione di WebSphere Application Server.
2. Andare a **Server > Server delle applicazioni** e selezionare **Server**.
3. Impostare la proprietà utilizzando il seguente processo:
   a. Selezionare il server (bcgdocmgr, bcgreceiver o bcgconsole).
   b. Nella pagina **Configurazione**, espandere **Gestione di processo e Java** nella sezione **Infrastruttura di server** della pagina e selezionare **Definizione processo.**
   c. Nella pagina **Configurazione definizione processo**, selezionare **Java Virtual Machine** nella sezione **Ulteriori proprietà**.
   d. Accodare quanto segue al valore esistente (se presente) nel campo Argomenti JVM generici: -Dcom.ibm.security.enableCRLDP=true.
4. Fare clic su **Applica** e poi su Salva per completare questa configurazione.
5. Riavviare il server.
6. Impostare questa proprietà in tutti i server nel cluster.

Configurazione di SSL in entrata per i componenti Console comunità e Destinatario

I keystore WebSphere Partner Gateway vengono preconfigurati in WebSphere Application Server. Questa sezione è valida solo se si stanno utilizzano keystore differenti.

Per configurare SSL per la Console comunità e il Destinatario in WebSphere Partner Gateway, effettuare la seguente procedura.

1. Ottenere le seguenti informazioni:
   - Nomi del percorso completo del file della chiave e del file truststore; ad esempio per il Destinatario: <*DirProdotto*>/common/security/keystore/bcgSecurity.jks e <*DirProdotto*>/common/security/keystore/bcgSecurityTrust.jks

     È necessario inserire questi nomi correttamente. Nell'ambiente UNIX, questi nomi fanno distinzione tra maiuscole e minuscole.
   - Le nuove password per ogni file.
   - Il formato di ogni file. Questo deve essere scelto da uno dei valori JKS, JCEKS, o PKCS12. Inserire questo valore esattamente in maiuscole come mostrato.
   - Il percorso nel file di script denominato bcgssl.jacl.
2. Aprire una finestra Console comunità e passare a /<*DirProdotto*>/bin. Per modificare le password non è necessario che il server sia in esecuzione.

3. Inserire il seguente comando, sostituendo i valori che sono inclusi in <>. È necessario inserire tutti i valori.

```
./bcgwsadmin.sh -f /<DirProdotto>/
scripts/bcgssl.jacl -conntype NONE install
<keyFile_pathname>
<keyFile_password> <keyFile_format> <trustFile_pathname>
<trustFile_password> <trustFile_format>
```

4. Avviare il server. Se il server non riesce ad avviarsi, questo potrebbe essere dovuto a un errore quando si esegue bcgssl.jacl. Se si commette un errore, è possibile rieseguire lo script e correggerlo.
5. Se è stato utilizzato bcgClientAuth.jacl per impostare la proprietà clientAuthentication SSL, ripristinarlo dopo aver utilizzato bcgssl.jacl. Questo perché bcgssl.jacl sovrascrive i valori che potrebbero essere impostati per l'autenticazione del client con il valore false.

Nota:

1. Ripetere queste procedure per la Console, sostituendo **console** con **destinatario** nel nome del percorso.
2. La configurazione per SSL, keystore e truststore può essere eseguita anche utilizzando la console di gestione di WebSphere Application Server.

Per impostazione predefinita, WebSphere Partner Gateway supporta un keystore e truststore per il destinatario e la console. Tuttavia, è possibile utilizzare keystore e truststore separati per il destinatario e la console in modalità distribuita completa. Per utilizzare keystore e truststore per il destinatario e la console, eseguire la configurazione utilizzando la console di gestione WAS per il destinatario:

1. Creare un keystore per il keystore del destinatario. Fare riferimento alla sezione Creazione configurazione keystore nella documentazione WAS.
2. Creare un truststore per il truststore del destinatario. Fare riferimento alla sezione *<Creazione di una configurazione keystore*nella documentazione WAS *<Protezione delle applicazioni e del relativo ambiente.*
3. Creare una configurazione SSL per il destinatario ed impostare keystore e truststore in quella configurazione. Selezionare l'alias richiesto da utilizzare per l'autenticazione del server nel keystore. Impostare il gestore sicuro su **IbmPKIX**. Fare riferimento alla sezione *Creazione di una configurazione Secure Socket Layer*nella documentazione WAS *Protezione delle applicazioni e del relativo ambiente.*
4. Impostare questa configurazione SSL in ogni server bcgreceiver sovrascrivendo la configurazione SSL ereditata. Impostare l'alias da utilizzare per l'autenticazione del server.
5. Riavviare ogni server bcgreceiver.

La procedura è simile per la configurazione della console. Fare riferimento alle sezioni appropriate nella documentazione WAS *Protezione delle applicazioni e del relativo ambiente.*

1. Creare un keystore per il keystore della console.
2. Creare un truststore per il truststore della console.
3. Creare una configurazione SSL per la console ed impostare keystore e truststore in quella configurazione. Selezionare l'alias richiesto da utilizzare per l'autenticazione del server nel keystore. Impostare il gestore sicuro su **IbmPKIX.**
4. Impostare questa configurazione SSL in ogni server bcgconsole sovrascrivendo la configurazione SSL ereditata. Impostare l'alias da utilizzare per l'autenticazione del server.

5. Riavviare ogni server bcgconsole.

Per ulteriori informazioni sulle operazioni con keystore, truststore, configurazione SSL, e le configurazioni dell'endpoint, fare riferimento alla documentazione WAS *Protezione delle applicazioni e del relativo ambiente*.

Nota: Al momento, NodeDefaultTrustStore fa riferimento a trust.p12. Se NodeDefaultTrustStore è impostato per il nodo bcg, allora bcgSecurityTrust.jks non verrà utilizzato. È necessario aggiungere i certificati del firmatario da bcgSecurityTrust.jks a trust.p12 come richiesto.

Caricamento certificati utilizzando la procedura guidata

Informazioni su questa attività

Come un operatore hub è possibile caricare i certificati per partner interni o esterni:

- Caricare la chiave privata per i partner interni.
- Caricare i certificati pubblici per i partner esterni.
- Caricare il certificato root e CA intermedio.
- Caricare una catena di certificati da un truststore.

La procedura guidata di caricamento dei certificati viene fornita per caricare i certificati. Utilizzando la procedura guidata è possibile associare il certificato ad un utilizzo (Firma / verifica / Codifica / decodifica /SSL), associarlo ad una o più modalità operative, aggiungerlo ad un insieme (esistente o nuovo), selezionare il certificato in modo che diventi il certificato predefinito per tutte le connessioni partecipanti o selezionare una connessione specifica in cui verrà utilizzato questo insieme di certificati. L'opzione di associare il certificato alla connessione non appare se il certificato non è associato ad un insieme. Mentre si carica il certificato, verificare che questo sia valido o comunque non scaduto. Operazioni per caricare i certificati per i partner (interni o esterni) utilizzando la procedura guidata:

1. Dal menu di navigazione, fare clic su **Amministrazione account** > **Profilo** > **Certificati**.
2. Selezionare il partner e fare clic su **Certificati**.
3. Fare clic su **Carica certificato**.
4. Nella pagina **Seleziona partner, Posizione file, Password** della procedura guidata, immettere i seguenti valori:
   - **A quale partner appartiene questo certificato**: Selezionare il partner da associare al certificato appena caricato. Fare clic su Cerca per trovare un partner specifico o un sottoinsieme di partner. Se il partner è un Operatore hub o un Partner interno, immettere la posizione del certificato, la posizione della chiave privata e la password (OPPURE) Fornire il truststore o il keystore con la password. Per il Partner esterno, immettere la posizione del certificato (OPPURE) fornire la posizione del truststore che contiene la catena di certificato.
   - **È un certificato root e intermedio**: Selezionare questa casella di spunta se il certificato è root ed intermedio.

     Nota: Il tipo di certificato root ed intermedio si applica solo al profilo amministratore hub, in questo modo la casella di spunta Certificato root e intermedio è visibile solo quando il partner selezionato è l'amministratore hub. Inoltre, per i profili amministratore hub, la casella di spunta Certificato root e intermedio è disponibile solo se si seleziona Carica certificato.

- **Posizione certificato**: Fare clic su **Sfoglia** per selezionare la posizione del certificato (pubblica/privata).
- **Chiave privata:** Fare clic su **Sfoglia** per selezionare la chiave privata del certificato.
- **Password:** Se il certificato dispone di una password, immettere il valore.
- **Posizione Truststore (o) Keystore:** Fare clic su **Sfoglia** per selezionare la posizione Truststore (o) Keystore. Truststore è un file che contiene una raccolta di certificati CA attendibili e root. Keystore è una raccolta di chiavi private con i certificati root attendibili e CA.
- **Password:** Se la posizione Truststore (o) Keystore dispone di una password, immettere il valore.
- **Tipo:** Selezionare il tipo di Truststore (o) Keystore. I valori disponibili nell'elenco a discesa sono: JKS, JCEKS e PKCS12.

.

5. Fare clic su **Avanti** per andare alla pagina **Dettagli certificato** della procedura guidata. La pagina **Seleziona end-entity e certificati CA** della procedura guidata si apre quando si caricano i certificati tramite un truststore che ha più di un certificato. Viene visualizzato l'elenco di certificati disponibili nel truststore.
6. Selezionare un certificato nella pagina **Seleziona certificato end-entity da caricare** della procedura guidata. Se il Keystore dispone di più chiavi private, allora insieme alla chiave privata è necessario immettere la password per la chiave, se è diversa.
7. Nella pagina **Seleziona certificato end-entity e certificato CA** della procedura guidata, immettere i seguenti valori:
   - **Il keystore contiene più di un certificato end-entity. Selezionare il certificato da caricare?** - L'elenco a discesa ha un elenco di tutti i certificati end-entity. Selezionare il certificato da caricare.
   - **Password** - Se il keystore dispone di una password, selezionare questa casella di spunta ed immettere la password nella casella di testo.
   - **Selezionare l'elenco di certificati root e CA intermedi da caricare**- Dal riquadro dell'elenco, selezionare i certificati root e CA intermedi da caricare.
8. Fare clic su **Avanti** per andare alla pagina **Dettagli certificato** della procedura guidata.
9. Nella pagina **Dettagli certificato** della procedura guidata, immettere i seguenti dettagli del certificato:
   - **Nome certificato foglia** - Il nome del certificato foglia. Il nome del campo dipende da se si tratta di Certificato foglia, Certificato CA root o Certificato CA intermedio.
   - **Descrizione** - La descrizione del Certificato foglia.
   - **Tipo certificato** - Associare questo certificato ad un tipo certificato. I tipi differenti supportati sono Firma digitale, Verifica della firma digitale, Codifica, Decodifica, Server SSL e Client SSL.
   - **Utilizzo certificato** - Associare un utilizzo per il certificato. I valori sono Primario e Secondario.
   - **Modalità operativa** - Immettere la modalità dell'operazione.
   - **Stato** - Selezionare abilitato o disabilitato in base a se si desidera abilitare o disabilitare un certificato dopo il caricamento. Il pulsante Avanti è abilitato solo se è abilitato il certificato.

- **Imposta gestione** - È possibile associare un certificato ad un insieme esistente o creare un nuovo insieme. Se il certificato è un certificato secondario, questo può essere associato ad un insieme esistente. È possibile associare il certificato a qualunque insieme per un partner interno con la codifica del tipo o per un partner esterno con SSL del tipo (Autorizzazione client in entrata) o Firma (Verifica).

10. Fare clic su **Avanti** per andare alla pagina Insieme della procedura guidata. Se il certificato è primario, non è necessario creare insiemi e associare il certificato ad un insieme e alla connessione partecipante. Se si è selezionata la casella di spunta **Crea nuovo insieme**, allora verrà aperta la pagina **Crea nuovo insieme** della procedura guidata- Altrimenti, si apre la pagina **Aggiungi ad esistente** della procedura guidata. Se il file contiene una chiave privata del partner interno o il certificato pubblico del partner esterno utilizzato per SSL / Firma digitale, allora è possibile fare clic su **Fine**.
11. Nella pagina **Crea nuovo insieme** della procedura guidata, immettere i dettagli del nuovo insieme. Per i certificati primari, non è necessario creare gli insiemi e associarne un certificato. Inserire i seguenti valori:
    - **Nome insieme** - Il nome dell'insieme.
    - **Descrizione** - La descrizione dell'insieme.
    - **Stato** - Selezionare abilitato o disabilitato. Se è disabilitato, il pulsante **Avanti** non verrà abilitato.
    - **Esegui impostazioni predefinite** - Selezionare questa casella di spunta se si desidera che questo insieme sia il predefinito.
12. Nella pagina **Aggiungi all'insieme esistente** della procedura guidata, selezionare gli insiemi a cui aggiungere il certificato. Inserire i seguenti valori:
    - **Selezionare dall'elenco di Insiemi disponibili per il tipo di certificato selezionato** - Dall'elenco, selezionare insiemi a cui aggiungere il certificato.
    - **Esegui impostazioni predefinite** - Selezionare questa casella di spunta se si desidera che questo insieme sia il predefinito.
13. Da **Crea nuovo insieme** o **Aggiungi a insieme esistente**, fare clic su **Avanti** per andare alla pagina **Impostazioni predefinite** della procedura guidata. Il pulsante **Avanti** viene abilitato solo se lo stato dell'insieme è abilitato.
14. Selezionare **abilitato** o **disabilitato** nello **Stato** in base a se si desidera abilitare o disabilitare il Certificato dopo il caricamento.

    Nota: Se si è selezionata la casella di spunta **Rendi insieme predefinito** nella pagina precedente (Crea nuovo insieme o Aggiungi ad insieme esistente), allora è necessario associare l'insieme ad una modalità operativa. Questo visualizza utilizzi di certificato rispetto alle modalità operative. La codifica verrà disabilitata per i partner interni. Il client SSL e la Firma digitale verranno disabilitati per i partner esterni.
15. Fare clic su **Avanti** per andare alla pagina Configurazione della procedura guidata. Se viene fatto clic su **Fine** e vi sono delle root mancanti o certificati CA intermedi, verrà richiesto il caricamento. Se viene fatto clic su "Sì" nella finestra di richiesta, si aprirà la prima pagina della procedura guidata. Fare clic su **Annulla** se si desidera eseguire il caricamento in un momento successivo.
16. Nella pagina di configurazione della procedura guidata, immettere i seguenti valori:

    Nota: La pagina Configurazione visualizza un elenco di utilizzi di certificato rispetto alle modalità operative. Il nome insieme corrente è pre-popolato per tutti, ma è possibile reimpostarlo.

- **Dal partner** - Questo campo verrà pre-popolato con il valore del partner interno.
- **Al partner** - Questo elenco a discesa viene pre-popolato con l'elenco di tutti i i partner esterni. È possibile selezionare il valore "Tutti" per includere tutti i partner esterni.
- **Dal package**: dall'elenco a discesa, selezionare il package Oggetti delle definizioni del flusso di documenti del partner interno.
- **Al package**: dall'elenco, selezionare il package Oggetti delle definizioni del flusso di documenti del partner esterno.

17. Fare clic su **Aggiungi altre connessioni** se si desidera associare l'insieme ad altre connessioni partecipanti.
18. Fare clic su **Aggiungi certificato secondario** per aggiungere un certificato secondario all'insieme corrente.
19. Fare clic su **Fine** per caricare il certificato. In caso ci siano root mancanti o certificati CA intermedi, verrà richiesto il caricamento. Se viene fatto clic su "Sì" nella finestra di richiesta, si aprirà la prima pagina della procedura guidata. Fare clic su **Annulla** nella finestra di richiesta se si desidera eseguire il caricamento in un momento successivo.

Creazione insiemi di certificato

Informazioni su questa attività

L'insieme di certificato viene introdotto in 6.1.1 per le seguenti funzioni di sicurezza:

- Autenticazione client SSL dei messaggi in uscita dal partner interno al partner esterno.
- Aggiunta firma digitale ai messaggi in uscita dal partner interno al partner esterno.
- Codifica messaggi in uscita dal partner interno al partner esterno.
- Gli insiemi non sono utilizzati per gli scenari in entrata, come la verifica del certificato di autenticazione client SSL del partner esterno nel truststore WebSphere Partner Gateway, la verifica della firma digitale del partner esterno e la decodifica dei messaggi codificati per il partner interno.

Per creare un nuovo insieme Certificato, seguire la procedura di seguito riportata:

1. Nella Console, passare a **Profilo** > **Partner** > **Elenco certificati** > **Elenco insiemi certificati**> **Crea insieme**.
2. Fare clic su **Certificato > Insiemi certificati > Crea insieme**.
3. Immettere il **Nome insieme** e la **Descrizione** per il nuovo insieme certificato.
4. Impostare il **Tipo certificato**.
5. Selezionare la casella di spunta **Abilitato** o **Disabilitato** per abilitare o disabilitare l'**Insieme certificato**.
6. Fare clic su **Carica certificato**

   Nota: L'elenco a discesa **Certificato principale** e **Certificato secondario** viene popolato in base al **Tipo di certificato** selezionato. Se ci sono certificati già creati e non associati ad alcun insieme, allora è possibile aggiungere i certificati all'insieme al momento creato. Se l'elenco dei certificati è vuoto, allora ci sarà un elenco a discesa vuoto.
7. Selezionare **Certificato principale** e **Certificato secondario** dall'elenco a discesa.
8. Fare clic su **Salva**.

Eliminazione insieme certificato

Informazioni su questa attività

1. Nella Console, passare a **Profilo** > **Partner** > **Elenco insieme certificato**. Questa vista elenca tutti i certificati creati per il partner.
2. Fare clic sull'icona **Elimina**. Prima dell'operazione di eliminazione, verificare di aver modificato tutti i riferimenti a questo insieme nella connessione.
3. Se l'insieme viene utilizzato da una o più connessioni, appare un messaggio di avvertimento. Per verificare dove viene utilizzato un certificato particolare, consultare "Certificato Whereused".
4. Nella finestra del messaggio di avvertimento, fare clic su **OK** per eliminare oppure fare clic su **Annulla** per interrompere l'eliminazione dell'insieme di certificati.

Certificato Whereused

Nella Console, passare a **Profilo** > **{Partner}** > **Elenco certificati** > **Elenco insiemi certificati** > **Whereused**. La vista risultante visualizza i dettagli seguenti:

- Dal partner
- Al partner
- Dal package
- Al package
- Client SSL
- Firma digitale
- Verifica della firma digitale
- Codifica
- Decodifica
- Validità.

Nota: Il certificato potrebbe non essere valido a causa dei seguenti motivi: Se non c'è un certificato principale, il certificato principale è disabilitato, l'insieme è disabilitato il principale è scaduto e non esiste un secondario e, entrambi il primario ed il secondario sono scaduti.

Configurazione di SSL per il destinatario/destinazione script FTP

Per il destinatario script FTP, il certificato di autenticazione del client SSL viene caricato nel profilo operatore Hub. Anche se i certificati vengono caricati per il partner interno, questo non sovrascrive le impostazioni globali.

Fornitura del certificato predefinito per tutti i partner interni

Poiché WebSphere Partner Gateway supporta più partner interni, ognuno deve caricare chiavi private. Nel caso di un'organizzazione che desidera condividere un certificato con le unità dell'organizzazione, è necessario caricare il certificato per ogni partner interno. Per semplificare ciò, è possibile fornire un'opzione predefinita in modo che venga utilizzato un certificato particolare per tutti i partner interni.

Nella Console, passare a **Certificati** > **Carica certificati**. Caricare i certificati e fornire dettagli del tipo certificato, dell'utilizzo e della modalità operativa. Quando si salvano le informazioni specificate, il certificato/le chiavi sono caricate al livello

dell'operatore hub. Durante il runtime il valore predefinito fornito al livello dell'operatore hub viene utilizzato in assenza di qualunque certificato.

Riepilogo certificato

La Tabella 30 riepiloga il modo in cui vengono utilizzati i certificati in WebSphere Partner Gateway. Le posizioni dei certificati vengono illustrate in parentesi "( )".

Tabella 30. Informazioni di riepilogo certificato

Metodo recapito messaggio (si veda la nota 1)	**Certificato operatore hub**	**Ottenere il certificato e CA dal partner**	**CA (consultare la nota 2)**	**Fornire il certificato al partner (consultare la nota 3)**	**Commenti**
SSL in entrata	Installare sull'SSL da parte del server di WebSphere Application. (Posizionare nel keystore di WebSphere Application Server.)	Certificato autofirmato del partner.	Necessario solo se viene utilizzata l'autenticazione del client. (Posizionare il CA o il certificato autofirmato nel trust-store di WebSphere Application Server.)	Il certificato dell'operatore dell'hub, se autofirmato, o il certificato root CA, se richiesto, se è autenticato da CA.	
SSL in uscita	Se viene utilizzata l'autenticazione del client. (WebSphere Partner Gateway)	Certificato root CA o certificato del server del partner se è autenticato da CA.	WebSphere Partner Gateway	Il certificato dell'operatore dell'hub, se autofirmato, o il certificato CA, se firmato da terzi.	
Decodifica in entrata	Chiave privata (WebSphere Partner Gateway)	N/A	Se il certificato è firmato da CA, i certificati CA devono essere caricati come certificati Root/Intermedio.	Certificato operatore hub	Per la codifica del messaggio
Verifica della firma digitale in entrata	N/A	Certificato per la convalida utilizzato per la firma digitale. (WebSphere Partner Gateway)	WebSphere Partner Gateway	NA	Per la verifica e il non rifiuto
Codifica in uscita	N/A	Utilizzare il certificato ottenuto dal partner. (Il certificato è stato installato nel profilo del partner)	Catena di certificati CA per il certificato client, se non è autofirmato	N/A	Per la codifica di messaggi in uscita

Tabella 30. Informazioni di riepilogo certificato (Continua)

Metodo recapito messaggio (si veda la nota 1)	Certificato operatore hub	Ottenere il certificato e CA dal partner	CA (consultare la nota 2)	Fornire il certificato al partner (consultare la nota 3)	Commenti
Firma in uscita	Chiave privata e certificato (WebSphere Partner Gateway)	N/A	Catena di certificati CA.	Facoltativo, in base al partner; dare il certificato WebSphere Partner Gateway	
Convalida di certificato in ID di business	N/A	Caricare nel profilo del partner			Convalida che questo certificato è valido per l'ID di business durante la verifica client SSL

Notes:

1. Un messaggio in entrata è quello che entra in WebSphere Partner Gateway da un partner. Un messaggio in uscita è quello che esce da WebSphere Partner Gateway ad un partner.
2. Se il certificato è stato emesso dal CA, il certificato CA emesso deve essere memorizzato. Si applica al certificato Operatore hub o al certificato del partner.
3. Se è coinvolta una chiave privata, il certificato corrisponde alla chiave privata.

Conformità FIPS

WebSphere Partner Gateway è conforme allo standard FIPS (Federal Information processing Standard), in modo specifico allo standard FIPS 140-2. **IBMJCEFIPS** è il provider JCE conforme a FIPS. Il provider **IBMJSSE2 JSSE** utilizza **IBM JCE** e non contiene il codice per la crittografia, in questo modo non è necessario che sia certificato per la conformità FIPS. Il provider **IBMJSSEFIPS JSSE** è conforme a FIPS, ma si consiglia di utilizzare il provider **IBMJSSE2** in WebSphere Partner Gateway, poiché è l'ultimo provider e supporta più algoritmi e ha migliorato l'utilità. Il prodotto può essere eseguito in modalità FIPS o non FIPS. Se la modalità FIPS viene configurata e viene utilizzato l'algoritmo approvato diverso da FIPS, viene generato un evento di errore e la transazione del documento viene arrestata. L'algoritmo PKCS#12 non è approvato da FIPS, quindi non è possibile caricare i file PKCS#12 in modalità FIPS. È necessario essere un amministratore per configurare WesbSphere Partner Gateway affinché venga eseguito in FIPS o in modalità predefinita. Per la modalità FIPS, PKCS#12 può essere caricato nella console di WebSphere Partner Gateway in formato JCEKS o JKS utilizzando iKeyman.

La modalità FIPS supporta i keystore JKS e JCEKS, ma non supporta i keystore PKCS#12. La console consente il caricamento di certificato e chiave in formato JKS o JCEKS. Nello schermo **Caricamento keystore**, selezionare il formato dall'elenco a discesa **Formato keystore**. I valori disponibili nell'elenco a discesa **Formato keystore** sono: PKCS#12, JKS e JCEKS.

Configurazione di WebSphere Partner Gateway per l'esecuzione in modalità FIPS

Informazioni su questa attività

Per configurare WebSphere Partner Gateway affinché venga eseguito in modalità FIPS, utilizzare la seguente procedura:

1. Impostare i provider FIPS nel file **java.security**.
2. Impostare la proprietà di sistema **bcg.FIPSMode** su ″true″ nella console di WebSphere Partner Gateway.
3. Impostare il provider IBMJCEFIPS prima del provider IBMJCE nel file java.security. Il file java.security si trova nella directory <Installazione WAS>/java/jre/lib/security.
4. Impostare le classi della factory socket abilitate a FIPS per la factory socket JSSE e la factory socket server.
5. Riavviare tutti i server.

   Nota: Un evento informativo viene generato per indicare che il prodotto è in esecuzione in modalità FIPS.

Configurazione di WebSphere Partner Gateway per l'esecuzione in modalità predefinita

Informazioni su questa attività

Per configurare WebSphere Partner Gateway affinché venga eseguito in modalità predefinita, utilizzare la seguente procedura:

1. Nella console di WebSphere Partner Gateway, impostare la proprietà di sistema **bcg.FIPSMode** sul valore ″False″.
2. Reimpostare le impostazioni per la factory socket JSSE, la factory socket del server e i provider nel file **java.security**, come menzionato di seguito.
   a. Rimuovere la proprietà di sistema **com.ibm.jsse2.JSSEFIPS=true** dalle proprietà JVM generiche per ciascun server.
   b. Reimpostare i valori delle seguenti proprietà ai loro valori originali:
      - ssl.SocketFactory.provider
      - ssl.SocketFactory.provider
   c. Per ogni installazione di WAS, commentare il provider IBMJCEFIPS e rinumerare i provider, a partire da 1, nel file **java.security**.
3. Riavviare i server.

   Nota: Un evento informativo viene generato per indicare la modalità. In modalità predefinita, tutti gli algoritmi supportati possono essere utilizzati inclusi gli algoritmi approvati non FIPS.

Configurazione dei provider IBM JSSE per la modalità FIPS

Informazioni su questa attività

Per configurare i provider IBM JSSE per la modalità FIPS, utilizzare la seguente procedura:

1. Impostare la proprietà di sistema **com.ibm.jsse2.JSSEFIPS** sul valore ″True″. Ciò viene eseguito impostando le proprietà di sistema JVM per il server delle applicazioni, mediante l'utilizzo della console di gestione di WAS. Passare alla

pagina <Server>/Gestione di processo e Java/Definizione processo/Java Virtual Machine e specificare la proprietà **-Dcom.ibm.jsse2.JSSEFIPS=true**. Tale impostazione deve essere eseguita per ciascun server.

2. Impostare le seguenti proprietà di sicurezza per il provider IBMJSSE2 per gestire tutte le richieste JSSE:
   - ssl.SocketFactory.provider = com.ibm.jsse2.SSLSocketFactoryImpl
   - ssl.ServerSocketFactory.provider = com.ibm.jsse2.SSLServerSocketFactoryImpl
3. Aggiungere il provider IBMJCEFIPS, com.ibm.crypto.fips.provider.IBMJCEFIPS, all'elenco di provider prima del provider IBMJCE. Non eliminare il provider IBMJCE, poiché è obbligatorio per il supporto KeyStore.

   Nota: Solo il protocollo TLS è supportato quando IBMJSSE2 si trova in modalità FIPS.

Algoritmi supportati in modalità FIPS e non FIPS

I seguenti algoritmi sono supportati in FIPS:

- Diffie-Hellman
- RSA, DSA
- SHA-1, SHA-256, SHA-384, SHA-512.
- AES, DES, TDES (Triple DES)
- FIPS 186-2 – Algoritmo per la generazione di Pseudo Random Number
- Transport layer security: TLSv1
- Formato keystore: JKS, JCEKS
- Keyed message digest algorithm: hmac-sha1

I seguenti algoritmi sono supportati in WebSphere Partner Gateway:

- Crittografia asimmetrica: RSA, DSA
- Funzione hash: SHA-1, MD5, SHA256, SHA512, RIPEMD160
- Crittografia simmetrica: AES, DES, 3DES, RC2 (Tutto con modalità CBC)
- PRNG: IBMSecureRandom
- Algoritmo di firma: dsa-sha1, rsa-sha1
- Keyed message digest algorithm: hmac-sha1
- Transport layer security: SSLv3, TLSv1
- Formato keystore: PKCS#12
- Keyed message digest algorithm: hmac-sha1

I seguenti algoritmi non sono supportati in FIPS ma sono supportati in WebSphere Partner Gateway:

- Funzione hash: MD5, RIPEMD160
- Crittografia simmetrica: RC2, RC5
- PRNG: L'algoritmo PRNG predefinito potrebbe non essere approvato da FIPS.
- Provider IBMSecureRandom PRNG (tutti i casi di WebSphere Partner Gateway).
- Transport layer security: SSLv3
- Formato keystore: PKCS#12

Capitolo 14. Gestione di avvisi

Gli avvisi di WebSphere Partner Gateway vengono utilizzati per notificare il personale chiave delle oscillazioni insolite nel volume di trasmissioni ricevuto o quando si verificano errori di elaborazione del documento di business.

Un'opzione fornita nel modulo Visualizzatore, Visualizzatore eventi, consente di identificare e risolvere gli errori di elaborazione.

Panoramica di avvisi

Un avviso è costituito da un messaggio e-mail basato su testo, inviato ai contatti sottoscritti o ad un elenco di distribuzione del personale chiave. Gli avvisi si basano sulla ricorrenza di un evento del sistema (avviso in base all'evento) o al volume del flusso del documento previsto (avviso in base al volume).

- Utilizzare un **avviso in base al volume** per ricevere la notifica di un incremento o riduzione nel volume delle trasmissioni.

  Ad esempio, se l'utente è un partner esterno, è possibile creare un avviso basato sul volume che informa l'utente nel caso in cui non sono ricevute trasmissioni dal partner interno in qualsiasi giorno lavorativo (impostare il Volume su Volume zero, impostare la frequenza su Quotidiano e selezionare dal lunedì al venerdì nell'opzione Giorni della settimana). Questo avviso può evidenziare delle difficoltà della trasmissione di rete del partner interno.

  Se l'utente è un partner esterno, è anche possibile creare un avviso basato sul volume che avvisa l'utente nel caso in cui il numero di trasmissioni dal partner interno supera la quota normale. Ad esempio, se, di solito, si ricevono circa 1000 trasmissioni al giorno, è possibile impostare il Volume previsto su 1000 e la Deviazione di percentuale su 25%. L'avviso notifica quando vengono ricevute oltre le 1250 trasmissioni al giorno (notifica anche quando il volume delle trasmissioni è al di sotto di 750). Questo avviso può identificare un aumento della domanda da parte del partner interno che, nel tempo, potrebbe richiedere che l'utente proceda all'aggiunta di altri server all'ambiente. Per ulteriori informazioni sugli avvisi basati sul volume, consultare la sezione " Creazione di un avviso basato sul volume" a pagina 284.

  Nota:

  1. Gli avvisi basati sul volume monitorano il volume riguardo al tipo di documento scelto alla creazione dell'avviso. WebSphere Partner Gateway visualizza solo i documenti che contengono il tipo di documento scelto nell'avviso e crea gli avvisi solo quando tutti i criteri di avviso risultano soddisfatti.
  2. Il partner esterno può creare solo un avviso basato sul volume sul volume di documenti inviato al partner interno. Per configurare un avviso basato sul volume di documenti inviatogli dal partner interno, il partner esterno deve richiedere all'amministratore hub di configurare detto avviso per suo conto, specificando il partner esterno come proprietario dell'avviso. Un partner interno può inoltre creare avvisi basati sul volume da inviare a partner esterni.

- Utilizzare un **avviso in base all'evento** per ricevere la notifica quando si verificano errori durante l'elaborazione del documento. Ad esempio, è possibile creare un avviso che notifica se l'elaborazione dei documenti ha esito negativo a

causa di errori di convalida o poiché i documenti duplicati sono stati ricevuti. È anche possibile creare gli avvisi che consentono di rilevare quando un certificato sta per scadere.

I codici di evento predefiniti di WebSphere Partner Gateway saranno utilizzati per creare gli avvisi in base all'evento. Sono presenti cinque tipi di eventi: Debug, Informazioni, Avvertenza, Errore, Critico. All'interno di ciascun tipo di evento, esistono molti eventi. È possibile visualizzare e selezionare gli eventi predefiniti nella pagina Avviso: eventi. Ad esempio, 240601 Errore di riprova AS o 108001 Non un certificato. Per ulteriori informazioni sugli avvisi in base all'evento, consultare la sezione " Creazione di un avviso basato sugli eventi" a pagina 287.

Suggerimento:

- Utilizzare un avviso basato sul volume per ricevere la notifica se il volume di trasmissione del Partner interno o del partner esterno previsto va al di sotto del limiti operativi. Questo avviso può evidenziare le difficoltà di trasmissione della rete del partner esterno o del partner interno.
- Utilizzare un avviso in base all'evento per ricevere la notifica di errori nell'elaborazione del documento. Ad esempio, è possibile creare un avviso in base all'evento che notifica se l'elaborazione dei documenti ha avuto esito negativo a causa di errori di convalida.

Nota: per inviare gli avvisi, è necessario configurare un server e-mail per gli avvisi. Gli avvisi vengono configurati nella pagina Attributi del motore degli avvisi individuabile facendo clic su **Gestione sistema** > **Gestione DocMgr** > **Motore avvisi**. Per ulteriori informazioni sulla configurazione del server e-mail degli avvisi, consultare la sezione "Updating alert mail addresses" in *WebSphere Partner Gateway Partner Guide*.

Visualizzazione o modifica di contatti e dettagli dell'avviso

Informazioni su questa attività

Il partner interno può visualizzare tutti gli avvisi, a prescindere dal Proprietario avviso (il creatore dell'avviso).

1. Fare clic su **Amministrazione account** > **Avvisi**. Il sistema visualizza la pagina Ricerca avviso.
2. Selezionare i criteri di ricerca negli elenchi a discesa; immettere il Nome avviso. È anche possibile fare clic su **Cerca** senza selezionare i criteri di ricerca (il sistema visualizza tutti gli avvisi).
3. Fare clic su **Cerca**. Il sistema visualizza la pagina Risultati della ricerca degli avvisi.
4. Fare clic sull'icona Visualizza dettagli per visualizzare i dettagli di un avviso.
5. Fare clic sull'icona Modifica per modificare i dettagli di un avviso.
6. Modificare le informazioni come richiesto.
7. Fare clic sulla scheda the **Notifica**.
8. Selezionare un partner (solo partner interno o amministratore hub). Il partner interno può visualizzare tutti gli avvisi a prescindere dal Proprietario avviso.
9. Modificare i contatti per questo avviso, se desiderato.
10. Fare clic su **Salva**.

Ricerca avvisi

Informazioni su questa attività

1. Fare clic su **Amministrazione account** > **Avvisi**. Il sistema visualizza la pagina Ricerca avviso.
2. Selezionare i criteri di ricerca negli elenchi a discesa; immettere il Nome avviso. È anche possibile fare clic su **Cerca** senza selezionare i criteri di ricerca (il sistema visualizza tutti gli avvisi).

Tabella 31. Criteri di ricerca degli avvisi per i partner

Valore	Descrizione
Tipo di avviso	Volume, evento o tutti i tipi di avviso.
Nome avviso	Il nome dell'avviso.
Stato avviso	Gli avvisi che sono abilitati, disabilitati o tutti gli avvisi.
Contatti sottoscritti	I contatti assegnati dell'avviso. Le selezioni sono Ha sottoscrittori, Nessun sottoscrittore o Tutti.
Risultati per pagina	Controlla il modo in cui sono visualizzati i risultati di ricerca.

Tabella 32. Criteri di ricerca di avviso per il partner interno e l'amministratore hub

Valore	Descrizione
Proprietario avviso	Creatore dell'avviso.
Partner avviso	Il partner a cui si applica l'avviso.
Tipo di avviso	Volume, evento o tutti i tipi di avviso.
Nome avviso	Il nome dell'avviso.
Stato avviso	Gli avvisi che sono abilitati, disabilitati o tutti gli avvisi.
Contatti sottoscritti	I contatti assegnati dell'avviso. Le selezioni sono Ha sottoscrittori, Nessun sottoscrittore o Tutti.
Risultati per pagina	Controlla il modo in cui sono visualizzati i risultati di ricerca.

3. Fare clic su **Cerca**. Il sistema visualizza un elenco di avvisi che soddisfano i criteri di ricerca, se presenti.

Disabilitazione o abilitazione di un avviso

1. Fare clic su **Amministrazione account** > **Avvisi**. Il sistema visualizza la pagina Ricerca avviso.
2. Selezionare i criteri di ricerca negli elenchi a discesa; immettere il Nome avviso.
3. Fare clic su **Cerca**. Il sistema visualizza un elenco di avvisi che soddisfano i criteri di ricerca, se presenti.
4. Rilevare l'avviso e fare clic su **Disabilitato** o **Abilitato** in Stato. Solo l'amministratore hub e il proprietario avviso (creatore dell'avviso) sono autorizzati a modificare lo Stato avviso.

Eliminazione di un avviso

1. Fare clic su **Amministrazione account** > **Avvisi**. Il sistema visualizza la pagina Ricerca avviso.
2. Selezionare i criteri di ricerca negli elenchi a discesa; immettere il Nome avviso.
3. Fare clic su **Cerca**. Il sistema visualizza un elenco di avvisi che soddisfano i criteri di ricerca, se presenti.

4. Rilevare l'avviso e fare clic sull'icona Elimina per eliminare. Solo l'amministratore hub e il proprietario avviso (creatore dell'avviso) possono rimuovere un avviso.

Aggiunta di un nuovo contatto ad un avviso esistente

Informazioni su questa attività

1. Fare clic su **Amministrazione account** > **Avvisi**. Il sistema visualizza la pagina Ricerca avviso.
2. Inserire i criteri di ricerca nell'elenco a discesa; immettere il Nome avviso.
3. Fare clic su **Cerca**. Il sistema visualizza un elenco di avvisi che soddisfano i criteri di ricerca, se presenti.
4. Fare clic sull'icona Visualizza dettagli per visualizzare i dettagli di un avviso.
5. Fare clic sull'icona Modifica per modificare i dettagli di un avviso.
6. Fare clic sulla scheda the **Notifica**.
7. Selezionare un partner (solo partner interno e amministratore hub).
8. Se il contatto che si desidera aggiungere viene elencato nella casella di testo Contatti, selezionare il contatto e fare clic su **Sottoscrivi**. Andare al passo 13.

   Se il contatto che si desidera aggiungere non viene elencato nella casella di testo Contatti, fare clic su **Aggiungi nuovo inserimento nei contatti**. Il sistema visualizza la finestra a comparsa Crea nuovo contatto.

   L'opzione Aggiungi nuovo inserimento nei contatti viene presentata solo al Proprietario avviso per creare i contatti associati al Proprietario avviso. Questa funzione non consente al Proprietario avviso di aggiungere contatti per i Partner avviso.
9. Immettere il nome del contatto, l'indirizzo e-mail, i numeri di telefono e di fax.
10. Selezionare lo Stato avviso del contatto.
    - Selezionare **Abilitato** per iniziare ad inviare i messaggi e-mail a questo contatto quando il sistema genera questo avviso.
    - Selezionare **Disabilitato** se non si desidera inviare i messaggi e-mail a questo contatto quando il sistema genera questo avviso.
11. Selezionare la visibilità del contatto.
    - Selezionare **Locale** per rendere visibile il contatto solo alla propria organizzazione.
    - Selezionare **Globale** per rendere visibile il contatto all'amministratore hub e al partner interno. Queste parti possono sottoscrivere il contatto agli avvisi.
12. Per salvare il contatto, fare clic su **Salva**. Fare clic su **Salva e Sottoscrivi** per salvare il contatto e aggiungere il contatto all'elenco dei contatti per questo avviso.
13. Fare clic su **Salva**.

Creazione di un avviso basato sul volume

Informazioni su questa attività

1. Fare clic su **Amministrazione account** > **Avvisi**. Il sistema visualizza la pagina Ricerca avviso.
2. Fare clic su **Crea** nell'angolo in alto a destra della pagina. Il sistema visualizza la scheda Definizioni avvisi.

3. Selezionare **Avviso volume** per **Tipo di avviso** (si tratta dell'impostazione predefinita). Il sistema visualizza le caselle di testo appropriate per un avviso di volume.
4. Inserire un **Nome avviso** per l'avviso.
5. Selezionare un **Proprietario avviso** per l'avviso.
6. Selezionare un **Partner** con diritti a creare un avviso basato sul volume (solo partner interno e amministratore hub).
7. Selezionare **Package**, **Protocollo**, e **Tipo di documento** negli elenchi a discesa. Il Package, Protocollo ed il Tipo di documento selezionato devono corrispondere al Package, Protocollo e Tipo di documento del partner esterno di origine.
8. Selezionare una delle tre opzioni di volume (Previsto, Intervallo o Volume zero), quindi proseguire con il passo 9:
   - **Previsto** - Selezionare Previsto se si desidera creare un avviso quando il volume del tipo di documento viene deviato dalla quantità esatta. Utilizzare la seguente procedura per creare un avviso sul volume del tipo di documento previsto:
     a. Nella casella di testo Volume, inserire il numero dei tipi di documenti previsto da ricevere entro un determinato intervallo di tempo selezionato nella fase 9. Inserire solo un numero positivo; l'avviso non funziona se viene immesso un numero negativo.
     b. Nella casella di testo Deviazione di percentuale, immettere un numero che definisce il limite da cui il volume del tipo di documento può deviare prima di attivare l'avviso. Ad esempio:
        – Se Volume = 20 e Deviazione di percentuale = 10, un volume del flusso del documento inferiore a 18 o superiore a 22 attiva un avviso.
        – Se Volume = 20 e Deviazione di percentuale = 0, qualsiasi volume del flusso del documento diverso da 20 attiva un avviso.
   - **Intervallo**. Selezionare Intervallo per creare un avviso se il volume del flusso del documento non è compreso in un intervallo massimo o minimo. Per creare un avviso in base ad un intervallo di valori, utilizzare la seguente procedura:
     a. Nella casella di testo Min, immettere il numero minimo dei flussi di documenti previsto da ricevere entro un determinato intervallo di tempo scelto nella fase 9. Un avviso viene attivato solo se il volume del flusso del documento è al di sotto di questa quantità.
     b. Nella casella di testo Max, immettere il numero massimo dei flussi di documenti previsto da ricevere entro un determinato intervallo di tempo, selezionato nella fase 9.

        Nota: entrambe le caselle di testo Min e Max devono essere compilate durante la creazione di un avviso in base all'intervallo del volume.
   - **Volume zero**. Selezionare Volume zero per attivare un avviso se nessun flusso di documento si verifica entro un determinato intervallo di tempo, scelto nella fase 9.
9. Selezionare Quotidiano o Intervallo per l'intervallo di tempo (Frequenza) che il sistema utilizza per monitorare il volume del flusso del documento per la creazione degli avvisi.
   - **Quotidiano**. Selezionare Quotidiano per monitorare il volume del flusso del documento in uno o più giorni correnti della settimana o del mese. Ad esempio, selezionare Quotidiano se si monitora il volume del flusso del

documento solo in uno o più giorni specifici della settimana (ad esempio, Lunedì o Lunedì e Martedì) o mese (ad esempio, il primo ed il quindicesimo).

- **Intervallo**. Selezionare Intervallo per monitorare il volume del flusso del documento tra i due giorni della settimana o del mese. Ad esempio, selezionare Intervallo per monitorare il volume del flusso del documento in tutti i giorni compresi tra lunedì e venerdì o tutti i giorni compresi tra il quinto ed il ventesimo di ogni mese.

10. Selezionare il Tempo di avvio ed il Tempo di fine (giorno di 24 ore) in cui il sistema monitora il volume del flusso del documento per i giorni selezionati nella fase successiva. Quando la frequenza Intervallo è stata selezionata, il volume del flusso del documento viene monitorato dal Tempo di avvio del primo giorno dell'intervallo fino al Tempo di fine dell'ultimo giorno dell'intervallo.
11. Selezionare i giorni appropriati durante la settimana o il mese in cui si verifica il monitoraggio degli avvisi. Se è stato selezionato Quotidiano come frequenza, selezionare i giorni correnti della settimana o i giorni del mese per il monitoraggio degli avvisi. Se è stato selezionato Intervallo come frequenza, selezionare due giorni durante la settimana o due giorni durante il mese in cui si verifica il monitoraggio degli avvisi.
12. Selezionare lo **Stato avviso** di questo avviso come Abilitato o Disabilitato.
13. Fare clic su **Salva**.
14. Fare clic sulla scheda **Notifica**.
15. Fare clic sull'icona Modifica.
16. Selezionare un partner (solo partner interno e amministratore hub).
17. Se il contatto che si desidera aggiungere viene elencato nella casella di testo Contatti, selezionare il contatto e fare clic su **Sottoscrivi**. Andare al passo 22.

    Se il contatto che si desidera aggiungere non viene elencato nella casella di testo Contatti, fare clic su **Aggiungi nuovo inserimento nei contatti**. Il sistema visualizza la finestra a comparsa Crea nuovo contatto.

    L'opzione Aggiungi nuovo inserimento nei contatti viene presentata solo al Proprietario avviso per creare i contatti associati al Proprietario avviso. Questa funzione non consente al Proprietario avviso di aggiungere contatti per i Partner avviso.
18. Immettere il nome del contatto, l'indirizzo e-mail, i numeri di telefono e di fax.
19. Selezionare lo Stato avviso del contatto.
    - Selezionare **Abilitato** per iniziare ad inviare i messaggi e-mail a questo contatto quando il sistema genera questo avviso.
    - Selezionare **Disabilitato** se non si desidera inviare i messaggi e-mail a questo contatto quando il sistema genera questo avviso.
20. Selezionare la visibilità del contatto.
    - Selezionare **Locale** per rendere visibile il contatto solo alla propria organizzazione.
    - Selezionare **Globale** per rendere visibile il contatto all'amministratore hub e al partner interno. Queste parti possono sottoscrivere il contatto agli avvisi.
21. Fare clic su **Salva** per salvare il contatto; fare clic su **Salva & Sottoscrivi** per aggiungere il contatto all'elenco dei contatti per questo avviso.
22. Fare clic su **Salva**.

Nota: le modifiche apportate agli avvisi in base al volume, in seguito al periodo di monitoraggio originale, diventano effettive al successivo giorno del periodo di monitoraggio. Ad esempio, un avviso monitora dalle 1 alle 15:00 dal mercoledì al giovedì. Il mercoledì alle 16:00, l'avviso viene modificato per monitorare dalle 17:00 alle 19:00. L'avviso non esegue il monitoraggio due volte il mercoledì; la modifica diventa effettiva il giovedì.

Creazione di un avviso basato sugli eventi

Informazioni su questa attività

1. Fare clic su **Amministrazione account** > **Avvisi**. Il sistema visualizza la pagina Ricerca avviso.
2. Fare clic su **Crea** nell'angolo in alto a destra della pagina. Il sistema visualizza la scheda Definizioni avvisi.
3. Selezionare **Avviso eventi** per **Tipo di avviso**. Il sistema visualizza le caselle di testo appropriate per un avviso in base all'evento.
4. Inserire un **Nome avviso** per l'avviso.
5. Selezionare un **Proprietario avviso** per l'avviso.
6. Selezionare un **Partner** che attiverà l'avviso (questa opzione è disponibile solo per il partner interno e l'amministratore hub). Selezionare l'opzione Qualsiasi partner per associare l'avviso a tutti i partner del sistema. Quando viene effettuata una ricerca dell'avviso e viene selezionata l'opzione Qualsiasi partner come Partner avviso, il sistema visualizza tutti gli avvisi che non sono associati ad un determinato partner.
7. Selezionare il **Tipo evento**: Debug, Informazioni, Avvertenza, Errore, Critico o Tutti.
8. Selezionare il **Nome evento** che attiva l'avviso, ad esempio, BCG240601 Errore di riprova AS, o 108001 Non un certificato. Per creare un avviso che notifica quando un certificato sta per scadere, selezionare una delle seguenti opzioni:
   - BCG108005 Scadenza del certificato in 60 giorni
   - BCG108006 Scadenza del certificato in 30 giorni
   - BCG108007 Scadenza del certificato in 15 giorni
   - BCG108008 Scadenza del certificato in 7 giorni
   - BCG108009 Scadenza del certificato in 2 giorni

   Nota: per elencare un evento, è necessario che sia accettabile. Per rendere accettabile un evento, consultare la sezione "Specifica degli eventi notificabili" a pagina 293.
9. Selezionare lo stato di questo avviso: Abilitato o Disabilitato.
10. Fare clic su **Salva**.
11. Fare clic sulla scheda **Notifica**.
12. Selezionare la **Modalità di notifica**: notifica tutte le parti relative o Notifica solo i contatti sottoscritti. I contatti sottoscritti vengono notificati dalla modalità ***Notifica solo ai contatti sottoscritti***. Durante la creazione degli avvisi, se viene selezionata la modalità di notifica dell'avviso ***Notifica a tutte le parti relative***, la notifica viene inviata a tutte le parti correlate all'evento per il quale viene definito l'avviso. Le parti correlate all'evento sono i contatti combinati di Partecipante di origine, Partecipante di destinazione e Proprietario avviso.
13. Selezionare un **Partner** (solo partner interno e amministratore hub).

14. Dai contatti elencati nella casella di testo **Contatti**, selezionare il contatto che si desidera notificare e fare clic su **Sottoscrivi**.
15. Selezionare la Modalità di recapito:
    - **Invia avvisi immediatamente**. Quando si seleziona questa opzione, il sistema invia le notifiche di avviso al contatto quando si verifica l'avviso. Per gli avvisi critici, utilizzare questa opzione.
    - **Archivia avvisi per**. Quando si seleziona questa opzione, è possibile specificare quando si desidera il contatto per ricevere le notifiche di avviso. Per gli avvisi non critici, utilizzare questa opzione.

      Le due opzioni di questa sezione, Conteggio e Ora, non si escludono a vicenda.

      Se si seleziona l'opzione **Conteggio**, è necessario selezionare sempre l'opzione Ora.
      – Se il numero di avvisi (Conteggio) è stato raggiunto durante il limite di tempo selezionato (Ora), il sistema genera una notifica di avviso.
      – Se un avviso si verifica ma il numero di avvisi (Conteggio) non è raggiunto durante il limite di tempo selezionato (Ora), il sistema genera una notifica di avviso alla fine del limite di tempo.

      L'opzione **Ora** può essere utilizzata senza l'opzione Conteggio, ma l'opzione Conteggio deve essere sempre associata ad un limite di tempo (Ora).
      – **Conteggio**. Quando si seleziona questa opzione è necessario utilizzare anche l'opzione Ora. Immettere un numero (n). Si tratta del numero di avvisi che deve verificarsi durante il determinato intervallo di tempo (Ora) prima che il sistema invia una notifica di avviso al contatto dell'avviso.

        Di seguito viene riportato un esempio di come queste due opzioni funzionano insieme:

        Nell'esempio, l'opzione Archivia avvisi per è stata impostata su 10 per Conteggio (10 avvisi) e 2 per Ora (intervallo di tempo di 2 ore). Il sistema conserva tutte le notifiche per questo avviso fino a 10 che si verificano in un periodo di due ore o fino alla fine dell'intervallo di tempo raggiunto.

        Quando il conteggio dell'avviso raggiunge 10 in un periodo di 2 ore, il sistema invia tutte le notifiche di avviso per questo avviso al contatto.

        Se un avviso si verifica e 10 avvisi non si verificano durante il limite di tempo (due ore), il sistema invia una notifica di avviso al contatto dell'avviso alla fine del limite di tempo.
      – **Ora**. Selezionare il numero di ore (n). Il sistema conserva la notifica di avviso per n ore. Ogni n ore, il sistema invia tutte le notifiche di avviso conservate al contatto.

        Ad esempio, se si inserisce 2, il sistema conserva tutte le notifiche per questo avviso che si verificano ogni due ore. Quando l'intervallo di due ore scade, il sistema invia tutte le notifiche di avviso per questo avviso al contatto.
16. Fare clic su **Salva**.

Capitolo 15. Inizializzazione flusso di errori

In WebSphere Partner Gateway, come amministratore, è possibile controllare gli eventi con errore che si verificano durante l'elaborazione dei documenti. Un documento può generare un errore dal destinatario o il gestore documento. Per un documento con errori, l'errore corrispondente o l'evento critico viene registrato nel Motore eventi. Gli avvisi possono essere creati per inviare notifiche email ad uno o più sottoscrittori.

Inoltre, un amministratore può effettivamente inizializzare un flusso documento di errore per un partner interno, esterno o per entrambi. Questo documento di errore verrà inizializzato per un documento che ha generato errore in base all'errore stesso o all'evento critico. Questo flusso di documento di errore può essere in formato WebSphere partner Gateway o in formato servizio Web. È possibile configurare il formato nella configurazione Flusso di errori per un evento.

Configurazione documento flusso di errori

Informazioni su questa attività

La scheda Flusso di errori nella console consente all'operatore di impostare il richiamo del Flusso errori o del servizio Web per determinati eventi di errore:

1. Passare alla scheda **Amministrazione account** > **Flusso di errore**. L'elenco flusso di errore dispone di icone di visualizzazione ed eliminazione per ogni flusso di errore.
2. Fare clic sull'icona **Visualizza** per avviare lo schermo di configurazione del flusso di errori in modalità di sola lettura.
3. Nella configurazione vista, fare clic sull'icona **Modifica** per modificare la configurazione del flusso di errori. Nella configurazione vista, fare clic su **Crea** per visualizzare o modificare la configurazione del flusso di errori nella modalità di creazione.
4. Nella modalità di modifica, sono disponibili i seguenti valori di configurazione:
   - **Nome** - nome configurazione documento flusso di errori.
   - **Partner** - dall'elenco a discesa selezionare il tipo di partner e fare clic su Cerca per trovare il proprio partner. Il partner può essere interno o esterno.
   - **Nome evento** - questo elenco a discesa elenca solo gli eventi di tipo ″Errore″ o ″Critico″.
   - **Tipo flusso errore** - questo può essere Documento di flusso errore o Richiama un servizio Web.
   - **Servizio Web da richiamare** - questo elenco a discesa elenca tutte le operazioni dei servizi Web caricati configurati nella Definizione del flusso documenti.
   - **Invia a** - Seleziona i destinatari del documento con errori. Questo può essere ″Mittente″ o ″Destinatario″ o ″Entrambi″.
5. Fare clic su **Salva**.
6. Abilitare le capacità B2B del flusso di errori configurato.
7. Se viene richiamato il servizio Web, creare l'interazione e attivare la Connessione partecipante.

Le definizioni documento flusso di errore per XML ed i servizi Web sono caricate in WebSphere Partner Gateway per impostazione predefinita. È possibile abilitarle per i partner interni o esterni e creare le seguenti connessioni:

- Connessione XML Documento flusso di errore.
- Documento flusso di errore sui servizi Web per lo stile documento.
- Documento flusso di errore sui servizi Web per lo stile RPC.

Limitazioni

1. Il documento del flusso di errori sui servizi Web ha le seguenti limitazioni:
   - La richiesta di servizi Web deve essere una richiesta unidirezionale.
   - Se lo stile di bind è **documento**, il tipo di parametro di immissione è l'elemento **ErrorFlowDocument**, definito in BCGErrorFlowSchema.xsd.
   - Se lo stile di bind è **rpc**, il tipo parametro di immissione sarà **Stringa** e il numero di parametri di input è uno.
2. L'instradamento del flusso di errori non funzionerà nel caso di ID di business errati. Se viene richiesto il documento del flusso di errori per un evento particolare e anche se l'elaborazione del documento di business che ha degli ID non corretti non riesce con lo stesso evento configurato, l'instradamento del flusso di errori non funzionerà dato che gli ID di business specificati non sono validi.

Capitolo 16. Completamento della configurazione

Questo capitolo descrive le attività aggiuntive che è possibile effettuare per configurare l'hub. Sono incluse le seguenti sezioni:

Nota: è necessario utilizzare sempre la stessa istanza del browser con cui si accede alla Console comunità per apportare modifiche alla configurazione di WebSphere Partner Gateway. L'utilizzo simultaneo di più istanze del browser può causare l'eliminazione delle modifiche di configurazione.

Supporto file di grandi dimensioni per i documenti AS

Il supporto file di grandi dimensioni con un ordine di dimensione in GB è stato esteso per AS2 e AS3. A partire dalla versione 6.1.1, la dimensione massima del file elaborata utilizzando matrici di byte è configurabile. Quando la quantità di memoria assegnata è maggiore della dimensione heap disponibile, si verifica un errore OutOfMemoryError. Se la dimensione di dati è inferiore alla memoria disponibile, potrebbe verificarsi OutOfMemoryError se la memoria assegnata aumenta la memoria disponibile. Al runtime viene determinato se la dimensione del file configurato può essere supportata in base alla memoria heap disponibile. È possibile specificare la dimensione file massima che è possibile utilizzare con le matrici byte utilizzando la proprietà **bcg.maximumFileSizeForByteArrays**. Il valore della proprietà bcg.maximumFileSizeForByteArrays è in MB. Se la dimensione file è superiore al valore di questa proprietà, questa viene elaborata utilizzando gli stream. Se la dimensione file è inferiore al valore di questa proprietà e se non è disponibile memoria sufficiente, viene generato un evento di errore BCG210050.

Quando si accede come operatore hub, passare alle schede **Gestione sistema** > **Attributi comuni**. Sovrascrivere il valore predefinito della proprietà **bcg.maximumFileSizeForByteArrays** per specificare la dimensione file massima da utilizzare con le matrici di byte. Aumentare il valore di questa proprietà per una migliore prestazione.

Abilitazione all'utilizzo delle API

Informazioni su questa attività

WebSphere Partner Gateway fornisce una serie di API che possono essere utilizzate per accedere a determinate funzioni generalmente effettuate sulla Console comunità. Queste API sono descritte nel manuale *WebSphere Partner Gateway Programmer Guide*.

Attenersi a questa procedura per abilitare l'utilizzo di API basate su XML in modo che i partner possano effettuare chiamate API al server WebSphere Partner Gateway.

1. Dal menu principale, fare clic su **Gestione sistema > Gestione funzione > API di gestione**.
2. Fare clic sull'icona **Modifica** accanto a **Abilita API basate su XML**.
3. Selezionare la casella di spunta per abilitare l'utilizzo dell'API basato su XML.
4. Fare clic su **Salva**.

Risultati

Nota: L'API di gestione basata su XML è considerata obsoleta nella versione 6.1.

Per eseguire le attività di creazione e aggiornamento, è possibile utilizzare il nuovo programma di utilità di migrazione introdotto da WebSphere Partner Gateway versione 6.1 invece dell'API di gestione. Le attività di creazione e aggiornamento precedentemente eseguite solo utilizzando l'API di gestione, ora possono essere eseguite utilizzando un file di importazione della migrazione che contiene le informazioni nuove o aggiornate.

Il file di importazione è descritto dallo schema XML fornito con il programma di utilità di migrazione. È possibile utilizzare uno strumento di sviluppo come Rational Application Developer per produrre un file XML di importazione conforme allo schema. Importando questo file con il programma di utilità di migrazione, è possibile caricare delle nuove definizioni di partner, compresi i contatti e gli ID di business per i partner. È anche possibile aggiornare le definizioni di partner esistenti importandole con il programma di utilità di migrazione. L'API di gestione consente anche di elencare alcune delle risorse di configurazione in un sistema. Una esportazione completa del sistema utilizzando il programma di utilità di migrazione fornisce degli elenchi di capacità partner, connessioni partner e ricevitori (destinatari) nel file xml esportato.

Il file batch **bcgmigrate.bat/bcgmigrate.sh** viene utilizzato per iniziare il processo di migrazione. Durante l'esecuzione del comando bcgmigrate, assicurarsi di disporre dell'autorizzazione all'**esecuzione** del file per (bcgmigrate.bat/ bcgmigrate.sh). Ciò vale soprattutto per la piattaforma UNIX.

Specifica delle code utilizzate per gli eventi

Informazioni su questa attività

È possibile configurare l'hub per recapitare gli eventi ad una coda esterna che viene configurata mediante la configurazione JMS.

La configurazione JMS predefinita viene stabilita quando si installa l'hub. È possibile vedere alcuni di questi valori nella pagina Proprietà di pubblicazione evento.

Per puntare ad una configurazione JMS differente, fornire i valori di configurazione appropriati per la pubblicazione di eventi alle code di messaggistica interne o ad altri server di messaggistica WebSphere Partner Gateway / WAS. Inoltre, modificare il nome della coda per fare in modo che corrisponda a quello in cui gli eventi vengono pubblicati.

Per indicare dove è necessario recapitare gli eventi:

1. Dal menu principale, fare clic su **Gestione sistema> Gestione DocMgr > Motore eventi > Eventi esterni**.
2. Fare clic sull'icona **Modifica** accanto a **Abilita consegna evento**.

3. Selezionare la casella di spunta **Abilita recapito evento** per attivare la pubblicazione dell'evento.
4. Se i valori predefiniti sono corretti per l'installazione, non modificarli. I valori predefiniti supportano il recapito degli eventi nella coda denominata DeliveryQ fornita dal server JMS configurato al momento dell'installazione.

   Se si desidera modificare dove recapitare gli eventi, aggiornare i campi, utilizzando le seguenti informazioni come riferimento:

   - Inserire i valori per **ID utente** e **Password**, se richiesti per accedere alla coda
   - Per **Nome factory coda JMS**, inserire il nome della Factory di connessione coda JMS dal file JMS .bindings che si sta utilizzando.

     Nota: in alcune versioni di Windows (precedenti a XP), potrebbe essere necessario modificare il valore predefinito il campo **Nome factory coda JMS**, se si desidera utilizzare la funzione Recapito eventi predefinita. Potrebbe essere necessario modificare il valore di **Nome factory coda JMS** da: `WBIC/QCF` a `WBIC\\QCF`.
   - Per **Tipo di messaggio JMS**, inserire il tipo di messaggio che viene recapitato. Le scelte sono byte o testo.
   - Per **Nome coda JMS**, inserire il nome della coda JMS nella quale gli eventi vengono pubblicati. Questa coda deve essere già definita nel file JMS .bindings che si utilizza in WebSphere MQ.

     Nota: in alcune versioni di Windows (precedenti a XP), potrebbe essere necessario modificare il valore predefinito del campo **Nome coda JMS**, se si desidera utilizzare la funzione Recapito eventi. Potrebbe essere necessario modificare il valore per **Nome coda JMS** da `WBIC/DeliveryQ` a `WBIC\\DeliveryQ. WBIC/QCF`.
   - Per **Nome factory JNDI**, inserire il nome utilizzato per accedere al file .bindings. Il valore predefinito fornisce l'accesso al collegamento predefinito nel file system.
   - Per **Package URL del provider**, inserire un URL che fornisce l'accesso al file di collegamento JMS. Questo URL deve essere conforme al nome factory JNDI. Questo campo è facoltativo e, quando non viene riempito, utilizza il percorso predefinito del file system per i collegamenti JMS.
   - Per **Gruppo caratteri messaggio**, inserire il gruppo di caratteri da utilizzare quando si crea il messaggio byte sulla coda JMS. Il valore predefinito è UTF-8. Questo campo è rilevante solo per i messaggi byte.
   - Per **URL provider JMS**, inserire l'URL del provider JMS. Questo campo è facoltativo e quando non viene riempito, utilizza il provider JMS predefinito identificato al momento dell'installazione.
5. Fare clic su **Salva**.

Specifica degli eventi notificabili

Informazioni su questa attività

Quando si verificano eventi in WebSphere Partner Gateway, viene generato un codice di evento. Grazie alla pagina Codici evento, è possibile impostare lo stato notificabile del codice di evento. Quando un evento viene impostato come notificabile, viene visualizzato nell'elenco Nome evento della pagina Avviso. È quindi possibile impostare un avviso per l'evento.

Per indicare quali eventi devono essere notificabili:

1. Fare clic su **Ammin hub > Configurazione hub > Codici evento**. Viene visualizzata la pagina Codici evento.
2. Per ogni evento da rendere notificabile:
   a. Fare clic sull'icona **Visualizza i dettagli** accanto al codice evento. Viene visualizzata la pagina Dettagli codici eventi.
   b. Selezionare **Notificabile**.
   c. Fare clic su **Salva**.

Aggiornamento di un trasporto definito dall'utente

Come descritto negli argomenti Capitolo 7, "Definizione dei destinatari", a pagina 55 e Capitolo 11, "Creazione delle destinazioni", a pagina 213, è possibile caricare un file XML che descrive un trasporto definito dall'utente. Per caricare il file, utilizzare **Gestisci tipi di trasporti**. Una volta caricato un file XML, il trasporto diventa disponibile per l'uso quando si definisce una destinazione o un destinatario.

Il file XML che descrive il trasporto definito dall'utente include gli attributi per il trasporto. Questi attributi vengono visualizzati (nella sezione **Attributi usuali di trasporto**) nella pagina di destinazione o del destinatario, quando si specifica un trasporto definito dall'utente. Ad esempio, un trasporto definito dall'utente per una destinazione potrebbe includere l'attributo DestinationRetryCount.

L'utente che ha scritto il file XML che descrive il trasporto può aggiornare gli attributi (aggiungendo, eliminando o modificando gli attributi). Se il file XML è stato modificato, utilizzare di nuovo **Gestisci tipi di trasporto** per caricare il file. Eventuali modifiche apportate agli attributi sono visualizzate nella pagina di destinazione o del destinatario.

Esempi

WebSphere Partner Gateway viene fornito con alcuni esempi, che a loro volta forniscono una funzionalità personalizzata e delle illustrazioni. Tali package vengono trovati nella directory in cui viene estratta l'installazione di WebSphere Partner Gateway, nelle cartelle **DevelopmentKits** e **Integration**.

La cartella DevelopmentKits contiene i seguenti esempi:

- API di gestione: le API di gestione sono state eliminate dalla versione 6.1, viene utilizzato il programma di utilità per la migrazione del partner per le attività di creazione e aggiornamento.
- Migrazione: contiene degli esempi per la configurazione dell'esportazione e dell'importazione.
  - Configurazione dell'esportazione: illustra la procedura per esportare le configurazioni di WebSphere Partner Gateway utilizzando un componente java dal file script della riga comandi.
  - Configurazione dell'importazione: illustra la procedura per importare le configurazioni di WebSphere Partner Gateway utilizzando un componente java dal file script della riga comandi.
- Uscite utente: è composto da esempi per la scrittura di codice uscita utente personalizzato, per la traduzione e la convalida.
  - L'esempio *EDITransTypeBusinessProcess* fornisce la funzionalità personalizzata per i documenti EDI che passano attraverso il sistema. Questa uscita utente di

esempio è progettata per analizzare il tipo di transazione EDI da un documento EDI X12. Modificando i criteri di analisi, è possibile estrarre altri valori.

  - L'esempio *custom translation user exit* fornisce la funzionalità di traduzione per un documento XML in entrata.
  - L'esempio *custom validation user exit* fornisce la funzionalità di convalida per un documento XML in entrata.
- Scenari di esempio: è composto da esempi che forniscono le linee guida per la configurazione di un sistema WebSphere Partner Gateway per i protocolli menzionati di seguito, con No packaging oltre a AS packaging. Per ciascun protocollo, viene fornito anche il file di importazione della configurazione.
  - XML personalizzato
  - EDI-X12
  - Documenti binari

La cartella Integration contiene i seguenti esempi di integrazione:

- Integrazione di WebSphere Transformation Extender: un esempio che mostra l'integrazione con WebSphere Transformation Extender, per convertire un documento XML in un file non codificato.
- Esempio di WebSphere Business Integration Message Broker : un esempio che mostra come WebSphere Partner Gateway comunica con WebSphere Business Integration Message Broker.
- Integrazione di WebSphere Process Server: un esempio che mostra come WebSphere Partner Gateway si integra con WebSphere Process Server su JMS.
- Integrazione di WebSphere Interchange Server: un esempio che mostra come WebSphere Partner Gateway si integra con Interchange Server utilizzando HTTP e JMS.

Capitolo 17. Editor CPP/CPA

L'editor CPP/CPA è un plugin eclipse che supporta la creazione del documento CPP/CPA dal modello e consente all'utente di eseguire modifiche utilizzando il formato della tabella. Inoltre, gestisce la convalida dei dati e dello schema.

Prerequisiti:

- E' richiesto WID/RAD versioni 6.1 e successive
- Posizionare il plug-in dell'editor CPP/A scaricato nella cartella del plug-in di IDE

E' possibile creare anche un documento CPA (Collaboration-Protocol Agreement) da due documenti CPP (Collaboration-Protocol Profile). CPP definisce le capacità di una parte utilizzata in un Electronic Business con altre parti. CPA descrive l'accordo di scambio dei massaggi tra le due parti. Per creare un CPP, immettere i valori per i singoli elementi XML (i singoli elementi XML sono composti da diversi attributi) tramite l'interfaccia utente dell'editor. Dopo aver creato il documento CPA utilizzando l'editor e il relativo stato è "CONCORDATO", è possibile importarlo in WebSphere Partner Gateway. I file importati creano automaticamente:

- I partner
- I gateway B2B
- Le interazioni e le connessioni

Inoltre, definisce automaticamente le definizioni del documento e abilita le capacità B2B richieste.

E' possibile effettuare le seguenti operazioni utilizzando l'interfaccia utente dell'editor CPP/CPA:

- "Creazione di un documento CPP"
- "Creazione del documento CPA" a pagina 298
- "Modifica di valori nell'editor" a pagina 298

Per fare in modo che l'editor CPP/CPA sia l'editor predefinito, effettuare le seguenti operazioni:

1. Nell'ambiente del plugin eclipse, fare clic sul menu **Finestra** e selezionare **Preferenze**
2. Nella finestra preferenze, fare clic su **Generale > Editor > Associazione file**.
3. Selezionare "*.xml" nell'elenco **Tipi di file** e "Editor multi-pagina CPPEditor" nell'elenco **Editor associati**.
4. Fare clic su **Predefinito**.

Creazione di un documento CPP

Per creare un documento CPP, procedere nel modo seguente:

1. In IDE, selezionare **File** >**Nuovo**.
2. Nella finestra **Nuovo**, selezionare **CPAEditor**> **File CPP**
3. Fare clic su **Avanti** e immettere i valori del contenitore CPP/CPA.
4. Fare clic su **Fine**. Il nuovo file viene creato nel contenitore specificato.

5. Se CPAEditor è stato configurato come predefinito, modificare i valori nel modello. In caso contrario, il file verrà aperto nell'editor XML. Per aprire il file in CPAEditor, fare clic con il tasto destro del mouse e selezionare **Apri con** > **Editor multi-pagina CPAEditor**.
6. Immettere i valori per gli attributi di tutti gli elementi. Per alcuni attributi, è possibile selezionare il valore appropriato dalle opzioni differenti.
7. Fare clic su **Salva**. Viene visualizzato un messaggio indicante la conferma della creazione di un documento CPP.

Creazione del documento CPA

E' necessario selezionare una delle seguenti opzioni:

- Caso 1: Creazione di un CPA utilizzando un modello, consente di immettere i valori per i singoli elementi XML (i singoli elementi XML sono formati da diversi attributi) tramite l'interfaccia utente dell'editor.
- Caso 2: Creazione di un CPA da due CPP

Per creare un CPA utilizzando un modello, procedere nel seguente modo:

1. In IDE, selezionare **File** >**Nuovo**.
2. Nella finestra **Nuovo**, selezionare **CPAEditor**> **File CPA**
3. Fare clic su **Avanti** e immettere i valori del contenitore CPP/CPA.
4. Fare clic su **Fine**. Il nuovo file viene creato nel contenitore specificato.
5. Se CPAEditor è stato configurato come predefinito, modificare i valori nel modello. In caso contrario, il file verrà aperto nell'editor XML. Per aprire il file in CPAEditor, fare clic con il tasto destro del mouse e selezionare **Apri con** > **Editor multi-pagina CPPEditor**.
6. Immettere i valori per gli attributi di tutti gli elementi. Per alcuni attributi, è possibile selezionare il valore appropriato dalle opzioni differenti.
7. Fare clic su **Salva**. Viene visualizzato un messaggio indicante la conferma della creazione di un documento CPA.

Per creare un CPA da due CPP, procedere nel seguente modo:

1. In IDE, fare clic su **File** > **Nuovo** > **Altro**.
2. Nella finestra **Nuovo**, selezionare **CPAEditor** > **Unisci i CPP**.
3. Fare clic su **Avanti**
4. Immettere i valori del contenitore CPP/CPA e il percorso e i nomi dei file CPP che si desidera unire.
5. Fare clic su **Fine**. I file uniti vengono creati nel contenitore specificato.
6. Se CPAEditor è stato configurato come predefinito, modificare i valori nel modello. In caso contrario, il file verrà aperto nell'editor XML. Per aprire il file in CPAEditor, fare clic con il tasto destro del mouse e selezionare **Apri con** > **Editor multi-pagina CPPEditor**.

Modifica di valori nell'editor

Per modificare i valori nella tabella dell'editor, posizionare il cursore sulla cella e modificare i valori. Ogni elemento PartyInfo ha un partyName univoco associato ad esso. I vari elementi secondari che vengono generati in PartyInfo sono PartyId, PartyRef, Collaboration Role, Certificate, SecurityDetails, DeliveryChannel, Transport, DocExchange e OverrideMshActionBinding. Questi valori sono

disponibili in tabelle differenti nell'editor CPP/CPA. PartyName viene utilizzato come identificativo univoco per associare gli elementi secondari di PartyInfo con l'elemento PartyInfo corrispondente.

Ad esempio, l'elemento Certificate che è un elemento secondario dell'elemento PartyInfo può essere generato una o più volte. L'elemento PartyInfo può generarsi più volte in un CPP.

Capitolo 18. Esempi di base

In questa appendice vengono forniti esempi di configurazione dell'hub. Sono incluse le seguenti sezioni:

- " Configurazione di base – Scambio di documenti EDI pass through"
- " Configurazione di base - Impostazione della protezione per documenti in entrata e in uscita" a pagina 307
- "Estensione della configurazione di base" a pagina 312

Per gli esempi di scambio EDI che includono l'operazione di deenveloping, la conversione, l'operazione di enveloping e la trasmissione del riconoscimento funzionale, viene fornita un'appendice separata. Fare riferimento a Capitolo 19, "Esempi EDI", a pagina 319.

Lo scopo di questi esempi è di fornire una rapida panoramica dei passi richiesti per configurare un sistema. Se si utilizzano tali esempi per configurare il sistema di cui si dispone, modificare le informazioni specifiche (ad esempio, i nomi e gli ID di business) in base alle esigenze dell'azienda.

Configurazione di base – Scambio di documenti EDI pass through

In questo esempio, la configurazione dell'hub è abbastanza semplice—due destinatari sono stati definiti (uno per i documenti che arrivano nell'hub da un partner e uno per i documenti che arrivano nell'hub dal sistema di back-end del partner interno). Gli scambi impostati in questo esempio utilizzano le definizioni del documento fornite da WebSphere Partner Gateway; quindi, è necessario solo creare le interazioni in base a questi flussi. Nessun XML personalizzato viene utilizzato in questo esempio.

Questo esempio mostra uno scambio tra un'applicazione di back-end del partner interno ed un partner esterno (Partner due).

Configurazione dell'hub

Durante l'impostazione dell'hub, la prima fase è creare due destinatari.

- Un destinatario HTTP (definito "HttpReceiver") per ricevere i documenti su HTTP (dal Partner due) che devono essere inviati al sistema di back-end del partner interno
- Un destinatario Directory file (definito "FileSystemReceiver") per richiamare i documenti dal file system (dal sistema di back-end del partner interno) che devono essere inviati al Partner due)

Definizione dei destinatari

Informazioni su questa attività

Per creare un destinatario al fine di ricevere i documenti su HTTP, procedere nel modo seguente:

1. Fare clic su **Amministrazione hub > Configurazione hub > Destinatari**.
2. Fare clic su **Crea destinatario**.
3. Per Nome destinatari, inserire: **HttpReceiver**.

4. Dall'Elenco dei trasporti, selezionare **HTTP/S**.
5. Per la Modalità operativa, utilizzare il valore predefinito **Produzione**.
6. Per l'URI, digitare: **/bcgreceiver/submit**
7. Fare clic su **Salva**.

Quindi, creare un destinatario per eseguire il polling di una directory sul file system. La creazione del destinatario crea automaticamente una nuova directory sul file system.

Per creare il destinatario file-system:

1. Fare clic su **Amministrazione hub > Configurazione hub > Destinatari**.
2. Fare clic su **Crea destinatario**.
3. Per Nome destinatari, inserire: **FileSystemReceiver**.
4. Dall'Elenco dei trasporti, selezionare **Directory file**.
5. Per la Modalità operativa predefinita, utilizzare il valore predefinito **Produzione**.
6. Per il percorso root del documento, digitare: **\temp\FileSystemReceiver**

   Nota: all'interno della directory temp sarà creata la directory FileSystemReceiver. Verificare che la directory temp esista nel file system.
7. Fare clic su **Salva**.

Definizione delle interazioni e dei tipi di documenti

Informazioni su questa attività

In questo esempio, viene configurato lo scambio di documenti conformi allo standard EDI-X12. In questo esempio, i documenti vengono trasmessi semplicemente tramite l'hub. Non viene eseguito l'deenveloping dello scambio EDI e non si verifica alcuna conversione. Per un esempio di apertura di uno scambio, di conversione delle transazioni e di invio di notifiche, consultare la sezione Capitolo 22, "Attributi", a pagina 413.

In questa sezione, vengono descritti i seguenti scambi:

- Invio di un documento EDI-X12, senza impacchettamento, dal partner interno al Partner due
- Invio di un documento EDI-X12, impacchettato in AS2, dal Partner due al partner interno

A causa dell'impacchettamento e dei protocolli interessati, non è necessario creare una nuova definizione del documento. I package, i protocolli ed i tipi di documenti sono quelli predefiniti nel sistema.

Tuttavia, è necessario definire le interazioni in base a questi tipi di documenti predefiniti.

Creare la prima interazione, in cui il formato di origine è un documento formattato ISA conforme allo standard EDI-X12 e senza impacchettamento, mentre la destinazione è un documento formattato ISA conforme allo standard EDI-X12 con impacchettamento AS.

1. Fare clic su **Amministrazione hub > Configurazione hub> Definizione documento**.
2. Fare clic su **Crea interazione**.

3. Dalla colonna **Origine**, espandere:
   a. **Package: Nessuno**
   b. **Protocollo: EDI-X12**
4. Fare clic su **Tipo documento: ISA**
5. Dalla colonna **Destinazione**, espandere:
   a. **Package: AS**
   b. **Protocollo: EDI-X12**
6. Fare clic su **Tipo documento: ISA**
7. Nell'elenco **Azione**, selezionare **Pass Through**.
8. Fare clic su **Salva**.

Creare la seconda interazione, in cui il formato di origine è un documento formattato ISA conforme allo standard EDI-X12 con impacchettamento AS e il formato di destinazione è un documento formattato ISA conforme allo standard EDI-X12 senza impacchettamento:

1. Fare clic su **Crea interazione**.
2. Dalla colonna **Origine**, espandere:
   a. **Package:AS**
   b. **Protocollo: EDI-X12**
3. Fare clic su **Tipo documento: ISA**
4. Dalla colonna **Destinazione**, espandere:
   a. **Package: Nessuno**
   b. **Protocollo: EDI-X12**
5. Fare clic su **Tipo documento:ISA**
6. Nell'elenco **Azione**, selezionare **Pass Through**.
7. Fare clic su **Salva**.

Creazione dei partner e delle connessioni del partner

In questo esempio, un partner esterno è stato creato, oltre al partner interno. Le destinazioni per i partner includono i trasporti standard, e nessun punto di configurazione è stato definito per le destinazioni.

Creazione di partner

Creare due nuovi partner. Per definire il partner interno:

1. Fare clic su **Amministrazione account** nel menu principale. La pagina Ricerca del partner è la vista predefinita.
2. Fare clic su **Crea**.
3. Per **Nome accesso azienda**, digitare: **Gestcom**.
4. Per **Nome visualizzato partner**, immettere: **Comm Man**.
5. Per **Tipo di partner**, selezionare **Partner interno**.
6. Fare clic su **Nuovo** in **ID di business**.
7. Lasciare **Tipo** come **DUNS** e inserire un valore identificativo di **123456789**.

   Nota: in tutto il manuale, i numeri DUNS sono solo esempi.
8. Fare clic su **Nuovo** in **ID di business**.
9. Selezionare **Forma libera** e inserire un valore Identificativo di **12-3456789**
10. Fare clic su **Salva**.

Per definire il Partner due:

1. Fare clic su **Amministrazione account > Profili > Partner**.
2. Fare clic su **Crea**.
3. Per **Nome accesso azienda**, digitare: **partnerTwo**
4. Per **Nome visualizzato partner**, immettere: **Partner due**
5. Per **Tipo di partner**, selezionare il **Partner esterno.**
6. Fare clic su **Nuovo** in **ID di business**.
7. Lasciare **Tipo** come **DUNS** e inserire **987654321** come Identificativo.
8. Fare clic su **Nuovo** in **ID di business**.
9. Selezionare **Forma libera** e inserire un valore Identificativo di **98-7654321**
10. Fare clic su **Salva**.

Adesso sono stati definiti sia il partner interno che il Partner due sull'hub.

I passi successivi sono la configurazione delle destinazioni sia per il partner interno che per il Partner due.

Creazione delle destinazioni

Informazioni su questa attività

Prima di creare una destinazione directory file per il partner interno, è necessario creare la struttura di directory utilizzata da questa destinazione. Creare una nuova directory FileSystemDestination sull'unità root. Questa directory sarà utilizzata dal partner interno per memorizzare i file ricevuti dai partner esterni.

Nel caso del partner interno, la destinazione rappresenta il punto di entrata nel sistema di back-end.

Per creare una destinazione per il partner interno:

1. Fare clic su **Amministrazione account > Profili > Partner**.
2. Fare clic su **Cerca**.
3. Selezionare **Partner interno** facendo clic sull'icona **Visualizza dettagli**.
4. Nella barra di navigazione orizzontale fare clic su **Destinazioni**.
5. Fare clic su **Crea**.
6. Per **Nome destinazione**, immettere: **FileSystemDestination**
7. Per **Trasporto**, selezionare **Directory file**.
8. Per **Indirizzo**, immettere: **file://C:\FileSystemDestination**
9. Fare clic su **Salva**.

Quindi, impostare questa destinazione creata di recente come destinazione predefinita per il partner interno.

1. Per visualizzare tutte le destinazioni configurate per il partner interno, fare clic su **Elenco**.
2. Fare clic su **Visualizza destinazioni predefinite**.
3. Nell'elenco **Produzione**, selezionare **FileSystemDestination**.
4. Fare clic su **Salva**.

Creare una destinazione per il Partner due

1. Fare clic su **Amministrazione account > Profili > Partner**.

2. Fare clic su **Cerca** e quindi selezionare **Partner due** facendo clic sull'icona **Visualizza dettagli**.
3. Nella barra di navigazione orizzontale fare clic su **Destinazioni**.
4. Fare clic su **Crea**.
5. Per **Nome destinazione**, immettere: **HttpDestination**
6. Per **Trasporto**, selezionare **HTTP/1.1**.
7. Per **Indirizzo**, immettere: **http://<***IP_address***>:80/input/AS2**, dove <*IP_address*> rappresenta il computer del Partner due.
8. Per **Nome utente**, digitare: **Gest com**
9. Per **Password**, digitare: **commMan**
10. Fare clic su **Salva**.

Questo esempio presume che il Partner due richieda un nome utente ed una password per qualsiasi partner che accede al sistema.

Per questo partner è necessario definire nuovamente una destinazione predefinita.

1. Fare clic su **Elenco** seguito da **Visualizza destinazioni predefinite**.
2. Nell'elenco **Produzione**, selezionare **HttpDestination**.
3. Fare clic su **Salva**.

Impostazione delle capacità B2B

Informazioni su questa attività

Definire quindi le capacità B2B per il partner interno.

1. Nel menu principale, fare clic su **Amministrazione account > Profili > Partner**.
2. Fare clic su **Cerca**.
3. Selezionare **Partner interno** facendo clic sull'icona **Visualizza dettagli**.
4. Fare clic su **Capacità B2B** dalla barra di navigazione orizzontale.
5. Impostare l'Origine e la Destinazione per Package: Nessuno, Protocollo: EDI-X12 e Tipo documento: ISA effettuando la seguente procedura:
   a. Fare clic sull'icona **Il ruolo non è attivo** sotto **Imposta origine** per **Package: Nessuno**
   b. Fare clic sull'icona **Il ruolo non è attivo** sotto **Imposta destinazione** per **Package: Nessuno**
   c. Fare clic sull'icona **Espandi** accanto a **Package: Nessuno**.
   d. Fare clic sull'icona **Il ruolo non è attivo** per **Protocollo: EDI-X12 (ALL)** sia per l'origine che per la destinazione.
   e. Fare clic sull'icona **Espandi** accanto a **Protocollo: EDI-X12 (ALL)**.
   f. Fare clic sull'icona **Il ruolo non è attivo** per **Tipo documento: ISA** per l'origine e la destinazione.

Quindi, impostare le capacità B2B per il Partner due.

1. Nel menu principale, fare clic su **Amministrazione account > Profili > Partner**.
2. Fare clic su **Cerca**.
3. Selezionare Partner due facendo clic sull'icona **Visualizza dettagli**.
4. Fare clic su **Capacità B2B** dalla barra di navigazione orizzontale.
5. Selezionare Imposta origine e Imposta destinazione per Package: AS, Protocollo: EDI-X12 e Tipo documento: ISA effettuando la seguente procedura:

a. Fare clic sull'icona **Il ruolo non è attivo** sotto **Imposta origine** per **Package: AS**
b. Fare clic sull'icona **Il ruolo non è attivo** sotto **Imposta destinazione** per **Package: AS**
c. Fare clic sull'icona **Espandi** accanto a **Package: AS**.
d. Fare clic sull'icona **Il ruolo non è attivo** per **Protocollo: EDI-X12 (ALL)** sia per l'origine che per la destinazione.
e. Fare clic sull'icona **Espandi** accanto a **Protocollo: EDI-X12 (ALL)**.
f. Fare clic sull'icona **Il ruolo non è attivo** per **Tipo documento: ISA** per l'origine e la destinazione.

Definizione delle connessioni del partner

Informazioni su questa attività

Definire la connessione del partner per i documenti EDI senza impacchettamento che provengono dal partner interno per essere distribuiti al Partner due.

1. Fare clic su **Amministrazione account > Connessioni**.
2. Nell'elenco **Origine**, selezionare **Partner interno**.
3. Nell'elenco **Destinazione**, selezionare **Partner due**.
4. Fare clic su **Cerca**.
5. Fare clic su **Attiva** per la connessione con i seguenti dettagli:
   a. **Origine**
      1) Package: **Nessuno (N/A)**
      2) Protocollo: **EDI-X12 (ALL)**
      3) Tipo documento: **ISA(ALL)**
   b. **Destinazione**
      1) Package: **AS (N/A)**
      2) Protocollo: **EDI-X12 (ALL)**
      3) Tipo documento: **ISA(ALL)**

Definire quindi la connessione per i documenti EDI inclusi nell'impacchettamento AS2 che provengono dal Partner due per essere distribuiti al partner interno, senza impacchettamento. Questo è molto simile alla connessione definita nella sezione precedente, tranne per il fatto che si configureranno anche gli attributi AS2.

1. Fare clic su **Amministrazione account > Connessioni**.
2. Nell'elenco **Origine**, selezionare **Partner due**
3. Nell'elenco **Destinazione**, selezionare **Partner interno**.
4. Fare clic su **Cerca**.
5. Fare clic su **Attiva** per la connessione con i seguenti dettagli:
   a. **Origine**
      1) Package: **AS (N/A)**
      2) Protocollo: **EDI-X12 (ALL)**
      3) Tipo documento: **ISA(ALL)**
   b. **Destinazione**
      1) Package: **Nessuno (N/A)**
      2) Protocollo: **EDI-X12 (ALL)**
      3) Tipo documento: **ISA(ALL)**

In seguito, selezionare Attributi accanto alla casella **Package: AS (N/A)** per il Partner due.

1. Modifica il package: Attributi AS (N\D) spostandosi nella pagina e facendo clic sull'icona **Espandi** accanto a **Package: AS (N/A)**.
2. Inserire un valore (AS1) dell'indirizzo e-mail AS MDN. Questo può essere un qualsiasi indirizzo e-mail valido.
3. Inserire un valore (AS2) AS MDN HTTP URL. Inserirlo nel seguente modo: **http://<***IP_address***>:57080/bcgreceiver/submit,** laddove<*IP_address*> rappresenta l'hub.
4. Fare clic su **Salva**.

Configurazione di base - Impostazione della protezione per documenti in entrata e in uscita

In questa sezione, viene spiegato in che modo aggiungere i seguenti tipi di protezione alla configurazione di base:

- Autenticazione del server SSL (Secure Socket Layer)
- Codifica
- Firme digitali

Impostazione dell'autenticazione SSL per i documenti in entrata

Informazioni su questa attività

In questa sezione, si utilizza lo strumento iKeyman per impostare l'autenticazione del server, in modo che il Partner due possa inviare i documenti AS2 su HTTPS.

Per impostare l'autenticazione del server, effettuare le seguenti procedure:

1. Iniziare l'applicazione iKeyman, aprendo il file ikeyman.bat dalla directory /<*DirProdotto*>/was/bin.
2. Aprire il keystore predefinito del Destinatario, bcgSecurity.jks. Dalla barra dei menu, selezionare **Apertura del file database della chiave**. In una installazione predefinita, bcgSecurity.jks si trova nella directory: <*DirProdotto*>/common/security/keystore
3. Quando richiesto, inserire la password predefinita per bcgSecurity.jks. Questa password è WebAS.
4. Se questa è la prima volta che è stato aperto bcgSecurity.jks, eliminare il certificato "fittizio".

La fase successiva è quella della creazione di un nuovo certificato autofirmato. La creazione di un certificato personale autofirmato crea una chiave privata e una pubblica nel file di memorizzazione delle chiavi del server.

Per creare un nuovo certificato autofirmato:

1. Fare clic su **Nuovo auto firmato**.
2. Fornire l'etichetta della chiave del certificato che viene utilizzata per identificare esclusivamente il certificato nella memoria delle chiavi. Utilizzare l'etichetta **selfSignedCert**.
3. Inserire il Nome comune del server. Questa è l'identità principale e universale per il certificato. Deve unicamente identificare il principale che rappresenta.
4. Inserire il nome dell'organizzazione.

5. Accettare tutti gli altri valori predefiniti e fare clic su **OK**.

Presumere che il Partner due voglia inviare un messaggio EDI su AS2 utilizzando l'HTTP di protezione. Per il Partner due è necessario fare riferimento al certificato pubblico (creato come parte della creazione del certificato autofirmato) per poter eseguire le seguenti operazioni.

Per abilitare il Partner due a utilizzare il certificato pubblico, esportare il certificato pubblico dal file di memorizzazione delle chiavi del server nel seguente modo:

1. Selezionare il certificato autofirmato recentemente creato dall'utilità IBM Key Management.
2. Fare clic su **Estrai certificato**.
3. Modificare il tipo di Dati in **Dati DER binari**.
4. Fornire il nome di file **commManPublic** e fare clic su **OK**.

Infine, si utilizza iKeyman per esportare il certificato autofirmato e la coppia di chiavi private nella forma di un file PKCS12. Questo file PCKS12 viene utilizzato per la codifica, descritta in una sezione successiva.

Per esportare il certificato autofirmato e la coppia di chiave privata:

1. Fare clic su **Esporta/Importa**.
2. Modificare il tipo di file Chiave in **PKCS12**.
3. Fornire il nome di file **commManPrivate** e fare clic su **OK**.
4. Inserire una password per proteggere il file PKCS12 di destinazione. Confermare la password e fare clic su **OK**.

Nota: arrestare e riavviare il Ricevitore per rendere effettive queste modifiche.

La password inserita viene utilizzata successivamente quando si importa questo certificato privato nell'hub.

Il Partner due deve inoltre effettuare alcune procedure di configurazione, compresa l'importazione del certificato e la modifica dell'indirizzo al quale inviare i documenti AS2. Ad esempio, Partner due deve modificare l'indirizzo in:

`https://<IP_address>:57443/bcgreceiver/submit`

dove <*IP_address*> si riferisce all'hub.

Adesso, il certificato autofirmato inserito nella memoria delle chiavi predefinita del Destinatario viene presentato nel Partner due ogni qual volta il Partner due invia un documento sull'HTTP sicuro.

Per impostare la situazione inversa, il Partner due deve impostare l'hub con una chiave SSL nella forma di un file .der (in questo caso, partnerTwoSSL.der). Se necessario, il Partner due deve anche modificare la configurazione per consentire la ricezione dei documenti sul trasporto HTTPS.

Caricare il file partner due, partnerTwoSSL.der, nel profilo dell'Operatore hub come certificato root. Un certificato root è un certificato rilasciato dall'Autorità di certificazione utilizzato quando si stabilisce una catena di certificati. In questo esempio, PartnerTwo ha generato il certificato, che è caricato come certificato root per consentire all'hub il riconoscimento e la fiducia del mittente.

Caricare partnerTwoSSL.der nell'hub:

1. Nel menu principale, fare clic su **Amministrazione account > Profili > Partner**.
2. Fare clic su **Cerca**.
3. Selezionare **Operatore hub** facendo clic sull'icona **Visualizza dettagli**.
4. Fare clic sui **Certificati** e quindi su **Carica certificato**.
5. Impostare il **Tipo di certificato** come **Certificato root ed intermedio**.
6. Modificare la Descrizione in **Certificato SSL Partner due**.
7. Impostare lo **Stato** come **Abilitato**.
8. Fare clic su **Sfoglia** e navigare nella directory nella quale è stato salvato partnerTwoSSL.der.
9. Selezionare il certificato e fare clic su **Apri**.
10. Fare clic su **Carica** e fare clic su **Salva**.

Per utilizzare HTTP sicuro, modificare la destinazione del Partner due.

1. Fare clic su **Amministrazione account > Profili > Partner** nella barra di navigazione orizzontale.
2. Fare clic su **Cerca** e quindi selezionare Partner due facendo clic sull'icona **Visualizza dettagli**.
3. Nella barra di navigazione orizzontale fare clic su **Destinazioni**. Quindi selezionare HttpDestination facendo clic sull'icona **Visualizza dettagli**.
4. Modificarlo facendo clic sull'icona **Modifica**.
5. Modificare il valore del trasporto in **HTTPS/1.1**
6. Modificare il valore dell'indirizzo come segue: **https://<***IP_address***>:443/input/AS2**, dove <*IP_address*> corrisponde alla macchina del Partner due.
7. Tutti gli altri valori possono rimanere invariati. Fare clic su **Salva**.

Impostazione della codifica

Informazioni su questa attività

Questa sezione fornisce le procedure per l'impostazione della codifica.

Partner due deve necessariamente effettuare le procedure di configurazione (ad esempio, importazione del certificato pubblico e del certificato autofirmato) ed impostare la codifica sui documenti inviati all'hub.

WebSphere Partner Gateway utilizza la chiave privata quando si decodificano i documenti. Per consentire all'hub di procedere, caricare prima la chiave privata estratta dal certificato autofirmato nella Console comunità. Effettuare questa attività registrata nella Console comunità come Operatore Hub ed installare il certificato nel profilo.

Per caricare il file PKCS12:

1. Fare clic su **Amministrazione account > Profili > Partner** nella barra di navigazione orizzontale.
2. Fare clic su **Cerca**.
3. Selezionare **Operatore hub** facendo clic sull'icona **Visualizza dettagli**.
4. Fare clic su **Certificati** e quindi su **Carica PKCS12**.
5. Selezionare la casella di spunta alla sinistra della **Codifica**.
6. Modificare la Descrizione in **CommManPrivate**.
7. Selezionare **Abilitato**.

8. Fare clic su **Sfoglia** e navigare nella directory nella quale il file PKCS12, commManPrivate.p12, viene memorizzato.
9. Selezionare il file e fare clic su **Apri**.
10. Inserire la password fornita per il file PKCS12.
11. Lasciare la Modalità operativa su **Produzione**.
12. Fare clic su **Carica** e quindi su **Salva**.

È stata completata la configurazione richiesta per consentire ad un partner di inviare transazioni codificate mediante HTTP sicuro all'hub.

Nella seguente sezione, la procedura precedente viene invertita— l'hub invia la transazione EDI codificata sull'HTTP sicuro.

Il Partner due deve generare una coppia di chiavi di decodifica del documento (in questo esempio, partnerTwoDecrypt.der) e rendere disponibile il certificato pubblico all'hub.

Come precedentemente citato, la chiave pubblica sarà utilizzata dall'hub durante la codifica delle transazioni da inviare al partner. A tal fine, caricare il certificato della chiave pubblica nell'hub.

1. Nel menu principale, fare clic su **Amministrazione account > Profili > Partner**.
2. Fare clic su **Cerca**.
3. Selezionare Partner due facendo clic sull'icona **Visualizza dettagli**.
4. Fare clic sui **Certificati** dalla barra di navigazione orizzontale.
5. Fare clic su **Carica certificato**.
6. Selezionare la casella di spunta accanto a **Codifica**.
7. Modificare la Descrizione per leggere **Codifica Partner due**.
8. Impostare lo stato in **Abilitato**.
9. Fare clic su **Sfoglia**.
10. Navigare nella directory nella quale il certificato di codifica, partnerTwoDecrypt.der, viene memorizzato.
11. Selezionare il certificato e fare clic su **Apri**.
12. Lasciare la Modalità operativa su **Produzione**
13. Fare clic su **Carica** e fare clic su **Salva**.

Risultati

Il passo finale nella configurazione dell'hub per inviare i messaggi codificati su HTTP protetto mediante AS2 è quello di modificare la connessione del partner che esiste tra il partner interno ed il Partner due.

Per modificare la connessione del partner dalla Console comunità:

1. Nella barra di navigazione orizzontale, fare clic su **Amministrazione account > Connessioni**.
2. Nell'elenco **Origine**, selezionare **Gest com**.
3. Nell'elenco **Destinazione**, selezionare **Partner due**.
4. Fare clic su **Cerca**.
5. Fare clic sul pulsante **Attributi** per la destinazione.

6. Da Riepilogo connessione, si noti che l'attributo **Codificato AS** dispone del valore corrente di **No**. Modificare tale valore facendo clic sull'icona **Espandi** accanto al **Package: AS (N/A)**.

   Nota: è necessario spostarsi nella pagina perché questa opzione si visualizzi.
7. Nell'elenco, aggiornare l'attributo **Codificato AS** su **Sì**, quindi fare clic su **Salva**.

Impostazione della firma del documento

Informazioni su questa attività

Quando si firma in maniera digitale una transazione o un messaggio, WebSphere Partner Gateway utilizza una chiave privata per creare la firma e firmare. Il partner che riceve tale messaggio utilizza la chiave pubblica per convalidare la firma. WebSphere Partner Gateway utilizza firme digitali a questo scopo.

Questa sezione contiene la procedura richiesta per configurare l'hub e un partner da utilizzare con le firme digitali.

Il Partner due deve effettuare eventuali procedure di configurazione (ad esempio, creare un documento autofirmato denominato, in questo esempio, partnerTwoSigning.der) e configurare la firma dei documenti. Il Partner due deve rendere partnerTwoSigning.der disponibile all'hub.

Per caricare il certificato digitale nell'hub:

1. Fare clic su **Amministrazione account > Profili > Partner** nella barra di navigazione orizzontale.
2. Fare clic su **Cerca**.
3. Selezionare Partner due facendo clic sull'icona **Visualizza dettagli**.
4. Scegliere **Certificati** dalla barra di navigazione orizzontale.
5. Fare clic su **Carica certificato**.
6. Selezionare la casella di spunta accanto a **Firma digitale**.
7. Modificare Descrizione in **Firma CommMan**.
8. Impostare lo **Stato** in **Abilitato**.
9. Fare clic su **Sfoglia**.
10. Navigare nella directory nella quale il certificato digitale, partnerTwoSigning.der, viene salvato, selezionare il certificato e fare clic su **Apri**.
11. Fare clic su **Carica** seguito da **Salva**.

Questo completa la configurazione iniziale per le firme digitali.

Il partner utilizza il certificato pubblico per autenticare le transazioni firmate inviate all'hub.

L'hub utilizza la chiave privata per firmare in maniera digitale le transazioni in uscita, inviate al partner. Abilitare prima la chiave privata per la firma digitale.

Per abilitare la chiave privata per la firma digitale, procedere nel modo seguente:

1. Fare clic su **Amministrazione account > Profili > Certificati** dalla barra di navigazione orizzontale.
2. Fare clic sull'icona **Visualizza dettagli** accanto a **Operatore hub**.

3. Fare clic sull'icona **Visualizza dettagli** accanto a **CommManPrivate**.

   Nota: questo era il certificato privato caricato nell'hub precedentemente.
4. Fare clic sull'icona **Modifica**.
5. Selezionare la casella di spunta accanto a **Firma digitale**.

   Nota: se fosse presente più di un certificato di firma digitale, indicare il principale e il secondario selezionando **Principale** o **Secondario** dall'elenco **Utilizzo certificato**.
6. Fare clic su **Salva**.

Modificare quindi gli attributi della connessione del partner esistente tra il partner interno e il Partner due per un adeguamento all'AS2 firmato.

Per alterare gli attributi della connessione del partner, procedere nel modo seguente:

1. Nella barra di navigazione orizzontale, fare clic su **Amministrazione account > Connessioni**.
2. Nell'elenco **Origine** selezionare **Partner interno**.
3. Selezionare **Partner due** dall'elenco di **Destinazione**.
4. Fare clic su **Cerca**.
5. Fare clic sul pulsante **Attributi** per Partner due.
6. Modificare l'attributo **Firmato AS** facendo clic sull'icona **Espandi** accanto a **Package: AS (N/A)**.
7. Selezionare **Sì** dall'elenco **Firmato AS**.
8. Fare clic su **Salva**.

È stata completata la configurazione richiesta per inviare una transazione AS2 firmata da WebSphere Partner Gateway al partner.

Estensione della configurazione di base

Questa sezione riporta il modo in cui modificare la configurazione di base descritta in questa appendice. Mediante gli stessi partner e l'impostazione descritta in precedenza (un partner interno, utilizzando un ID DUNS di 123456789 e una destinazione directory file ed un partner denominato PartnerTwo con un ID DUNS di 987654321 e una destinazione HTTP), questa sezione descrive come aggiungere il supporto per:

- Il trasporto FTP
- I documenti XML personalizzati
- I file binari (senza impacchettamento)

Creazione di un destinatario FTP

Informazioni su questa attività

Il destinatario FTP riceve i file e li trasferisce al Gestore documenti per l'elaborazione. Come descritto nella sezione "Configurazione del server FTP per ricevere i documenti" a pagina 33, prima di poter creare un destinatario FTP, è necessario che un server FTP sia stato installato ed è necessario creare una directory FTP e configurare un server FTP.

In questo esempio, si presume che il server FTP sia stato configurato per il Partner due e che la directory root sia c:/ftproot.

1. Fare clic su **Amministrazione hub > Configurazione hub > Destinatari**.
2. Fare clic su **Crea destinatario**.
3. Immettere le seguenti informazioni:
   a. Nome destinatari: **FTP_Receiver**
   b. Trasporto: **Directory FTP**
   c. Directory root FTP: **C:/ftproot**
4. Fare clic su **Salva**.

Impostazione dell'hub per la ricezione di file binari

In questa sezione, vengono descritti i passi necessari per configurare l'hub in modo da ricevere documenti binari che il Partner due desidera inviare al partner interno.

Creazione di un'interazione per i documenti binari

Informazioni su questa attività

Per impostazione predefinita, WebSphere Partner Gateway fornisce quattro documenti binari che implicano interazioni. Diversamente, fornire un'interazione per i documenti binari compresi come Nessuno per un partner con il documento già compreso come Nessuno. In questa sezione, si crea l'interazione necessaria per consentire ai documenti binari il pass through al sistema.

1. Fare clic su **Amministrazione hub > Configurazione hub> Definizione documento**.
2. Fare clic su **Crea interazione**.
3. Da **Origine** selezionare: **Package: Nessuno Protocollo: Binario (1.0) Tipo documento: Binario (1.0)**.
4. Da **Destinazione** selezionare: **Package: Nessuno Protocollo: Binario (1.0) Tipo documento: Binario (1.0)**.
5. Nell'elenco **Azione**, selezionare **Pass Through**.
6. Fare clic su **Salva**.

Aggiornamento delle capacità B2B per il partner interno

Informazioni su questa attività

In questa sezione, viene mostrato in che modo configurare il partner interno in modo da essere in grado di accettare i documenti binari.

1. Fare clic su **Amministrazione account > Profili > Partner**.
2. Fare clic su **Cerca**.
3. Fare clic sull'icona **Visualizza dettagli** accanto a **Gest com**.
4. Fare clic su **Capacità B2B**.
5. Fare clic sull'icona **Il ruolo non è attivo** sotto **Imposta Destinazione** per **Package: Nessuno** in modo da abilitarlo.
6. Fare clic sull'icona **Espandi** accanto a **Package: Nessuno**.
7. Fare clic sull'icona **Il ruolo non è attivo** per **Protocollo: Binario (1.0)** in **Imposta destinazione**.
8. Fare clic sull'icona **Espandi** accanto a **Protocollo: Binario (1.0)**.
9. Infine, fare clic sull'icona **Il ruolo non è attivo** per **Tipo documento: Binario (1.0)** in **Imposta destinazione**.

Aggiornamento delle capacità B2B per Partner due
Informazioni su questa attività

Questa sezione mostra in che modo configurare Partner due per essere in grado di inviare i documenti binari.

1. Fare clic su **Amministrazione account > Profili > Partner**.
2. Fare clic su **Cerca**.
3. Fare clic sull'icona **Visualizza dettagli** accanto a Partner due.
4. Fare clic su **Capacità B2B**.
5. Fare clic sull'icona **Il ruolo non è attivo** in **Imposta origine** per **Package: Nessuno** in modo da abilitarlo.
6. Fare clic sull'icona **Espandi** accanto a **Package: Nessuno**.
7. Fare clic sull'icona **Il ruolo non è attivo** per **Protocollo: Binario (1.0)** in **Imposta origine**.
8. Fare clic sull'icona **Espandi** accanto a **Protocollo: Binario (1.0)**.
9. Infine, fare clic sull'icona **Il ruolo non è attivo** per **Tipo documento: Binario (1.0)** in **Imposta origine**.

Creazione di una nuova connessione del partner
Informazioni su questa attività

Questa sezione mostra come configurare una nuova connessione del partner tra il partner interno ed il Partner due per i documenti binari.

1. Fare clic su **Amministrazione account > Connessioni**.
2. Selezionare **Partner due** nell'elenco **Origine**.
3. Nell'elenco **Destinazione** selezionare **Partner interno**.
4. Fare clic su **Cerca**.
5. Individuare la connessione **Nessuna (N/A), Binaria (1.0), Binaria (1.0)** in **Nessuna (N/A), Binaria (1.0), Binaria (1.0)** e fare clic su **Attiva** per attivarla.

Impostazione dell'hub per i documenti XML personalizzati

Come descritto in "Elaborazione documento XML personalizzato" a pagina 151, è necessario configurare l'hub per instradare i file XML personalizzati. In questa sezione, vengono descritti i passaggi necessari per configurare il Gestore documenti, in modo da instradare il seguente documento XML:

```
<?xml versione="1.0" codifica="UTF-8"?>
<!DOCTYPE Tester>
<Tester type="Test type A">
    <From>987654321</From>
    <To>123456789</To>
</Tester>
```

In questo esempio, il Gestore documenti utilizza RootTag per identificare il tipo di documento XML. Quindi estrae i valori dai campi From e To per identificare gli identificativi di business Dal partner e Al partner.

Creazione del formato di definizione del protocollo CustomXML
Informazioni su questa attività

La prima fase prevede la creazione di un nuovo protocollo per l'XML personalizzato che si desidera scambiare.

1. Fare clic su **Amministrazione hub > Configurazione hub> Definizione documento**.
2. Fare clic su **Crea definizione di documento**.
3. Selezionare **Protocollo** nell'elenco **Tipo di definizione di documento**.
4. Immettere le seguenti informazioni:
   a. Codice: **XML personalizzato**
   b. Versione: **1.0**
   c. Descrizione: **Definizione del protocollo di esempio**
5. Impostare il **Livello di documento** su **No**.
6. Impostare **Stato** su **Abilitato**.
7. Impostare **Visibilità: Amministratore hub** su **Sì**.
8. Impostare **Visibilità: Partner interno** su **Sì**.
9. Impostare **Visibilità: Partner** su **Sì**.
10. Selezionare:
    a. Package: **AS**
    b. Package: **Nessuno**
    c. Package: **Integrazione backend**.
11. Fare clic su **Salva**.

Creazione di una definizione del documento Tester_XML

Informazioni su questa attività

La seconda fase è creare una definizione del documento per il nuovo protocollo.

1. Fare clic su **Amministrazione hub > Configurazione hub> Definizione documento**.
2. Fare clic su **Crea definizione di documento**.
3. Selezionare **Tipo documento** nell'elenco **Tipo di definizione di documento**.
4. Immettere le seguenti informazioni:
   a. Nome: **Tester_XML**
   b. Versione: **1.0**
   c. Descrizione: **Tipo di documento XML personalizzato di esempio**
5. Impostare **Livello documento** su **Sì**.
6. Impostare **Stato** su **Abilitato**.
7. Impostare **Visibilità: Amministratore hub** su **Sì**.
8. Impostare **Visibilità: Partner interno** su **Sì**.
9. Impostare **Visibilità: Partner** su **Sì**.
10. Fare clic sull'icona **Espandi** accanto a **Package: AS** e selezionare **Protocollo: CustomXML**.
11. Fare clic sull'icona **Espandi** accanto a **Package: Nessuno** e selezionare **Protocollo: CustomXML**.
12. Fare clic sull'icona **Espandi** accanto a **Package: Integrazione backend** e selezionare **Protocollo: CustomXML**.
13. Fare clic su **Salva**.

Creazione del formato Tester_XML
Informazioni su questa attività

Infine, creare il formato XML associato al nuovo protocollo.

1. Fare clic su **Amministrazione hub > Configurazione hub > Formati XML**.
2. Fare clic su **Crea una famiglia di documenti**.
3. Immettere o selezionare le seguenti informazioni:
   a. Nome famiglia: **Famiglia di esempio**
   b. Protocollo: **XML personalizzato 1.0**
   c. Tipo famiglia: **Tag root**
   d. Opzione File di grandi dimensioni: **Nessuno**
   e. Identificativo di famiglia: **Tester**
4. Fare clic su **Salva**.
5. Nella pagina risultante Famiglia di documenti, fare clic su **Crea formato XML**.
6. Nell'elenco Tipo documento, selezionare **Tester_XML**.
7. Per il valore Identificativo del formato, immettere **Test type A**.
8. Per l'espressione XPath per l'Identificativo del formato, immettere **/Tester/@type**.
9. Lasciare il campo Spazio nome del prefisso vuoto (nessuno spazio nome viene utilizzato nel documento) ed il Tipo di ritorno come **Testo**.
10. Immettere **1** nel campo di valore Versione del formato e il campo Espressione XPath. Modificare il Tipo di ritorno su **Costante**. Questo significa che tutti i documenti con l'identificativo Formato "Tester" avranno la versione corretta per una corrispondenza con questo formato. Si verifica poiché la versione per tutti i documenti sarà 1 e la versione di questo formato è anche 1. Quindi, la versione corrisponde sempre.
11. Immettere **/Tester/From** per l'espressione XPath per l'identificativo di business Origine.
12. Immettere **/Tester/To** per l'espressione XPath per l'identificativo di business Destinazione.
13. Lasciare i campi restanti nel formato in cui si trovano. Sono facoltativi e non sono stati utilizzati in questo esempio.
14. Fare clic su **Salva**.

Creazione di un'interazione per i documenti Tester_XML
Informazioni su questa attività

Quindi, è disponibile un nuovo protocollo ed un tipo di documento con cui viene impostata un'interazione.

1. Fare clic su **Amministrazione hub > Configurazione hub> Definizione documento**.
2. Fare clic su **Crea interazione**.
3. Da **Origine**, selezionare:
   a. Package: **Nessuno**
   b. Protocollo: **XML personalizzato (1.0)**
   c. Tipo documento: **Tester_XML (1.0)**.
4. Da **Destinazione** selezionare:
   a. Package: **Nessuno**
   b. Protocollo: **XML personalizzato (1.0)**

c. Tipo documento: **Tester_XML (1.0)**.

5. Nell'elenco **Azione**, selezionare **Pass Through**.
6. Fare clic su **Salva**.

Aggiornamento delle capacità B2B per il partner interno

Informazioni su questa attività

Per consentire lo scambio del documento XML personalizzato, è necessario aggiornare le capacità B2B dei partner.

Abilitare il partner interno per ricevere (rappresentare la destinazione) i documenti Tester_XML.

1. Fare clic su **Amministrazione account > Profili > Partner**.
2. Fare clic su **Cerca**.
3. Nell'elenco dei partner selezionare il partner interno. (Questo esempio presume che il partner interno abbia l'identificativo di business 123456789.)
4. Fare clic su **Capacità B2B**.
5. Fare clic sull'icona **Il ruolo non è attivo** sotto **Imposta Destinazione** per **Package: Nessuno** in modo da abilitarlo.
6. Fare clic sull'icona **Espandi** accanto a **Package: Nessuno**.
7. Fare clic sull'icona **Il ruolo non è attivo** per **Protocollo: XML personalizzato (1.0)** di **Imposta destinazione**.
8. Fare clic sull'icona **Espandi** posta accanto al **Protocollo: XML personalizzato (1.0)**.
9. Infine, fare clic sull'icona **Il ruolo non è attivo** per **Tipo documento: Tester_XML (1.0)** di **Imposta destinazione**.

Aggiornamento delle capacità B2B per Partner due

Informazioni su questa attività

Aggiornare le capacità B2B del Partner due per consentire lo scambio dei messaggi mediante il nuovo formato XML personalizzato.

Abilitare Partner due affinché sia l'origine dei documenti Tester_XML. (L'esempio presume che il Partner due abbia l'identificativo di business 987654321.)

1. Fare clic su **Amministrazione account > Profili > Partner**.
2. Fare clic su **Cerca**.
3. Nell'elenco dei partner, selezionare **Partner due**. (Questo esempio presume che il Partner due abbia l'identificativo di business 987654321.)
4. Fare clic su **Capacità B2B**.
5. Fare clic sull'icona **Il ruolo non è attivo** in **Imposta origine** per **Package: Nessuno** in modo da abilitarlo.
6. Fare clic sull'icona **Espandi** accanto a **Package: Nessuno**.
7. Fare clic sull'icona **Il ruolo non è attivo** per **Protocollo: XML personalizzato (1.0)** di **Imposta origine**.
8. Fare clic sull'icona **Espandi** posta accanto al **Protocollo: XML personalizzato (1.0)**.
9. Infine, fare clic sull'icona **Il ruolo non è attivo** per **Tipo documento: Tester_XML (1.0)** di **Imposta origine**.

Creazione di una nuova connessione del partner

Informazioni su questa attività

Infine, creare una nuova connessione del partner.

1. Fare clic su **Amministrazione account > Connessioni.**
2. Selezionare **Partner due** nell'elenco **Origine**.
3. Nell'elenco **Destinazione** selezionare **Partner interno**.
4. Fare clic su **Cerca**.
5. Rilevare **Nessuno (N/A), XML personalizzato (1.0), Tester_XML(1.0)**sulla connessione **Nessuno (N/A), XML personalizzato (1.0), Tester_XML (1.0)** e fare clic su **Attiva** per attivarla.

Instradamento di un documento mediante XML personalizzato

Copiare il file XML di esempio dall'inizio di questo esempio e incollarlo in un editor testi. Salvare il file sulla macchina con il nome desiderato. Durante l'invio del file all'hub trascinarlo nella directory utilizzata dal destinatario file. Visualizzarlo nel Visualizzatore documenti e verificare che il documento sia stato instradato dal Partner due al partner interno utilizzando la connessione definita.

Capitolo 19. Esempi EDI

In questa appendice, vengono forniti esempi di invio o ricezione di scambi EDI e conversione degli stessi nei e dai documenti ROD (dati orientati al record).

Gli esempi contenuti in questa appendice non sono correlati a quelli contenuti in Capitolo 18, “Esempi di base”, a pagina 301. Le destinazioni ed i profili nuovi sono stati creati per gli esempi di questa appendice.

Nota: un esempio di scambio EDI che viene trasmesso tramite l'hub (nessun deenveloping o nessuna conversione) viene incluso in Capitolo 18, “Esempi di base”, a pagina 301.

Ciascuno di questi quattro esempi è autonomo rispetto all'altro. Se, ad esempio, si segue l'esempio EDI in XML, si visualizzano tutti i passaggi (dalla creazione di destinazioni tramite l'attivazione di connessioni) di questo esempio.

In questa appendice, sono contenuti i seguenti argomenti:

- “ Esempio da EDI a ROD”
- “ Esempio da EDI a XML” a pagina 333
- “ Esempio da XML a EDI” a pagina 338
- “ Esempio da ROD a EDI” a pagina 345

Lo scopo di questi esempi è di fornire una rapida panoramica dei passi richiesti per configurare un sistema. Se si utilizzano tali esempi per configurare il sistema di cui si dispone, modificare le informazioni specifiche (ad esempio, i nomi e gli ID di business) in base alle esigenze dell'azienda.

Esempio da EDI a ROD

In questa sezione, viene fornito un esempio di invio di una transazione EDI (in una busta) all'hub, in cui viene convertita in un documento ROD (record-oriented-data) ed inviata al partner interno.

Deenveloping e conversione di uno scambio EDI

Informazioni su questa attività

In questo esempio, si presume che l'esperto delle mappature di Data Interchange Services abbia creato una mappa di conversione che utilizza una transazione EDI 850 standard (definita con il dizionario X12V5R1, corrispondente alla versione 5010 di X12) e la converte in un documento ROD (record-oriented document) che verrà elaborato dall'applicazione di back-end del partner interno. In questo esempio, la mappa viene denominata S_DT_EDI_TO_ROD.eif.

Lo specialista della mappatura Data Interchange Services può esportare la mappa di conversione direttamente nel database WebSphere Partner Gateway. In alternativa, lo specialista della mappatura Data Interchange Services può inviare il file, nel qual caso si utilizza l'utilità bcgDISImport per l'importazione in WebSphere Partner Gateway. In questa appendice, si presume il secondo scenario.

Importazione della mappa di conversione
Informazioni su questa attività

In questa sezione, vengono descritti i passaggi per importare una mappa di conversione che utilizzerà l'input EDI e lo convertirà nel formato ROD. Nel processo di importazione della mappa di conversione, si importa anche la definizione del documento associato alla mappa.

Prima che sia possibile importare la mappa di conversione, lo specialista della mappatura Data Interchange Services deve inviarla all'utente. Questo insieme di passaggi tiene conto che il file S_DT_EDI_TO_ROD.eif si trovi sul sistema.

1. Aprire la finestra dei comandi.
2. Immettere il seguente comando o script:
   - In un sistema UNIX:

     ```
     <DirProdotto>/bin/bcgDISImport.sh <database_user_ID>
     <password> S_DT_EDI_TO_ROD.eif
     ```

   - In un sistema Windows:

     ```
     <DirProdotto>\bin\bcgDISImport.bat <database_user_ID>
     <password> S_DT_EDI_TO_ROD.eif
     ```

     dove *<database_user_ID>* e *<password>* corrispondono ai valori utilizzati al momento dell'installazione del database come parte dell'installazione di WebSphere Partner Gateway.

Verifica delle definizioni documenti e della mappa di conversione
Informazioni su questa attività

Per verificare se le mappe di conversione e le definizioni documenti importate sono disponibili nella Console comunità, procedere nel modo seguente:

1. Fare clic su **Amministrazione hub > Configurazione hub > Mappe > Mappe di conversione**.

   Viene visualizzata la mappa S_DT_EDI_TO_ROD.
2. Fare clic sull'icona **Visualizza dettagli** accanto alla mappa.

   Sono visualizzate le definizioni documenti a cui è associata questa mappa:

Tabella 33. Definizione documento associata alla mappa

Origine	Destinazione
Package: N/A Protocollo: X12V5R1 (ALL)Tipo documento: 850 (ALL)	Package: Nessuno Protocollo: DEMO850CL_DICTIONARY(ALL) Tipo documento: DEMO850CLSUW (ALL)

La mappa S_DT_EDI_TO_ROD è stata definita per utilizzare una transazione X12 850 (che aderisce allo standard X12V5R1) e la converte in un protocollo personalizzato (DEMO850CL_DICTIONARY) e un tipo di documento (DEMO850CLSUW).

Configurazione di un destinatario
Informazioni su questa attività

In questa sezione, viene creato un destinatario di directory del file-system per l'hub:

1. Fare clic su **Amministrazione hub > Configurazione hub > Destinatari** e fare clic su **Crea destinatario**.

2. Per Nome destinatari, inserire: **EDIFileTarget**
3. Dall'Elenco dei trasporti, selezionare **Directory file**.
4. Per Percorso root, digitare: **/Data/Manager/editarget**
5. Fare clic su **Salva**.

Il partner invia lo scambio EDI a questo destinatario.

Creazione delle interazioni
Informazioni su questa attività

Si creano due interazioni, una per la busta EDI e l'altra per la transazione nella busta EDI.

Creare un'interazione che rappresenta la busta EDI.

1. Fare clic su **Amministrazione hub > Configurazione hub> Definizione documento**.
2. Fare clic su **Crea interazione**.
3. In **Origine**, espandere **Package: Nessuno** e **Protocollo: EDI-X12** e selezionare **Tipo documento: ISA**.
4. In **Destinazione**, espandere **Package: N/A** e **Protocollo: EDI-X12** e selezionare **Tipo documento: ISA.**
5. Nell'elenco Azione, selezionare **Deenveloping di EDI**.

   Nota: in questa interazione, non si verifica alcuna conversione. Lo scambio EDI è in fase di deenveloping, dando come risultato una singola transazione (850). Di conseguenza, non è necessaria una mappa di conversione per questa transazione.
6. Fare clic su **Salva**.

Creare un'interazione che abbia un'origine che rappresenti la transazione 850 ed una destinazione che rappresenti il documento convertito.

1. Fare clic su **Amministrazione hub > Configurazione hub> Definizione documento**.
2. Fare clic su **Crea interazione**.
3. In **Origine**, espandere **Package: N/A** e **Protocollo: X12V5R1** e selezionare **Tipo documento: 850**.
4. In **Destinazione**, espandere **Package: Nessuno** e **Protocollo: DEMO850CL_DICTIONARY** e selezionare **Tipo documento: DEMO850CLSUW**.
5. Nell'elenco delle mappe di conversione, selezionare **S_DT_EDI_TO_ROD**.
6. Nell'elenco delle azioni, selezionare **Convalida EDI e conversione EDI**.
7. Fare clic su **Salva**.

Questa interazione rappresenta la conversione di una transazione EDI X12 850 standard in un formato differente e, di conseguenza, è necessario selezionare una mappa di conversione.

Creazione di partner
Informazioni su questa attività

In questo esempio, sono disponibili due partner: il partner interno (Gestore) e un partner esterno (TP1).

Creare il profilo del Partner interno:

1. Fare clic su **Amministrazione account > Profili > Partner** e fare clic su **Crea**.
2. Per Nome accesso azienda, immettere: **Gestcom**
3. Per Nome visualizzato partner: immettere **Gestore**
4. Per Tipo di partner, selezionare **Partner interno**.
5. Fare clic su **Nuovo** per l'ID di business e immettere `000000000` come ID di figura a mano libera.

   Nota: è necessario selezionare Figura a mano libera e non DUNS.
6. Fare di nuovo clic su **Nuovo** per l'ID di business e immettere `01-000000000` come ID in forma libera.
7. Fare clic su **Salva**.

Creare il secondo partner:

1. Fare clic su **Amministrazione account > Profili > Partner** e fare clic su **Crea**.
2. Per Nome accesso azienda, digitare: **TP1**
3. Per Nome visualizzato partner, immettere **TP1**
4. Per Tipo di partner, selezionare **Partner esterno**.
5. Fare clic su **Nuovo** per l'ID di business e immettere `000000001` come ID di figura a mano libera.

   Nota: è necessario selezionare Figura a mano libera e non DUNS.
6. Fare di nuovo clic su **Nuovo** per l'ID di business e immettere `01-000000001` come ID di figura a mano libera.
7. Fare clic su **Salva**.

Creazione delle destinazioni

Informazioni su questa attività

Nell'esempio, creare le destinazioni di directory file per entrambi i partner. Creare una destinazione per il Gestore:

1. Fare clic su **Amministrazione account > Profili > Partner** e su **Cerca**.
2. Fare clic sull'icona **Visualizza dettagli** accanto al profilo Gestore.
3. Fare clic su **Destinazioni** e poi su **Crea**.
4. Immettere i seguenti valori per la destinazione. È necessario che la directory di file (l'intero percorso) sia già presente sul file system.
   a. Per Nome, inserire **ManagerFileDestination**.
   b. Nell'elenco dei trasporti, selezionare **Directory file**.
   c. Per Indirizzo, inserire: **file://Data/Manager/filedestination**
   d. Fare clic su **Salva**.
5. Fare clic su **Elenco** per elencare tutte le destinazioni per il partner interno.
6. Fare clic su **Visualizza destinazioni predefinite**.
7. Nell'elenco **Produzione**, selezionare la destinazione creata nella fase 4.
8. Fare clic su **Salva**.

Quindi, creare una destinazione per il partner.

1. Fare clic su **Amministrazione account > Profili > Partner** e su **Cerca**.
2. Selezionare l'altro partner creato per questo esempio facendo clic sull'icona **Visualizza dettagli**, posta accanto a **TP1**.

3. Fare clic su **Destinazioni** e poi su **Crea**.
4. Immettere i seguenti valori per la destinazione. La directory file (l'intero percorso) deve già esistere.
   a. Per Nome, inserire **TP1FileDestination**.
   b. Dall'Elenco dei trasporti, selezionare **Directory file**.
   c. Per Indirizzo, inserire: **file://Data/TP1/filedestination**
   d. Fare clic su **Salva**.
5. Fare clic su **Elenco** per elencare tutte le destinazioni del partner.
6. Fare clic su **Visualizza destinazioni predefinite**.
7. Nell'elenco **Produzione**, selezionare la destinazione creata nella fase 4.
8. Fare clic su **Salva**.

Impostazione delle capacità B2B
Informazioni su questa attività

Abilitare le capacità B2B dei due partner di questo scambio. In questo esempio, lo scambio EDI è stato creato con un partner esterno (TP1) e sarà distribuito al partner interno.

1. Fare clic su **Amministrazione account > Profili > Partner** e su **Cerca**.
2. Fare clic sull'icona **Visualizza dettagli** per il partner di origine per questo esempio (**TP1**).
3. Fare clic su **Capacità B2B**.
4. Abilitare due gruppi di capacità per il partner di origine.
   a. Abilitare la definizione del documento che rappresenta la busta EDI:
      1) Fare clic sull'icona **Il ruolo non è attivo** in **Imposta origine** per **Package: Nessuno** in modo da abilitarlo.
      2) Espandere **Package: Nessuno**.
      3) Fare clic sull'icona **Il ruolo non è attivo** sotto **Imposta origine** per **Protocollo EDI-X12 (ALL)**.
      4) Espandere **Protocollo: EDI-X12 (ALL)**
      5) Fare clic sull'icona **Il ruolo non è attivo** di **Imposta origine** per **Tipo documento: ISA (ALL)**.
   b. Quindi, abilitare la definizione del documento che rappresenta la transazione 850:
      1) Fare clic sull'icona **Il ruolo non è attivo** in **Imposta origine** per **Package: N/A** per abilitarlo.
      2) Espandere **Package: N/A**.
      3) Fare clic sull'icona **Il ruolo non è attivo** sotto **Imposta origine** per **Protocollo: X12V5R1 (ALL)** .
      4) Espandere **Protocollo: X12V5R1 (ALL)**.
      5) Fare clic sull'icona **Il ruolo non è attivo** di **Imposta origine** per **Tipo documento: 850**.
5. Fare clic su **Amministrazione account > Profili > Partner** e su **Cerca**.
6. Fare clic sull'icona **Visualizza dettagli** per il partner di destinazione per questo esempio (**Gestore**).
7. Fare clic su **Capacità B2B**.
8. Abilitare due gruppi di capacità per il partner di destinazione.
   a. Abilitare la definizione del documento che rappresenta la busta:

1) Fare clic sull'icona **Il ruolo non è attivo** in **Imposta destinazione** per **Package: N/A** per abilitarlo.
2) Espandere **Package: N/A**.
3) Fare clic sull'icona **Il ruolo non è attivo** sotto **Imposta destinazione** per **Protocollo: EDI-X12 (ALL)** .
4) Espandere **Protocollo: EDI-X12 (ALL)**.
5) Fare clic sull'icona **Il ruolo non è attivo** di **Imposta destinazione** per **Tipo documento: ISA (ALL)**.

b. Quindi, abilitare la definizione del documento che rappresenta il documento convertito:
1) Fare clic sull'icona **Il ruolo non è attivo** sotto **Imposta Destinazione** per **Package: Nessuno** in modo da abilitarlo.
2) Espandere **Package: Nessuno**.
3) Fare clic sull'icona **Il ruolo non è attivo** sotto **Imposta destinazione** per **Protocollo: DEMO850CL_DICTIONARY (ALL)**.
4) Espandere **Protocollo: DEMO850CL_DICTIONARY (ALL)**.
5) Fare clic sull'icona **Il ruolo non è attivo** di **Imposta destinazione** per **Tipo documento: DEMO850CLSUW(ALL)**.

Attivazione delle connessioni
Informazioni su questa attività

Per attivare le connessioni:

1. Fare clic su **Amministrazione account > Connessioni**.
2. Selezionare **TP1** dall'elenco Origine.
3. Selezionare **Gestore** dall'elenco Destinazione.
4. Fare clic su **Cerca**.
5. Fare clic su **Attiva** per la connessione che rappresenta la busta:

Tabella 34. Connessione busta

Origine	Destinazione
Package: Nessuno (N/A) Protocollo: EDI-X12 (ALL) Tipo documento: ISA (ALL)	Package: N/A (N/A) Protocollo: EDI-X12 (ALL) Tipo documento: ISA (ALL)

6. Fare clic su **Attiva** per la connessione che rappresenta la transazione 850 per il documento convertito:

Tabella 35. Connessione di transazione EDI al documento ROD

Origine	Destinazione
Package: N/A (N/A) Protocollo: X12V5R1Tipo documento: 850 (ALL)	Package: Nessuno (N/A) Protocollo: DEMO850CL_DICTIONARY (ALL) Tipo documento: DEMO850CLSUW (ALL)

Aggiunta di attributi
Informazioni su questa attività

Impostare l'attributo che consente i documenti con ID duplicati:

1. Fare clic su **Amministrazione hub > Configurazione hub> Definizione documento**.
2. Fare clic sull'icona **Espandi** accanto a **Package: Nessuno**.

3. Fare clic sull'icona **Modifica valori dell'attributo** accanto a **Protocollo: EDI-X12**.
4. Scorrere la sezione Attributi di contesto del Tipo documenti della pagina. Alla riga **Consenti documenti con ID duplicati**, selezionare **Sì** dall'elenco.
5. Fare clic su **Salva**.

A questo punto, se TP1 inviasse uno scambio EDI che contiene una transazione 850 al partner interno, lo scambio EDI verrebbe sottoposto a deenveloping, dando come risultato una transazione 850. La transazione 850 viene quindi convertita nel tipo di documento DEMO850CLSUW ed il documento convertito viene inviato alla destinazione del partner interno.

Aggiunta di un TA1 allo scambio

In X12, il TA1 è un segmento opzionale che può essere utilizzato per riconoscere la ricezione di uno scambio. Il mittente può richiedere un TA1 dal destinatario impostando l'elemento 14 di ISA Interchange Control Header su **1**. L'attributo Consenti una richiesta in WebSphere Partner Gateway può essere utilizzato per controllare se TA1 viene inviato quando il mittente lo richiede.

La mappa &WDI_TA1_ACK viene installata durante l'installazione di WebSphere Partner Gateway, cosicché non è necessario importarla.

Creazione delle associazioni

Informazioni su questa attività

Per associare la mappa ad una definizione del documento, effettuare la seguente procedura:

1. Fare clic su **Amministrazione hub > Configurazione hub > Mappe > Mappe RF EDI**.

   Viene visualizzata la mappa &WDI_TA1_ACK.
2. Fare clic sull'icona **Visualizza dettagli** accanto alla mappa.

   Si visualizzano le informazioni sulla mappa nonché una cartella per ciascun tipo di package disponibile sul sistema.
3. Creare l'associazione alla definizione del documento effettuando la seguente procedura:
   a. Selezionare la casella di spunta accanto a **Package: Nessuno**, quindi espandere la cartella.
   b. Selezionare la casella di spunta accanto a **Protocollo: EDI-X12 (ALL)**, quindi espandere la cartella.
   c. Selezionare la casella posta accanto a **Tipo documento: ISA (ALL)**.
   d. Fare clic su **Salva**.

È stata creata un'associazione tra la mappa &WDI_TA1_ACK1 e la definizione del documento per la busta.

Creazione delle interazioni

Informazioni su questa attività

Creare un'interazione che rappresenti la transazione TA1.

1. Fare clic su **Amministrazione hub > Configurazione hub> Definizione documento**.
2. Fare clic su **Crea interazione**.

3. In **Origine**, espandere **Package: N/A** e **Protocollo: &X44TA1** e selezionare **Tipo documento: TA1**.
4. In **Destinazione**, espandere **Package: N/A** e **Protocollo: &X44TA1** e selezionare **Tipo documento: TA1**.
5. Nell'elenco Azione, selezionare **Pass Through**.
6. Fare clic su **Salva**.

Creare un'interazione che abbia un'origine che rappresenti la busta EDI che conterrà il TA1.

1. Fare clic su **Amministrazione hub > Configurazione hub> Definizione documento**.
2. Fare clic su **Crea interazione**.
3. In **Origine**, espandere **Package: N/A** e **Protocollo: EDI-X12** e selezionare **Tipo documento: ISA**.
4. In **Destinazione**, espandere **Package: Nessuno** e **Protocollo: EDI-X12** e selezionare **Tipo documento: ISA.**
5. Nell'elenco Azione, selezionare **Pass Through**.
6. Fare clic su **Salva**.

Abilitazione delle capacità B2B

Informazioni su questa attività

Quindi, aggiungere le interazioni create di recente alle capacità B2B dei partner.

1. Fare clic su **Amministrazione account > Profili > Partner** e su **Cerca**.
2. Fare clic sull'icona **Visualizza dettagli** per il partner di origine per questo esempio (**Gestore**).

   Nota: TA1 passa dal partner che riceve il documento ROD al partner che lo invia. In questo esempio, il Gestore è l'origine di TA1 e TP1 del partner è la destinazione.
3. Fare clic su **Capacità B2B**.
4. Abilitare due gruppi di capacità per il partner di origine.
   a. Abilitare le capacità per TA1.
      1) Fare clic sull'icona **Il ruolo non è attivo** in **Imposta origine** per **Package: N/A** per abilitarlo.
      2) Espandere **Package: N/A**.
      3) Fare clic sull'icona **Il ruolo non è attivo** sotto **Imposta origine** per **Protocollo: &X44TA1**.
      4) Espandere **Protocollo: &X44TA1**.
      5) Fare clic sull'icona **Il ruolo non è attivo** in **Imposta origine** per **Tipo documento: TA1 (ALL)**.
   b. In seguito, abilitare le capacità per la busta:
      1) Fare clic sull'icona **Il ruolo non è attivo** in **Imposta origine** per **Package: N/A** per abilitarlo.
      2) Espandere **Package: N/A**.
      3) Fare clic sull'icona **Il ruolo non è attivo** sotto **Imposta origine** per **Protocollo: EDI-X12**.
      4) Espandere **Protocollo: EDI-X12 (ALL)**.
      5) Fare clic sull'icona **Il ruolo non è attivo** di **Imposta origine** per **Tipo documento: ISA (ALL)**.

5. Fare clic su **Amministrazione account > Profili > Partner** e su **Cerca**.
6. Fare clic sull'icona **Visualizza dettagli** per il partner di destinazione per questo esempio (**TP1**).
7. Fare clic su **Capacità B2B**.
8. Abilitare due gruppi di capacità per il partner di destinazione.
   a. Abilitare la definizione del documento che rappresenta TA1:
      1) Fare clic sull'icona **Il ruolo non è attivo** in **Imposta destinazione** per **Package: N/A** per abilitarlo.
      2) Espandere **Package: N/A**.
      3) Fare clic sull'icona **Il ruolo non è attivo** sotto **Imposta destinazione** per **Protocollo: &X44TA1 (ALL)**.
      4) Espandere **Protocollo: &X44TA1 (ALL)**.
      5) Fare clic sull'icona **Il ruolo non è attivo** in **Imposta destinazione** per **Tipo documento: TA1 (ALL)**.
   b. Quindi, abilitare la definizione del documento che rappresenta la busta EDI:
      1) Fare clic sull'icona **Il ruolo non è attivo** sotto **Imposta Destinazione** per **Package: Nessuno** in modo da abilitarlo.
      2) Espandere **Package: Nessuno**.
      3) Fare clic sull'icona **Il ruolo non è attivo** sotto **Imposta destinazione** per **Protocollo: EDI-X12 (ALL)** .
      4) Espandere **Protocollo: EDI-X12 (ALL)**.
      5) Fare clic sull'icona **Il ruolo non è attivo** in **Imposta destinazione** per **Tipo documento: ISA (ALL)**.

Creazione del profilo busta

Informazioni su questa attività

Quindi, creare il profilo busta che contiene un TA1:

1. Fare clic su **Amministrazione hub > Configurazione hub > EDI > Profilo busta**.
2. Fare clic su **Crea**.
3. Immettere il nome del profilo: **EnvProf1**.
4. Nell'elenco degli standard EDI, selezionare **X12**.
5. Il pulsante **Generale** è stato selezionato per impostazione predefinita. Immettere i seguenti valori per gli attributi generali di busta:
   - INTCTLLEN: **9**
   - GRPCTLLEN: **9**
   - TRXCTLLEN: **9**
   - MAXDOCS: **1000**
6. Fare clic su pulsante **Scambio** e digitare i seguenti valori per gli attributi dello scambio:
   - ISA01: **01**
   - ISA02: **ISA0000002**
   - ISA03: **02**
   - ISA04: **ISA0000004**
   - ISA11: \
   - ISA12: **00501**
   - ISA15: **T**

7. Fare clic su **Salva**.

Attivazione delle connessioni del partner
Informazioni su questa attività

Per attivare le connessioni:

1. Fare clic su **Amministrazione account > Connessioni**.
2. Selezionare **Gestore** dall'elenco Origine.
3. Selezionare **TP1** dall'elenco Destinazione.
4. Fare clic su **Cerca**.
5. Attivare la connessione che rappresenta TA1.

Tabella 36. Connessione TA1

Origine	Destinazione
Package: N/A (N/A) Protocollo: &X44TA1 (ALL) Tipo documento: TA1 (ALL)	Package: N/A (N/A) Protocollo: &X44TA1 (ALL) Tipo documento: TA1 (ALL)

6. Attivare la connessione che rappresenta la busta:

Tabella 37. Connessione busta

Origine	Destinazione
Package: N/A (N/A) Protocollo: EDI-X12 (ALL) Tipo documento: ISA (ALL)	Package: Nessuno (N/A) Protocollo: EDI-X12 (ALL) Tipo documento: ISA (ALL)

Configurazione degli attributi
Informazioni su questa attività

Per specificare gli attributi per il profilo busta:

1. Fare clic su **Amministrazione account > Profili > Partner** e su **Cerca**.
2. Selezionare **TP1** dall'elenco.
3. Fare clic su **Capacità B2B**.
4. Fare clic sull'icona **Espandi** accanto a **Package: Nessuno**.
5. Fare clic sull'icona **Modifica** accanto a **Protocollo: EDI-X12 (ALL)**.
6. Nella riga **Consenti una richiesta TA1**, selezionare **Sì**.
7. Fare clic su **Salva**.
8. Fare clic di nuovo su **Capacità B2B**.
9. Fare clic sull'icona **Espandi** accanto a **Package: N/A**.
10. Fare clic su **Modifica** accanto a **Protocollo: &X44TA1 (ALL)**.
11. Specificare i seguenti attributi:
    a. Nella riga Profilo busta, selezionare **EnvProf1** dall'elenco.
    b. Nella riga Qualificatore scambio, selezionare **01**.
    c. Nella riga Identificativo scambio, selezionare **000000001**.
    d. Nella riga Indicatore utilizzo scambio, selezionare **T**.
12. Fare clic su **Salva**.

In questa serie di attività, è stato aggiunto un riconoscimento TA1 allo scambio. Quando lo scambio viene ricevuto, WebSphere Partner Gateway invia il TA1 indietro al mittente (TP1). Il TA1 viene inviato in una busta conforme al profilo busta EnvProf1.

Aggiunta di una mappa FA

In questa sezione, viene descritto come aggiungere un riconoscimento funzionale standard (997) al flusso descritto in " Esempio da EDI a ROD" a pagina 319. Il riconoscimento funzionale fornisce una conferma al mittente che la transazione è stata ricevuta.

Nota: questo esempio è simile a " Aggiunta di un TA1 allo scambio" a pagina 325. Tuttavia, non è direttamente correlato a quell'esempio. Invece, viene creato sulle attività eseguite in " Esempio da EDI a ROD" a pagina 319.

WebSphere Partner Gateway è costituito da una serie di nomi di mappe di notifica funzionale che iniziano con $DT_FA. Ciò è seguito dal nome del messaggio di riconoscimento funzionale e la versione e la release del messaggio. Ad esempio, la versione 2 della release 4 del messaggio di riconoscimento funzionale 997 viene denominata $DT_997V2R4. Per un elenco delle mappe fornito con WebSphere Partner Gateway, consultare la sezione "Impostazione dei riconoscimenti" a pagina 208.

Creazione delle associazioni

Informazioni su questa attività

Per associare la mappa ad una definizione del documento, effettuare la seguente procedura:

1. Fare clic su **Amministrazione hub > Configurazione hub > Mappe > Mappe RF EDI**.

   Viene visualizzata la mappa &DT_FA997V2R4.
2. Fare clic sull'icona **Visualizza dettagli** accanto alla mappa.

   Si visualizzano le informazioni sulla mappa nonché una cartella per ciascun tipo di package disponibile sul sistema.
3. Creare l'associazione alla definizione del documento effettuando la seguente procedura:
   a. Selezionare la casella di spunta accanto a **Package: N/A** ed espandere la cartella.
   b. Selezionare la casella di spunta accanto a **Protocollo: X12V5R1**, quindi espandere la cartella.
   c. Selezionare la casella posta accanto a **Tipo documento: 850**.
   d. Fare clic su **Salva**.

Questa mappa di notifica funzionale 997 è stata associata al protocollo X12.

Creazione delle interazioni

Informazioni su questa attività

Creazione di un'interazione che rappresenta la notifica 997.

1. Fare clic su **Amministrazione hub > Configurazione hub> Definizione documento**.
2. Fare clic su **Crea interazione**.
3. In **Origine**, espandere **Package: N/A** e **Protocollo: &DT99724** e selezionare **Tipo documento: 997**.
4. In **Destinazione**, espandere **Package: N/A** e **Protocollo: &DT99724** e selezionare **Tipo documento: 997**.
5. Nell'elenco Azione, selezionare **Pass Through**.

6. Fare clic su **Salva**.

Creare un'interazione che rappresenta la busta.

1. Fare clic su **Amministrazione hub > Configurazione hub> Definizione documento**.
2. Fare clic su **Crea interazione**.
3. Espandere **Package: N/A** e **Protocollo: EDI-X12** e selezionare **Tipo documento: ISA**.
4. Espandere **Package: Nessuno** e **Protocollo: EDI-X12** e selezionare **Tipo documento: ISA**.
5. Nell'elenco Azione, selezionare **Pass Through**.
6. Fare clic su **Salva**.

Abilitazione delle capacità B2B

Informazioni su questa attività

Quindi, aggiungere le interazioni create di recente alle capacità B2B dei partner.

1. Fare clic su **Amministrazione account > Profili > Partner** e su **Cerca**.
2. Fare clic sull'icona **Visualizza dettagli** per il partner di origine per questo esempio (**Gestore**).

   Nota: il riconoscimento funzionale passa dal partner che riceve il documento ROD al partner che lo invia. In questo esempio, il Gestore è l'origine del riconoscimento funzionale ed TP1 del partner è la destinazione.
3. Fare clic su **Capacità B2B**.
4. Abilitare due gruppi di capacità per il partner di origine.
   a. Abilitare le capacità per RF.
      1) Fare clic sull'icona **Il ruolo non è attivo** in **Imposta origine** per **Package: N/A** per abilitarlo.
      2) Espandere **Package: N/A**.
      3) Fare clic sull'icona **Il ruolo non è attivo** sotto **Imposta origine** per **Protocollo: &DT99724**.
      4) Espandere **Protocollo: &DT99724**.
      5) Fare clic sull'icona **Il ruolo non è attivo** in **Imposta origine** per **Tipo documento: 997 (ALL)**.
   b. In seguito, abilitare le capacità per la busta:
      1) Fare clic sull'icona **Il ruolo non è attivo** in **Imposta origine** per **Package: N/A** per abilitarlo.
      2) Espandere **Package: N/A**.
      3) Fare clic sull'icona **Il ruolo non è attivo** sotto **Imposta origine** per **Protocollo: EDI-X12**.
      4) Espandere **Protocollo: EDI-X12 (ALL)**.
      5) Fare clic sull'icona **Il ruolo non è attivo** di **Imposta origine** per **Tipo documento: ISA (ALL)**.
5. Fare clic su **Amministrazione account > Profili > Partner** e su **Cerca**.
6. Fare clic sull'icona **Visualizza dettagli** per il partner di destinazione per questo esempio (**TP1**).
7. Fare clic su **Capacità B2B**.
8. Abilitare due gruppi di capacità per il partner di destinazione.

a. Abilitare la definizione del documento che rappresenta 997:
   1) Fare clic sull'icona **Il ruolo non è attivo** in **Imposta destinazione** per **Package: N/A** per abilitarlo.
   2) Espandere **Package: N/A**.
   3) Fare clic sull'icona **Il ruolo non è attivo** sotto **Imposta destinazione** per **Protocollo: &DT99724 (ALL)**.
   4) Espandere **Protocollo: &DT99724 (ALL)**.
   5) Fare clic sull'icona **Il ruolo non è attivo** in **Imposta destinazione** per **Tipo documento: 997 (ALL)**.

b. Quindi, abilitare la definizione del documento che rappresenta la busta EDI:
   1) Fare clic sull'icona **Il ruolo non è attivo** sotto **Imposta Destinazione** per **Package: Nessuno** in modo da abilitarlo.
   2) Espandere **Package: Nessuno**.
   3) Fare clic sull'icona **Il ruolo non è attivo** sotto **Imposta destinazione** per **Protocollo: EDI-X12 (ALL)** .
   4) Espandere **Protocollo: EDI-X12 (ALL)**.
   5) Fare clic sull'icona **Il ruolo non è attivo** in **Imposta destinazione** per **Tipo documento: ISA(ALL)**.

Creazione del profilo busta

Informazioni su questa attività

Si crea, in seguito, il profilo busta che contiene il 997: Un riconoscimento funzionale, come una transazione, deve essere sottoposto a enveloping prima che possa essere inviato.

1. Fare clic su **Amministrazione hub > Configurazione hub > EDI > Profilo busta**.
2. Fare clic su **Crea**.
3. Immettere il nome del profilo: **EnvProf1**.
4. Nell'elenco degli standard EDI, selezionare **X12**.
5. Il pulsante **Generale** è stato selezionato per impostazione predefinita. Immettere i seguenti valori per gli attributi generali di busta:
   - INTCTLLEN: **9**
   - GRPCTLLEN: **9**
   - TRXCTLLEN: **9**
   - MAXDOCS: **1000**
6. Fare clic su pulsante **Scambio** e digitare i seguenti valori per gli attributi dello scambio:
   - ISA01: **01**
   - ISA02: **ISA0000002**
   - ISA03: **02**
   - ISA04: **ISA0000004**
   - ISA11: \
   - ISA12: **00501**
   - ISA15: **T**
7. Fare clic su **Salva**.

Attivazione delle connessioni del partner
Informazioni su questa attività

Per attivare le connessioni:

1. Fare clic su **Amministrazione account > Connessioni**.
2. Selezionare **Gestore** dall'elenco Origine.
3. Selezionare **TP1** dall'elenco Destinazione.
4. Fare clic su **Cerca**.
5. Fare clic su **Attiva** per la connessione che rappresenta il riconoscimento funzionale 997:

Tabella 38. Connessione riconoscimento funzionale

Origine	Destinazione
Package: N/A (N/A) Protocollo: &DT99724 (ALL) Tipo documento: 997 (ALL)	Package: N/A (N/A) Protocollo: &DT99724 (ALL) Tipo documento: 997 (ALL)

6. Fare clic su **Attiva** per la connessione che rappresenta la busta EDI inviata nuovamente al creatore dello scambio:

Tabella 39. Connessione busta

Origine	Destinazione
Package: N/A (N/A) Protocollo: EDI-X12 (ALL) Tipo documento: ISA (ALL)	Package: Nessuno (N/A) Protocollo: EDI-X12 (ALL) Tipo documento: ISA (ALL)

Configurazione di attributi
Informazioni su questa attività

In primo luogo, si specifica la mappa FA da utilizzare:

1. Fare clic su **Amministrazione account > Profili > Partner** e su **Cerca**.
2. Selezionare **TP1** dall'elenco.
3. Fare clic su **Capacità B2B**.
4. Fare clic sull'icona **Espandi** accanto a **Package: N/A**.
5. Fare clic sull'icona **Modifica** accanto a **Protocollo: X12V5R1 (ALL)**.
6. Nella riga Mappa FA, selezionare **&DT_FA997V2R4**.
7. Fare clic di nuovo su **Capacità B2B**.
8. Fare clic sull'icona **Espandi** accanto a **Package: N/A**.
9. Fare clic su **Modifica** accanto a **Protocollo: &DT99724 (ALL)**.
10. Specificare i seguenti attributi:
    a. Nella riga Profilo busta, selezionare **EnvProf1** dall'elenco.
    b. Nella riga Qualificatore scambio, selezionare **01**.
    c. Nella riga Identificativo scambio, selezionare **000000001**.
    d. Nella riga Indicatore utilizzo scambio, selezionare **T**.
11. Fare clic su **Salva**.

In questa serie di attività, è stato aggiunto il riconoscimento funzionale EDI-X12 997 allo scambio, cosicché quando il partner interno riceve il documento, invia di nuovo il 997 al mittente (TP1). Il 997 viene inviato in una busta conforme al profilo busta EnvProf1.

Esempio da EDI a XML

In questa sezione viene fornito un esempio di invio di una transazione EDI (all'interno di una busta) all'hub, in cui viene convertita in un documento XML e inviata al partner interno.

In questo esempio, si presume che lo specialista della mappatura Data Interchange Services abbia creato una mappa di conversione che utilizza una transazione EDI 879 standard (definita con il dizionario X12V5R1, corrispondente alla versione 5010 di X12) e la converte in un documento XML che verrà elaborato dall'applicazione di back-end del partner interno. In questo esempio, la mappa viene denominata S_DT_EDI_TO_XML.eif.

Lo specialista della mappatura Data Interchange Services può esportare la mappa di conversione direttamente nel database WebSphere Partner Gateway. In alternativa, lo specialista della mappatura Data Interchange Services può inviare il file, nel qual caso si utilizza l'utilità bcgDISImport per l'importazione in WebSphere Partner Gateway. In questa appendice, si presume il secondo scenario.

Importazione della mappa di conversione

Informazioni su questa attività

In questa sezione, vengono descritti i passaggi per importare una mappa di conversione che utilizzerà l'input EDI e lo convertirà nel formato XML. Nel processo di importazione della mappa di conversione, si importa anche la definizione del documento associato alla mappa.

Prima che sia possibile importare la mappa di conversione, lo specialista della mappatura Data Interchange Services deve inviarla all'utente. Questo insieme di passaggi tiene conto che il file S_DT_EDI_TO_XML.eif si trovi sul sistema.

1. Aprire la finestra dei comandi.
2. Immettere il seguente comando o script:
   - In un sistema UNIX:

     ```
     <DirProdotto>/bin/bcgDISImport.sh <database_user_ID>
      <password> S_DT_EDI_TO_XML.eif
     ```

   - In un sistema Windows:

     ```
     <DirProdotto>\bin\bcgDISImport.bat <database_user_ID>
      <password> S_DT_EDI_TO_XML.eif
     ```

     dove *<database_user_ID>* e *<password>* corrispondono ai valori utilizzati al momento dell'installazione del database come parte dell'installazione di WebSphere Partner Gateway.

Verifica delle definizioni documenti e della mappa di conversione

Informazioni su questa attività

Per verificare se le mappe di conversione e le definizioni documenti importate sono disponibili nella Console comunità, procedere nel modo seguente:

1. Fare clic su **Amministrazione hub > Configurazione hub > Mappe > Mappe di conversione**.

   Viene visualizzata la mappa S_DT_EDI_TO_XML.
2. Fare clic sull'icona **Visualizza dettagli** accanto alla mappa.

Sono visualizzate le definizioni documenti a cui è associata questa mappa:

Tabella 40. Definizione documento associata alla mappa

Origine	Destinazione
Package: N/A Protocollo: X12V5R1Tipo documento: 879 (ALL)	Package: Nessuno Protocollo: FVT-XML-TEST (ALL) Tipo documento: WWRE_ITEMCREATIONINTERNAL (ALL)

La mappa S_DT_EDI_TO_XML è stata definita per utilizzare una transazione X12 879 (conforme allo standard X12V5R1) e la converte in un protocollo personalizzato.

Configurazione di un destinatario

Informazioni su questa attività

In questa sezione, viene creato un destinatario di directory del file-system per l'hub:

1. Fare clic su **Amministrazione hub > Configurazione hub > Destinatari** e fare clic su **Crea destinatario**.
2. Per Nome destinatari, inserire: **EDIFileTarget**
3. Dall'Elenco dei trasporti, selezionare **Directory file**.
4. Per Percorso root, digitare: **/Data/Manager/editarget**
5. Fare clic su **Salva**.

Il partner invia lo scambio EDI a questo destinatario.

Creazione delle interazioni

Informazioni su questa attività

Si creano due interazioni, una per la busta EDI e l'altra per la transazione nella busta EDI.

Creare un'interazione che rappresenta la busta EDI.

1. Fare clic su **Amministrazione hub > Configurazione hub > Definizione documento** > **Crea interazione**.
2. Espandere **Package: Nessuno** e **Protocollo: EDI-X12** e selezionare **Tipo documento: ISA**.
3. Espandere **Package: N/A** e **Protocollo: EDI-X12** e selezionare **Tipo documento: ISA.**
4. Nell'elenco Azione, selezionare **Deenveloping di EDI**.

   Nota: in questa interazione, non si verifica alcuna conversione. Lo scambio EDI è in fase di deenveloping, dando come risultato una singola transazione (879). Di conseguenza, non è necessaria una mappa di conversione per questa transazione.
5. Fare clic su **Salva**.

Creare un'interazione che abbia un'origine che rappresenti la transazione 879 ed una destinazione che rappresenti il documento convertito.

1. Fare clic su **Amministrazione hub > Configurazione hub> Definizione documento**.

2. Fare clic su **Crea interazione**.
3. Espandere **Package: N/A** e **Protocollo: X12V5R1** e selezionare **Tipo documento: 879**.
4. Espandere **Package: Nessuno** e **Protocollo: FVT-XML-TEST** e selezionare **Tipo documento: WWRE_ITEMCREATIONINTERNAL**.
5. Nell'elenco delle mappe di conversione, selezionare **S_DT_EDI_TO_XML**.
6. Nell'elenco delle azioni, selezionare **Convalida EDI e conversione EDI**.
7. Fare clic su **Salva**.

Questa interazione rappresenta la conversione di una transazione EDI X12 879 standard in un formato differente e, di conseguenza, è necessario selezionare una mappa di conversione.

Creazione di partner

Informazioni su questa attività

In questo esempio, sono disponibili due partner: il partner interno (Gestore) e un partner esterno (TP1).

Creare il profilo del Partner interno:

1. Fare clic su **Amministrazione account > Profili > Partner** e fare clic su **Crea**.
2. Per Nome accesso azienda, immettere: **Gestcom**
3. Per Nome visualizzato partner: immettere **Gestore**
4. Per Tipo di partner, selezionare **Partner interno**.
5. Fare clic su **Nuovo** per l'ID di business e immettere `000000000` come ID di figura a mano libera.

   Nota: è necessario selezionare Figura a mano libera e non DUNS.
6. Fare di nuovo clic su **Nuovo** per l'ID di business, quindi immettere `01-000000000` come ID di figura a mano libera.
7. Fare clic su **Salva**.

Creare il secondo partner:

1. Fare clic su **Amministrazione account > Profili > Partner** e fare clic su **Crea**.
2. Per Nome accesso azienda, digitare: **TP1**
3. Per Nome visualizzato partner, immettere **TP1**
4. Per Tipo di partner, selezionare **Partner esterno**.
5. Fare clic su **Nuovo** per l'ID di business e immettere `000000001` come ID di figura a mano libera.

   Nota: è necessario selezionare Figura a mano libera e non DUNS.
6. Fare di nuovo clic su **Nuovo** per l'ID di business e immettere `01-000000001` come ID di figura a mano libera.
7. Fare clic su **Salva**.

Creazione delle destinazioni

Informazioni su questa attività

Nell'esempio, creare le destinazioni di directory file per entrambi i partner. Creare una destinazione per il Gestore:

1. Fare clic su **Amministrazione account > Profili > Partner** e su **Cerca**.
2. Fare clic sull'icona **Visualizza dettagli** accanto al profilo Gestore.
3. Fare clic su **Destinazioni** e poi su **Crea**.
4. Immettere i seguenti valori per la destinazione. È necessario che la directory di file (l'intero percorso) sia già presente sul file system.
   a. Per Nome, inserire **ManagerFileDestination**.
   b. Nell'elenco dei trasporti, selezionare **Directory file**.
   c. Per Indirizzo, inserire: **file://Data/Manager/filedestination**
   d. Fare clic su **Salva**.
5. Fare clic su **Elenco** per elencare tutte le destinazioni per il partner interno.
6. Fare clic su **Visualizza destinazioni predefinite**.
7. Nell'elenco **Produzione**, selezionare la destinazione creata nella fase 4.
8. Fare clic su **Salva**.

Quindi, creare una destinazione per il partner.

1. Fare clic su **Amministrazione account > Profili > Partner** e su **Cerca**.
2. Selezionare l'altro partner creato per questo esempio facendo clic sull'icona **Visualizza dettagli**, posta accanto a **TP1**.
3. Fare clic su **Destinazioni** e poi su **Crea**.
4. Immettere i seguenti valori per la destinazione. La directory file (l'intero percorso) deve già esistere.
   a. Per Nome, inserire **TP1FileDestination**.
   b. Dall'Elenco dei trasporti, selezionare **Directory file**.
   c. Per Indirizzo, inserire: **file://Data/TP1/filedestination**
   d. Fare clic su **Salva**.
5. Fare clic su **Elenco** per elencare tutte le destinazioni del partner.
6. Fare clic su **Visualizza destinazioni predefinite**.
7. Nell'elenco **Produzione**, selezionare la destinazione creata nella fase 4.
8. Fare clic su **Salva**.

Impostazione delle capacità B2B

Informazioni su questa attività

Abilitare le capacità B2B dei due partner di questo scambio. In questo esempio, lo scambio EDI è stato creato con un partner esterno (TP1) e sarà distribuito al partner interno.

1. Fare clic su **Amministrazione account > Profili > Partner** e su **Cerca**.
2. Fare clic sull'icona **Visualizza dettagli** per il partner di origine per questo esempio (**TP1**).
3. Fare clic su **Capacità B2B**.
4. Abilitare due gruppi di capacità per il partner di origine.
   a. Abilitare la definizione del documento che rappresenta la busta EDI:
      1) Fare clic sull'icona **Il ruolo non è attivo** in **Imposta origine** per **Package: Nessuno** in modo da abilitarlo.
      2) Espandere **Package: Nessuno**.
      3) Fare clic sull'icona **Il ruolo non è attivo** sotto **Imposta origine** per **Protocollo EDI-X12 (ALL)**.

4) Espandere **Protocollo: EDI-X12 (ALL)**
5) Fare clic sull'icona **Il ruolo non è attivo** di **Imposta origine** per **Tipo documento: ISA (ALL)**.

b. Quindi, abilitare la definizione del documento che rappresenta la transazione:
1) Fare clic sull'icona **Il ruolo non è attivo** in **Imposta origine** per **Package: N/A** per abilitarlo.
2) Espandere **Package: N/A**.
3) Fare clic sull'icona **Il ruolo non è attivo** sotto **Imposta origine** per **Protocollo: X12V5R1 (ALL)** .
4) Espandere **Protocollo: X12V5R1 (ALL)**.
5) Fare clic sull'icona **Il ruolo non è attivo** in **Imposta origine** per **Tipo documento: 879**.

5. Fare clic su **Amministrazione account > Profili > Partner** e su **Cerca**.
6. Fare clic sull'icona **Visualizza dettagli** per il partner di destinazione per questo esempio (**Gestore**).
7. Fare clic su **Capacità B2B**.
8. Abilitare due gruppi di capacità per il partner di destinazione.
a. Abilitare la definizione del documento:
1) Fare clic sull'icona **Il ruolo non è attivo** in **Imposta destinazione** per **Package: N/A** per abilitarlo.
2) Espandere **Package: N/A**.
3) Fare clic sull'icona **Il ruolo non è attivo** sotto **Imposta destinazione** per **Protocollo: EDI-X12 (ALL)** .
4) Espandere **Protocollo: EDI-X12 (ALL)**.
5) Fare clic sull'icona **Il ruolo non è attivo** di **Imposta destinazione** per **Tipo documento: ISA (ALL)**.

b. Quindi, abilitare la definizione del documento che rappresenta il documento convertito:
1) Fare clic sull'icona **Il ruolo non è attivo** sotto **Imposta Destinazione** per **Package: Nessuno** in modo da abilitarlo.
2) Espandere **Package: Nessuno**.
3) Fare clic sull'icona **Il ruolo non è attivo** sotto **Imposta destinazione** per **Protocollo: FVT-XML-TEST (ALL)** .
4) Espandere **Protocollo: FVT-XML-TEST (ALL)**.
5) Fare clic sull'icona **Il ruolo non è attivo** in **Imposta destinazione** per **Tipo documento: WWRE_ITEMCREATIONINTERNAL(ALL)**.

Attivazione delle connessioni

Informazioni su questa attività

Per attivare le connessioni:

1. Fare clic su **Amministrazione account > Connessioni**.
2. Selezionare **TP1** dall'elenco Origine.
3. Selezionare **Gestore** dall'elenco Destinazione.
4. Fare clic su **Cerca**.

5. Fare clic su **Attiva** per la connessione che rappresenta la busta:

Tabella 41. Connessione busta

Origine	Destinazione
Package: Nessuno (N/A) Protocollo: EDI-X12 (ALL) Tipo documento: ISA (ALL)	Package: N/A (N/A) Protocollo: EDI-X12 (ALL) Tipo documento: ISA (ALL)

6. Fare clic su **Attiva** per la connessione che rappresenta la transazione 879 per il documento convertito:

Tabella 42. Transazione EDI per la connessione del documento XML

Origine	Destinazione
Package: N/A (N/A) Protocollo: X12V5R1 (ALL)Tipo documento: 879 (ALL)	Package: Nessuno (N/A) Protocollo: FVT-XML-TEST (ALL) Tipo documento: WWRE_ITEMCREATIONINTERNAL (ALL)

Quindi, se TP1 inviasse uno scambio EDI che contiene una transazione 879 al partner interno, lo scambio EDI verrebbe sottoposto a deenveloping, determinando così una transazione 879. Quindi, la transazione 879 deve essere convertita e il documento convertito deve essere inviato alla destinazione del partner interno.

Esempio da XML a EDI

Questa sezione fornisce un esempio del partner interno che invia un documento XML all'hub, dove viene convertito in una transazione EDI, sottoposto a enveloping in uno scambio EDI ed inviato ad un partner.

In questo esempio, supporre che lo specialista della mappatura Data Interchange Services abbia creato una mappa di conversione che utilizza un documento XML e la converte in una transazione EDI 850 standard (definita con il dizionario MX12V3R1) che sarà elaborata dal partner. In questo esempio, la mappa viene denominata S_DT_XML_TO_EDI.eif.

Lo specialista della mappatura Data Interchange Services può esportare la mappa di conversione direttamente nel database WebSphere Partner Gateway. In alternativa, lo specialista della mappatura Data Interchange Services può inviare il file, nel qual caso si utilizza l'utilità bcgDISImport per l'importazione in WebSphere Partner Gateway. In questa appendice, si presume il secondo scenario.

Importazione della mappa di conversione

Informazioni su questa attività

In questa sezione, vengono descritti i passaggi per importare una mappa di conversione che utilizzerà l'input XML e la si convertirà in una transazione EDI. Nel processo di importazione della mappa di conversione, si importa anche la definizione del documento associato alla mappa.

Prima che sia possibile importare la mappa di conversione, lo specialista della mappatura Data Interchange Services deve inviarla all'utente. Questo insieme di passaggi tiene conto che il file S_DT_XML_TO_EDI.eif si trovi sul sistema.

1. Aprire la finestra dei comandi.
2. Immettere il seguente comando o script:

- In un sistema UNIX:

  ```
  <DirProdotto>/bin/bcgDISImport.sh <database_user_ID>
   <password> S_DT_XML_TO_EDI.eif
  ```

- In un sistema Windows:

  ```
  <DirProdotto>\bin\bcgDISImport.bat <database_user_ID>
   <password> S_DT_XML_TO_EDI.eif
  ```

  dove *<database_user_ID>* e *<password>* corrispondono ai valori utilizzati al momento dell'installazione del database come parte dell'installazione di WebSphere Partner Gateway.

Verifica delle definizioni documenti e della mappa di conversione

Informazioni su questa attività

Per verificare se le mappe di conversione e le definizioni documenti importate sono disponibili nella Console comunità, procedere nel modo seguente:

1. Fare clic su **Amministrazione hub > Configurazione hub > Mappe > Mappe di conversione**.

   Viene visualizzata la mappa S_DT_XML_TO_EDI.
2. Fare clic sull'icona **Visualizza dettagli** accanto alla mappa.

   Sono visualizzate le definizioni documenti a cui è associata questa mappa:

Tabella 43. Definizioni documento associate alla mappa

Origine	Destinazione
Package: Nessuno Protocollo: FVT-XML-TEST (ALL) Tipo documento: ICGCPO (ALL)	Package: N/A Protocollo: MX12V3R1 (ALL) Tipo documento: 850 (ALL)

La mappa S_DT_XML_TO_EDI è stata definita per utilizzare un documento XML e convertirlo in transazione EDI.

Configurazione di un destinatario

Informazioni su questa attività

In questa sezione, viene creato un destinatario di directory del file-system per l'hub:

1. Fare clic su **Amministrazione hub > Configurazione hub > Destinatari** e fare clic su **Crea destinatario**.
2. Per Nome destinatari, immettere: **XMLFileTarget**
3. Dall'Elenco dei trasporti, selezionare **Directory file**.
4. Per Percorso root, digitare: **/Data/Manager/xmltarget**
5. Nell'elenco Punto di configurazione, selezionare **Preelaborazione**.
6. Selezionare **com.ibm.bcg.edi.receiver.preprocesshandler.XMLSplitterHandler** dall'Elenco disponibile e fare clic su **Aggiungi** per spostarlo nell'Elenco configurato.
7. Fare clic su **Salva**.

Il partner interno invia il documento XML a questo destinatario.

Creazione delle interazioni

Informazioni su questa attività

Creare due interazioni - una per la conversione da XML a EDI e una per la busta EDI.

Creare un'interazione che disponga di un'origine che rappresenta il documento XML e una destinazione che rappresenta la transazione 850 convertita.

1. Fare clic su **Amministrazione hub > Configurazione hub> Definizione documento**.
2. Fare clic su **Crea interazione**.
3. Espandere **Package: Nessuno** e **Protocollo: FVT-XML-TEST** e selezionare **Tipo documento: ICGCPO**.
4. Espandere **Package: N/A** e **Protocollo: MX12V3R1** e selezionare **Tipo documento: 850**.
5. Nell'elenco delle mappe di conversione, selezionare **S_DT_XML_TO_EDI**.
6. Nell'elenco Azione, selezionare **Convalida EDI e conversione XML**.
7. Fare clic su **Salva**.

Questa interazione rappresenta la conversione di un documento XML in transazione EDI e, di conseguenza, è necessario selezionare una mappa di conversione.

Creare un'interazione che rappresenta la busta EDI.

1. Fare clic su **Amministrazione hub > Configurazione hub> Definizione documento**.
2. Fare clic su **Crea interazione**.
3. Espandere **Package: N/A** e **Protocollo: EDI-X12** e selezionare **Tipo documento: ISA**.
4. Espandere **Package: Nessuno** e **Protocollo: EDI-X12** e selezionare **Tipo documento: ISA.**
5. Nell'elenco Azione, selezionare **Pass Through**.

   Nota: in questa interazione, non si verifica alcuna conversione.
6. Fare clic su **Salva**.

Creazione di partner

Informazioni su questa attività

In questo esempio, sono disponibili due partner: il partner interno (Gestore) e un partner esterno (TP1).

Creare il profilo del Partner interno:

1. Fare clic su **Amministrazione account > Profili > Partner** e fare clic su **Crea**.
2. Per Nome accesso azienda, immettere: **Gestcom**
3. Per Nome visualizzato partner, immettere: **Gestore**.
4. Per Tipo di partner, selezionare **Partner interno**.
5. Fare clic su **Nuovo** per l'ID di business e immettere `000000000` come ID di figura a mano libera.

Nota: è necessario selezionare Figura a mano libera e non DUNS.

6. Fare di nuovo clic su **Nuovo** per l'ID di business, quindi immettere `01-000000000` come ID in forma libera.
7. Fare clic su **Salva**.

Creare il secondo partner:

1. Fare clic su **Amministrazione account > Profili > Partner** e fare clic su **Crea**.
2. Per Nome accesso azienda, digitare: **TP1**
3. Per Nome visualizzato partner, immettere **TP1**
4. Per Tipo di partner, selezionare **Partner esterno**.
5. Fare clic su **Nuovo** per l'ID di business e immettere `000000001` come ID di figura a mano libera.

   Nota: è necessario selezionare Figura a mano libera e non DUNS.
6. Fare di nuovo clic su **Nuovo** per l'ID di business, quindi immettere `01-000000001` come ID in forma libera.
7. Fare clic su **Salva**.

Creazione delle destinazioni

Informazioni su questa attività

Nell'esempio, creare le destinazioni di directory file per entrambi i partner. Creare una destinazione per il Gestore:

1. Fare clic su **Amministrazione account > Profili > Partner** e su **Cerca**.
2. Fare clic sull'icona **Visualizza dettagli** accanto al profilo Gestore.
3. Fare clic su **Destinazioni** e poi su **Crea**.
4. Immettere i seguenti valori per la destinazione. È necessario che la directory di file (l'intero percorso) sia già presente sul file system.
   a. Per Nome, inserire **ManagerFileDestination**.
   b. Nell'elenco dei trasporti, selezionare **Directory file**.
   c. Per Indirizzo, inserire: **file://Data/Manager/filedestination**
   d. Fare clic su **Salva**.
5. Fare clic su **Elenco** per elencare tutte le destinazioni per il partner interno.
6. Fare clic su **Visualizza destinazioni predefinite**.
7. Nell'elenco **Produzione**, selezionare la destinazione creata nella fase 4.
8. Fare clic su **Salva**.

Quindi, creare una destinazione per il partner.

1. Fare clic su **Amministrazione account > Profili > Partner** e su **Cerca**.
2. Selezionare l'altro partner creato per questo esempio facendo clic sull'icona **Visualizza dettagli**, posta accanto a **TP1**.
3. Fare clic su **Destinazioni** e poi su **Crea**.
4. Immettere i seguenti valori per la destinazione. La directory file (l'intero percorso) deve già esistere.
   a. Per Nome, inserire **TP1FileDestination**.
   b. Dall'Elenco dei trasporti, selezionare **Directory file**.
   c. Per Indirizzo, inserire: **file://Data/TP1/filedestination**
   d. Fare clic su **Salva**.

5. Fare clic su **Elenco** per elencare tutte le destinazioni del partner.
6. Fare clic su **Visualizza destinazioni predefinite**.
7. Nell'elenco **Produzione**, selezionare la destinazione creata nella fase 4 a pagina 341.
8. Fare clic su **Salva**.

Impostazione delle capacità B2B

Informazioni su questa attività

Abilitare le capacità B2B dei due partner di questo scambio. In questo esempio, il documento XML è stato creato dal partner interno e sarà distribuito al partner esterno.

1. Fare clic su **Amministrazione account > Profili > Partner** e su **Cerca**.
2. Fare clic sull'icona **Visualizza dettagli** per il partner di origine per questo esempio (**ComMan**).
3. Fare clic su **Capacità B2B**.
4. Abilitare tre gruppi di capacità per il partner di origine.
   a. Abilitare la definizione del documento che rappresenta il documento XML:
      1) Fare clic sull'icona **Il ruolo non è attivo** in **Imposta origine** per **Package: Nessuno** in modo da abilitarlo.
      2) Espandere **Package: Nessuno**.
      3) Fare clic sull'icona **Il ruolo non è attivo** in **Imposta origine** per **Protocollo: FVT-XML-TEST (ALL)**.
      4) Espandere **Protocollo: FVT-XML-TEST (ALL)**.
      5) Fare clic sull'icona **Il ruolo non è attivo** in **Imposta origine** per **Tipo documento: ICGCPO (ALL)**.
   b. Quindi, abilitare la definizione del documento che rappresenta il documento convertito:
      1) Fare clic sull'icona **Il ruolo non è attivo** in **Imposta origine** per **Package: N/A** per abilitarlo.
      2) Espandere **Package: N/A**.
      3) Fare clic sull'icona **Il ruolo non è attivo** sotto **Imposta origine** per **Protocollo: MX12V3R1 (ALL)** .
      4) Espandere **Protocollo: MX12V3R1 (ALL)**.
      5) Fare clic sull'icona **Il ruolo non è attivo** di **Imposta origine** per **Tipo documento: 850**.
   c. Quindi, abilitare la definizione del documento che rappresenta la busta EDI:
      1) Fare clic sull'icona **Il ruolo non è attivo** in **Imposta origine** per **Package: N/A** per abilitarlo.
      2) Espandere **Package: N/A**.
      3) Fare clic sull'icona **Il ruolo non è attivo** sotto **Imposta origine** per **Protocollo EDI-X12 (ALL)**.
      4) Espandere **Protocollo: EDI-X12 (ALL)**
      5) Fare clic sull'icona **Il ruolo non è attivo** di **Imposta origine** per **Tipo documento: ISA (ALL)**.
5. Fare clic su **Amministrazione account > Profili > Partner** e su **Cerca**.
6. Fare clic sull'icona **Visualizza dettagli** per il partner di destinazione per questo esempio (**TP1**).

7. Fare clic su **Capacità B2B**.
8. Abilitare due gruppi di capacità per il partner di destinazione.
   a. Abilitare la definizione del documento che rappresenta la transazione EDI 850:
      1) Fare clic sull'icona **Il ruolo non è attivo** in **Imposta destinazione** per **Package: N/A** per abilitarlo.
      2) Espandere **Package: N/A**.
      3) Fare clic sull'icona **Il ruolo non è attivo** sotto **Imposta destinazione** per **Protocollo: MX12V3R1 (ALL)** .
      4) Espandere **Protocollo: MX12V3R1 (ALL)**.
      5) Fare clic sull'icona **Il ruolo non è attivo** in **Imposta destinazione** per **Tipo documento: 850 (ALL)**.
   b. Quindi, abilitare la definizione del documento:
      1) Fare clic sull'icona **Il ruolo non è attivo** sotto **Imposta Destinazione** per **Package: Nessuno** in modo da abilitarlo.
      2) Espandere **Package: Nessuno**.
      3) Fare clic sull'icona **Il ruolo non è attivo** sotto **Imposta destinazione** per **Protocollo: EDI-X12 (ALL)** .
      4) Espandere **Protocollo: EDI-X12 (ALL)**.
      5) Fare clic sull'icona **Il ruolo non è attivo** in **Imposta destinazione** per **Tipo documento: ISA(ALL)**.

Creazione del profilo busta

Informazioni su questa attività

Si crea, in seguito, il profilo busta che contiene la transazione 850 convertita:

1. Fare clic su **Amministrazione hub > Configurazione hub > EDI > Profilo busta**.
2. Fare clic su **Crea**.
3. Immettere il nome del profilo: **EnvProf1**.
4. Nell'elenco degli standard EDI, selezionare **X12**.
5. Il pulsante **Generale** è stato selezionato per impostazione predefinita. Immettere i seguenti valori per gli attributi generali di busta:
   - INTCTLLEN: **9**
   - GRPCTLLEN: **9**
   - TRXCTLLEN: **9**
   - MAXDOCS: **1000**
6. Fare clic su pulsante **Scambio** e digitare i seguenti valori per gli attributi dello scambio:
   - ISA01: **01**
   - ISA02: **ISA0000002**
   - ISA03: **02**
   - ISA04: **ISA0000004**
   - ISA11: **U**
   - ISA12: **00301**
   - ISA15: **T**
7. Fare clic su **Salva**.

Creazione del formato XML

Informazioni su questa attività

In questa sezione, si crea il formato XML personalizzato.

1. Fare clic su **Amministrazione hub > Configurazione hub > Formati XML**.
2. Fare clic su **Crea formato XML**.
3. Per Formato di instradamento, selezionare **FVT-XML-TEST ALL**.
4. Per Tipo di file, selezionare **XML**.
5. Per Tipo di identificativo, selezionare **Tag root** e digitare **MMDoc**.
6. Per ID di business di origine, selezionare **Costante** e digitare **000000000**.
7. Per ID di business di destinazione, selezionare **Costante** e digitare **000000001**.
8. Per Tipo di documento di origine, selezionare **Costante** e inserire **ICGCPO**.
9. Per Versione del tipo di documento di origine, selezionare **Costante** e inserire **ALL**.
10. Fare clic su **Salva**.

Attivazione delle connessioni

Informazioni su questa attività

Attivare le connessioni del partner:

1. Fare clic su **Amministrazione account > Connessioni**.
2. Selezionare **Gestore** dall'elenco Origine.
3. Selezionare **TP1** dall'elenco Destinazione.
4. Fare clic su **Cerca**.
5. Fare clic su **Attiva** per la seguente connessione:

Tabella 44. Connessione documento XML in transazione EDI

Origine	Destinazione
Package: Nessuno (N/A) Protocollo: FVT-XML-TEST (ALL) Tipo documento: ICGCPO (ALL)	Package: N/A (N/A) Protocollo: MX12V3R1 (ALL) Tipo documento: 850 (ALL)

6. Fare clic su **Attiva** per la connessione che rappresenta la busta EDI:

Tabella 45. Connessione busta EDI

Origine	Destinazione
Package: N/A (N/A) Protocollo: EDI-X12 (ALL) Tipo documento: ISA (ALL)	Package: Nessuno (N/A) Protocollo: EDI-X12 (ALL) Tipo documento: ISA (ALL)

Configurazione di attributi

Informazioni su questa attività

Configurare gli attributi Capacità B2B del partner di destinazione (TP1) e del partner di origine (Gestore):

1. Fare clic su **Amministrazione account > Profili > Partner** e su **Cerca**.
2. Fare clic sull'icona **Visualizza dettagli** accanto a **TPI** per selezionarla.
3. Fare clic su **Capacità B2B**.
4. Fare clic sull'icona **Espandi** accanto a **Package: N/A**.

5. Fare clic sull'icona **Modifica** accanto a **Protocollo: MX12V3R1**.
6. Specificare i seguenti attributi:
   a. Nella riga Profilo busta, selezionare **EnvProf1** dall'elenco.
   b. Nella riga Qualificatore scambio, selezionare **01**.
   c. Nella riga Identificativo scambio, selezionare **000000001**.
   d. Nella riga Indicatore utilizzo scambio, selezionare **T**.
7. Fare clic su **Salva**.
8. Fare clic su **Amministrazione account > Profili > Partner** e su **Cerca**.
9. Fare clic sull'icona Visualizza i dettagli accanto a **Gestore** per selezionarla.
10. Fare clic su **Capacità B2B**.
11. Fare clic sull'icona **Espandi** accanto a **Package: N/A**.
12. Fare clic sull'icona **Modifica** accanto a **Protocollo: MX12V3R1 (ALL)**.
13. Specificare i seguenti attributi:
    a. Nella riga Qualificatore scambio, selezionare **01**.
    b. Nella riga Identificativo scambio, selezionare **000000000**.
    c. Nella riga Indicatore utilizzo scambio, selezionare **T**.
14. Fare clic su **Salva**.

Quindi, se il partner di origine (il partner interno) ha inviato un documento XML al partner, esso verrà convertito (sull'hub) in una transazione EDI, sottoposto a enveloping e inviato alla destinazione del partner.

Esempio da ROD a EDI

Questa sezione fornisce un esempio del partner interno che invia un documento ROD all'hub, dove viene convertito in una transazione EDI, sottoposto a enveloping in uno scambio EDI e inviato ad un partner.

In questo esempio, si presume che lo specialista della mappatura Data Interchange Services abbia creato una mappa di conversione che utilizza un documento ROD (record-oriented document) e lo converte in una transazione EDI 850 standard (definita con il dizionario X12V5R1, corrispondente alla versione 5010 di X12) che sarà elaborata dal partner. In questo esempio, la mappa viene denominata S_DT_ROD_TO_EDI.eif.

Lo specialista della mappatura Data Interchange Services può esportare la mappa di conversione direttamente nel database WebSphere Partner Gateway. In alternativa, lo specialista della mappatura Data Interchange Services può inviare il file, nel qual caso si utilizza l'utilità bcgDISImport per l'importazione in WebSphere Partner Gateway. In questa appendice, si presume il secondo scenario.

Importazione della mappa di conversione

Informazioni su questa attività

In questa sezione, vengono descritti i passaggi per importare una mappa di conversione che utilizzerà l'input ROD e lo convertirà in una transazione X12. Nel processo di importazione della mappa di conversione, si importa anche la definizione del documento associato alla mappa.

Prima che sia possibile importare la mappa di conversione, lo specialista della mappatura Data Interchange Services deve inviarla all'utente. Questo insieme di passaggi tiene conto che il file S_DT_ROD_TO_EDI.eif si trovi sul sistema.

1. Aprire la finestra dei comandi.
2. Immettere il seguente comando o script:
   - In un sistema UNIX:

     ```
     <DirProdotto>/bin/bcgDISImport.sh <database_user_ID>
      <password> S_DT_ROD_TO_EDI.eif
     ```

   - In un sistema Windows:

     ```
     <DirProdotto>\bin\bcgDISImport.bat <database_user_ID>
      <password> S_DT_ROD_TO_EDI.eif
     ```

     dove *<database_user_ID>* e *<password>* corrispondono ai valori utilizzati al momento dell'installazione del database come parte dell'installazione di WebSphere Partner Gateway.

Verifica delle definizioni documenti e della mappa di conversione

Informazioni su questa attività

Per verificare se le mappe di conversione e le definizioni documenti importate sono disponibili nella Console comunità, procedere nel modo seguente:

1. Fare clic su **Amministrazione hub > Configurazione hub > Mappe > Mappe di conversione**.

   Viene visualizzata la mappa The S_DT_ROD_TO_EDI.
2. Fare clic sull'icona **Visualizza dettagli** accanto alla mappa.

   Sono visualizzate le definizioni documenti a cui è associata questa mappa:

Tabella 46. Definizioni documento associate alla mappa

Origine	Destinazione
Package: Nessuno Protocollo: ROD-TO-EDI_DICT (ALL) Tipo documento: DTROD-TO-EDI_ROD (ALL)	Package: N/A Protocollo: X12V5R1(ALL) Tipo documento: 850 (ALL)

La mappa S_DT_ROD_TO_EDI è stata definita per utilizzare un documento ROD associato al dizionario ROD-TO-EDI_DICT e convertirlo in una transazione X12 850 conforme allo standard X12V5R1.

Configurazione di un destinatario

Informazioni su questa attività

In questa sezione, viene creato un destinatario di directory del file-system per l'hub:

1. Fare clic su **Amministrazione hub > Configurazione hub > Destinatari** e fare clic su **Crea destinatario**.
2. Per Nome destinatari, inserire: **RODFileTarget**
3. Dall'Elenco dei trasporti, selezionare **Directory file**.
4. Per Percorso root, digitare: **/Data/Manager/rodtarget**
5. Nell'elenco Punto di configurazione, selezionare **Preelaborazione**.

6. Selezionare **com.ibm.bcg.edi.receiver.preprocesshandler.RODSplitterHandler** nell'Elenco disponibile e fare clic su **Aggiungi** per spostarlo nell'Elenco configurato.
7. Selezionare **com.ibm.bcg.edi.receiver.preprocesshandler.RODSplitterHandler** nell'Elenco configurati e fare clic su **Configura**.
8. Aggiungere i valori mostrati nella tabella:

Tabella 47. Attributi handler splitter ROD

Campo	Valore
From Packaging Name	Nessuno
From Packaging Version	N/A
From Protocol Name	ROD-TO-EDI_DICT
From Protocol Version	ALL
From Process Code	DTROD-TO-EDI_ROD
From Process Version	ALL
METADICTIONARY	ROD-TO-EDI_DICT
METADOCUMENT	DTROD-TO-EDI_ROD
METASYNTAX	rod
ENCODING	ascii
BCG_BATCHDOCS	ON

9. Fare clic su **Imposta valori**.
10. Fare clic su **Salva**.

Il partner interno invia il documento ROD a questa destinazione.

Creazione delle interazioni

Informazioni su questa attività

Si creano due interazioni, una per la busta EDI che verrà inviata dall'hub e l'altra per la conversione del documento ROD in EDI.

Creare un'interazione che abbia un'origine che rappresenti il documento ROD ed una destinazione che rappresenti il documento X12.

1. Fare clic su **Amministrazione hub > Configurazione hub> Definizione documento**.
2. Fare clic su **Crea interazione**.
3. Espandere **Package: Nessuno** e **Protocollo: ROD-TO-EDI_DICT**, quindi selezionare **DTROD-TO-EDI_ROD**.
4. Espandere **Package: N/A** e **Protocollo: X12V5R1** e selezionare **Tipo documento: 850**.
5. Nell'elenco delle mappe di conversione, selezionare **S_DT_ROD_TO_EDI**.
6. Nell'elenco Azione, selezionare **Convalida EDI e conversione EDI**.
7. Fare clic su **Salva**.

Questa interazione rappresenta la conversione di un documento ROD in transazione X12 standard e, di conseguenza, è necessario selezionare una mappa di conversione.

Creare un'interazione che rappresenta la busta EDI.

1. Fare clic su **Amministrazione hub > Configurazione hub> Definizione documento**.
2. Fare clic su **Crea interazione**.
3. Espandere **Package: N/A** e **Protocollo: EDI-X12** e selezionare **Tipo documento: ISA**.
4. Espandere **Package: Nessuno** e **Protocollo: EDI-X12** e selezionare **Tipo documento: ISA.**
5. Nell'elenco Azione, selezionare **Pass Through**.

   Nota: in questa interazione, non si verifica alcuna conversione. Questa interazione è valida per lo scambio EDI.
6. Fare clic su **Salva**.

Creazione di partner

Informazioni su questa attività

In questo esempio, sono disponibili due partner: il partner interno (Gestore) e un partner esterno (TP1).

Creare il profilo del Partner interno:

1. Fare clic su **Amministrazione account > Profili > Partner** e fare clic su **Crea**.
2. Per Nome accesso azienda, immettere: **Gestcom**
3. Per Nome visualizzato partner: immettere **Gestore**
4. Per Tipo di partner, selezionare **Partner interno**.
5. Fare clic su **Nuovo** per l'ID di business e immettere `000000000` come ID di figura a mano libera.

   Nota: è necessario selezionare Figura a mano libera e non DUNS.
6. Fare di nuovo clic su **Nuovo** per l'ID di business e immettere `01-000000000` come ID in forma libera.
7. Fare clic su **Salva**.

Creare il secondo partner:

1. Fare clic su **Amministrazione account > Profili > Partner** e fare clic su **Crea**.
2. Per Nome accesso azienda, digitare: **TP1**
3. Per Nome visualizzato partner, immettere **TP1**
4. Per Tipo di partner, selezionare **Partner esterno**.
5. Fare clic su **Nuovo** per l'ID di business e immettere `000000001` come ID di figura a mano libera.

   Nota: è necessario selezionare Figura a mano libera e non DUNS.
6. Fare di nuovo clic su **Nuovo** per l'ID di business e immettere `01-000000001` come ID di figura a mano libera.
7. Fare clic su **Salva**.

Creazione delle destinazioni

Informazioni su questa attività

Nell'esempio, creare le destinazioni di directory file per entrambi i partner. Creare una destinazione per il Gestore:

1. Fare clic su **Amministrazione account > Profili > Partner** e su **Cerca**.
2. Fare clic sull'icona **Visualizza dettagli** accanto al profilo Gestore.
3. Fare clic su **Destinazioni** e poi su **Crea**.
4. Immettere i seguenti valori per la destinazione. È necessario che la directory di file (l'intero percorso) sia già presente sul file system.
   a. Per Nome, inserire **ManagerFileDestination**.
   b. Nell'elenco dei trasporti, selezionare **Directory file**.
   c. Per Indirizzo, inserire: **file://Data/Manager/filedestination**
   d. Fare clic su **Salva**.
5. Fare clic su **Elenco** per elencare tutte le destinazioni per il partner interno.
6. Fare clic su **Visualizza destinazioni predefinite**.
7. Dall'elenco **Produzione**, selezionare la destinazione creata nella fase 4
8. Fare clic su **Salva**.

Quindi, creare una destinazione per il partner.

1. Fare clic su **Amministrazione account > Profili > Partner** e su **Cerca**.
2. Selezionare l'altro partner creato per questo esempio facendo clic sull'icona **Visualizza dettagli**, posta accanto a **TP1**.
3. Fare clic su **Destinazioni** e poi su **Crea**.
4. Immettere i seguenti valori per la destinazione. La directory file (l'intero percorso) deve già esistere.
   a. Per Nome, inserire **TP1FileDestination**.
   b. Dall'Elenco dei trasporti, selezionare **Directory file**.
   c. Per Indirizzo, inserire: **file://Data/TP1/filedestination**
   d. Fare clic su **Salva**.
5. Fare clic su **Elenco** per elencare tutte le destinazioni del partner.
6. Fare clic su **Visualizza destinazioni predefinite**.
7. Nell'elenco **Produzione**, selezionare la destinazione creata nella fase 4.
8. Fare clic su **Salva**.

Impostazione delle capacità B2B

Informazioni su questa attività

Abilitare le capacità B2B dei due partner di questo scambio. In questo esempio, il documento ROD è stato creato dal partner interno e sarà distribuito al partner esterno (TP1).

1. Fare clic su **Amministrazione account > Profili > Partner** e su **Cerca**.
2. Fare clic sull'icona **Visualizza dettagli** per il partner di origine per questo esempio (**Gestore**).
3. Fare clic su **Capacità B2B**.
4. Abilitare due gruppi di capacità per il partner di origine.
   a. Abilitare la definizione del documento che rappresenta il documento ROD:

1) Fare clic sull'icona **Il ruolo non è attivo** in **Imposta origine** per **Package: Nessuno** in modo da abilitarlo.
2) Espandere **Package: Nessuno**.
3) Fare clic sull'icona **Il ruolo non è attivo** in **Imposta origine** per **Protocollo: ROD-TO-EDI_DICT (ALL)**.
4) Espandere **Protocollo: ROD-TO-EDI_DICT (ALL)**.
5) Fare clic sull'icona **Il ruolo non è attivo** in **Imposta origine** per **Tipo documento: DTROD-TO-EDI_ROD (ALL)**.

b. Quindi, abilitare la definizione del documento che rappresenta la busta EDI:
1) Fare clic sull'icona **Il ruolo non è attivo** in **Imposta origine** per **Package: N/A** per abilitarlo.
2) Espandere **Package: N/A**.
3) Fare clic sull'icona **Il ruolo non è attivo** sotto **Imposta origine** per **Protocollo EDI-X12 (ALL)**.
4) Espandere **Protocollo: EDI-X12 (ALL)**
5) Fare clic sull'icona **Il ruolo non è attivo** di **Imposta origine** per **Tipo documento: ISA (ALL)**.

5. Fare clic su **Amministrazione account > Profili > Partner** e su **Cerca**.
6. Fare clic sull'icona **Visualizza dettagli** per il partner di destinazione per questo esempio (**TP1**).
7. Fare clic su **Capacità B2B**.
8. Abilitare due gruppi di capacità per il partner di destinazione.
a. Abilitare la definizione del documento che rappresenta la transazione EDI 850:
1) Fare clic sull'icona **Il ruolo non è attivo** in **Imposta destinazione** per **Package: N/A** per abilitarlo.
2) Espandere **Package: N/A**.
3) Fare clic sull'icona **Il ruolo non è attivo** sotto **Imposta destinazione** per **Protocollo: X12V5R1 (ALL)**.
4) Espandere **Protocollo: X12V5R1 (ALL)**.
5) Fare clic sull'icona **Il ruolo non è attivo** in **Imposta destinazione** per **Tipo documento: 850 (ALL)**.

b. Quindi, abilitare la definizione del documento che rappresenta la busta:
1) Fare clic sull'icona **Il ruolo non è attivo** sotto **Imposta Destinazione** per **Package: Nessuno** in modo da abilitarlo.
2) Espandere **Package: Nessuno**.
3) Fare clic sull'icona **Il ruolo non è attivo** sotto **Imposta destinazione** per **Protocollo: EDI-X12 (ALL)** .
4) Espandere **Protocollo: EDI-X12 (ALL)**.
5) Fare clic sull'icona **Il ruolo non è attivo** in **Imposta destinazione** per **Tipo documento: ISA (ALL)**.

Creazione del profilo busta

Informazioni su questa attività

Si crea, in seguito, il profilo busta che contiene la transazione 850 convertita:

1. Fare clic su **Amministrazione hub > Configurazione hub > EDI > Profilo busta**.

2. Fare clic su **Crea**.
3. Immettere il nome del profilo: **EnvProf1**.
4. Nell'elenco degli standard EDI, selezionare **X12**.
5. Il pulsante **Generale** è stato selezionato per impostazione predefinita. Immettere i seguenti valori per gli attributi generali di busta:
   - INTCTLLEN: **9**
   - GRPCTLLEN: **9**
   - TRXCTLLEN: **9**
   - MAXDOCS: **1000**
6. Fare clic su pulsante **Scambio** e digitare i seguenti valori per gli attributi dello scambio:
   - ISA01: **01**
   - ISA02: **ISA0000002**
   - ISA03: **02**
   - ISA04: **ISA0000004**
   - ISA11: \
   - ISA12: **00501**
   - ISA15: **T**
7. Fare clic su **Salva**.

Attivazione delle connessioni

Informazioni su questa attività

Per attivare le connessioni:

1. Fare clic su **Amministrazione account > Connessioni**.
2. Selezionare **Gestore** dall'elenco Origine.
3. Selezionare **TP1** dall'elenco Destinazione.
4. Fare clic su **Cerca**.
5. Fare clic su **Attiva** per la connessione che rappresenta il documento ROD alla transazione EDI:

Tabella 48. Connessione ROD a EDI

Origine	Destinazione
Package: N/A (N/A) Protocollo: ROD-TO-EDI_DICT (ALL) Tipo documento: DTROD-TO-EDI_ROD (ALL)	Package: Nessuno (N/A) Protocollo: X12V5R1 (ALL) Tipo documento: 850

6. Fare clic su **Attiva** per la connessione che rappresenta la busta:

Tabella 49. Connessione busta

Origine	Destinazione
Package: Nessuno (N/A) Protocollo: EDI-X12 (ALL) Tipo documento: ISA (ALL)	Package: N/A (N/A) Protocollo: EDI-X12 (ALL) Tipo documento: ISA (ALL)

Configurazione di attributi

Informazioni su questa attività

Per specificare gli attributi per il profilo busta:

1. Fare clic su **Amministrazione account > Profili > Partner** e su **Cerca**.
2. Selezionare **TP1** dall'elenco.
3. Fare clic su **Capacità B2B**.
4. Fare clic sull'icona **Espandi** accanto a **Package: N/A**.
5. Fare clic sull'icona **Modifica** accanto a **Protocollo: X12V5R1**.
6. Specificare i seguenti attributi:
   a. Nella riga Profilo busta, selezionare **EnvProf1** dall'elenco.
   b. Nella riga Qualificatore scambio, selezionare **01**.
   c. Nella riga Identificativo scambio, selezionare **000000001**.
   d. Nella riga Indicatore utilizzo scambio, selezionare **T**.
7. Fare clic su **Salva**.

Quindi, se il partner interno ha inviato un documento ROD all'hub, il documento e lo converte in una transazione 850, che verrà quindi sottoposta a enveloping e inviata alla destinazione del partner.

Capitolo 20. Informazioni aggiuntive su RosettaNet

In questa appendice, vengono fornite le informazioni aggiuntive sul supporto RosettaNet. Sono incluse le seguenti sezioni:

- “Disattivazione PIP”
- “ Trasmissione della notifica dell’errore”
- “Creazione dei package di definizione del documento PIP” a pagina 355
- “Package di definizione del documento PIP” a pagina 367

Disattivazione PIP

Informazioni su questa attività

Dopo il caricamento di un package PIP in WebSphere Partner Gateway, è impossibile rimuoverlo. Tuttavia, è possibile disattivare il PIP in modo che non sia possibile utilizzarlo.

Per disattivare un PIP per tutte le comunicazioni con i partner, effettuare la seguente procedura:

1. Fare clic su **Amministrazione hub > Configurazione hub> Definizione documento**.
2. Espandere le definizioni del documento per rivelare il Tipo di documento del PIP che si desidera disabilitare.
3. Nella colonna Stato del package, fare clic su **Abilitato**. La colonna Stato visualizza **Disabilitato** e WebSphere Partner Gateway non è in grado di utilizzare la definizione del documento per il PIP.

Per disattivare una comunicazione PIP con un determinato partner, disattivare la connessione al partner definito per il PIP.

Trasmissione della notifica dell’errore

IP 0A1

Se si verifica un errore durante l’elaborazione del messaggio PIP, WebSphere Partner Gateway utilizza PIP 0A1 come meccanismo di trasmissione dell’errore al partner o al sistema di back-end che ha inviato il messaggio. Specificare, ad esempio, che un sistema di back-end inizia un PIP 3A4. WebSphere Partner Gateway elabora il messaggio RNSC ed invia un messaggio RosettaNet ad un partner. WebSphere Partner Gateway attende la risposta al messaggio di RosettaNet fino a quando il tempo di attesa raggiunge il limite di timeout. Una volta verificato, WebSphere Partner Gateway crea un PIP 0A1 e lo invia al partner. PIP 0A1 identifica la condizione di eccezione in modo tale che il partner possa quindi compensare l’errore del PIP 3A4.

Per fornire la notifica di errore, caricare un package 0A1 e creare una connessione PIP al partner utilizzando questo package.

Aggiornamento delle informazioni sul contatto

Per modificare le informazioni di contatto di RosettaNet con il PIP 0A1, è necessario modificare il file BCG.Properties, posizionato nella directory *<DirProdotto>*/router/lib/config.

Questi campi popolano le informazioni di contatto nel PIP 0A1. Il fax è facoltativo (il valore può essere vuoto), ma il resto è obbligatorio.

- **bcg.0A1.fromContactName**
- **bcg.0A1.fromEMailAddr**
- **bcg.0A1.fromPhoneNbr**
- **bcg.0A1.fromFaxNbr**

I numeri di telefono sono limitati a 30 byte in lunghezza. Gli altri campi non sono limitati in lunghezza. Quando i valori vengono modificati, è necessario riavviare Gestore documenti.

Modifica dei Valori dell'attributo RosettaNet

Informazioni su questa attività

Per il supporto RosettaNet, una definizione del documento del tipo di azione ha una serie specifica di attributi. Questi attributi forniscono le informazioni utilizzate per convalidare i messaggi PIP, per definire i ruoli e i servizi utilizzati in PIP e per definire la risposta all'azione. I package PIP forniti da WebSphere Partner Gateway definiscono automaticamente i valori per gli attributi che solitamente non è necessario modificare.

Per modificare gli attributi RosettaNet di una definizione del documento di azione, effettuare la seguente procedura:

1. Fare clic su **Amministrazione hub > Configurazione hub > Definizione documento.**
2. Fare clic sull'icona **Espandi** per espandere singolarmente un nodo al livello di definizione del documento appropriato o selezionare **Tutti** per espandere l'intera struttura ad albero.
3. La colonna Azioni per ogni azione contiene l'icona **Modifica i valori dell'attributo di RosettaNet** degli attributi RosettaNet. Fare clic sull'icona per modificare gli attributi RosettaNet dell'azione. Console comunità visualizza un elenco di attributi definiti negli attributi RosettaNet.
4. Completare i seguenti parametri in Attributi RosettaNet. (Questi attributi sono definiti automaticamente quando un PIP viene caricato nel sistema).

Tabella 50. Attributi RosettaNet

Attributo RosettaNet	Descrizione
Nome DTD	Identifica il nome dell'azione del PIP nel DTD fornito da RosettaNet
Dal servizio	Contiene il nome del servizio del componente di rete del partner o del sistema di back-end che invia il messaggio
Al servizio	Contiene il nome del servizio del componente di rete del partner o sistema di back-end che riceve il messaggio
Dal ruolo	Contiene il nome del ruolo del partner o del sistema di back-end che invia il messaggio

Tabella 50. Attributi RosettaNet (Continua)

Attributo RosettaNet	Descrizione
Al ruolo	Contiene il nome del ruolo del partner o del sistema di backend che riceve il messaggio
Tag root	Contiene il nome dell'elemento root nel documento XML associato al XML
Risposta da nome azione	Identifica l'Azione successiva da effettuare nel PIP

Nota: se la Console visualizza il messaggio `Non sono stati trovati attributi`, gli attributi non sono stati definiti.

5. Se la Console visualizza questo messaggio per una definizione di livello inferiore, la definizione può ancora funzionare dato che eredita gli attributi della definizione di livello superiore. L'aggiunta di attributi e i relativi valori sovrascrivono gli attributi ereditati e modificano la funzione della definizione del documento.
6. Fare clic su **Salva**.

Creazione dei package di definizione del documento PIP

Informazioni su questa attività

Poiché RosettaNet aggiunge PIP di volta in volta, potrebbe essere necessario creare i package PIP per supportare questi nuovi PIP o per supportare gli aggiornamenti nei PIP. Eccetto quando indicato, le procedure di questa sezione descrivono il modo in cui creare il package di definizione del documento PIP per PIP 5C4 V01.03.00. WebSphere Partner Gateway fornisce un package di definizione del documento PIP per PIP 5C4 V01.02.00. Le procedure, quindi, documentano come eseguire l'aggiornamento. Tuttavia, la creazione di un package di definizione del documento PIP è simile e le procedure identificano eventuali fasi aggiuntive.

Prima di iniziare, scaricare le specifiche PIP da www.rosettanet.org per la nuova versione e se si effettua un aggiornamento, per la versione precedente. Se, ad esempio, si effettua l'aggiornamento descritto nelle procedure, scaricare 5C4_DistributeRegistrationStatus_V01_03_00.zip e 5C4_DistributeRegistrationStatus_V01_02_00.zip. La specifica include i seguenti tipi di file:

- Direttive del messaggio XML RosettaNet - File HTML, quali ad esempio 5C4_MG_V01_03_00_RegistrationStatusNotification.htm, che definiscono la cardinalità, il vocabolario e la struttura, nonché i valori degli elementi dati consentiti e i tipi di valori del PIP.
- Schema dei messaggi XML RosettaNet - File DTD, quali ad esempio 5C4_MS_V01_03_RegistrationStatusNotification.dtd, che definiscono l'ordine o la sequenza, la denominazione degli elementi, la composizione e gli attributi del PIP.
- Specifica PIP - il file DOC come 5C4_Spec_V01_03_00.doc che fornisce i comandi delle prestazioni di business per PIP.
- Note di release PIP - File DOC, quale ad esempio 5C4_V01_03_00_ReleaseNotes.doc, che descrive la differenza tra questa versione e quella precedente.

La creazione o l'aggiornamento di un package di definizione del documento PIP richiama le seguenti procedure:

- Creazione dei file XSD
- Creazione del file XML
- Creazione dei package

Creazione dei file XSD

Informazioni su questa attività

Un package di definizione del documento PIP contiene i file dello schema XML che definiscono i formati del messaggio ed i valori consentiti per gli elementi. La seguente procedura descrive in che modo creare questi file in base ai contenuti del file delle specifiche PIP.

Si crea almeno un file XSD per ogni file DTD nel file delle specifiche PIP. Per l'esempio di aggiornamento in PIP 5C4 V01.03.00, dato che il formato del messaggio è cambiato, la procedura descrive in che modo creare il file BCG_5C4RegistrationStatusNotification_V01.03.xsd come esempio. Per informazioni sui file XSD, vedere "Informazioni sulla convalida" a pagina 365.

Per creare i file XSD per il package di definizione del documento PIP, effettuare la seguente procedura:

1. Importare o caricare il file DTD nell'editor XML come WebSphere Studio Application Developer. Ad esempio, caricare il file 5C4_MS_V01_03_RegistrationStatusNotification.dtd.
2. Utilizzo dell'editor XML, convertire il DTD in uno schema XML. Le seguenti procedure descrivono in che modo fare ciò utilizzando Application Developer:
   a. Nella schermata di Navigazione del possibile XML, aprire il progetto che contiene il file DTD.
   b. Fare clic con il pulsante destro del mouse sul file DTD e selezionare **Genera > schema XML**.
   c. Nella schermata generale, digitare o selezionare dove salvare il nuovo file XSD. Nel campo Nome file, immettere il nome del nuovo file XSD. Nel caso dell'esempio, è preferibile immettere un nome come BCG_5C4RegistrationStatusNotification_V01.03.xsd.
   d. Fare clic su **Fine**.
3. Compensare per gli elementi che presentano valori di cardinalità multipli nelle indicazioni XML di RosettaNet aggiungendo le specifiche al nuovo file XSD. Le indicazioni mostrano gli elementi nel messaggio utilizzando un albero e visualizzando la cardinalità di ogni elemento alla sinistra dell'elemento.

   In generale, gli elementi nelle indicazioni corrispondono alle definizioni degli elementi nel file DTD. Tuttavia, le indicazioni potrebbero contenere alcuni elementi che presentano gli stessi nomi, ma diverse cardinalità. Dato che il DTD non può fornire la cardinalità in questo caso, è necessario modificare l'XSD. Ad esempio, il file delle indicazioni 5C4_MG_V01_03_00_RegistrationStatusNotification.htm presenta una definizione per ContactInformation online 15 che presenta cinque elementi child con le seguenti cardinalità:

   1 contactName

   0..1 EmailAddress

   0..1 facsimileNumber

   0..1 PhysicalLocation

   0..1 telephoneNumber

La definizione di ContactInformation sulla riga 150 presenta quattro elementi child con le seguenti cardinalità:

1 contactName

1 EmailAddress

0..1 facsimileNumber

1 telephoneNumber

Nel file XSD, tuttavia, ogni elemento child di ContactInformation presenta una cardinalità che è conforme ad entrambe le definizioni:

```
<xsd:element name="ContactInformation">
  <xsd:complexType>
    <xsd:sequence>
      <xsd:element ref="contactName"/>
      <xsd:element maxOccurs="1" minOccurs="0" ref="EmailAddress"/>
      <xsd:element maxOccurs="1" minOccurs="0" ref="facsimileNumber"/>
      <xsd:element maxOccurs="1" minOccurs="0" ref="PhysicalLocation"/>
      <xsd:element maxOccurs="1" minOccurs="0" ref="telephoneNumber"/>
    </xsd:sequence>
  </xsd:complexType>
</xsd:element>
```

Se si aggiorna il package di definizione del documento PIP in base ad un'altra versione del package e si desidera riutilizzare una definizione dell'altra versione, effettuare la seguente procedura per ognuna di queste definizioni:

a. Eliminare la definizione dell'elemento. Ad esempio, eliminare l'elemento di Contact Information.

b. Aprire il package di definizione del documento PIP della versione sostituita. Ad esempio, aprire il file BCG_Package_RNIFV02.00_5C4V01.02.zip.

c. Trovare la definizione che si desidera riutilizzare. Ad esempio, la definizione ContactInformation_type7 nel file BCG_ContactInformation_Types.xsd corrisponde alla definizione necessaria per la riga 15 delle indicazioni.

```
<xsd:complexType name="ContactInformation_type7">
  <xsd:sequence>
    <xsd:element name="contactName" type="common_FreeFormText_R"/>
    <xsd:element name="EmailAddress" type="common_EmailAddres_R"
        minOccurs="0"/>
    <xsd:element name="facsimileNumber"
        type="common_CommunicationsNumber_R" minOccurs="0"/>
    <xsd:element name="PhysicalLocation"
        type="PhysicalLocation_type1" minOccurs="0" />
    <xsd:element name="telephoneNumber"
        type="common_CommunicationsNumber_R minOccurs="0" />
  </xsd:sequence>
</xsd:complexType>
```

d. Nel nuovo file XSD creato per il package di definizione del documento PIP aggiornato, creare un riferimento al file XSD che contiene la definizione che si desidera riutilizzare. Ad esempio, creare un riferimento a BCG_ContactInformation_Types.xsd nel file BCG_5C4RegistrationStatusNotification_V01.03.xsd nel seguente modo:

```
<xsd:include schemaLocation="BCG_ContactInformation_Types.xsd"/>
```

e. Nel nuovo file XSD, eliminare l'attributo di rif di qualsiasi elemento che si riferisce all'elemento eliminato. Aggiungere un attributo del tipo che si riferisce alla definizione che si sta riutilizzando. Ad esempio, nell'elemento productProviderFieldApplicationEngineer, eliminare *ref="Informazioni di contatto"* ed aggiungere le seguenti informazioni:

```
nome="ContactInformation"
 tipo="ContactInformation_type7"
```

Se si crea o si aggiorna un package di definizione del documento PIP e la definizione richiesta non esiste nell'altra versione, effettuare la seguente procedura per ciascuna istanza dell'elemento, rilevato nelle istruzioni:

a. Eliminare la definizione dell'elemento. Ad esempio, eliminare l'elemento di Contact Information.

b. Creare la definizione di sostituzione. Ad esempio, creare la definizione ContactInformation_localType1 per farla corrispondere alla definizione nella riga 15 delle indicazioni.

```
<xsd:complexType name="ContactInformation_localType1">
  <xsd:sequence>
    <xsd:element ref="contactName"/>
    <xsd:element maxOccurs="1" minOccurs="0" ref="EmailAddress"/>
    <xsd:element maxOccurs="1" minOccurs="0"
        ref="facsimileNumber"/>
    <xsd:element maxOccurs="1" minOccurs="0"
        ref="PhysicalLocation"/>
    <xsd:element maxOccurs="1" minOccurs="0"
        ref="telephoneNumber"/>
  </xsd:sequence>
</xsd:complexType>
```

c. Per gli eventuali elementi che si riferiscono all'elemento eliminato, eliminare l'attributo di rif e aggiungere un attributo del tipo che si riferisce al tipo complesso appropriato nella procedura precedente. Ad esempio, nell'elemento productProviderFieldApplicationEngineer, eliminare *ref="Informazioni di contatto"* ed aggiungere le seguenti informazioni:

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

In Figura 35 viene mostrato l'elemento productProviderFieldApplicationEngineer prima che venga modificato.

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

Figura 35. Elemento productProviderFieldApplicationEngineer prima della modifica

In Figura 36 viene mostrato l'elemento productProviderFieldApplicationEngineer ù dopo che viene modificato.

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

Figura 36. Elemento productProviderFieldApplicationEngineer dopo la modifica

4. Specificare i valori di enumerazione per gli elementi che possono avere solo valori specifici. Le indicazioni definiscono i valori di enumerazione nelle tabelle nella sezione Informazioni sulle indicazioni.

   Ad esempio, in un messaggio PIP 5C4 V01.03.00, GlobalRegistrationComplexityLevelCode può avere solo i seguenti valori: Superiore alla media, Medio, Massimo, Minimo, Nessuno e Alcuni.

Se si aggiorna il package di definizione del documento PIP in base ad un'altra versione del package e si desidera riutilizzare una serie di valori di enumerazione dell'altra versione, effettuare la seguente procedura per ogni serie:

a. Eliminare la definizione per l'elemento. Ad esempio, eliminare l'elemento GlobalRegistrationComplexityLevelCode:
b. Aprire il package di definizione del documento PIP della versione sostituita. Ad esempio, aprire il file BCG_Package_RNIFV02.00_5C4V01.02.zip.
c. Trovare la definizione che contiene i valori di enumerazione che si desidera riutilizzare. Ad esempio, la definizione _GlobalRegistrationComplexityLevelCode nel file BCG_GlobalRegistrationComplexityLevelCode.xsd contiene le definizioni del valore di enumerazione definite dalla tabella Istanza entità.

```
<xsd:simpleType name="_GlobalRegistrationComplexityLevelCode">
  <xsd:restriction base="xsd:string">
    <xsd:enumeration value="Above average"/>
    <xsd:enumeration value="Average"/>
    <xsd:enumeration value="Maximum"/>
    <xsd:enumeration value="Minimum"/>
    <xsd:enumeration value="None"/>
    <xsd:enumeration value="Some"/>
  </xsd:restriction>
</xsd:simpleType>
```

d. Nel nuovo file XSD creato per il package di definizione del documento PIP aggiornato, creare un riferimento al file XSD che contiene la definizione che si desidera riutilizzare. Ad esempio, creare un riferimento in BCG_GlobalRegistrationComplexityLevelCode.xsd e nel file BCG_5C4RegistrationStatusNotification_V01.03.xsd nel seguente modo:

```
<xsd:include schemaLocation=
    "BCG_GlobalRegistrationComplexityLevelCode_Types.xsd" />
```

e. Nel nuovo file XSD, eliminare l'attributo di rif di qualsiasi elemento che si riferisce all'elemento eliminato. Aggiungere un attributo del tipo che si riferisce alla definizione che si sta riutilizzando. Ad esempio, nell'elemento DesignAssemblyInformation, eliminare *ref*="GlobalRegistrationComplexityLevelCode" e aggiungere le seguenti informazioni:

```
name="GlobalRegistrationComplexityLevelCode"
type="_GlobalRegistrationComplexityLevelCode"
```

Se si crea o si aggiorna un package di definizione del documento PIP e le definizioni del valore di enumerazione richieste non esistono nell'altra versione, effettuare la seguente procedura per qualsiasi elemento con i valori enumerati nelle istruzioni:

a. Eliminare la definizione dell'elemento. Ad esempio, eliminare l'elemento GlobalRegistrationComplexityLevelCode.
b. Creare la definizione di sostituzione. Ad esempio, creare la definizione GlobalRegistrationComplexityLevelCode_localType ed includere le definizioni del valore di enumerazione come descritto dalla tabella.

```
<xsd:simpleType
    name="GlobalRegistrationComplexityLevelCode_localType">
  <xsd:restriction base="xsd:string">
    <xsd:enumeration value="Above average"/>
    <xsd:enumeration value="Average"/>
    <xsd:enumeration value="Maximum"/>
    <xsd:enumeration value="Minimum"/>
```

```
          <xsd:enumeration value="None"/>
          <xsd:enumeration value="Some"/>
        </xsd:restriction>
      </xsd:simpleType>
```

c. Per gli eventuali elementi che si riferiscono all'elemento eliminato, eliminare l'attributo di rif e aggiungere un attributo del tipo che si riferisce al tipo complesso appropriato nella procedura precedente. Ad esempio, eliminare *ref="GlobalRegistrationComplexityLevelCode"* e aggiungere le seguenti informazioni:

```
name="GlobalRegistrationComplexityLevelCode"
type="GlobalRegistrationComplexityLevelCode_localType"
```

In Figura 37 viene mostrato l'elemento Element prima che venga modificato.

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

Figura 37. Elemento DesignAssemblyInformation prima della modifica

In Figura 38 a pagina 361 viene mostrato l'elemento Element dopo che viene modificato.

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

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

Figura 38. Elemento DesignAssemblyInformation dopo la modifica

5. Impostare il tipo di dati, la lunghezza minima, la lunghezza massima e la rappresentazione delle entità dei dati. Le Direttive del messaggio XML RosettaNet forniscono queste informazioni nella tabella Entità dei dati di business fondamentali:

   Se si aggiorna il package di definizione del documento PIP in base all'altra versione del package e si desidera riutilizzare una definizione di entità dati dell'altra versione, effettuare la seguente procedura per ciascuna serie:

   a. Eliminare la definizione per l'elemento di entità dei dati. Ad esempio, eliminare l'elemento Data e ora.
   b. Aprire il package di definizione del documento PIP della versione sostituita. Ad esempio, aprire il file BCG_Package_RNIFV02.00_5C4V01.02.zip.
   c. Trovare la definizione che si desidera riutilizzare. Ad esempio, il file _common_DateStamp_R nel file BCG_common.xsd contiene la seguente definizione, conforme con le informazioni fornite nelle indicazioni.

      ```
      <xsd:simpleType name="_common_DateStamp_R">
        <xsd:restriction base="xsd:string">
          <xsd:pattern value="[0-9]{8}Z" />
        </xsd:restriction>
      </xsd:simpleType>
      ```

   d. Nel nuovo file XSD creato per il package di definizione del documento PIP aggiornato, creare un riferimento al file XSD che contiene la definizione che si desidera riutilizzare. Ad esempio, creare un riferimento in BCG_common.xsd nel file BCG_5C4RegistrationStatusNotification_V01.03.xsd come segue:

      ```
      <xsd:include schemaLocation="BCG_common.xsd" />
      ```

   e. Nel nuovo file XSD, eliminare l'attributo di rif di qualsiasi elemento che si riferisce all'elemento eliminato. Aggiungere un attributo del tipo che si riferisce alla definizione che si sta riutilizzando. Ad esempio, nell'elemento DesignAssemblyInformation, eliminare *ref*="DateStamp" ed aggiungere le seguenti informazioni:

      ```
      name="DateStamp" type="_common_DateStamp_R"
      ```

Se si crea o si aggiorna un package di definizione del documento PIP e la definizione di entità dati richiesta non esiste nell'altra versione, effettuare la seguente procedura per ogni elemento di entità dati:

a. Eliminare la definizione dell'elemento. Ad esempio, eliminare l'elemento Data e ora.
b. Creare la definizione di sostituzione. Ad esempio, utilizzare il tipo di dati, la lunghezza minima, la lunghezza massima e le informazioni di rappresentazione per creare la definizione DateStamp_localType.

```
<xsd:simpleType name="DateStamp_localType">
  <xsd:restriction base="xsd:string">
    <xsd:pattern value="[0-9]{8}Z" />
  </xsd:restriction>
</xsd:simpleType>
```

c. Per gli eventuali elementi che si riferiscono all'elemento eliminato, eliminare l'attributo di rif e aggiungere un attributo del tipo che si riferisce al tipo complesso appropriato nella procedura precedente. Ad esempio, eliminare *ref="DateStamp"* ed aggiungere le seguenti informazioni:

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

In Figura 39 viene mostrato l'elemento Element beginDate prima che venga modificato.

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

Figura 39. Elemento data di inizio prima della modifica

In Figura 40 viene mostrato l'elemento Element beginDate dopo che viene modificato.

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

Figura 40. Elemento data di inizio dopo la modifica

Creazione di un file XML

Informazioni su questa attività

Una volta creati i file XSD per il package di definizione del documento PIP, è possibile creare il file XML per il package RNIF e il file XML per il package Integrazione backend. Ad esempio, questi package vengono denominati BCG_Package_RNIFV02.00_5C4V01.03.zip e BCG_Package_RNSC1.0_RNIFV02.00_5C4V01.03.zip. La seguente procedura descrive in che modo creare il file XML per il package RNIF:

1. Estrarre il file XML da un file del package di definizione del documento PIP RNIF. Se si sta effettuando l'aggiornamento, estrarre il file dalla versione precedente del package (ad esempio BCG_Package_RNIFV02.00_5C4V01.02.zip). Se si crea un nuovo package, estrarre il file da un package di definizione del

documento PIP ch è simile a quello che si sta creando. Ad esempio, se si sta creando un package per supportare un PIP di due azioni, copiare il file XML da un altro package PIP di due azioni.

2. Copiare il file e ridenominarlo in modo appropriato (ad esempio, BCG_RNIFV02.00_5C4V01.03.xml).
3. Nel nuovo file, aggiornare gli elementi che contengono le informazione sul PIP. Ad esempio, la seguente tabella elenca le informazione necessarie da aggiornare nell'esempio 5C4 PIP. Si noti che le informazioni potrebbero apparire più di una volta nel file. Assicurarsi di aggiornare tutte le istanze.

Tabella 51. Informazioni di aggiornamento 5C4 PIP

Informazioni da modificare	**Valore vecchio**	**Valore nuovo**
ID PIP	5C4	5C4
Versione del PIP	V01.02	V01.03
Il nome del file DTD del messaggio di richiesta senza l'estensione del file	5C4_MS_V01_02_ RegistrationStatusNotification	5C4_MS_V01_03_ RegistrationStatusNotification
Il nome del file DTD del messaggio di conferma senza l'estensione del file (solo per i PIP di due azioni)	N/A	N/A
Il nome del file XSD del messaggio di richiesta senza l'estensione del file	BCG_5C4RegistrationStatus Notification_V01.02	BCG_5C4RegistrationStatus Notification_V01.03
Il nome del file XSD del messaggio di conferma senza l'estensione del file (solo per i PIP di due azioni)	N/A	N/A
Il nome dell'elemento root nel file XSD per il messaggio di richiesta	Pip5C4RegistrationStatus Notification	Pip5C4RegistrationStatus Notification
Il nome dell'elemento root nel file XSD per il messaggio di conferma (per i PIP di due azioni solo)	N/A	N/A

4. Aprire il documento della specifica PIP e utilizzarlo per aggiornare le informazioni elencate nella seguente tabella. Se si sta effettuando un aggiornamento, confrontare le specifiche per le versioni poiché questi valori potrebbero non dover essere aggiornati.

Tabella 52. Le informazioni di aggiornamento 5C4 PIP dalla specifica PIP

Informazioni da aggiornare	**Descrizione**	**Valore nel package 5C4**
Nome attività	Specificato nella Tabella 3-2	Stato di registrazione di distribuzione

Tabella 52. Le informazioni di aggiornamento 5C4 PIP dalla specifica PIP (Continua)

Informazioni da aggiornare	Descrizione	Valore nel package 5C4
Nome del ruolo di iniziatore	Specificato nella Tabella 3-1	Fornitore del prodotto
Nome del ruolo del risponditore	Specificato nella Tabella 3-1	Creatore della domanda
Nome azione della richiesta	Specificato nella Tabella 4-2	Notifica dello stato di registrazione
Nome azione di conferma	Specificato nella Tabella 4-2 (solo per i PIP di due azioni)	N/A

5. Aggiornare i valori dell'attributo del package. Se si sta effettuando un aggiornamento, confrontare le specifiche per le versioni poiché questi valori potrebbero non dover essere aggiornati.

   Nota: se si crea il package Integrazione backend, ignorare questa fase e andare al passo 6 a pagina 365.

Tabella 53. Aggiornamenti dell'attributo 5C4 PIP

Informazioni da aggiornare	Descrizione	Valore nel package 5C4	Percorso dell'elemento nel file XML
NonRepudiation Required	Specificato nella Tabella 3-3	N	ns1:Package ns1:Protocol ns1:Process ns1:Attribute (Its ATTRIBUTEKEY is NonRepudiationRequired) ns1:AttributeValue AttributePickListItem ATTRVALUEKEY
NonRepudiationOf Receipt	Specificato nella Tabella 3-3	N	ns1:Package ns1:Protocol ns1:Process ns1:Attribute (Its ATTRIBUTEKEY is NonRepudiationOfReceipt) ns1:AttributeValue AttributePickListItem ATTRVALUEKEY
DigitalSignature Required	Specificato nella Tabella 5-1	Y	ns1:Package ns1:Protocol ns1:Process ns1:Attribute (Its ATTRIBUTEKEY is DigitalSignatureRequired) ns1:AttributeValue AttributePickListItem ATTRVALUEKEY
TimeToAcknowledge	Specificato nella Tabella 3-3	2 (120 min)	ns1:Package ns1:Protocol ns1:Process ns1:Attribute (Its ATTRIBUTEKEY is TimeToAcknowledge) ns1:AttributeValue ATTRVALUE
TimeToPerform	Specificato nella Tabella 3-3	2 (120 min)	ns1:Package ns1:Protocol ns1:Process ns1:Attribute (Its ATTRIBUTEKEY is TimeToPerform) ns1:AttributeValue ATTRVALUE
RetryCount	Specificato nella Tabella 3-3	3	ns1:Package ns1:Protocol ns1:Process ns1:Attribute (Its ATTRIBUTEKEY is RetryCount) ns1:AttributeValue ATTRVALUE

6. Aggiornare gli elementi ns1:Package/ns1:Protocol/GuidelineMap per rimuovere i file XSD non utilizzati e aggiungere i file XSD creati o utilizzati come riferimento.

Per creare il package di Integrazione Backend, ripetere i passaggi compresi tra 1 a pagina 362 e 6, tranne che le seguenti differenze:

- Nel passaggio 1 a pagina 362, estrarre il file XML dal package di Integrazione Backend (ad esempio, BCG_Package_RNSC1.0_RNIFV02.00_5C4V01.02.zip).
- Non effettuare il passo 5 a pagina 364.

Dopo aver creato l'XML e i file XSD, si è pronti per creare i package del flusso di documentazione PIP.

Creazione del package

Informazioni su questa attività

Per creare il package RNIF, eseguire questi passaggi:

1. Creare una directory GuidelineMaps e copiare i file XSD del package in questa directory.
2. Creare una directory Packages e copiare il file XML RNIF in questa directory.
3. Andare alla directory parent e creare un package di definizione del documento PIP (file ZIP) che contiene le directory GuidelineMaps e Packages. È necessario conservare la struttura della directory nel file ZIP.

Per creare il package di Integrazione Backend, eseguire i passaggi compresi tra 1 e 3 ma utilizzare il file XML Integrazione Backend invece che il file RNIF.

Dopo aver creato il package PIP, è possibile caricarlo mediante la procedura descritta in "Package del tipo di documenti RNIF e PIP" a pagina 108.

Informazioni sulla convalida

WebSphere Partner Gateway convalida il contenuto del servizio di un messaggio di RosettaNet mediante le mappe di convalida. Queste mappe di convalida definiscono la struttura di un messaggio valido e definiscono la cardinalità, il formato e i valori validi (enumerazione) degli elementi nel messaggio. All'interno di ogni package di definizione del documento PIP, WebSphere Partner Gateway fornisce le mappe di convalida come file XSD nella directory GuidelineMaps.

Dato che RosettaNet specifica il formato di un messaggio PIP, generalmente non è necessario personalizzare le mappe di convalida. Tuttavia, è possibile consultare la sezione "Creazione dei package di definizione del documento PIP" a pagina 355 per le informazioni sulle fasi richieste per aggiornare i file XSD, utilizzati per convalidare i messaggi e come creare un package di definizione del documento PIP personalizzato.

Cardinalità

La cardinalità determina il numero di volte in cui un particolare elemento può o deve essere visualizzato in un messaggio. Nella mappe di convalida, gli attributi minOccurs e maxOccurs determinano la cardinalità dell'attributo come mostrato nel seguente esempio preso da BCG_5C4RegistrationStatusNotification_V01.02.xsd:

```
<xsd:element name="GeographicRegion" type="GeographicRegionType"
    minOccurs="0"/>
```

Se WebSphere Partner Gateway non deve verificare la cardinalità di un elemento, i valori degli attributi minOccurs e maxOccurs dell'elemento nella mappa di convalida sono ″0″ e ″unbounded″ rispettivamente, come mostrato nel seguente esempio:

```
<xsd:element name="DesignRegistrationIdentification"
    type="DesignRegistrationIdentificationType2"
    minOccurs="0" maxOccurs="unbounded"/>
```

Formato

Il formato determina la disposizione o il layout dei dati per il tipo di un elemento. Nelle mappe di convalida, il tipo ha una o più restrizioni come mostrato nei seguenti esempi:

Esempio 1

```
<xsd:simpleType name="_common_LineNumber_R">
  <xsd:restriction base="xsd:string">
    <xsd:minLength value="1" />
    <xsd:maxLength value="6" />
  </xsd:restriction>
</xsd:simpleType>
```

Tutti gli elementi del tipo All _common_LineNumber_R in un messaggio devono essere le stringhe e devono essere da 1 a 6 caratteri di lunghezza.

Esempio 2

```
<xsd:simpleType name="_GlobalLocationIdentifier">
  <xsd:restriction base="xsd:string">
    <xsd:pattern value="[0-9]{9}.{1,4}" />
  </xsd:restriction>
</xsd:simpleType>
```

Tutti gli elementi del tipo _GlobalLocationIdentifier in un messaggio devono essere le stringhe e devono avere nove caratteri dei dati numerici seguiti da uno a quattro caratteri di dati alfanumerici. La lunghezza minima è quindi di 10 caratteri e la massima è di 13.

Esempio 3

```
<xsd:element name="DayOfMonth">
  <xsd:simpleType>
    <xsd:restriction base="xsd:positiveInteger">
      <xsd:totalDigits value="2" />
      <xsd:minInclusive value="1" />
      <xsd:maxInclusive value="31" />
    </xsd:restriction>
  </xsd:simpleType>
</xsd:element>
```

Tutti gli elementi del tipo _DayofMonth contenuti in un messaggio devono essere interi positivi e devono avere uno o due caratteri e un valore compreso tra 1 e 31, inclusivo.

Enumerazione

L'enumerazione determina i valori validi per un elemento. Nelle mappe di convalida, il tipo di elemento ha uno o più restrizioni di enumerazione come mostrato nel seguente esempio:

```
<xsd:simpleType name="_local_GlobalDesignRegistrationNotificationCode">
  <xsd:restriction base="xsd:string">
    <xsd:enumeration value="È" />
    <xsd:enumeration value="Update" />
  </xsd:restriction>
</xsd:simpleType>
```

Tutti gli elementi del tipo _local_GlobalDesignRegistrationNotificationCode in un messaggio devono avere solo ″Initial″ o ″Update″ per i propri valori.

Package di definizione del documento PIP

Nelle sezioni successive, vengono mostrati i package di definizione del documento PIP forniti da WebSphere Partner Gateway per ogni PIP. All'interno di ogni package sono presenti un file XML contenuto in una directory Packages e diversi file XSD contenuti in una directory GuidelineMaps, che sono comuni a tutti i package di definizione del documento PIP per il PIP.

0A1 Notifica di errore V1.0

Nella seguente sezione, viene descritto il contenuto del package PIP 0A1 Notifica di errore V1.0.

Contenuto del file del package

Nella seguente tabella vengono mostrati i file ZIP e i file XML corrispondenti per il PIP 0A1 Notifica di errore V1.0. Le mappe della direttiva comune a tutte le versioni vengono mostrate nella sezione successiva.

Tabella 54. File ZIP e XML del PIP 0A1 Notifica di errore V1.0

Nome file ZIP	Nome file XML
BCG_Package_RNIF1.1_0A11.0.zip	BCG_RNIF1.1_0A11.0.xml
BCG_Package_RNSC1.0_RNIF1.1_0A11.0.zip	BCG_RNSC1.0_RNIF1.1_0A11.0.xml

Contenuto della mappa della direttiva

In questa sezione, vengono elencate le mappe della direttiva per 0A1 Notifica di errore V1.0:

- 0A1FailureNotification_1.0.xml
- BCG_0A1FailureNotification_1.0.xsd
- BCG_common.xsd
- BCG_GlobalPartnerClassificationCode.xsd
- BCG_GlobalPartnerRoleClassificationCode.xsd
- BCG_string_len_0.xsd
- BCG_xml.xsd

0A1 Notifica di errore V02.00

Nella seguente sezione, viene descritto il contenuto del package PIP 0A1 Notifica di errore V02.00.

Contenuto del file del package

Nella seguente tabella vengono mostrati i file ZIP e i file XML corrispondenti per il PIP 0A1 Notifica di errore V02.00. Le mappe della direttiva comune a tutte le versioni vengono mostrate nella sezione successiva.

Tabella 55. File ZIP e XML del PIP 0A1 Notifica di errore V02.00

Nome file ZIP	Nome file XML
BCG_Package_RNIFV02.00_0A1V02.00.zip	BCG_RNIFV02.00_0A1V02.00.xml
BCG_Package_RNSC1.0_RNIFV02.00_0A1V02.00.zip	BCG_RNSC1.0_RNIFV02.00_0A1V02.00.xml

Contenuto della mappa della direttiva

In questa sezione, vengono elencate le mappe della direttiva per 0A1 Notifica di errore V02.00:

- 0A1FailureNotification_V02.00.xml
- BCG_0A1FailureNotification_V02.00.xsd
- BCG_common.xsd
- BCG_GlobalPartnerClassificationCode.xsd
- BCG_GlobalPartnerRoleClassificationCode.xsd
- BCG_string_len_0.xsd
- BCG_xml.xsd

2A1 Distribuzione informazioni nuovo prodotto

Nella seguente sezione, viene descritto il contenuto del package PIP 2A1 Distribuzione informazioni nuovo prodotto.

Contenuto del file del package

Nella seguente tabella vengono mostrati i file ZIP e i file XML corrispondenti per il PIP 2A1 Distribuzione informazioni nuovo prodotto. Le mappe della direttiva comune a tutte le versioni vengono mostrate nella sezione successiva.

Tabella 56. File ZIP e XML di 2A1 Distribuzione informazioni nuovo prodotto

Nome file ZIP	Nome file XML
BCG_Package_RNIF1.1_2A1V02.00.zip	BCG_RNIF1.1_2A1V02.00.xml
BCG_Package_RNIFV02.00_2A1V02.00.zip	BCG_RNIFV02.00_2A1V02.00.xml
BCG_Package_RNSC1.0_RNIF1.1_2A1V02.00.zip	BCG_RNSC1.0_RNIF1.1_2A1V02.00.xml
BCG_Package_RNSC1.0_RNIFV02.00_2A1V02.00.zip	BCG_RNSC1.0_RNIFV02.00_2A1V02.00.xml

Contenuto della mappa della direttiva

In questa sezione, vengono elencate le mappe della direttiva per 2A1 Distribuzione informazioni nuovo prodotto:

- BCG_2A1ProductCatalogInformationNotification_V02.00.xsd
- BCG_BusinessDescription_Types.xsd
- BCG_BusinessDescription_Types_V422.xsd
- BCG_BusinessDescription_Types_V43.xsd
- BCG_BusinessTaxIdentifier_Types.xsd

- BCG_common.xsd
- BCG_common_V422.xsd
- BCG_common_V43.xsd
- BCG_ContactInformation_Types.xsd
- BCG_ContactInformation_Types_V422.xsd
- BCG_ContactInformation_Types_V43.xsd
- BCG_GlobalCountryCode.xsd
- BCG_GlobalCurrencyCode.xsd
- BCG_GlobalDocumentReferenceTypeCode.xsd
- BCG_GlobalIntervalCode.xsd
- BCG_GlobalLeadTimeClassificationCode_V43.xsd
- BCG_GlobalMonetaryAmountTypeCode.xsd
- BCG_GlobalPackageTypeCode_V422.xsd
- BCG_GlobalPartnerClassificationCode_V43.xsd
- BCG_GlobalPartnerRoleClassificationCode_V422.xsd
- BCG_GlobalPriceTypeCode_V43.xsd
- BCG_GlobalProductAssociationCode_V43.xsd
- BCG_GlobalProductLifeCycleStatusCode.xsd
- BCG_GlobalProductProcurementTypeCode_V43.xsd
- BCG_GlobalProductTypeCode_V43.xsd
- BCG_GlobalProductUnitofMeasureCode_V43.xsd
- BCG_GlobalProprietaryProductIdentificationTypeCode_V43.xsd
- BCG_GlobalStandardClassificationSchemeCode_V43.xsd
- BCG_GlobalWarrantyTypeCode_V43.xsd
- BCG_InvoiceChargeTypeCode_V422.xsd
- BCG_NationalExportControlClassificationCode.xsd
- BCG_PartnerDescription_Types_V43.xsd
- BCG_PhysicalAddress_Types.xsd
- BCG_PhysicalAddress_Types_V422.xsd
- BCG_string_len_0.xsd
- BCG_xml.xsd

2A12 Distribuzione master prodotto

Nella seguente sezione, viene descritto il contenuto del package PIP 2A12 Distribuzione master prodotto.

Contenuto del file del package

Nella seguente tabella vengono mostrati i file ZIP e i file XML corrispondenti al PIP 2A12 Distribuzione master prodotto. Le mappe della direttiva comune a tutte le versioni vengono mostrate nella sezione successiva.

Tabella 57. File ZIP e XML di 2A12 Distribuzione master prodotto

Nome file ZIP	Nome file XML
BCG_Package_RNIF1.1_2A12V01.03.zip	BCG_RNIF1.1_2A12V01.03.xml
BCG_Package_RNIFV02.00_2A12V01.03.zip	BCG_RNIFV02.00_2A12V01.03.xml
BCG_Package_RNSC1.0_RNIF1.1_2A12V01.03.zip	BCG_RNSC1.0_RNIF1.1_2A12V01.03.xml

Tabella 57. File ZIP e XML di 2A12 Distribuzione master prodotto (Continua)

Nome file ZIP	Nome file XML
BCG_Package_RNSC1.0_RNIFV02.00_2A12V01.03.zip	BCG_RNSC1.0_RNIFV02.00_2A12V01.03.xml

Contenuto della mappa della direttiva

In questa sezione, vengono elencate le mappe della direttiva per 2A12 Distribuzione master prodotto:

- BCG_2A12ProductMasterNotification_V01.03.xsd
- BCG_BusinessDescription_Types.xsd
- BCG_BusinessTaxIdentifier_Types.xsd
- BCG_common.xsd
- BCG_ContactInformation_Types.xsd
- BCG_GlobalAssemblyLevelCode.xsd
- BCG_GlobalCountryCode.xsd
- BCG_GlobalIntervalCode.xsd
- BCG_GlobalLeadTimeClassificationCode.xsd
- BCG_GlobalPartnerClassificationCode.xsd
- BCG_GlobalPartnerRoleClassificationCode.xsd
- BCG_GlobalProductLifeCycleStatusCode.xsd
- BCG_GlobalProductProcurementTypeCode.xsd
- BCG_GlobalProductUnitOfMeasureCode.xsd
- BCG_PartnerDescription_Types.xsd
- BCG_PhysicalAddress_Types.xsd
- BCG_string_len_0.xsd
- BCG_xml.xsd

3A1 Richiesta quotazione

Nella seguente sezione viene descritto il contenuto del package PIP 3A1 Richiesta quotazione.

Contenuto del file del package

Nella seguente tabella vengono mostrati i file ZIP e i file XML corrispondenti per il PIP 3A1 Richiesta quotazione. Le mappe della direttiva comune a tutte le versioni vengono mostrate nella sezione successiva.

Tabella 58. File ZIP e XML di 3A1 Richiesta quotazione

Nome file ZIP	Nome file XML
BCG_Package_RNIF1.1_3A1V02.00.zip	BCG_RNIF1.1_3A1V02.00.xml
BCG_Package_RNIFV02.00_3A1V02.00.zip	BCG_RNIFV02.00_3A1V02.00.xml
BCG_Package_RNSC1.0_RNIF1.1_3A1V02.00.zip	BCG_RNSC1.0_RNIF1.1_3A1V02.00.xml
BCG_Package_RNSC1.0_RNIFV02.00_3A1V02.00.zip	BCG_RNSC1.0_RNIFV02.00_3A1V02.00.xml

Contenuto della mappa della direttiva

In questa sezione, vengono elencate le mappe della direttiva per 3A1 Richiesta quotazione:

- BCG_3A1QuoteConfirmation_V02.00.xsd
- BCG_3A1QuoteRequest_V02.00.xsd
- BCG_BusinessDescription_Types.xsd
- BCG_BusinessTaxIdentifier_Types.xsd
- BCG_common.xsd
- BCG_ContactInformation_Types.xsd
- BCG_GlobalCountryCode.xsd
- BCG_GlobalCurrencyCode.xsd
- BCG_GlobalGovernmentPriorityRatingCode.xsd
- BCG_GlobalMonetaryAmountTypeCode.xsd
- BCG_GlobalPartnerClassificationCode.xsd
- BCG_GlobalPartnerRoleClassificationCode.xsd
- BCG_GlobalProductSubstitutionReasonCode.xsd
- BCG_GlobalProductTermsCode.xsd
- BCG_GlobalProductUnitOfMeasureCode.xsd
- BCG_GlobalQuoteLineItemStatusCode.xsd
- BCG_GlobalQuoteTypeCode.xsd
- BCG_GlobalStockIndicatorCode.xsd
- BCG_GlobalTaxExemptionCode.xsd
- BCG_PartnerDescription_Types.xsd
- BCG_PhysicalAddress_Types.xsd
- BCG_string_len_0.xsd
- BCG_xml.xsd

3A2 Richiesta prezzo e disponibilità

Nella seguente sezione viene descritto il contenuto del package PIP 3A2 Richiesta prezzo e disponibilità.

Contenuto del file del package

Nella seguente tabella vengono mostrati i file ZIP e i file XML corrispondenti per il PIP 3A2 Richiesta prezzo e disponibilità. Le mappe della direttiva comune a tutte le versioni vengono mostrate nella sezione successiva.

Tabella 59. File ZIP e XML di 3A2 Richiesta prezzo e disponibilità

Nome file ZIP	Nome file XML
BCG_Package_RNIF1.1_3A2R02.01.zip	BCG_RNIF1.1_3A2R02.01.xml
BCG_Package_RNIFV02.00_3A2R02.01.zip	BCG_RNIFV02.00_3A2R02.01.xml
BCG_Package_RNSC1.0_RNIF1.1_3A2R02.01.zip	BCG_RNSC1.0_RNIF1.1_3A2R02.01.xml
BCG_Package_RNSC1.0_RNIFV02.00_3A2R02.01.zip	BCG_RNSC1.0_RNIFV02.00_3A2R02.01.xml

Contenuto della mappa della direttiva

In questa sezione, vengono elencate le mappe della direttiva per 3A2 Richiesta prezzo e disponibilità:

- BCG_3A2PriceAndAvailabilityRequest_R02.01.xsd
- BCG_3A2PriceAndAvailabilityResponse_R02.01.xsd
- BCG_BusinessDescription_Types.xsd
- BCG_BusinessTaxIdentifier_Types.xsd
- BCG_common.xsd
- BCG_ContactInformation_Types.xsd
- BCG_GlobalCountryCode.xsd
- BCG_GlobalCurrencyCode.xsd
- BCG_GlobalCustomerAuthorizationCode.xsd
- BCG_GlobalPartnerClassificationCode.xsd
- BCG_GlobalPricingTypeCode.xsd
- BCG_GlobalProductAvailabilityCode.xsd
- BCG_GlobalProductStatusCode.xsd
- BCG_GlobalProductSubstitutionReasonCode.xsd
- BCG_GlobalProductUnitOfMeasureCode.xsd
- BCG_PartnerDescription_Types.xsd
- BCG_PhysicalAddress_Types.xsd
- BCG_string_len_0.xsd
- BCG_xml.xsd

3A4 Richiesta ordine di acquisto V02.00

Nella seguente sezione viene descritto il contenuto del package PIP 3A4 Richiesta ordine di acquisto V02.00.

Contenuto del file del package

Nella seguente tabella vengono mostrati i file ZIP e i file XML corrispondenti per il PIP 3A4 Richiesta ordine di acquisto. Le mappe della direttiva comune a tutte le versioni vengono mostrate nella sezione successiva.

Tabella 60. File ZIP e XML di 3A4 Richiesta ordine di acquisto

Nome file ZIP	Nome file XML
BCG_Package_RNIF1.1_3A4V02.00.zip	BCG_RNIF1.1_3A4V02.00.xml
BCG_Package_RNIFV02.00_3A4V02.00.zip	BCG_RNIFV02.00_3A4V02.00.xml
BCG_Package_RNSC1.0_RNIF1.1_3A4V02.00.zip	BCG_RNSC1.0_RNIF1.1_3A4V02.00.xml
BCG_Package_RNSC1.0_RNIFV02.00_3A4V02.00.zip	BCG_RNSC1.0_RNIFV02.00_3A4V02.00.xml

Contenuto della mappa della direttiva

In questa sezione vengono elencate le mappe della direttiva per 3A4 Richiesta ordine di acquisto:

- BCG_3A4PurchaseOrderConfirmation_V02.00.xsd
- BCG_3A4PurchaseOrderRequest_V02.00.xsd
- BCG_BusinessDescription_Types.xsd

- BCG_BusinessDescription_Types_V422.xsd
- BCG_BusinessTaxIdentifier_Types.xsd
- BCG_common.xsd
- BCG_common_V422.xsd
- BCG_ContactInformation_Types.xsd
- BCG_GlobalAccountClassificationCode.xsd
- BCG_GlobalConfirmationTypeCode.xsd
- BCG_GlobalCountryCode.xsd
- BCG_GlobalCreditCardClassificationCode.xsd
- BCG_GlobalCurrencyCode.xsd
- BCG_GlobalDocumentReferenceTypeCode.xsd
- BCG_GlobalDocumentReferenceTypeCode_V422.xsd
- BCG_GlobalFinanceTermsCode.xsd
- BCG_GlobalGovernmentPriorityRatingCode.xsd
- BCG_GlobalMonetaryAmountTypeCode.xsd
- BCG_GlobalPartnerClassificationCode.xsd
- BCG_GlobalPartnerRoleClassificationCode_V422.xsd
- BCG_GlobalPaymentConditionCode.xsd
- BCG_GlobalPriceUnitOfMeasureCode.xsd
- BCG_GlobalProductSubstitutionReasonCode.xsd
- BCG_GlobalProductUnitOfMeasureCode.xsd
- BCG_GlobalPurchaseOrderAcknowledgmentReasonCode.xsd
- BCG_GlobalPurchaseOrderFillPriorityCode.xsd
- BCG_GlobalPurchaseOrderStatusCode.xsd
- BCG_GlobalPurchaseOrderTypeCode.xsd
- BCG_GlobalShipmentTermsCode.xsd
- BCG_GlobalShipmentTermsCode_V422.xsd
- BCG_GlobalShippingServiceLevelCode.xsd
- BCG_GlobalSpecialFulfillmentRequestCode.xsd
- BCG_GlobalSpecialHandlingCode_V422.xsd
- BCG_GlobalTaxExemptionCode.xsd
- BCG_GlobalTaxExemptionCode_V422.xsd
- BCG_InvoiceChargeTypeCode.xsd
- BCG_PartnerDescription_Types.xsd
- BCG_PhysicalAddress_Types.xsd
- BCG_PhysicalAddress_Types_V422.xsd
- BCG_string_len_0.xsd
- BCG_xml.xsd

3A4 Richiesta ordine di acquisto V02.02

Nella seguente sezione viene descritto il contenuto del package PIP 3A4 Richiesta ordine di acquisto V02.02.

Contenuto del file del package

Nella seguente tabella vengono mostrati i file ZIP e i file XML corrispondenti per il PIP 3A4 Richiesta ordine di acquisto. Le mappe della direttiva comune a tutte le versioni vengono mostrate nella sezione successiva.

Tabella 61. File ZIP e XML di 3A4 Richiesta ordine di acquisto

Nome file ZIP	Nome file XML
BCG_Package_RNIF1.1_3A4V02.02.zip	BCG_RNIF1.1_3A4V02.02.xml
BCG_Package_RNIFV02.00_3A4V02.02.zip	BCG_RNIFV02.00_3A4V02.02.xml
BCG_Package_RNSC1.0_RNIF1.1_3A4V02.02.zip	BCG_RNSC1.0_RNIF1.1_3A4V02.02.xml
BCG_Package_RNSC1.0_RNIFV02.00_3A4V02.02.zip	BCG_RNSC1.0_RNIFV02.00_3A4V02.02.xml

Contenuto della mappa della direttiva

In questa sezione vengono elencate le mappe della direttiva per 3A4 Richiesta ordine di acquisto:

- BCG_3A4PurchaseOrderConfirmation_V02.02.xsd
- BCG_3A4PurchaseOrderRequest_V02.02.xsd
- BCG_BusinessDescription_Types.xsd
- BCG_BusinessTaxIdentifier_Types.xsd
- BCG_common.xsd
- BCG_ContactInformation_Types.xsd
- BCG_GlobalAccountClassificationCode.xsd
- BCG_GlobalConfirmationTypeCode.xsd
- BCG_GlobalCountryCode.xsd
- BCG_GlobalCreditCardClassificationCode.xsd
- BCG_GlobalCurrencyCode.xsd
- BCG_GlobalDocumentReferenceTypeCode.xsd
- BCG_GlobalFinanceTermsCode.xsd
- BCG_GlobalGovernmentPriorityRatingCode.xsd
- BCG_GlobalMonetaryAmountTypeCode.xsd
- BCG_GlobalPartnerClassificationCode.xsd
- BCG_GlobalPartnerRoleClassificationCode.xsd
- BCG_GlobalPaymentConditionCode.xsd
- BCG_GlobalPriceUnitOfMeasureCode.xsd
- BCG_GlobalProductSubstitutionReasonCode.xsd
- BCG_GlobalProductUnitOfMeasureCode.xsd
- BCG_GlobalPurchaseOrderAcknowledgmentReasonCode.xsd
- BCG_GlobalPurchaseOrderFillPriorityCode.xsd
- BCG_GlobalPurchaseOrderStatusCode.xsd
- BCG_GlobalPurchaseOrderTypeCode.xsd
- BCG_GlobalShipmentTermsCode.xsd
- BCG_GlobalShippingServiceLevelCode.xsd
- BCG_GlobalSpecialFulfillmentRequestCode.xsd
- BCG_GlobalSpecialHandlingCode.xsd

- BCG_GlobalTaxExemptionCode.xsd
- BCG_InvoiceChargeTypeCode.xsd
- BCG_PartnerDescription_Types.xsd
- BCG_PhysicalAddress_Types.xsd
- BCG_string_len_0.xsd
- BCG_xml.xsd

3A5 Query stato ordine

Nella seguente sezione, viene descritto il contenuto del package PIP 3A5 Query stato ordine.

Contenuto del file del package

Nella seguente tabella vengono mostrati i file ZIP e i file XML corrispondenti per il PIP 3A5 Query statoordine. Le mappe della direttiva comune a tutte le versioni vengono mostrate nella sezione successiva.

Tabella 62. File ZIP e XML di 3A5 Query stato ordine

Nome file ZIP	Nome file XML
BCG_Package_RNIF1.1_3A5R02.00.zip	BCG_RNIF1.1_3A5R02.00.xml
BCG_Package_RNIFV02.00_3A5R02.00.zip	BCG_RNIFV02.00_3A5R02.00.xml
BCG_Package_RNSC1.0_RNIF1.1_3A5R02.00.zip	BCG_RNSC1.0_RNIF1.1_3A5R02.00.xml
BCG_Package_RNSC1.0_RNIFV02.00_3A5R02.00.zip	BCG_RNSC1.0_RNIFV02.00_3A5R02.00.xml

Contenuto della mappa della direttiva

In questa sezione, vengono elencate le mappe della direttiva per 3A5 Query stato ordine:

- BCG_3A5PurchaseOrderStatusQuery_R02.00.xsd
- BCG_3A5PurchaseOrderStatusResponse_R02.00.xsd
- BCG_BusinessDescription_Types.xsd
- BCG_BusinessTaxIdentifier_Types.xsd
- BCG_common.xsd
- BCG_ContactInformation_Types.xsd
- BCG_GlobalAccountClassificationCode.xsd
- BCG_GlobalCountryCode.xsd
- BCG_GlobalCreditCardClassificationCode.xsd
- BCG_GlobalCurrencyCode.xsd
- BCG_GlobalCustomerTypeCode.xsd
- BCG_GlobalDocumentReferenceTypeCode.xsd
- BCG_GlobalFinanceTermsCode.xsd
- BCG_GlobalFreeOnBoardCode.xsd
- BCG_GlobalGovernmentPriorityRatingCode.xsd
- BCG_GlobalLineItemStatusCode.xsd
- BCG_GlobalOrderQuantityTypeCode.xsd
- BCG_GlobalPartnerClassificationCode.xsd
- BCG_GlobalPartnerRoleClassificationCode.xsd

- BCG_GlobalProductSubstitutionReasonCode.xsd
- BCG_GlobalProductUnitOfMeasureCode.xsd
- BCG_GlobalPurchaseOrderAcknowledgmentReasonCode.xsd
- BCG_GlobalPurchaseOrderFillPriority
- BCG_GlobalPurchaseOrderStatusCode.xsd
- BCG_GlobalPurchaseOrderTypeCode.xsd
- BCG_GlobalShipmentTermsCode.xsd
- BCG_GlobalShippingServiceLevelCode.xsd
- BCG_GlobalSpecialFulfillmentRequestCode.xsd
- BCG_GlobalSpecialHandlingCode.xsd
- BCG_GlobalTaxExemptionCode.xsd
- BCG_GlobalTransportEventCode.xsd
- BCG_PartnerDescription_Types.xsd
- BCG_PhysicalAddress_Types.xsd
- BCG_string_len_0.xsd
- BCG_xml.xsd

3A6 Distribuzione stato ordine

Nella seguente sezione viene descritto il contenuto del package PIP 3A6 Distribuzione stato ordine.

Contenuto del file del package

Nella seguente tabella vengono mostrati i file ZIP e i file XML corrispondenti per il PIP 3A6 Distribuzione stato ordine. Le mappe della direttiva comune a tutte le versioni vengono mostrate nella sezione successiva.

Tabella 63. File ZIP e XML di 3A6 Distribuzione stato ordine

Nome file ZIP	Nome file XML
BCG_Package_RNIF1.1_3A6V02.02.zip	BCG_RNIF1.1_3A6V02.02.xml
BCG_Package_RNIFV02.00_3A6V02.02.zip	BCG_RNIFV02.00_3A6V02.02.xml
BCG_Package_RNSC1.0_RNIF1.1_3A6V02.02.zip	BCG_RNSC1.0_RNIF1.1_3A6V02.02.xml
BCG_Package_RNSC1.0_RNIFV02.00_3A6V02.02.zip	BCG_RNSC1.0_RNIFV02.00_3A6V02.02.xml

Contenuto della mappa della direttiva

In questa sezione, vengono elencate le mappe della direttiva per 3A6 Distribuzione stato ordine:

- BCG_3A6PurchaseOrderStatusNotification_V02.02.xsd
- BCG_BusinessDescription_Types.xsd
- BCG_BusinessTaxIdentifier_Types.xsd
- BCG_common.xsd
- BCG_ContactInformation_Types.xsd
- BCG_GlobalAccountClassificationCode.xsd
- BCG_GlobalCountryCode.xsd
- BCG_GlobalCreditCardClassificationCode.xsd
- BCG_GlobalCurrencyCode.xsd

- BCG_GlobalDocumentReferenceTypeCode.xsd
- BCG_GlobalFinanceTermsCode.xsd
- BCG_GlobalGovernmentPriorityRatingCode.xsd
- BCG_GlobalLineItemStatusCode.xsd
- BCG_GlobalMonetaryAmountTypeCode.xsd
- BCG_GlobalNotificationReasonCode.xsd
- BCG_GlobalOrderQuantityTypeCode.xsd
- BCG_GlobalPartnerClassificationCode.xsd
- BCG_GlobalPartnerRoleClassificationCode.xsd
- BCG_GlobalPaymentConditionCode.xsd
- BCG_GlobalPriceUnitOfMeasureCode.xsd
- BCG_GlobalProductSubstitutionReasonCode.xsd
- BCG_GlobalProductUnitOfMeasureCode.xsd
- BCG_GlobalPurchaseOrderAcknowledgmentReasonCode.xsd
- BCG_GlobalPurchaseOrderFillPriorityCode.xsd
- BCG_GlobalPurchaseOrderStatusCode.xsd
- BCG_GlobalPurchaseOrderTypeCode.xsd
- BCG_GlobalShipmentTermsCode.xsd
- BCG_GlobalShippingServiceLevelCode.xsd
- BCG_GlobalSpecialFulfillmentRequestCode.xsd
- BCG_GlobalSpecialHandlingCode.xsd
- BCG_GlobalTaxExemptionCode.xsd
- BCG_GlobalTrackingReferenceTypeCode.xsd
- BCG_InvoiceChargeTypeCode.xsd
- BCG_PartnerDescription_Types.xsd
- BCG_PhysicalAddress_Types.xsd
- BCG_string_len_0.xsd
- BCG_xml.xsd

3A7 Notifica aggiornamento ordine di acquisto

Nella seguente sezione viene descritto il contenuto del package PIP 3A7 Notifica aggiornamento ordine di acquisto.

Contenuto del file del package

Nella seguente tabella vengono mostrati i file ZIP e i file XML corrispondenti per il PIP 3A7 Notifica aggiornamento ordine di acquisto. Le mappe della direttiva comune a tutte le versioni vengono mostrate nella sezione successiva.

Tabella 64. File ZIP e XML di 3A7 Notifica aggiornamento ordine di acquisto

Nome file ZIP	Nome file XML
BCG_Package_RNIF1.1_3A7V02.02.zip	BCG_RNIF1.1_3A7V02.02.xml
BCG_Package_RNIFV02.00_3A7V02.02.zip	BCG_RNIFV02.00_3A7V02.02.xml
BCG_Package_RNSC1.0_RNIF1.1_3A7V02.02.zip	BCG_RNSC1.0_RNIF1.1_3A7V02.02.xml
BCG_Package_RNSC1.0_RNIFV02.00_3A7V02.02.zip	BCG_RNSC1.0_RNIFV02.00_3A7V02.02.xml

Contenuto della mappa della direttiva

In questa sezione, vengono elencate le mappe della direttiva per 3A7 Notifica aggiornamento ordine di acquisto:

- BCG_3A7PurchaseOrderUpdateNotification_V02.02.xsd
- BCG_BusinessDescription_Types.xsd
- BCG_BusinessTaxIdentifier_Types.xsd
- BCG_common.xsd
- BCG_ContactInformation_Types.xsd
- BCG_GlobalAccountClassificationCode.xsd
- BCG_GlobalActionCode.xsd
- BCG_GlobalConfirmationTypeCode.xsd
- BCG_GlobalCountryCode.xsd
- BCG_GlobalCreditCardClassificationCode.xsd
- BCG_GlobalCurrencyCode.xsd
- BCG_GlobalDocumentReferenceTypeCode.xsd
- BCG_GlobalFinanceTermsCode.xsd
- BCG_GlobalGovernmentPriorityRatingCode.xsd
- BCG_GlobalMonetaryAmountTypeCode.xsd
- BCG_GlobalPartnerClassificationCode.xsd
- BCG_GlobalPartnerRoleClassificationCode.xsd
- BCG_GlobalPaymentConditionCode.xsd
- BCG_GlobalPriceUnitOfMeasureCode.xsd
- BCG_GlobalProductSubstitutionReasonCode.xsd
- BCG_GlobalProductUnitOfMeasureCode.xsd
- BCG_GlobalPurchaseOrderAcknowledgmentReasonCode.xsd
- BCG_GlobalPurchaseOrderFillPriorityCode.xsd
- BCG_GlobalPurchaseOrderStatusCode.xsd
- BCG_GlobalPurchaseOrderTypeCode.xsd
- BCG_GlobalShipmentTermsCode.xsd
- BCG_GlobalShippingServiceLevelCode.xsd
- BCG_GlobalSpecialFulfillmentRequestCode.xsd
- BCG_GlobalSpecialHandlingCode.xsd
- BCG_GlobalTaxExemptionCode.xsd
- BCG_InvoiceChargeTypeCode.xsd
- BCG_PartnerDescription_Types.xsd
- BCG_PhysicalAddress_Types.xsd
- BCG_string_len_0.xsd
- BCG_xml.xsd

3A8 Richiesta modifica ordine di acquisto V01.02

Nella seguente sezione viene descritto il contenuto del package PIP 3A8 Richiesta modifica ordine di acquisto V01.02.

Contenuto del file del package

Nella seguente tabella vengono mostrati i file ZIP e i file XML corrispondenti per il PIP 3A8 Richiesta modifica ordine di acquisto. Le mappe della direttiva comune a tutte le versioni vengono mostrate nella sezione successiva.

Tabella 65. File ZIP e XML di 3A8 Richiesta modifica ordine di acquisto

Nome file ZIP	Nome file XML
BCG_Package_RNIF1.1_3A8V01.02.zip	BCG_RNIF1.1_3A8V01.02.xml
BCG_Package_RNIFV02.00_3A8V01.02.zip	BCG_RNIFV02.00_3A8V01.02.xml
BCG_Package_RNSC1.0_RNIF1.1_3A8V01.02.zip	BCG_RNSC1.0_RNIF1.1_3A8V01.02.xml
BCG_Package_RNSC1.0_RNIFV02.00_3A8V01.02.zip	BCG_RNSC1.0_RNIFV02.00_3A8V01.02.xml

Contenuto della mappa della direttiva

In questa sezione, vengono elencate le mappe della direttiva per 3A8 Richiesta modifica ordine di acquisto:

- BCG_3A8PurchaseOrderChangeConfirmation_V01.02.xsd
- BCG_3A8PurchaseOrderChangeRequest_V01.02.xsd
- BCG_BusinessDescription_Types.xsd
- BCG_BusinessTaxIdentifier_Types.xsd
- BCG_common.xsd
- BCG_ContactInformation_Types.xsd
- BCG_GlobalAccountClassificationCode.xsd
- BCG_GlobalActionCode.xsd
- BCG_GlobalConfirmationTypeCode.xsd
- BCG_GlobalCountryCode.xsd
- BCG_GlobalCreditCardClassificationCode.xsd
- BCG_GlobalCurrencyCode.xsd
- BCG_GlobalDocumentReferenceTypeCode.xsd
- BCG_GlobalFinanceTermsCode.xsd
- BCG_GlobalGovernmentPriorityRatingCode.xsd
- BCG_GlobalMonetaryAmountTypeCode.xsd
- BCG_GlobalPartnerClassificationCode.xsd
- BCG_GlobalPartnerRoleClassificationCode.xsd
- BCG_GlobalPaymentConditionCode.xsd
- BCG_GlobalPriceUnitOfMeasureCode.xsd
- BCG_GlobalProductSubstitutionReasonCode.xsd
- BCG_GlobalProductUnitOfMeasureCode.xsd
- BCG_GlobalPurchaseOrderAcknowledgmentReasonCode.xsd
- BCG_GlobalPurchaseOrderFillPriorityCode.xsd
- BCG_GlobalPurchaseOrderStatusCode.xsd
- BCG_GlobalPurchaseOrderTypeCode.xsd
- BCG_GlobalShipmentTermsCode.xsd
- BCG_GlobalShippingServiceLevelCode.xsd
- BCG_GlobalSpecialFulfillmentRequestCode.xsd

- BCG_GlobalSpecialHandlingCode.xsd
- BCG_GlobalTaxExemptionCode.xsd
- BCG_InvoiceChargeTypeCode.xsd
- BCG_PartnerDescription_Types.xsd
- BCG_PhysicalAddress_Types.xsd
- BCG_string_len_0.xsd
- BCG_xml.xsd

3A8 Richiesta modifica ordine di acquisto V01.03

Nella seguente sezione, viene descritto il contenuto del package PIP 3A8 Richiesta modifica ordine di acquisto V01.03.

Contenuto del file del package

Nella seguente tabella vengono mostrati i file ZIP e i file XML corrispondenti per il PIP 3A8 Richiesta modifica ordine di acquisto. Le mappe della direttiva comune a tutte le versioni vengono mostrate nella sezione successiva.

Tabella 66. File ZIP e XML di 3A8 Richiesta modifica ordine di acquisto

Nome file ZIP	Nome file XML
BCG_Package_RNIF1.1_3A8V01.03.zip	BCG_RNIF1.1_3A8V01.03.xml
BCG_Package_RNIFV02.00_3A8V01.03.zip	BCG_RNIFV02.00_3A8V01.03.xml
BCG_Package_RNSC1.0_RNIF1.1_3A8V01.03.zip	BCG_RNSC1.0_RNIF1.1_3A8V01.03.xml
BCG_Package_RNSC1.0_RNIFV02.00_3A8V01.03.zip	BCG_RNSC1.0_RNIFV02.00_3A8V01.03.xml

Contenuto della mappa della direttiva

In questa sezione, vengono elencate le mappe della direttiva per 3A8 Richiesta modifica ordine di acquisto:

- BCG_3A8PurchaseOrderChangeConfirmation_V01.03.xsd
- BCG_3A8PurchaseOrderChangeRequest_V01.03.xsd
- BCG_BusinessDescription_Types.xsd
- BCG_BusinessDescription_Types_V43.xsd
- BCG_BusinessTaxIdentifier_Types.xsd
- BCG_common.xsd
- BCG_common_V422.xsd
- BCG_common_V43.xsd
- BCG_ContactInformation_Types.xsd
- BCG_GlobalAccountClassificationCode.xsd
- BCG_GlobalActionCode.xsd
- BCG_GlobalConfirmationTypeCode.xsd
- BCG_GlobalCountryCode.xsd
- BCG_GlobalCreditCardClassificationCode.xsd
- BCG_GlobalCurrencyCode.xsd
- BCG_GlobalDocumentReferenceTypeCode.xsd
- BCG_GlobalFinanceTermsCode.xsd
- BCG_GlobalFreeOnBoardCode_V422.xsd

- BCG_GlobalGovernmentPriorityRatingCode.xsd
- BCG_GlobalMonetaryAmountTypeCode.xsd
- BCG_GlobalPartnerClassificationCode_V43.xsd
- BCG_GlobalPartnerRoleClassificationCode_V43.xsd
- BCG_GlobalPaymentConditionCode.xsd
- BCG_GlobalProductSubstitutionReasonCode.xsd
- BCG_GlobalProductUnitOfMeasureCode_V43.xsd
- BCG_GlobalPurchaseOrderAcknowledgmentReasonCode.xsd
- BCG_GlobalPurchaseOrderFillPriorityCode.xsd
- BCG_GlobalPurchaseOrderStatusCode.xsd
- BCG_GlobalPurchaseOrderTypeCode.xsd
- BCG_GlobalShipmentTermsCode.xsd
- BCG_GlobalShippingServiceLevelCode.xsd
- BCG_GlobalSpecialFulfillmentRequestCode.xsd
- BCG_GlobalSpecialHandlingCode_V43.xsd
- BCG_GlobalTaxExemptionCode.xsd
- BCG_GlobalTransportEventCode.xsd
- BCG_InvoiceChargeTypeCode_V422.xsd
- BCG_PartnerDescription_Types.xsd
- BCG_PartnerDescription_Types_V43.xsd
- BCG_PhysicalAddress_Types.xsd
- BCG_string_len_0.xsd
- BCG_xml.xsd

3A9 Richiesta cancellazione ordine di acquisto

Nella seguente sezione, viene descritto il contenuto del package PIP 3A9 Richiesta cancellazione ordine di acquisto.

Contenuto del file del package

Nella seguente tabella vengono mostrati i file ZIP e i file XML corrispondenti per il PIP 3A9 Richiesta cancellazione ordine di acquisto. Le mappe della direttiva comune a tutte le versioni vengono mostrate nella sezione successiva.

Tabella 67. File ZIP e XML di 3A9 Richiesta cancellazione ordine di acquisto

Nome file ZIP	Nome file XML
BCG_Package_RNIF1.1_3A9V01.01.zip	BCG_RNIF1.1_3A9V01.01.xml
BCG_Package_RNIFV02.00_3A9V01.01.zip	BCG_RNIFV02.00_3A9V01.01.xml
BCG_Package_RNSC1.0_RNIF1.1_3A9V01.01.zip	BCG_RNSC1.0_RNIF1.1_3A9V01.01.xml
BCG_Package_RNSC1.0_RNIFV02.00_3A9V01.01.zip	BCG_RNSC1.0_RNIFV02.00_3A9V01.01.xml

Contenuto della mappa della direttiva

In questa sezione, vengono elencate le mappe della direttiva per 3A9 Richiesta cancellazione ordine di acquisto:

- BCG_3A9PurchaseOrderCancellationConfirmation_V01.01.xsd
- BCG_3A9PurchaseOrderCancellationRequest_V01.01.xsd

- BCG_BusinessDescription_Types.xsd
- BCG_BusinessTaxIdentifier_Types.xsd
- BCG_common.xsd
- BCG_ContactInformation_Types.xsd
- BCG_GlobalCountryCode.xsd
- BCG_GlobalPartnerClassificationCode.xsd
- BCG_GlobalPurchaseOrderCancellationCode.xsd
- BCG_GlobalPurchaseOrderCancellationResponseCode.xsd
- BCG_PartnerDescription_Types.xsd
- BCG_PhysicalAddress_Types.xsd
- BCG_string_len_0.xsd
- BCG_xml.xsd

3B2 Notifica anticipo spedizione

Nella seguente sezione, viene descritto il contenuto del package PIP 3B2 Notifica anticipo spedizione.

Contenuto del file del package

Nella seguente tabella vengono mostrati i file ZIP e i file XML corrispondenti per il PIP 3B2 Notifica anticipo spedizione. Le mappe della direttiva comune a tutte le versioni vengono mostrate nella sezione successiva.

Tabella 68. File ZIP e XML di 3B2 Notifica anticipo spedizione

Nome file ZIP	Nome file XML
BCG_Package_RNIF1.1_3B2V01.01.zip	BCG_RNIF1.1_3B2V01.01.xml
BCG_Package_RNIFV02.00_3B2V01.01.zip	BCG_RNIFV02.00_3B2V01.01.xml
BCG_Package_RNSC1.0_RNIF1.1_3B2V01.01.zip	BCG_RNSC1.0_RNIF1.1_3B2V01.01.xml
BCG_Package_RNSC1.0_RNIFV02.00_3B2V01.01.zip	BCG_RNSC1.0_RNIFV02.00_3B2V01.01.xml

Contenuto della mappa della direttiva

In questa sezione, vengono elencate le mappe della direttiva per 3B2 Notifica anticipo spedizione:

- BCG_3B2AdvanceShipmentNotification_V01.01.xsd
- BCG_BusinessDescription_Types.xsd
- BCG_BusinessTaxIdentifier_Types.xsd
- BCG_common.xsd
- BCG_ContactInformation_Types.xsd
- BCG_GlobalCountryCode.xsd
- BCG_GlobalDocumentReferenceTypeCode.xsd
- BCG_GlobalIncotermsCode.xsd
- BCG_GlobalLotQuantityClassificationCode.xsd
- BCG_GlobalPackageTypeCode.xsd
- BCG_GlobalPartnerClassificationCode.xsd
- BCG_GlobalPhysicalUnitOfMeasureCode.xsd
- BCG_GlobalProductUnitOfMeasureCode.xsd

- BCG_GlobalShipDateCode.xsd
- BCG_GlobalShipmentChangeDispositionCode.xsd
- BCG_GlobalShipmentModeCode.xsd
- BCG_GlobalShippingServiceLevelCode.xsd
- BCG_GlobalTrackingReferenceTypeCode.xsd
- BCG_NationalExportControlClassificationCode.xsd
- BCG_PartnerDescription_Types.xsd
- BCG_PhysicalAddress_Types.xsd
- BCG_string_len_0.xsd
- BCG_xml.xsd

3B3 Distribuzione stato spedizione

Nella seguente sezione, viene descritto il contenuto del package PIP 3B3 Distribuzione stato spedizione.

Contenuto del file del package

Nella seguente tabella vengono mostrati i file ZIP e i file XML corrispondenti per il PIP 3B3 Distribuzione stato spedizione. Le mappe della direttiva comune a tutte le versioni vengono mostrate nella sezione successiva.

Tabella 69. File ZIP e XML di 3B3 Distribuzione stato spedizione

Nome file ZIP	Nome file XML
BCG_Package_RNIF1.1_3B3R01.00.zip	BCG_RNIF1.1_3B3R01.00.xml
BCG_Package_RNIFV02.00_3B3R01.00.zip	BCG_RNIFV02.00_3B3R01.00.xml
BCG_Package_RNSC1.0_RNIF1.1_3B3R01.00.zip	BCG_RNSC1.0_RNIF1.1_3B3R01.00.xml
BCG_Package_RNSC1.0_RNIFV02.00_3B3R01.00.zip	BCG_RNSC1.0_RNIFV02.00_3B3R01.00.xml

Contenuto della mappa della direttiva

In questa sezione, vengono elencate le mappe della direttiva per 3B3 Distribuzione stato spedizione:

- 3B3 Distribute Shipment Status_R01.00.xsd
- BCG_BusinessDescription_Types.xsd
- BCG_BusinessDescription_Types_V422.xsd
- BCG_BusinessDescription_Types_V43.xsd
- BCG_BusinessTaxIdentifier_Types.xsd
- BCG_common_V422.xsd
- BCG_common_V43.xsd
- BCG_ContactInformation_Types.xsd
- BCG_ContactInformation_Types_V422.xsd
- BCG_ContactInformation_Types_V43.xsd
- BCG_GlobalCountryCode.xsd
- BCG_GlobalDocumentReferenceTypeCode_V43.xsd
- BCG_GlobalPartnerClassificationCode_V43.xsd
- BCG_GlobalShipmentDispositionCode.xsd
- BCG_GlobalShipmentModeCode.xsd

- BCG_GlobalShipmentStatusCode_V43.xsd
- BCG_GlobalShipmentStatusReportingLevelCode_V43.xsd
- BCG_GlobalTrackingReferenceTypeCode.xsd
- BCG_PartnerDescription_Types_V43.xsd
- BCG_PhysicalAddress_Types.xsd
- BCG_PhysicalAddress_Types_V422.xsd
- BCG_PhysicalAddress_Types_V423.xsd
- BCG_string_len_0.xsd
- BCG_xml.xsd

3B11 Notifica ordine di spedizione

Nella seguente sezione, viene descritto il contenuto del package PIP 3B11 Notifica ordine di spedizione.

Contenuto del file del package

Nella seguente tabella vengono mostrati i file ZIP e i file XML corrispondenti per il PIP 3B11 Notifica ordine di spedizione. Le mappe della direttiva comune a tutte le versioni vengono mostrate nella sezione successiva.

Tabella 70. File ZIP e XML di 3B11 Notifica ordine di spedizione

Nome file ZIP	Nome file XML
BCG_Package_RNIF1.1_3B11R01.00A.zip	BCG_RNIF1.1_3B11R01.00A.xml
BCG_Package_RNIFV02.00_3B11R01.00A.zip	BCG_RNIFV02.00_3B11R01.00A.xml
BCG_Package_RNSC1.0_RNIF1.1_3B11R01.00A.zip	BCG_RNSC1.0_RNIF1.1_3B11R01.00A.xml
BCG_Package_RNSC1.0_RNIFV02.00_3B11R01.00A.zip	BCG_RNSC1.0_RNIFV02.00_3B11R01.00A.xml

Contenuto della mappa della direttiva

In questa sezione, vengono elencate le mappe della direttiva per 3B11 Notifica ordine di spedizione:

- 3B11 ShippingOrderNotification_R01.00A.xsd
- BCG_BusinessDescription_Types.xsd
- BCG_BusinessDescription_Types_V422.xsd
- BCG_BusinessTaxIdentifier_Types.xsd
- BCG_common.xsd
- BCG_ContactInformation_Types.xsd
- BCG_ContactInformation_Types_V422.xsd
- BCG_GlobalCountryCode.xsd
- BCG_GlobalCurrencyCode.xsd
- BCG_GlobalDocumentReferenceTypeCode_V422.xsd
- BCG_GlobalFreightPaymentTermsCode_V422.xsd
- BCG_GlobalIncotermsCode.xsd
- BCG_GlobalOrderAdminCode_V422.xsd
- BCG_GlobalPartnerClassificationCode.xsd
- BCG_GlobalPartnerRoleClassificationCode.xsd
- BCG_GlobalProductUnitOfMeasureCode.xsd

- BCG_GlobalShipDateCode.xsd
- BCG_GlobalShipmentModeCode.xsd
- BCG_GlobalShippingServiceLevelCode.xsd
- BCG_GlobalSpecialHandlingCode.xsd
- BCG_GlobalWarrantyTypeCode_V43.xsd
- BCG_PartnerDescription_Types.xsd
- BCG_PartnerDescription_Types_V422.xsd
- BCG_PhysicalAddress_Types.xsd
- BCG_string_len_0.xsd
- BCG_xml.xsd

3B12 Richiesta ordine di spedizione

Nella seguente sezione, viene descritto il contenuto del package PIP 3B12 Richiesta ordine di spedizione.

Contenuto del file del package

Nella seguente tabella vengono mostrati i file ZIP e i file XML corrispondenti per il PIP 3B12 Richiesta ordine di spedizione. Le mappe della direttiva comune a tutte le versioni vengono mostrate nella sezione successiva.

Tabella 71. File ZIP e XML di 3B12 Richiesta ordine di spedizione

Nome file ZIP	Nome file XML
BCG_Package_RNIF1.1_3B12V01.01.zip	BCG_RNIF1.1_3B12V01.01.xml
BCG_Package_RNIFV02.00_3B12V01.01.zip	BCG_RNIFV02.00_3B12V01.01.xml
BCG_Package_RNSC1.0_RNIF1.1_3B12V01.01.zip	BCG_RNSC1.0_RNIF1.1_3B12V01.01.xml
BCG_Package_RNSC1.0_RNIFV02.00_3B12V01.01.zip	BCG_RNSC1.0_RNIFV02.00_3B12V01.01.xml

Contenuto della mappa della direttiva

In questa sezione, vengono elencate le mappe della direttiva per 3B12 Richiesta ordine di spedizione:

- BCG_3B12ShippingOrderConfirmation_V01.01.xsd
- BCG_3B12ShippingOrderRequest_V01.01.xsd
- BCG_BusinessTaxIdentifier_Types.xsd
- BCG_common.xsd
- BCG_common_V422.xsd
- BCG_ContactInformation_Types.xsd
- BCG_ContactInformation_Types_V422.xsd
- BCG_GlobalCountryCode.xsd
- BCG_GlobalCurrencyCode.xsd
- BCG_GlobalDocumentReferenceTypeCode.xsd
- BCG_GlobalIncotermsCode.xsd
- BCG_GlobalPackageTypeCode.xsd
- BCG_GlobalPartnerClassificationCode.xsd
- BCG_GlobalPartnerRoleClassificationCode.xsd
- BCG_GlobalPhysicalUnitOfMeasureCode.xsd

- BCG_GlobalProductUnitOfMeasureCode.xsd
- BCG_GlobalShipDateCode.xsd
- BCG_GlobalShippingServiceLevelCode.xsd
- BCG_GlobalSpecialHandlingCode.xsd
- BCG_PartnerDescription_Types.xsd
- BCG_PartnerDescription_Types_V422.xsd
- BCG_PhysicalAddress_Types.xsd
- BCG_string_len_0.xsd
- BCG_xml.xsd

3B13 Notifica conferma ordine di spedizione

Nella seguente sezione, viene descritto il contenuto del package PIP 3B13 Notifica conferma ordine di spedizione.

Contenuto del file del package

Nella seguente tabella vengono mostrati i file ZIP e i file XML corrispondenti per il PIP 3B13 Notifica conferma ordine di spedizione. Le mappe della direttiva comune a tutte le versioni vengono mostrate nella sezione successiva.

Tabella 72. File ZIP e XML di 3B13 Notifica conferma ordine di spedizione

Nome file ZIP	Nome file XML
BCG_Package_RNIF1.1_3B13V01.01.zip	BCG_RNIF1.1_3B13V01.01.xml
BCG_Package_RNIFV02.00_3B13V01.01.zip	BCG_RNIFV02.00_3B13V01.01.xml
BCG_Package_RNSC1.0_RNIF1.1_3B13V01.01.zip	BCG_RNSC1.0_RNIF1.1_3B13V01.01.xml
BCG_Package_RNSC1.0_RNIFV02.00_3B13V01.01.zip	BCG_RNSC1.0_RNIFV02.00_3B13V01.01.xml

Contenuto della mappa della direttiva

In questa sezione, vengono elencate le mappe della direttiva per 3B13 Notifica conferma ordine di spedizione:

- BCG_3B13ShippingOrderConfirmationNotification_V01.01.xsd
- BCG_BusinessDescription_Types.xsd
- BCG_BusinessTaxIdentifier_Types.xsd
- BCG_common.xsd
- BCG_common_V422.xsd
- BCG_ContactInformation_Types.xsd
- BCG_GlobalCountryCode.xsd
- BCG_GlobalCurrencyCode.xsd
- BCG_GlobalDocumentReferenceTypeCode.xsd
- BCG_GlobalPartnerClassificationCode.xsd
- BCG_GlobalPartnerRoleClassificationCode.xsd
- BCG_GlobalPhysicalUnitOfMeasureCode.xsd
- BCG_GlobalProductUnitOfMeasureCode.xsd
- BCG_GlobalShipDateCode.xsd
- BCG_GlobalShippingServiceLevelCode.xsd
- BCG_GlobalSpecialHandlingCode.xsd

- BCG_GlobalTrackingReferenceTypeCode.xsd
- BCG_PartnerDescription_Types.xsd
- BCG_PhysicalAddress_Types.xsd
- BCG_string_len_0.xsd
- BCG_xml.xsd

3B14 Richiesta cancellazione ordine di spedizione

Nella seguente sezione, viene descritto il contenuto del package PIP 3B14 Richiesta cancellazione ordine di spedizione.

Contenuto del file del package

Nella seguente tabella vengono mostrati i file ZIP e i file XML corrispondenti per il PIP 3B14 Richiesta cancellazione ordine di spedizione. Le mappe della direttiva comune a tutte le versioni vengono mostrate nella sezione successiva.

Tabella 73. File ZIP e XML di 3B14 Richiesta cancellazione ordine di spedizione

Nome file ZIP	Nome file XML
BCG_Package_RNIF1.1_3B14V01.00.zip	BCG_RNIF1.1_3B14V01.00.xml
BCG_Package_RNIFV02.00_3B14V01.00.zip	BCG_RNIFV02.00_3B14V01.00.xml
BCG_Package_RNSC1.0_RNIF1.1_3B14V01.00.zip	BCG_RNSC1.0_RNIF1.1_3B14V01.00.xml
BCG_Package_RNSC1.0_RNIFV02.00_3B14V01.00.zip	BCG_RNSC1.0_RNIFV02.00_3B14V01.00.xml

Contenuto della mappa della direttiva

In questa sezione, vengono elencate le mappe della direttiva per 3B14 Richiesta cancellazione ordine di spedizione:

- 3B14_ShippingOrderCancellationConfirmation_V01.00.xsd
- 3B14_ShippingOrderCancellationRequest_V01.00.xsd
- BCG_common.xsd
- BCG_common_V422.xsd
- BCG_ContactInformation_Types.xsd
- BCG_GlobalDocumentReferenceTypeCode.xsd
- BCG_GlobalOrderAdminCode_V22.xsd
- BCG_GlobalPartnerRoleClassificationCode.xsd
- BCG_GlobalPartnerRoleClassificationCode_V43.xsd
- BCG_GlobalShippingOrderCancellationStatusReasonCode_V43.xsd
- BCG_PartnerDescription_Types.xsd
- BCG_PartnerDescription_Types_V43.xsd
- BCG_string_len_0.xsd
- BCG_xml.xsd

3B18 Notifica documentazione di spedizione

Nella seguente sezione, viene descritto il contenuto del package PIP 3B18 Notifica documentazione di spedizione.

Contenuto del file del package

Nella seguente tabella vengono mostrati i file ZIP e i file XML corrispondenti per il PIP 3B18 Notifica documentazione di spedizione. Le mappe della direttiva comune a tutte le versioni vengono mostrate nella sezione successiva.

Tabella 74. File ZIP e XML di 3B18 Notifica documentazione di spedizione

Nome file ZIP	Nome file XML
BCG_Package_RNIF1.1_3B18V01.00.zip	BCG_RNIF1.1_3B18V01.00.xml
BCG_Package_RNIFV02.00_3B18V01.00.zip	BCG_RNIFV02.00_3B18V01.00.xml
BCG_Package_RNSC1.0_RNIF1.1_3B18V01.00.zip	BCG_RNSC1.0_RNIF1.1_3B18V01.00.xml
BCG_Package_RNSC1.0_RNIFV02.00_3B18V01.00.zip	BCG_RNSC1.0_RNIFV02.00_3B18V01.00.xml

Contenuto della mappa della direttiva

In questa sezione, vengono elencate le mappe della direttiva per 3B18 Notifica documentazione di spedizione:

- BCG_3B18ShippingDocumentationNotification_V01.00.xsd
- BCG_BusinessDescription_Types.xsd
- BCG_BusinessDescription_Types_V422.xsd
- BCG_common_V422.xsd
- BCG_ContactInformation_Types.xsd
- BCG_GlobalCountryCode.xsd
- BCG_GlobalCurrencyCode.xsd
- BCG_GlobalDocumentReferenceTypeCode.xsd
- BCG_GlobalFreeOnBoardCode_V422.xsd
- BCG_GlobalFreightPaymentTermsCode_V422.xsd
- BCG_GlobalIncotermsCode.xsd
- BCG_GlobalMonetaryAmountTypeCode.xsd
- BCG_GlobalOrderAdminCode_V422.xsd
- BCG_GlobalPackageTypeCode_V422.xsd
- BCG_GlobalPartnerClassificationCode_V422.xsd
- BCG_GlobalPartnerRoleClassificationCode_V422.xsd
- BCG_GlobalPaymentTermsCode.xsd
- BCG_GlobalPhysicalUnitOfMeasureCode_V422.xsd
- BCG_GlobalPortIdentifierAuthorityCode_V422.xsd
- BCG_GlobalPortTypeCode_V422.xsd
- BCG_GlobalProductUnitOfMeasureCode.xsd
- BCG_GlobalShipDateCode.xsd
- BCG_GlobalShipmentModeCode.xsd
- BCG_GlobalShippingDocumentCode_V422.xsd
- BCG_GlobalShippingServiceLevelCode.xsd
- BCG_GlobalSpecialHandlingCode_V422.xsd
- BCG_GlobalTrackingReferenceTypeCode.xsd
- BCG_InvoiceChargeTypeCode_V422.xsd
- BCG_NationalExportControlClassificationCode.xsd

- BCG_PhysicalAddress_Types.xsd
- BCG_string_len_0.xsd
- BCG_xml.xsd

3C1 Restituzione prodotto

Nella seguente sezione, viene descritto il contenuto del package PIP 3C1 Restituzione prodotto.

Contenuto del file del package

Nella seguente tabella vengono mostrati i file ZIP e i file XML corrispondenti per il PIP 3C1 Restituzione prodotto. Le mappe della direttiva comune a tutte le versioni vengono mostrate nella sezione successiva.

Tabella 75. File ZIP e XML di 3C1 Restituzione prodotto

Nome file ZIP	Nome file XML
BCG_Package_RNIF1.1_3C1V01.00.zip	BCG_RNIF1.1_3C1V01.00.xml
BCG_Package_RNIFV02.00_3C1V01.00.zip	BCG_RNIFV02.00_3C1V01.00.xml
BCG_Package_RNSC1.0_RNIF1.1_3C1V01.00.zip	BCG_RNSC1.0_RNIF1.1_3C1V01.00.xml
BCG_Package_RNSC1.0_RNIFV02.00_3C1V01.00.zip	BCG_RNSC1.0_RNIFV02.00_3C1V01.00.xml

Contenuto della mappa della direttiva

In questa sezione, vengono elencate le mappe della direttiva per 3C1 Restituzione prodotto:

- BCG_3C1ReturnProductConfirmation_V01.00.xsd
- BCG_3C1ReturnProductRequest_V01.00.xsd
- BCG_BusinessDescription_Types.xsd
- BCG_BusinessDescription_Types_V43.xsd
- BCG_common.xsd
- BCG_common_V422.xsd
- BCG_common_V43.xsd
- BCG_ContactInformation_Types.xsd
- BCG_GlobalCurrencyCode.xsd
- BCG_GlobalDocumentReferenceTypeCode.xsd
- BCG_GlobalFailureTypeCode_V43.xsd
- BCG_GlobalPartnerClassificationCode_V43.xsd
- BCG_GlobalPartnerRoleClassificationCode_V43.xsd
- BCG_GlobalProductUnitOfMeasureCode_V43.xsd
- BCG_GlobalShippingServiceLevelCode.xsd
- BCG_PartnerDescription_Types.xsd
- BCG_PartnerDescription_Types_V43.xsd
- BCG_PhysicalAddress_Types.xsd
- BCG_string_len_0.xsd
- BCG_xml.xsd

3C3 Notifica della fattura

Nella seguente sezione, viene descritto il contenuto del package PIP 3C3 Notifica della fattura.

Contenuto del file del package

Nella seguente tabella vengono mostrati i file ZIP e i file XML corrispondenti per il PIP 3C3 Notifica della fattura. Le mappe della direttiva comune a tutte le versioni vengono mostrate nella sezione successiva.

Tabella 76. File ZIP e XML di 3C3 Notifica della fattura

Nome file ZIP	Nome file XML
BCG_Package_RNIF1.1_3C3V01.01.zip	BCG_RNIF1.1_3C3V01.01.xml
BCG_Package_RNIFV02.00_3C3V01.01.zip	BCG_RNIFV02.00_3C3V01.01.xml
BCG_Package_RNSC1.0_RNIF1.1_3C3V01.01.zip	BCG_RNSC1.0_RNIF1.1_3C3V01.01.xml
BCG_Package_RNSC1.0_RNIFV02.00_3C3V01.01.zip	BCG_RNSC1.0_RNIFV02.00_3C3V01.01.xml

Contenuto della mappa della direttiva

In questa sezione, vengono elencate le mappe della direttiva per 3C3 Notifica della fattura:

- BCG_3C3InvoiceNotification_V01.01.xsd
- BCG_BusinessDescription_Types.xsd
- BCG_BusinessTaxIdentifier_Types.xsd
- BCG_common.xsd
- BCG_ContactInformation_Types.xsd
- BCG_GlobalCountryCode.xsd
- BCG_GlobalCurrencyCode.xsd
- BCG_GlobalDocumentTypeCode.xsd
- BCG_GlobalMonetaryAmountTypeCode.xsd
- BCG_GlobalPartnerClassificationCode.xsd
- BCG_GlobalPartnerRoleClassificationCode.xsd
- BCG_GlobalPaymentTermsCode.xsd
- BCG_GlobalProductUnitOfMeasureCode.xsd
- BCG_GlobalSaleTypeCode.xsd
- BCG_GlobalShipmentTermsCode.xsd
- BCG_GlobalShippingServiceLevelCode.xsd
- BCG_GlobalSpecialHandlingCode.xsd
- BCG_InvoiceChargeTypeCode.xsd
- BCG_NationalExportControlClassificationCode.xsd
- BCG_PartnerDescription_Types.xsd
- BCG_PhysicalAddress_Types.xsd
- BCG_string_len_0.xsd
- BCG_xml.xsd

3C4 Notifica della fattura rifiutata

Nella seguente sezione, viene descritto il contenuto del package PIP 3C4 Notifica della fattura rifiutata.

Contenuto del file del package

Nella seguente tabella vengono mostrati i file ZIP e i file XML corrispondenti per il PIP 3C4 Notifica della fattura rifiutata. Le mappe della direttiva comune a tutte le versioni vengono mostrate nella sezione successiva.

Tabella 77. File ZIP e XML di 3C4 Notifica della fattura rifiutata

Nome file ZIP	Nome file XML
BCG_Package_RNIF1.1_3C4V01.00.zip	BCG_RNIF1.1_3C4V01.00.xml
BCG_Package_RNIFV02.00_3C4V01.00.zip	BCG_RNIFV02.00_3C4V01.00.xml
BCG_Package_RNSC1.0_RNIF1.1_3C4V01.00.zip	BCG_RNSC1.0_RNIF1.1_3C4V01.00.xml
BCG_Package_RNSC1.0_RNIFV02.00_3C4V01.00.zip	BCG_RNSC1.0_RNIFV02.00_3C4V01.00.xml

Contenuto della mappa della direttiva

In questa sezione, vengono elencate le mappe della direttiva per 3C4 Notifica della fattura rifiutata:

- BCG_3C4InvoiceRejectNotification_V01.00.xsd
- BCG_BusinessDescription_Types.xsd
- BCG_BusinessTaxIdentifier_Types.xsd
- BCG_common.xsd
- BCG_ContactInformation_Types.xsd
- BCG_GlobalCountryCode.xsd
- BCG_GlobalInvoiceRejectionCode.xsd
- BCG_GlobalMonetaryAmountTypeCode.xsd
- BCG_GlobalPartnerClassificationCode.xsd
- BCG_PartnerDescription_Types.xsd
- BCG_PhysicalAddress_Types.xsd
- BCG_string_len_0.xsd
- BCG_xml.xsd

3C6 Notifica dell'avviso di pagamento

Nella seguente sezione, viene descritto il contenuto del package PIP 3C6 Notifica dell'avviso di pagamento.

Contenuto del file del package

Nella seguente tabella vengono mostrati i file ZIP e i file XML corrispondenti per il PIP 3C6 Notifica dell'avviso di pagamento. Le mappe della direttiva comune a tutte le versioni vengono mostrate nella sezione successiva.

Tabella 78. File ZIP e XML di 3C6 Notifica dell'avviso di pagamento

Nome file ZIP	Nome file XML
BCG_Package_RNIF1.1_3C6V01.00.zip	BCG_RNIF1.1_3C6V01.00.xml
BCG_Package_RNIFV02.00_3C6V01.00.zip	BCG_RNIFV02.00_3C6V01.00.xml

Tabella 78. File ZIP e XML di 3C6 Notifica dell'avviso di pagamento (Continua)

Nome file ZIP	Nome file XML
BCG_Package_RNSC1.0_RNIF1.1_3C6V01.00.zip	BCG_RNSC1.0_RNIF1.1_3C6V01.00.xml
BCG_Package_RNSC1.0_RNIFV02.00_3C6V01.00.zip	BCG_RNSC1.0_RNIFV02.00_3C6V01.00.xml

Contenuto della mappa della direttiva

In questa sezione, vengono elencate le mappe della direttiva per 3C6 Notifica dell'avviso di pagamento:

- BCG_3C6RemittanceAdviceNotification_V01.00.xsd
- BCG_BusinessDescription_Types.xsd
- BCG_BusinessTaxIdentifier_Types.xsd
- BCG_common.xsd
- BCG_ContactInformation_Types.xsd
- BCG_GlobalCountryCode.xsd
- BCG_GlobalCurrencyCode.xsd
- BCG_GlobalDocumentTypeCode.xsd
- BCG_GlobalFinancialAdjustmentReasonCode.xsd
- BCG_GlobalInvoiceRejectionCode.xsd
- BCG_GlobalMonetaryAmountTypeCode.xsd
- BCG_GlobalPartnerClassificationCode.xsd
- BCG_GlobalPaymentMethodCode.xsd
- BCG_PartnerDescription_Types.xsd
- BCG_PhysicalAddress_Types.xsd
- BCG_string_len_0.xsd
- BCG_xml.xsd

3C7 Notifica di auto-fatturazione

Nella seguente sezione, viene descritto il contenuto del package PIP 3C7 Notifica di auto-fatturazione.

Contenuto del file del package

Nella seguente tabella vengono mostrati i file ZIP e i file XML corrispondenti per il PIP 3C7 Notifica di auto-fatturazione. Le mappe della direttiva comune a tutte le versioni vengono mostrate nella sezione successiva.

Tabella 79. File ZIP e XML di 3C7 Notifica di auto-fatturazione

Nome file ZIP	Nome file XML
BCG_Package_RNIF1.1_3C7V01.00.zip	BCG_RNIF1.1_3C7V01.00.xml
BCG_Package_RNIFV02.00_3C7V01.00.zip	BCG_RNIFV02.00_3C7V01.00.xml
BCG_Package_RNSC1.0_RNIF1.1_3C7V01.00.zip	BCG_RNSC1.0_RNIF1.1_3C7V01.00.xml
BCG_Package_RNSC1.0_RNIFV02.00_3C7V01.00.zip	BCG_RNSC1.0_RNIFV02.00_3C7V01.00.xml

Contenuto della mappa della direttiva

In questa sezione, vengono elencate le mappe della direttiva per 3C7 Notifica di auto-fatturazione:

- BCG_3C7SelfBillingInvoiceNotification_V01.00.xsd
- BCG_BusinessDescription_Types.xsd
- BCG_BusinessDescription_Types_V422.xsd
- BCG_BusinessTaxIdentifier_Types.xsd
- BCG_common.xsd
- BCG_common_V422.xsd
- BCG_ContactInformation_Types.xsd
- BCG_GlobalCountryCode.xsd
- BCG_GlobalCurrencyCode.xsd
- BCG_GlobalDocumentReferenceTypeCode.xsd
- BCG_GlobalDocumentTypeCode.xsd
- BCG_GlobalDocumentTypeCode_V422.xsd
- BCG_GlobalMonetaryAmountTypeCode.xsd
- BCG_GlobalPartnerClassificationCode.xsd
- BCG_GlobalPartnerRoleClassificationCode.xsd
- BCG_GlobalPaymentTermsCode.xsd
- BCG_GlobalProductUnitOfMeasureCode.xsd
- BCG_GlobalSaleTypeCode.xsd
- BCG_GlobalShipmentTermsCode.xsd
- BCG_GlobalShippingServiceLevelCode.xsd
- BCG_InvoiceChargeTypeCode.xsd
- BCG_NationalExportControlClassificationCode.xsd
- BCG_PartnerDescription_Types.xsd
- BCG_PhysicalAddress_Types.xsd
- BCG_string_len_0.xsd
- BCG_xml.xsd

3D8 Distribuzione attività in esecuzione

Nella seguente sezione, viene descritto il contenuto del package PIP 3D8 Distribuzione attività in esecuzione.

Contenuto del file del package

Nella seguente tabella vengono mostrati i file ZIP e i file XML corrispondenti per il PIP 3D8 Distribuzione attività in esecuzione. Le mappe della direttiva comune a tutte le versioni vengono mostrate nella sezione successiva.

Tabella 80. File ZIP e XML di 3D8 Distribuzione attività in esecuzione

Nome file ZIP	Nome file XML
BCG_Package_RNIF1.1_3D8V01.00.zip	BCG_RNIF1.1_3D8V01.00.xml
BCG_Package_RNIFV02.00_3D8V01.00.zip	BCG_RNIFV02.00_3D8V01.00.xml
BCG_Package_RNSC1.0_RNIF1.1_3D8V01.00.zip	BCG_RNSC1.0_RNIF1.1_3D8V01.00.xml
BCG_Package_RNSC1.0_RNIFV02.00_3D8V01.00.zip	BCG_RNSC1.0_RNIFV02.00_3D8V01.00.xml

Contenuto della mappa della direttiva

In questa sezione, vengono elencate le mappe della direttiva per 3D8 Distribuzione attività in esecuzione:

- BCG_3D8WorkInProcessNotification_V01.00.xsd
- BCG_BusinessDescription_Types.xsd
- BCG_BusinessTaxIdentifier_Types.xsd
- BCG_common.xsd
- BCG_ContactInformation_Types.xsd
- BCG_GlobalCountryCode.xsd
- BCG_GlobalDocumentReferenceTypeCode.xsd
- BCG_GlobalLotCode.xsd
- BCG_GlobalLotQuantityClassificationCode.xsd
- BCG_GlobalLotStatusCode.xsd
- BCG_GlobalPartnerClassificationCode.xsd
- BCG_GlobalPriorityCode.xsd
- BCG_GlobalProductUnitOfMeasureCode.xsd
- BCG_GlobalWorkInProcessLocationCode.xsd
- BCG_GlobalWorkInProcessPartTypeCode.xsd
- BCG_PartnerDescription_Types.xsd
- BCG_PhysicalAddress_Types.xsd
- BCG_string_len_0.xsd
- BCG_xml.xsd

4A1 Notifica di previsione strategica

Nella seguente sezione, viene descritto il contenuto del package PIP 4A1 Notifica di previsione strategica.

Contenuto del file del package

Nella seguente tabella vengono mostrati i file ZIP e i file XML corrispondenti per il PIP 4A1 Notifica di previsione strategica. Le mappe della direttiva comune a tutte le versioni vengono mostrate nella sezione successiva.

Tabella 81. File ZIP E XML di 4A1 Notifica di previsione strategica

Nome file ZIP	Nome file XML
BCG_Package_RNIF1.1_4A1V02.00.zip	BCG_RNIF1.1_4A1V02.00.xml
BCG_Package_RNIFV02.00_4A1V02.00.zip	BCG_RNIFV02.00_4A1V02.00.xml
BCG_Package_RNSC1.0_RNIF1.1_4A1V02.00.zip	BCG_RNSC1.0_RNIF1.1_4A1V02.00.xml
BCG_Package_RNSC1.0_RNIFV02.00_4A1V02.00.zip	BCG_RNSC1.0_RNIFV02.00_4A1V02.00.xml

Contenuto della mappa della direttiva

In questa sezione, vengono elencate le mappe della direttiva per 4A1 Notifica di previsione strategica:

- BCG_4A1StrategicForecastNotification_V02.00.xsd
- BCG_BusinessDescription_Types.xsd
- BCG_BusinessTaxIdentifier_Types.xsd

- BCG_common.xsd
- BCG_ContactInformation_Types.xsd
- BCG_GlobalCountryCode.xsd
- BCG_GlobalCurrencyCode.xsd
- BCG_GlobalForecastEventCode.xsd
- BCG_GlobalForecastIntervalCode.xsd
- BCG_GlobalForecastTypeCode.xsd
- BCG_GlobalPartnerClassificationCode.xsd
- BCG_GlobalPartnerReferenceTypeCode.xsd
- BCG_GlobalProductUnitOfMeasureCode.xsd
- BCG_PartnerDescription_Types.xsd
- BCG_PhysicalAddress_Types.xsd
- BCG_StrategicForecastQuantityTypeCode.xsd
- BCG_string_len_0.xsd
- BCG_xml.xsd

4A3 Notifica di previsione soglia release

Nella seguente sezione, viene descritto il contenuto del package PIP 4A3 Notifica di previsione soglia release.

Contenuto del file del package

Nella seguente tabella vengono mostrati i file ZIP e i file XML corrispondenti per il PIP 4A3 Notifica di previsione soglia release. Le mappe della direttiva comune a tutte le versioni vengono mostrate nella sezione successiva.

Tabella 82. File ZIP e XML di 4A3 Notifica di previsione soglia release

Nome file ZIP	Nome file XML
BCG_Package_RNIF1.1_4A3V02.00.zip	BCG_RNIF1.1_4A3V02.00.xml
BCG_Package_RNIFV02.00_4A3V02.00.zip	BCG_RNIFV02.00_4A3V02.00.xml
BCG_Package_RNSC1.0_RNIF1.1_4A3V02.00.zip	BCG_RNSC1.0_RNIF1.1_4A3V02.00.xml
BCG_Package_RNSC1.0_RNIFV02.00_4A3V02.00.zip	BCG_RNSC1.0_RNIFV02.00_4A3V02.00.xml

Contenuto della mappa della direttiva

In questa sezione, vengono elencate le mappe della direttiva per 4A3 Notifica di previsione soglia release:

- BCG_4A3ThresholdReleaseForecastNotification_V02.00.xsd
- BCG_BusinessDescription_Types.xsd
- BCG_BusinessTaxIdentifier_Types.xsd
- BCG_common.xsd
- BCG_ContactInformation_Types.xsd
- BCG_GlobalCountryCode.xsd
- BCG_GlobalCurrencyCode.xsd
- BCG_GlobalForecastEventCode.xsd
- BCG_GlobalForecastIntervalCode.xsd
- BCG_GlobalForecastInventoryTypeCode.xsd

- BCG_GlobalForecastReferenceTypeCode.xsd
- BCG_GlobalPartnerClassificationCode.xsd
- BCG_GlobalPartnerReferenceTypeCode.xsd
- BCG_GlobalProductUnitOfMeasureCode.xsd
- BCG_OrderForecastQuantityTypeCode.xsd
- BCG_PartnerDescription_Types.xsd
- BCG_PhysicalAddress_Types.xsd
- BCG_string_len_0.xsd
- BCG_xml.xsd

4A4 Notifica di previsione pianificazione release

Nella seguente sezione, viene descritto il contenuto del package PIP 4A4 Notifica di previsione pianificazione release.

Contenuto del file del package

Nella seguente tabella vengono mostrati i file ZIP e i file XML corrispondenti per il PIP 4A4 Notifica di previsione pianificazione release. PIP. Le mappe della direttiva comune a tutte le versioni vengono mostrate nella sezione successiva.

Tabella 83. File ZIP e XML di 4A4 Notifica di previsione pianificazione release

Nome file ZIP	Nome file XML
BCG_Package_RNIF1.1_4A4R02.00A.zip	BCG_RNIF1.1_4A4R02.00A.xml
BCG_Package_RNIFV02.00_4A4R02.00A.zip	BCG_RNIFV02.00_4A4R02.00A.xml
BCG_Package_RNSC1.0_RNIF1.1_4A4R02.00A.zip	BCG_RNSC1.0_RNIF1.1_4A4R02.00A.xml
BCG_Package_RNSC1.0_RNIFV02.00_4A4R02.00A.zip	BCG_RNSC1.0_RNIFV02.00_4A4R02.00A.xml

Contenuto della mappa della direttiva

In questa sezione, vengono elencate le mappe della direttiva per 4A4 Notifica di previsione pianificazione release:

- BCG_4A4PlanningReleaseForecastNotification_R02.00A.xsd
- BCG_BusinessDescription_Types.xsd
- BCG_BusinessTaxIdentifier_Types.xsd
- BCG_common.xsd
- BCG_ContactInformation_Types.xsd
- BCG_GlobalCountryCode.xsd
- BCG_GlobalCurrencyCode.xsd
- BCG_GlobalForecastInventoryTypeCode.xsd
- BCG_GlobalForecastQuantityTypeCode_V422.xsd
- BCG_GlobalForecastReferenceTypeCode.xsd
- BCG_GlobalIntervalCode.xsd
- BCG_GlobalPartnerClassificationCode.xsd
- BCG_GlobalPartnerReferenceTypeCode.xsd
- BCG_GlobalProductUnitOfMeasureCode.xsd
- BCG_GlobalTransportEventCode.xsd
- BCG_PartnerDescription_Types.xsd

- BCG_PhysicalAddress_Types.xsd
- BCG_PhysicalAddress_Types_V422.xsd
- BCG_string_len_0.xsd
- BCG_xml.xsd

4A5 Notifica di replica previsione

Nella seguente sezione, viene descritto il contenuto del package PIP 4A5 Notifica di replica previsione.

Contenuto del file del package

Nella seguente tabella vengono mostrati i file ZIP e i file XML corrispondenti per il PIP 4A5 Notifica di replica previsione. Le mappe della direttiva comune a tutte le versioni vengono mostrate nella sezione successiva.

Tabella 84. File ZIP e XML di 4A5 Notifica di replica previsione

Nome file ZIP	Nome file XML
BCG_Package_RNIF1.1_4A5V02.00.zip	BCG_RNIF1.1_4A5V02.00.xml
BCG_Package_RNIFV02.00_4A5V02.00.zip	BCG_RNIFV02.00_4A5V02.00.xml
BCG_Package_RNSC1.0_RNIF1.1_34A5V02.00.zip	BCG_RNSC1.0_RNIF1.1_34A5V02.00.xml
BCG_Package_RNSC1.0_RNIFV02.00_4A5V02.00.zip	BCG_RNSC1.0_RNIFV02.00_4A5V02.00.xml

Contenuto della mappa della direttiva

In questa sezione, vengono elencate le mappe della direttiva per 4A5 Notifica di replica previsione:

- BCG_4A5ForecastReplyNotification_V02.00.xsd
- BCG_BusinessDescription_Types.xsd
- BCG_BusinessTaxIdentifier_Types.xsd
- BCG_common.xsd
- BCG_ContactInformation_Types.xsd
- BCG_ForecastReplyQuantityTypeCode.xsd
- BCG_GlobalCountryCode.xsd
- BCG_GlobalCurrencyCode.xsd
- BCG_GlobalForecastEventCode.xsd
- BCG_GlobalForecastIntervalCode.xsd
- BCG_GlobalForecastInventoryTypeCode.xsd
- BCG_GlobalForecastReferenceTypeCode.xsd
- BCG_GlobalForecastResponseCode.xsd
- BCG_GlobalForecastRevisionReasonCode.xsd
- BCG_GlobalPartnerClassificationCode.xsd
- BCG_GlobalPartnerReferenceTypeCode.xsd
- BCG_GlobalProductUnitOfMeasureCode.xsd
- BCG_PartnerDescription_Types.xsd
- BCG_PhysicalAddress_Types.xsd
- BCG_string_len_0.xsd
- BCG_xml.xsd

4B2 Notifica di ricezione della spedizione

Nella seguente sezione, viene descritto il contenuto del package PIP 4B2 Notifica di ricezione della spedizione.

Contenuto del file del package

Nella seguente tabella vengono mostrati i file ZIP e i file XML corrispondenti per il PIP 4B2 Notifica di ricezione della spedizione. Le mappe della direttiva comune a tutte le versioni vengono mostrate nella sezione successiva.

Tabella 85. File ZIP e XML di 4B2 Notifica di ricezione della spedizione

Nome file ZIP	Nome file XML
BCG_Package_RNIF1.1_4B2V01.00.zip	BCG_RNIF1.1_4B2V01.00.xml
BCG_Package_RNIFV02.00_4B2V01.00.zip	BCG_RNIFV02.00_4B2V01.00.xml
BCG_Package_RNSC1.0_RNIF1.1_4B2V01.00.zip	BCG_RNSC1.0_RNIF1.1_4B2V01.00.xml
BCG_Package_RNSC1.0_RNIFV02.00_4B2V01.00.zip	BCG_RNSC1.0_RNIFV02.00_4B2V01.00.xml

Contenuto della mappa della direttiva

In questa sezione, vengono elencate le mappe della direttiva per 4B2 Notifica di ricezione della spedizione:

- BCG_4B2ShipmentReceiptNotification_V01.00.xsd
- BCG_BusinessDescription_Types.xsd
- BCG_BusinessTaxIdentifier_Types.xsd
- BCG_common.xsd
- BCG_ContactInformation_Types.xsd
- BCG_GlobalCountryCode.xsd
- BCG_GlobalDocumentReferenceTypeCode.xsd
- BCG_GlobalLotDiscrepancyReasonCode.xsd
- BCG_GlobalPartnerClassificationCode.xsd
- BCG_GlobalPartnerRoleClassificationCode.xsd
- BCG_GlobalProductUnitOfMeasureCode.xsd
- BCG_GlobalReceivingDiscrepancyCode.xsd
- BCG_GlobalReceivingDiscrepancyReasonCode.xsd
- BCG_GlobalSpecialFulfillmentRequestCode.xsd
- BCG_GlobalSpecialHandlingCode.xsd
- BCG_GlobalTrackingReferenceTypeCode.xsd
- BCG_PartnerDescription_Types.xsd
- BCG_PhysicalAddress_Types.xsd
- BCG_string_len_0.xsd
- BCG_xml.xsd

4B3 Notifica di consumo

Nella seguente sezione, viene descritto il contenuto del package PIP 4B3 Notifica di consumo.

Contenuto del file del package

Nella seguente tabella vengono mostrati i file ZIP e i file XML corrispondenti per il PIP 4B3 Notifica di consumo. Le mappe della direttiva comune a tutte le versioni vengono mostrate nella sezione successiva.

Tabella 86. File ZIP e XML 4B3 Notifica di consumo

Nome file ZIP	Nome file XML
BCG_Package_RNIF1.1_4B3V01.00.zip	BCG_RNIF1.1_4B3V01.00.xml
BCG_Package_RNIFV02.00_4B3V01.00.zip	BCG_RNIFV02.00_4B3V01.00.xml
BCG_Package_RNSC1.0_RNIF1.1_4B3V01.00.zip	BCG_RNSC1.0_RNIF1.1_4B3V01.00.xml
BCG_Package_RNSC1.0_RNIFV02.00_4B3V01.00.zip	BCG_RNSC1.0_RNIFV02.00_4B3V01.00.xml

Contenuto della mappa della direttiva

In questa sezione, vengono elencate le mappe della direttiva per 4B3 Notifica di consumo:

- BCG_4B3ConsumptionNotification_V01.00.xsd
- BCG_BusinessDescription_Types.xsd
- BCG_BusinessDescription_Types_V422.xsd
- BCG_BusinessDescription_Types_V43.xsd
- BCG_BusinessTaxIdentifier_Types.xsd
- BCG_common.xsd
- BCG_common_V43.xsd
- BCG_ContactInformation_Types.xsd
- BCG_ContactInformation_Types_V422.xsd
- BCG_ContactInformation_Types_V43.xsd
- BCG_GlobalCountryCode.xsd
- BCG_GlobalCurrencyCode.xsd
- BCG_GlobalDocumentReferenceTypeCode_V43.xsd
- BCG_GlobalInventoryCode_V43.xsd
- BCG_GlobalPartnerClassificationCode_V422.xsd
- BCG_GlobalPartnerClassificationCode_V43.xsd
- BCG_GlobalProductUnitOfMeasureCode.xsd
- BCG_PartnerDescription_Types_V43.xsd
- BCG_PhysicalAddress_Types.xsd
- BCG_string_len_0.xsd
- BCG_xml.xsd

4C1 Distribuzione report inventario V02.01

Nella seguente sezione, viene descritto il contenuto del package PIP 4C1 Distribuzione report inventario V02.01.

Contenuto del file del package

Nella seguente tabella vengono mostrati i file ZIP e i file XML corrispondenti per il PIP 4C1 Distribuzione report inventario. Le mappe della direttiva comune a tutte le versioni vengono mostrate nella sezione successiva.

Tabella 87. File ZIP e XML di 4C1 Distribuzione report inventario

Nome file ZIP	Nome file XML
BCG_Package_RNIF1.1_4C1V02.01.zip	BCG_RNIF1.1_4C1V02.01.xml
BCG_Package_RNIFV02.00_4C1V02.01.zip	BCG_RNIFV02.00_4C1V02.01.xml
BCG_Package_RNSC1.0_RNIF1.1_4C1V02.01.zip	BCG_RNSC1.0_RNIF1.1_4C1V02.01.xml
BCG_Package_RNSC1.0_RNIFV02.00_4C1V02.01.zip	BCG_RNSC1.0_RNIFV02.00_4C1V02.01.xml

Contenuto della mappa della direttiva

In questa sezione, vengono elencate le mappe della direttiva per 4C1 Distribuzione report inventario:

- BCG_4C1InventoryReportNotification_V02.01.xsd
- BCG_BusinessDescription_Types.xsd
- BCG_BusinessTaxIdentifier_Types.xsd
- BCG_common.xsd
- BCG_common_V422.xsd
- BCG_ContactInformation_Types.xsd
- BCG_ContactInformation_Types_V422.xsd
- BCG_GlobalCountryCode.xsd
- BCG_GlobalDocumentReferenceTypeCode.xsd
- BCG_GlobalInventoryCode.xsd
- BCG_GlobalPartnerClassificationCode.xsd
- BCG_GlobalPartnerRoleClassificationCode.xsd
- BCG_GlobalProductUnitOfMeasureCode.xsd
- BCG_PhysicalAddress_Types.xsd
- BCG_PhysicalAddress_Types_V422.xsd
- BCG_string_len_0.xsd
- BCG_xml.xsd

4C1 Distribuzione report inventario V02.03

Nella seguente sezione, viene descritto il contenuto del package PIP 4C1 Distribuzione report inventario V02.03.

Contenuto del file del package

Nella seguente tabella vengono mostrati i file ZIP e i file XML corrispondenti per il PIP 4C1 Distribuzione report inventario. Le mappe della direttiva comune a tutte le versioni vengono mostrate nella sezione successiva.

Tabella 88. File ZIP e XML di 4C1 Distribuzione report inventario

Nome file ZIP	Nome file XML
BCG_Package_RNIF1.1_4C1V02.03.zip	BCG_RNIF1.1_4C1V02.03.xml
BCG_Package_RNIFV02.00_4C1V02.03.zip	BCG_RNIFV02.00_4C1V02.03.xml
BCG_Package_RNSC1.0_RNIF1.1_4C1V02.03.zip	BCG_RNSC1.0_RNIF1.1_4C1V02.03.xml
BCG_Package_RNSC1.0_RNIFV02.00_4C1V02.03.zip	BCG_RNSC1.0_RNIFV02.00_4C1V02.03.xml

Contenuto della mappa della direttiva

In questa sezione, vengono elencate le mappe della direttiva per 4C1 Distribuzione report inventario:

- BCG_4C1InventoryReportNotification_V02.03.xsd
- BCG_BusinessDescription_Types.xsd
- BCG_BusinessTaxIdentifier_Types.xsd
- BCG_common.xsd
- BCG_ContactInformation_Types.xsd
- BCG_GlobalCountryCode.xsd
- BCG_GlobalDocumentReferenceTypeCode.xsd
- BCG_GlobalInventoryCode.xsd
- BCG_GlobalPartnerClassificationCode.xsd
- BCG_GlobalPartnerRoleClassificationCode.xsd
- BCG_GlobalProductUnitOfMeasureCode.xsd
- BCG_PhysicalAddress_Types.xsd
- BCG_string_len_0.xsd
- BCG_xml.xsd

5C1 Distribuzione elenco prodotto

Nella seguente sezione, viene descritto il contenuto del package PIP 5C1 Distribuzione elenco prodotto.

Contenuto del file del package

Nella seguente tabella vengono mostrati i file ZIP e i file XML corrispondenti per il PIP 5C1 Distribuzione elenco prodotto. Le mappe della direttiva comune a tutte le versioni vengono mostrate nella sezione successiva.

Tabella 89. File ZIP e XML di 5C1 Distribuzione elenco prodotto

Nome file ZIP	Nome file XML
BCG_Package_RNIF1.1_5C1V01.00.zip	BCG_RNIF1.1_5C1V01.00.xml
BCG_Package_RNIFV02.00_5C1V01.00.zip	BCG_RNIFV02.00_5C1V01.00.xml
BCG_Package_RNSC1.0_RNIF1.1_5C1V01.00.zip	BCG_RNSC1.0_RNIF1.1_5C1V01.00.xml
BCG_Package_RNSC1.0_RNIFV02.00_5C1V01.00.zip	BCG_RNSC1.0_RNIFV02.00_5C1V01.00.xml

Contenuto della mappa della direttiva

In questa sezione, vengono elencate le mappe della direttiva per 5C1 Distribuzione elenco prodotto:

- BCG_5C1ProductListNotification_V01.00.xsd
- BCG_BusinessDescription_Types.xsd
- BCG_BusinessTaxIdentifier_Types.xsd
- BCG_common.xsd
- BCG_ContactInformation_Types.xsd
- BCG_GlobalCountryCode.xsd
- BCG_GlobalCurrencyCode.xsd
- BCG_GlobalPartnerClassificationCode.xsd

- BCG_GlobalPartnerRoleClassificationCode.xsd
- BCG_GlobalPriceTypeCode.xsd
- BCG_PartnerDescription_Types.xsd
- BCG_PhysicalAddress_Types.xsd
- BCG_string_len_0.xsd
- BCG_xml.xsd

5C2 Richiesta registrazione progetto

Nella seguente sezione, viene descritto il contenuto del package PIP 5C2 Richiesta registrazione progetto.

Contenuto del file del package

Nella seguente tabella vengono mostrati i file ZIP e i file XML corrispondenti per il PIP 5C2 Richiesta registrazione progetto. Le mappe della direttiva comune a tutte le versioni vengono mostrate nella sezione successiva.

Tabella 90. File ZIP e XML di 5C2 Richiesta registrazione progetto

Nome file ZIP	Nome file XML
BCG_Package_RNIF1.1_5C2V01.00.zip	BCG_RNIF1.1_5C2V01.00.xml
BCG_Package_RNIFV02.00_5C2V01.00.zip	BCG_RNIFV02.00_5C2V01.00.xml
BCG_Package_RNSC1.0_RNIF1.1_5C2V01.00.zip	BCG_RNSC1.0_RNIF1.1_5C2V01.00.xml
BCG_Package_RNSC1.0_RNIFV02.00_5C2V01.00.zip	BCG_RNSC1.0_RNIFV02.00_5C2V01.00.xml

Contenuto della mappa della direttiva

In questa sezione, vengono elencate le mappe della direttiva per 5C2 Richiesta registrazione progetto:

- BCG_5C2DesignRegistrationConfirmation_V01.00.xsd
- BCG_5C2DesignRegistrationRequest_V01.00.xsd
- BCG_BusinessDescription_Types.xsd
- BCG_common.xsd
- BCG_common_V422.xsd
- BCG_common_V43.xsd
- BCG_ContactInformation_Types.xsd
- BCG_DesignWinStatusReasonCode_V43.xsd
- BCG_GlobalAttachmentDescriptionCode_V422.xsd
- BCG_GlobalCountryCode.xsd
- BCG_GlobalCurrencyCode.xsd
- BCG_GlobalDocumentReferenceTypeCode.xsd
- BCG_GlobalMimeTypeQualifierCode_V43.xsd
- BCG_GlobalMonetaryAmountTypeCode.xsd
- BCG_GlobalPartnerClassificationCode_V43.xsd
- BCG_GlobalPartnerRoleClassificationCode_V43.xsd
- BCG_GlobalPriceTypeCode_V43.xsd
- BCG_GlobalRegistrationComplexityLevelCode.xsd
- BCG_GlobalRegistrationInvolvementLevelCode.xsd

- BCG_InvoiceChargeTypeCode_V422.xsd
- BCG_PartnerDescription_Types.xsd
- BCG_PartnerDescription_Types_V43.xsd
- BCG_PhysicalAddress_Types.xsd
- BCG_string_len_0.xsd
- BCG_xml.xsd

5C4 Distribuzione stato registrazione

Nella seguente sezione, viene descritto il contenuto del package PIP 5C4 DDistribuzione stato registrazione.

Contenuto del file del package

Nella seguente tabella vengono mostrati i file ZIP e i file XML corrispondenti per il PIP 5C4 Distribuzione stato registrazione. Le mappe della direttiva comune a tutte le versioni vengono mostrate nella sezione successiva.

Tabella 91. File ZIP e XML di 5C4 Distribuzione stato registrazione

Nome file ZIP	Nome file XML
BCG_Package_RNIF1.1_5C4V01.02.zip	BCG_RNIF1.1_5C4V01.02.xml
BCG_Package_RNIFV02.00_5C4V01.02.zip	BCG_RNIFV02.00_5C4V01.02.xml
BCG_Package_RNSC1.0_RNIF1.1_5C4V01.023.zip	BCG_RNSC1.0_RNIF1.1_5C4V01.023.xml
BCG_Package_RNSC1.0_RNIFV02.00_5C4V01.02.zip	BCG_RNSC1.0_RNIFV02.00_5C4V01.02.xml

Contenuto della mappa della direttiva

In questa sezione, vengono elencate le mappe della direttiva per 5C4 Distribuzione stato registrazione:

- BCG_5C4RegistrationStatusNotification_V01.02.xsd
- BCG_BusinessDescription_Types.xsd
- BCG_BusinessTaxIdentifier_Types.xsd
- BCG_common.xsd
- BCG_ContactInformation_Types.xsd
- BCG_GlobalCountryCode.xsd
- BCG_GlobalPartnerClassificationCode.xsd
- BCG_GlobalPartnerRoleClassificationCode.xsd
- BCG_GlobalRegistrationComplexityLevelCode.xsd
- BCG_GlobalRegistrationInvolvementLevelCode.xsd
- BCG_PartnerDescription_Types.xsd
- BCG_PhysicalAddress_Types.xsd
- BCG_string_len_0.xsd
- BCG_xml.xsd

5D1 Richiesta sped. da magazzino e autorizzazione addebito

Nella seguente sezione, viene descritto il contenuto del package PIP 5D1 Richiesta sped. da magazzino e autorizzazione addebito.

Contenuto del file del package

Nella seguente tabella vengono mostrati i file ZIP e i file XML corrispondenti per il PIP 5D1 Richiesta sped. da magazzino e autorizzazione addebito. Le mappe della direttiva comune a tutte le versioni vengono mostrate nella sezione successiva.

Tabella 92. File ZIP e XML di 5D1 Richiesta sped. da magazzino e autorizzazione addebito

Nome file ZIP	Nome file XML
BCG_Package_RNIF1.1_5D1V01.00.zip	BCG_RNIF1.1_5D1V01.00.xml
BCG_Package_RNIFV02.00_5D1V01.00.zip	BCG_RNIFV02.00_5D1V01.00.xml
BCG_Package_RNSC1.0_RNIF1.1_5D1V01.00.zip	BCG_RNSC1.0_RNIF1.1_5D1V01.00.xml
BCG_Package_RNSC1.0_RNIFV02.00_5D1V01.00.zip	BCG_RNSC1.0_RNIFV02.00_5D1V01.00.xml

Contenuto della mappa della direttiva

Nella seguente sezione, viene descritto il contenuto del package PIP 5D1 Richiesta sped. da magazzino e autorizzazione addebito:

- BCG_5D1ShipFromStockAndDebitAuthorizationConfirmation_V01.00.xsd
- BCG_5D1ShipFromStockAndDebitAuthorizationRequest_V01.00.xsd
- BCG_BusinessDescription_Types.xsd
- BCG_BusinessTaxIdentifier_Types.xsd
- BCG_common.xsd
- BCG_ContactInformation_Types.xsd
- BCG_GlobalCountryCode.xsd
- BCG_GlobalCurrencyCode.xsd
- BCG_GlobalDocumentReferenceTypeCode.xsd
- BCG_GlobalPartnerClassificationCode.xsd
- BCG_GlobalPartnerRoleClassificationCode.xsd
- BCG_GlobalPriceTypeCode.xsd
- BCG_GlobalProductUnitOfMeasureCode.xsd
- BCG_GlobalShipFromStockAndDebitAuthorizationRejectionCode.xsd
- BCG_PartnerDescription_Types.xsd
- BCG_PhysicalAddress_Types.xsd
- BCG_string_len_0.xsd
- BCG_xml.xsd

6C1 Query concessione servizio

Nella seguente sezione, viene descritto il contenuto del package PIP 6C1 Query concessione servizio.

Contenuto del file del package

Nella seguente tabella vengono mostrati i file ZIP e i file XML corrispondenti per il PIP 6C1 Query concessione servizio. Le mappe della direttiva comune a tutte le versioni vengono mostrate nella sezione successiva.

Tabella 93. File ZIP e XML di 6C1 Query concessione servizio

Nome file ZIP	Nome file XML
BCG_Package_RNIF1.1_6C1V01.00.zip	BCG_RNIF1.1_6C1V01.00.xml
BCG_Package_RNIFV02.00_6C1V01.00.zip	BCG_RNIFV02.00_6C1V01.00.xml
BCG_Package_RNSC1.0_RNIF1.1_6C1V01.00.zip	BCG_RNSC1.0_RNIF1.1_6C1V01.00.xml
BCG_Package_RNSC1.0_RNIFV02.00_6C1V01.00.zip	BCG_RNSC1.0_RNIFV02.00_6C1V01.00.xml

Contenuto della mappa della direttiva

In questa sezione, vengono elencate le mappe della direttiva per 6C1 Query concessione servizio:

- BCG_6C1ServiceEntitlementQuery_V01.00.xsd
- BCG_6C1ServiceEntitlementStatusResponse_V01.00.xsd
- BCG_common_V43.xsd
- BCG_ContactInformation_Types.xsd
- BCG_ContactInformation_Types_V43.xsd
- BCG_GlobalCurrencyCode.xsd
- BCG_GlobalNotificationCode_V43.xsd
- BCG_GlobalPartnerClassificationCode_V43.xsd
- BCG_GlobalPaymentTypeCode_V43.xsd
- BCG_GlobalServiceDeliveryMethodCode_V43.xsd
- BCG_GlobalShippingServiceLevelCode.xsd
- BCG_GlobalWarrantyMethodCode_V43.xsd
- BCG_GlobalWarrantyProgramCode_V43.xsd
- BCG_GlobalWarrantyTypeCode_V43.xsd
- BCG_PartnerDescription_Types_V43.xsd
- BCG_string_len_0.xsd
- BCG_xml.xsd

6C2 Richiesta garanzia reclamo

Nella seguente sezione, viene descritto il contenuto del package PIP 6C2 Richiesta garanzia reclamo.

Contenuto del file del package

Nella seguente tabella vengono mostrati i file ZIP e i file XML corrispondenti per il PIP 6C2 Richiesta garanzia reclamo. Le mappe della direttiva comune a tutte le versioni vengono mostrate nella sezione successiva.

Tabella 94. File ZIP e XML di 6C2 Richiesta garanzia reclamo

Nome file ZIP	Nome file XML
BCG_Package_RNIF1.1_6C2V01.00.zip	BCG_RNIF1.1_6C2V01.00.xml
BCG_Package_RNIFV02.00_6C2V01.00.zip	BCG_RNIFV02.00_6C2V01.00.xml
BCG_Package_RNSC1.0_RNIF1.1_6C2V01.00.zip	BCG_RNSC1.0_RNIF1.1_6C2V01.00.xml
BCG_Package_RNSC1.0_RNIFV02.00_6C2V01.00.zip	BCG_RNSC1.0_RNIFV02.00_6C2V01.00.xml

Contenuto della mappa della direttiva

In questa sezione, vengono elencate le mappe della direttiva per 6C2 Richiesta garanzia reclamo:

- BCG_6C2WarrantyClaimConfirmation_V01.00.xsd
- BCG_6CWarrantyClaimRequest_V01.00.xsd
- BCG_common.xsd
- BCG_ContactInformation_Types.xsd
- BCG_GlobalCurrencyCode.xsd
- BCG_GlobalDocumentReferenceTypeCode.xsd
- BCG_GlobalFailureTypeCode_V43.xsd
- BCG_GlobalOperatingSystemCode_V43.xsd
- BCG_GlobalPartnerClassificationCode_V43.xsd
- BCG_GlobalPartnerRoleClassificationCode_V43.xsd
- BCG_GlobalPaymentTypeCode_V43.xsd
- BCG_GlobalServiceDeliveryMethodCode_V43.xsd
- BCG_GlobalWarrantyTypeCode_V43.xsd
- BCG_PartnerDescription_Types_V43.xsd
- BCG_string_len_0.xsd
- BCG_xml.xsd

7B1 Distribuzione attività in esecuzione

Nella seguente sezione, viene descritto il contenuto del package PIP 7B1 Distribuzione attività in esecuzione.

Contenuto del file del package

Nella seguente tabella vengono mostrati i file ZIP e i file XML corrispondenti per il PIP 7B1 Distribuzione attività in esecuzione. Le mappe della direttiva comune a tutte le versioni vengono mostrate nella sezione successiva.

Tabella 95. File ZIP e XML di 7B1 Distribuzione attività in esecuzione

Nome file ZIP	Nome file XML
BCG_Package_RNIF1.1_7B1V01.00.zip	BCG_RNIF1.1_7B1V01.00.xml
BCG_Package_RNIFV02.00_37B1V01.00.zip	BCG_RNIFV02.00_37B1V01.00.xml
BCG_Package_RNSC1.0_RNIF1.1_7B1V01.00.zip	BCG_RNSC1.0_RNIF1.1_7B1V01.00.xml
BCG_Package_RNSC1.0_RNIFV02.00_7B1V01.00.zip	BCG_RNSC1.0_RNIFV02.00_7B1V01.00.xml

Contenuto della mappa della direttiva

In questa sezione, vengono elencate le mappe della direttiva per 7B1 Distribuzione attività in esecuzione:

- BCG_7B1WorkInProcessNotification_V01.00.xsd
- BCG_BusinessDescription_Types.xsd
- BCG_BusinessTaxIdentifier_Types.xsd
- BCG_common.xsd
- BCG_ContactInformation_Types.xsd
- BCG_GlobalChangeReasonCode.xsd

- BCG_GlobalCountryCode.xsd
- BCG_GlobalDocumentReferenceTypeCode.xsd
- BCG_GlobalEquipmentTypeCode.xsd
- BCG_GlobalLotCode.xsd
- BCG_GlobalLotQuantityClassificationCode.xsd
- BCG_GlobalLotStatusCode.xsd
- BCG_GlobalPartnerClassificationCode.xsd
- BCG_GlobalPartnerRoleClassificationCode.xsd
- BCG_GlobalPriorityCode.xsd
- BCG_GlobalProductUnitOfMeasureCode.xsd
- BCG_GlobalWorkInProcessLocationCode.xsd
- BCG_GlobalWorkInProcessPartTypeCode.xsd
- BCG_GlobalWorkInProcessQuantityChangeCode.xsd
- BCG_GlobalWorkInProcessTypeCode.xsd
- BCG_PartnerDescription_Types.xsd
- BCG_PhysicalAddress_Types.xsd
- BCG_string_len_0.xsd
- BCG_xml.xsd

7B5 Notifica ordine attività industriale

Nella seguente sezione, viene descritto il contenuto del package PIP 7B5 Notifica ordine attività industriale.

Contenuto del file del package

Nella seguente tabella vengono mostrati i file ZIP e i file XML corrispondenti per il PIP 7B5 Notifica ordine attività industriale. Le mappe della direttiva comune a tutte le versioni vengono mostrate nella sezione successiva.

Tabella 96. File ZIP e XML di 7B5 Notifica ordine attività industriale

Nome file ZIP	Nome file XML
BCG_Package_RNIF1.1_7B5V01.00.zip	BCG_RNIF1.1_7B5V01.00.xml
BCG_Package_RNIFV02.00_7B5V01.00.zip	BCG_RNIFV02.00_7B5V01.00.xml
BCG_Package_RNSC1.0_RNIF1.1_7B5V01.00.zip	BCG_RNSC1.0_RNIF1.1_7B5V01.00.xml
BCG_Package_RNSC1.0_RNIFV02.00_7B5V01.00.zip	BCG_RNSC1.0_RNIFV02.00_7B5V01.00.xml

Contenuto della mappa della direttiva

In questa sezione, vengono elencate le mappe della direttiva per 7B5 Notifica ordine attività industriale:

- BCG_7B5NotifyOfManufacturingWorkOrder_V01.00.xsd
- BCG_BusinessDescription_Types.xsd
- BCG_BusinessTaxIdentifier_Types.xsd
- BCG_common.xsd
- BCG_ContactInformation_Types.xsd
- BCG_GlobalAttachmentDescriptionCode_V422.xsd
- BCG_GlobalBusinessActionCode_V422.xsd

- BCG_GlobalChangeReasonCode.xsd
- BCG_GlobalCountryCode.xsd
- BCG_GlobalDevicePackageTypeCode_V422.xsd
- BCG_GlobalDocumentReferenceTypeCode.xsd
- BCG_GlobalLineItemStatusCode.xsd
- BCG_GlobalLotCode.xsd
- BCG_GlobalMimeTypeQualifierCode_V422.xsd
- BCG_GlobalPackageTypeCode.xsd
- BCG_GlobalPartnerClassificationCode.xsd
- BCG_GlobalPartnerRoleClassificationCode.xsd
- BCG_GlobalPhysicalUnitOfMeasureCode.xsd
- BCG_GlobalPriorityCode.xsd
- BCG_GlobalProductUnitOfMeasureCode.xsd
- BCG_GlobalWorkInProcessLocationCode.xsd
- BCG_PartnerDescription_Types.xsd
- BCG_PhysicalAddress_Types.xsd
- BCG_string_len_0.xsd
- BCG_xml.xsd

7B6 Notifica replica ordine attività industriale

Nella seguente sezione, viene descritto il contenuto del package PIP 7B6 Notifica replica ordine attività industriale.

Contenuto del file del package

Nella seguente tabella vengono mostrati i file ZIP e i file XML corrispondenti per il PIP 7B6 Notifica replica ordine attività industriale. Le mappe della direttiva comune a tutte le versioni vengono mostrate nella sezione successiva.

Tabella 97. File ZIP e XML di 7B6 Notifica replica ordine attività industriale

Nome file ZIP	Nome file XML
BCG_Package_RNIF1.1_7B6V01.00.zip	BCG_RNIF1.1_7B6V01.00.xml
BCG_Package_RNIFV02.00_7B6V01.00.zip	BCG_RNIFV02.00_7B6V01.00.xml
BCG_Package_RNSC1.0_RNIF1.1_7B6V01.00.zip	BCG_RNSC1.0_RNIF1.1_7B6V01.00.xml
BCG_Package_RNSC1.0_RNIFV02.00_7B6V01.00.zip	BCG_RNSC1.0_RNIFV02.00_7B6V01.00.xml

Contenuto della mappa della direttiva

In questa sezione, vengono elencate le mappe della direttiva per 7B6 Notifica replica ordine attività industriale:

- BCG_7B6NotifyOfManufacturingWorkOrderReply_V01.00.xsd
- BCG_BusinessDescription_Types.xsd
- BCG_BusinessTaxIdentifier_Types.xsd
- BCG_common.xsd
- BCG_ContactInformation_Types.xsd
- BCG_GlobalChangeReasonCode.xsd
- BCG_GlobalCountryCode.xsd

- BCG_GlobalDocumentReferenceTypeCode.xsd
- BCG_GlobalLineItemStatusCode.xsd
- BCG_GlobalPartnerClassificationCode.xsd
- BCG_GlobalPartnerRoleClassificationCode.xsd
- BCG_GlobalProductUnitOfMeasureCode.xsd
- BCG_PartnerDescription_Types.xsd
- BCG_PhysicalAddress_Types.xsd
- BCG_string_len_0.xsd
- BCG_xml.xsd

Capitolo 21. Ulteriori informazioni CIDX

Questa appendice contiene le informazioni aggiuntive sul supporto CIDX. Sono incluse le seguenti sezioni:

- "Supporto per l'abilitazione del processo CIDX"
- "Creazione dei package di definizione del documento CIDX"

Supporto per l'abilitazione del processo CIDX

CIDX fornisce i seguenti due meccanismi per l'abilitazione del processo:

- **Abilitazione in base ai messaggi:** l'associazione dei documenti si basa su <RequestingDocumentIdentifier> e <ThisDocumentIdentifier>
- **Abilitazione in base al framework:** l'associazione dei documenti si basa sulla semantica dell'intestazione del servizio RNIF 1.1

Per l'abilitazione in base ai messaggi, i package PIP ad un'azione per le transazioni ChemXML sono obbligatori. Per l'abilitazione in base al framework, i package PIP a doppia azione per la transazioni ChemXML sono obbligatori. WebSphere Partner Gateway supporta entrambi i formati dell'abilitazione del processo. WebSphere Partner Gateway fornisce i package PIP a un'azione per ″E41 Order Create″ e ″E42 Order Response″.

Creazione dei package di definizione del documento CIDX

Potrebbe essere necessario creare i propri package CIDX per supportare gli altri messaggi CIDX. La procedura per creare i nuovi package di definizione del documento CIDX coincide con quella valida per RosettaNet.

Per ulteriori informazioni su RosettaNet, consultare l'Capitolo 20, "Informazioni aggiuntive su RosettaNet", a pagina 353

Capitolo 22. Attributi

Questa appendice descrive gli attributi che è possibile impostare dalla Console comunità. Sono descritti i seguenti attributi:

attributi EDI

Questa sezione contiene una descrizione degli attributi EDI che è possibile utilizzare durante l'impostazione degli scambi EDI. Alcuni di questi attributi sono predefiniti nella stringa di controllo che rappresenta la mappa di conversione associata al documento EDI. I valori impostati nella stringa di controllo (sul client Data Interchange Services) sostituiscono quelli immessi sulla Console comunità.

Attributi del profilo di busta

È possibile impostare vari attributi per un profilo della busta EDI. Gli attributi disponibili dipendono dal tipo EDI. In generale, gli attributi corrispondono ad uno standard EDI ed i valori consentiti dipendono dallo standard EDI rappresentato dal profilo della busta.

Nessuno degli attributi richiede un valore. Per alcuni di essi, viene utilizzato un valore predefinito, se non viene immesso alcun valore. Le tabelle in questa sezione elencano gli attributi che hanno dei valori predefiniti associati ed i loro valori predefiniti.

Nota: le proprietà del profilo della busta non elencate non dispongono di valori predefiniti. Si utilizza il valore di testo specificato, se non viene sostituito da proprietà generiche o specifiche della busta impostate nella mappa o in una connessione.

Attributi X12

Nelle tabelle contenute in questa sezione vengono elencati gli attributi X12 per i quali vengono forniti dei valori predefiniti.

attributi generali

In Tabella 98 a pagina 414 sono elencati gli attributi generali per i quali vengono forniti dei valori predefiniti.

Tabella 98. attributi generali

Nome campo	Necessario?	Descrizione	Val. predef.
INTCTLLEN (Lunghezza numero di controllo scambio)	No	Definisce una lunghezza specifica per il numero di controllo scambio. Se si immette un valore, deve essere un intero. In caso contrario, viene utilizzata la lunghezza predefinita.	9
GRPCTLLEN (Lunghezza numero di controllo gruppo)	No	Definisce una lunghezza specifica per il numero di controllo del gruppo. Se si immette un valore, deve essere un intero. In caso contrario, viene utilizzata la lunghezza predefinita.	9
TRXCTLLEN (Lunghezza numero di controllo transazione)	No	Definisce una lunghezza specifica per il numero di controllo della transazione. Se si immette un valore, deve essere un intero. In caso contrario, viene utilizzata la lunghezza predefinita.	9
ENVTYPE (Tipo busta)	No	Questo attributo non viene impostato dall'utente ma viene derivato dal tipo del profilo della busta creato.	X12
MAXDOCS (Numero max transazioni)	No	Numero massimo di transazioni in una busta. Se si immette un valore, deve essere un intero.	No numero massimo
CTLNUMFLAG (Numeri di controllo per ID transazione)	No	Sì indica che vengono conservati gruppi di numeri di controllo separati in base al tipo di transazione EDI. No indica che deve essere utilizzata una serie comune di numeri di controllo per tutti i tipi di transazione EDI.	No

attributi Interchange

Non viene richiesto alcun attributo X12 e gli attributi non hanno valori predefiniti.

Tabella 99. Attributi Gruppo

Nome campo	Necessario?	Descrizione	Val. predef.
GS01 (ID gruppo funzionale)	No	Identificativo del gruppo.	Il valore predefinito deriva dall'intestazione della stringa di controllo. È possibile visualizzare questo valore nel client Data Interchange Services cercando la colonna Gruppo funzionale nella pagina Definizioni documento EDI.
GS08 (Versione gruppo)	No	Versione del gruppo.	Il valore predefinito è quello standard.

Attributi Gruppo

In Tabella 99 vengono elencati gli attributi del gruppo per i quali vengono forniti dei valori predefiniti.

attributi Transazione

Non viene richiesto alcun attributo della transazione. Gli attributi non hanno valori predefiniti.

Attributi UCS

In questa sezione, viene descritto se i valori predefiniti vengono applicati ad uno scambio, gruppo e transazione UCS.

attributi generali

In Tabella 100 sono elencati gli attributi generali per i quali vengono forniti dei valori predefiniti.

Tabella 100. attributi generali

Nome campo	Necessario?	Descrizione	Val. predef.
INTCTLLEN (Lunghezza numero di controllo scambio)	No	Definisce una lunghezza specifica per il numero di controllo scambio. Se si immette un valore, deve essere un intero. In caso contrario, viene utilizzata la lunghezza predefinita.	5
GRPCTLLEN (Lunghezza numero di controllo gruppo)	No	Definisce una lunghezza specifica per il numero di controllo del gruppo. Se si immette un valore, deve essere un intero. In caso contrario, viene utilizzata la lunghezza predefinita.	9
TRXCTLLEN (Lunghezza numero di controllo transazione)	No	Definisce una lunghezza specifica per il numero di controllo della transazione. Se si immette un valore, deve essere un intero. In caso contrario, viene utilizzata la lunghezza predefinita.	9
ENVTYPE (Tipo busta)	No	Questo attributo non viene impostato dall'Ammin hub ma derivato dal tipo di profilo della busta creato.	UCS
MAXDOCS (Numero max transazioni)	No	Numero massimo di transazioni in una busta. Se si immette un valore, deve essere un intero.	No numero massimo
CTLNUMFLAG (Numeri di controllo per ID transazione)	No	Sì indica che vengono conservati gruppi di numeri di controllo separati in base al tipo di transazione EDI. No indica che deve essere utilizzata una serie comune di numeri di controllo per tutti i tipi di transazione EDI.	No

attributi Interchange

Non viene richiesto alcun attributo di scambio. Gli attributi non hanno valori predefiniti.

Attributi Gruppo

In Tabella 101 a pagina 416 vengono elencati gli attributi del gruppo per i quali vengono forniti dei valori predefiniti.

Tabella 101. Attributi Gruppo

Nome campo	Necessario?	Descrizione	Val. predef.
GS01 (ID gruppo funzionale)	No	Identificativo del gruppo.	Il valore predefinito deriva dall'intestazione della stringa di controllo. È possibile visualizzare questo valore nel client Data Interchange Services cercando la colonna Gruppo funzionale nella pagina Definizioni documento EDI.
GS08 (Versione gruppo)	No	Versione del gruppo.	Il valore predefinito è quello standard.

attributi Transazione

Non viene richiesto alcun attributo della transazione. Gli attributi non hanno valori predefiniti.

Attributi EDIFACT

In questa sezione, viene descritto se i valori predefiniti vengono applicati ad uno scambio, gruppo e messaggio EDIFACT.

attributi generali

In Tabella 102 sono elencati gli attributi generali per i quali vengono forniti dei valori predefiniti.

Tabella 102. attributi generali

Nome campo	Necessario?	Descrizione	Val. predef.
INTCTLLEN (Lunghezza numero di controllo scambio)	No	Definisce una lunghezza specifica per il numero di controllo scambio. Se si immette un valore, deve essere un intero. In caso contrario, viene utilizzata la lunghezza predefinita.	9
GRPCTLLEN (Lunghezza numero di controllo gruppo)	No	Definisce una lunghezza specifica per il numero di controllo del gruppo. Se si immette un valore, deve essere un intero. In caso contrario, viene utilizzata la lunghezza predefinita.	9
TRXCTLLEN (Lunghezza numero di controllo transazione)	No	Definisce una lunghezza specifica per il numero di controllo della transazione. Se si immette un valore, deve essere un intero. In caso contrario, viene utilizzata la lunghezza predefinita.	9
ENVTYPE (Tipo busta)	No	Questo attributo non viene impostato dall'Ammin hub ma derivato dal tipo di profilo della busta creato.	EDIFACT
EDIFACTGRP (Crea gruppi per EDI)	No	Questo valore è valido solo per i tipi di busta EDIFACT. (Il livello del gruppo è stato sostituito in EDIFACT). Sì indica che è necessario creare i gruppi funzionali (segmenti UNG/UNE) per EDIFACT DATA. No indica il contrario.	No

Tabella 102. attributi generali (Continua)

Nome campo	Necessario?	Descrizione	Val. predef.
MAXDOCS (Numero max transazioni)	No	Numero massimo di transazioni in una busta. Se si immette un valore, deve essere un intero.	No numero massimo
CTLNUMFLAG (Numeri di controllo per ID transazione)	No	Sì indica che vengono conservati gruppi di numeri di controllo separati in base al tipo di transazione EDI. No indica che deve essere utilizzata una serie comune di numeri di controllo per tutti i tipi di transazione EDI.	No

attributi Interchange

Non viene richiesto alcun attributo di scambio. Gli attributi non hanno valori predefiniti.

Attributi Gruppo

In Tabella 103 vengono elencati gli attributi del gruppo per i quali vengono forniti dei valori predefiniti.

Tabella 103. Attributi Gruppo

Nome campo	Necessario?	Descrizione	Val. predef.
UNG01 (ID gruppo funzionale)	No	Identificativo del gruppo.	Il valore predefinito deriva dall'intestazione della stringa di controllo. È possibile visualizzare questo valore nel client Data Interchange Services cercando la colonna Gruppo funzionale nella pagina Definizioni documento EDI.

Attributi messaggio

In Tabella 104 sono elencati gli attributi del messaggio per i quali vengono forniti dei valori predefiniti.

Tabella 104. Attributi messaggio

Nome campo	Necessario?	Descrizione	Val. predef.
UNH0201 (Tipo messaggio)	No	Tipo di messaggio.	Il valore predefinito deriva dall'intestazione della stringa di controllo. È possibile visualizzare questo valore nel client Data Interchange Services cercando nella pagina Definizioni documento EDI.
UNH0202 (Versione messaggio)	No	Versione del messaggio.	D
UNH0203 (release del messaggio)	No	Il release del messaggio.	Per valore standard
UNH0204 (Agenzia controllo)	No	Codice che identifica un'agenzia di controllo.	UN

Attributi di connessione e definizione del documento

Questa sezione elenca gli attributi di definizione del documento per la busta. Alcuni di questi attributi possono essere impostati solo a livello di protocollo o connessione, come indicato.

Attributi del separatore e del delimitatore

In questa sezione, vengono elencati i caratteri utilizzati come delimitatori o separatori in uno scambio EDI. In Tabella 105 viene mostrato l'attributo come appare sulla Console comunità, il termine corrispondente in X12 e EDIFACT (ISO 9735 versione 4, release 1), se l'attributo è necessario ed una descrizione dello stesso. Di seguito è riportata una tabella come esempio di come appaiono questi caratteri in un documento EDI.

Descrizioni attributo

Gli attributi del separatore e del delimitatore vengono elencati in Tabella 105.

Nota: alcuni caratteri (come notato) possono essere valori esadecimali. Possono essere valori Unicode o valori di un altro tipo di codifica. Per Unicode, utilizzare il formato \unnnn. Per altre codifiche, utilizzare il formato 0xnn.

Tabella 105. Attributi profilo busta

Attributo	Termine X12	Termine EDIFACT	Descrizione
delimitatore segmento	terminazione segmento	terminazione segmento	Si tratta di un carattere singolo, che appare sull'ultimo carattere di un segmento. Il carattere può essere un valore esadecimale. Il valore predefinito si basa sul tipo EDI. **X12** ~ (tilde) **EDIFACT** ' (apici) **UCS** ~ (tilde)
delimitatore elementi dati	separatore elemento dati	separatore elemento dati	Si tratta di un carattere singolo, che separa gli elementi dati di un segmento. Il carattere può essere un valore esadecimale. Il valore predefinito si basa sul tipo EDI. **X12** * (asterisco) **EDIFACT** + (segno più) **UCS** * (asterisco)
Delimitatore elemento secondario	separatore elemento componente	separatore elemento dati componente	Si tratta di un carattere singolo, che separa gli elementi di un componente di un elemento dati composto. Il carattere può essere un valore esadecimale. Il valore predefinito si basa sul tipo EDI. **X12** \ (barra inversa) **EDIFACT** : (due punti) **UCS** \ (barra inversa)

Tabella 105. Attributi profilo busta (Continua)

Attributo	Termine X12	Termine EDIFACT	Descrizione
carattere rilascio		carattere rilascio	Si tratta di un carattere singolo, che sostituisce il significato del carattere successivo, consentendo che appaia un carattere separatore in un elemento dati. Il carattere può essere un valore esadecimale. Si applica solo a EDIFACT. **EDIFACT** ? (punto interrogativo)
separatore elemento dati ripetitivo	separatore ripetitivo	separatore ripetitivo	Si tratta di un carattere singolo, che separa le istanze di un elemento dati ripetitivo. Questo carattere può essere un valore esadecimale. Il valore predefinito si basa sul tipo EDI per X12 o EDIFACT. **X12** ^ (accento circonflesso) **EDIFACT** * (asterisco)
notazione decimale		notazione decimale (sostituita)	Questo attributo è stato utilizzato in una formattazione decimale o analisi ed ora è stato sostituito. Può essere un punto o solo una virgola. Il valore predefinito è un punto.

Esempio struttura EDI

In questa sezione, viene mostrato uno scambio EDI semplice e come gli attributi descritti in Tabella 105 a pagina 418 vengono utilizzati in uno scambio.

Un messaggio EDI consiste di una serie di segmenti secondo un ordine particolare. Una segmento consiste di una serie di elementi. In un segmento, un elemento può essere un elemento dati semplice, che contiene solo un elemento di informazioni. Un elemento può essere anche un elemento dati composto, che contiene due o più elementi dati semplici. Gli elementi semplici che costituiscono un elemento composto vengono denominati elementi dati componente

Non c'è alcuna nidificazione di elementi dati composti. Un elemento dati composto può contenere solo elementi dati semplici, non altri composti. Sebbene non venga mostrato in questa sede, un elemento dati componente può essere definito anche elemento dati ripetitivo.

Considerare il seguente esempio:

```
ABC*123*AA\BB\CC*001^002^003*star?*power~
```

In questo esempio:

- ″ABC″ è il nome del segmento (EDIFACT richiama questo ″tag segmento″); dovrebbe essere chiamato ″segmento ABC″
- ″*″ (asterisco) corrisponde al separatore dell'elemento dati.

  Il nome dell'attributo corrispondente sulla Console comunità è Delimitatore segmento
- ″123″ è il primo elemento dati, un elemento dati semplice (cui si ci potrebbe riferire come a ABC01 in alcuni contesti)

- ″AA\BB\CC″ è il secondo elemento dati (ABC02), elemento dati composto costituito da elementi dati componente
  - ″\ ″ (barra rovesciata) è il separatore dell'elemento dati del componente

    Il nome dell'attributo corrispondente sulla Console comunità è delimitatore elementi dati
  - ″AA″ è il primo elemento dati del componente di ABC02 (che potrebbe essere indicato come ABC0201)
  - ″BB″ è il secondo elemento dati del componente di ABC02 (ABC0202)
  - ″CC″ è il terzo elemento dati del componente di ABC02 (ABC0203)
- ″001^002^003″ è il terzo elemento dati (ABC03), un elemento dati ripetitivo
  - ″^″ (accento circonflesso) è il separatore di ripetizione

    Il nome dell'attributo corrispondente sulla Console comunità è un carattere elemento dati ripetitivo.
  - ″001″,″002″, ″003″ sono le ripetizioni (tutte indicate come ABC03)
- ″star?*power″ è il quarto elemento dati (ABC04)
  - ″?″ (punto interrogativo) è il carattere di rilascio, che indica che l'asterisco successivo non viene considerato come separatore dell'elemento dati
  - ″star*power″ è il valore risultante di ABC04
- ″~″ (tilde) è la terminazione del segmento.

  Il nome dell'attributo corrispondente sulla Console comunità è Delimitatore segmento

Attributi EDI aggiuntivi

In questa sezione sono riportati gli ulteriori attributi EDI che è possibile impostare al livello per la definizione del documento o di connessione.

Tabella 106. Attributi EDI aggiuntivi

Attributo	Richiesto	Descrizione	Limitazioni	Val. predef.
Output segmento	No	Utilizzato nella conversione EDI/XML, questo indica se deve esserci una riga di interruzione dopo ogni segmento EDI o elemento XML.	Limitato al protocollo o alla connessione	Sì
Consenti documenti con ID documento duplicati	No	Sì indica che gli ID del documento duplicato (numeri di controllo scambio) sono consentiti. No indica che i numeri di controllo scambio duplicato devono essere considerati come un errore.	Limitato al protocollo o alla connessione	No
Livello max errore su conversione	No	Indica il numero massimo di errori che possono verificarsi durante una conversione prima che questa non riesca. I valori validi sono 0, 1 o 2. Se la mappa di conversione contiene un comando Errore per indicare un errore specificato dall'utente, e il parametro del livello del comando Errore è maggiore di questo valore, la conversione non riesce.	Limitato al protocollo o alla connessione	0

Tabella 106. Attributi EDI aggiuntivi (Continua)

Attributo	Richiesto	Descrizione	Limitazioni	Val. predef.
Mappa FA	No	Fornisce la mappa da utilizzare per la conversione del valore FA generico interno in quello specifico. **Nota:** selezionare questo attributo da un elenco di mappe identificato come mappe FA (tipo di mappa "K").	Limitato al protocollo o alla connessione	
Profilo busta	Sì	Nome del profilo della busta EDI da utilizzare per l'operazione di enveloping. Tutti i profili della busta definiti sono disponibili dall'elenco.		
Attivo XMLNS	No	Elaborazione dello spazio dei nomi per il documento XML di input. Questo attributo viene utilizzato dalla fase di conversione XML. I valori validi sono Sì o No.		Schema: Sì DTD: No
Livello max errore di convalida	No	Livello massimo accettabile dell'errore di convalida (gravità dell'errore da accettare prima di considerare la transazione ″non riuscita″). I valori validi sono 0, 1 o 2. **0** Consenti solo convalida senza errori **1** Non riesce per documenti che presentano solo errori di convalida degli elementi semplici **2** Non riesce per documenti che presentano solo errori di convalida su elementi o segmenti		0
Livello di convalida	No	Indica il livello di controllo da eseguire a livello di transazione. Un valore pari a 2 indica i valori impostati per gli attributi della tabella di convalida alfanumerica e quella del set di caratteri. Questo attributo si applica anche alla convalida dettagliata dell'attributo dei segmenti, se l'attributo è impostato su Sì. I valori validi sono 0, 1 o 2. **0** Esegue solo la convalida di base, come ad esempio il controllo di elementi e segmenti obbligatori mancanti e lunghezze minime o massime. Non convalidare i valori dell'elemento rispetto ai tipi di dati o agli elenchi di codici specificati nella definizione di transazione. **1** Esegue il livello 0 di convalida, più la convalida dei valori dell'elemento rispetto agli elenchi di codici specificati per l'elemento dati. **2** Esegue il livello 1 di convalida, più la convalida che il valore dell'elemento è corretto per il tipo di dati dell'elemento.		0

Tabella 106. Attributi EDI aggiuntivi (Continua)

Attributo	Richiesto	Descrizione	Limitazioni	Val. predef.
Tabella di convalida set di caratteri	No	Indica la tabella da utilizzare per la convalida del set di caratteri. Questa tabella viene utilizzata solo quando l'attributo del livello di convalida è 2. Questo attributo si riferisce alla tabella degli elenchi codici virtuali. L'utente può creare nuovi elenchi codici nella scheda Elenchi codici dell'area di mappatura nel client Data Interchange Services. Questa area contiene anche gli elenchi codici utilizzati per altri scopi, come ad esempio la convalida di certi elementi EDI.		CHARSET
Tabella di convalida alfanumerica	No	Indica la tabella da utilizzare per la convalida alfanumerica. Questa tabella viene utilizzata solo quando l'attributo del livello di convalida è 2. Questo attributo si riferisce alle tabelle dell'elenco codici virtuali. L'utente può creare nuovi elenchi codici nella scheda Elenchi codici dell'area di mappatura nel client Data Interchange Services. Questa area contiene anche gli elenchi codici utilizzati per altri scopi, come ad esempio la convalida di certi elementi EDI.		ALPHANUM
Attributo Genera info livello gruppo nel riconoscimento funzionale	No	Questo attributo si applica a EDI-X12. I valori validi sono Sì o No. **Sì** Genera info livello gruppo nel riconoscimento funzionale. **No** Genera dettagli completi riconoscimento funzionale (per ciascuna singola transazione e per i segmenti ed elementi in essa contenuti).	Limitato al protocollo o alla connessione	No
Anno controllo secolo	No	Quando le date vengono convertite da anni a due cifre in anni a quattro cifre, si presume che gli anni a due cifre dopo questo valore abbiano un valore di secolo pari a "19". Si presume che gli anni a due cifre uguali o prima di questo valore abbiano un valore di secolo pari a "20". L'intervallo valido è compreso tra 0 e 99.	Limitato al protocollo o alla connessione	10

Tabella 106. Attributi EDI aggiuntivi (Continua)

Attributo	Richiesto	Descrizione	Limitazioni	Val. predef.
Convalida dettagliata del segmento	No	Questo attributo si applica alle seguenti intestazioni ed elementi di coda del segmento: • X12 – ISA, IEA – GS, GE – ST, SE • EDIFACT – UNA – UNB, UNZ – UNG, UNE – UNH, UNT • UNTUCS – BG, EG – GS, GE – ST, SE I valori validi sono Sì o No. **Sì** Esegue la convalida dettagliata del segmento della busta. La profondità del controllo viene effettuata dall'attributo Livello di convalida. **No** Non esegue la convalida dettagliata del segmento della busta.	Limitato al protocollo o alla connessione	No
Sostituzione TA1	No	Consente la generazione di una richiesta TA1, se indicato nel segmento della busta Interchange. Si applica solo a EDI-X12. Se impostato su Sì, la richiesta TA1 viene generata se indicato nel segmento della busta Interchange. Se impostato su No, la richiesta TA1 non viene generata anche se indicato nel segmento della busta Interchange.	Limitato al protocollo o alla connessione	Sì
Eliminazione errore	No	Questo attributo viene utilizzato nell'elaborazione polimorfica. Nel caso di un batch che risulta da un'operazione di deenveloping, questo attributo indica se eliminare l'intero batch, se alcune transazioni non riescono. I valori validi sono Sì e No.	Limitato al protocollo o alla connessione	No
qualificatore profilo connessione 1	No	Questo attributo viene utilizzato dall'Enveloper per stabilire il profilo da utilizzare per la connessione di uno scambio. Le transazioni con valori differenti per questo attributo vengono inserite in scambi differenti.		
Qualificatore dello scambio	No	Il codice utilizzato per identificare il formato dell'identificativo del mittente o del destinatario dello scambio.		

Tabella 106. Attributi EDI aggiuntivi (Continua)

Attributo	Richiesto	Descrizione	Limitazioni	Val. predef.
Identificativo scambio	No	Identifica il mittente o il destinatario specifico del documento. Il tipo di dati immessi viene determinata dall'attributo del qualificatore di scambio.		
Indicatore utilizzo scambio	No	Indica se i documenti di origine convertiti sono classificati come documenti di Produzione, Verifica o Informazione. I valori validi sono P, T e I.		
Identificativo mittente applicazione gruppo	No	Identifica il mittente specifico della transazione. Questo attributo, quando accettato dai partner commerciali, facilita lo scambio all'interno di un'azienda.		
Identificativo destinatario applicazione gruppo	No	Identifica l'applicazione o il destinatario specifico della transazione. Questo attributo, quando accettato dai partner commerciali, facilita lo scambio all'interno di un'azienda.		
Instradamento inverso scambio	No	Indica l'indirizzo cui il destinatario deve recapitare le risposte.		
Indirizzo instradamento scambio	No	Il codice dell'indirizzo secondario per l'instradamento esterno.		
Qualificatore mittente applicazione di gruppo	No	Il codice utilizzato per identificare il formato dell'identificativo mittente dell'applicazione di gruppo.		
Qualificatore destinatario applicazione di gruppo	No	Il codice utilizzato per identificare il formato dell'identificativo del destinatario dell'applicazione di gruppo.		
Password applicazione gruppo	No	Questo attributo definisce le informazioni sulla sicurezza.		
limite temporale richiesto RF		Numero di minuti in seguito all'invio in cui è necessario restituire RF. Se il valore è vuoto, non è richiesta alcuna mappa RF.		

Proprietà del client Data Interchange Services

In questa sezione, vengono elencate le proprietà che possono essere impostate come parte della mappa di conversione nel client Data Interchange Services e negli attributi di WebSphere Partner Gateway corrispondenti.

Tabella 107. Proprietà della mappa ed attributi corrispondenti

Proprietà del client Data Interchange Services	Sostituisce l'attributo WebSphere Partner Gateway
AckReq	Notifica richiesta
Alphanum	Tabella di convalida alfanumerica
Charset	Tabella di convalida set di caratteri
CtlNumFlag	Numero di controllo per ID transazione

Tabella 107. Proprietà della mappa ed attributi corrispondenti (Continua)

Proprietà del client Data Interchange Services	Sostituisce l'attributo WebSphere Partner Gateway
EdiDecNot (Notazione decimale)	notazione decimale
EdiDeDlm (Separatore elemento dati)	delimitatore elementi dati
EdiDeSep (separatore elemento dati ripetitivo)	separatore elemento dati ripetitivo
EdifactGrp	Crea gruppi per EDI
EdiRlsChar (Carattere di rilascio)	carattere rilascio
EdiSeDlm (Separatore elemento dati componente)	Delimitatore elemento secondario
EdiSegDlm (Terminazione segmento)	delimitatore segmento
EnvProfName	Profilo busta
EnvType	Tipo busta
MaxDocs	Numero max di transazioni
Reroute	Instradamento inverso scambio
SegOutput	Output segmento
ValLevel	Livello di convalida
ValErrLevel	Livello max errore di convalida
ValMap	Mappa di convalida

In Tabella 108 vengono elencate le proprietà aggiuntive del client Data Interchange Services e gli attributi WebSphere Partner Gateway associati.

Tabella 108. Proprietà del client Data Interchange Services ed attributi associati

Proprietà del client Data Interchange Services	Sostituisce l'attributo WebSphere Partner Gateway
IchgCtlNum	Numero di controllo scambio
IchgSndrQl	Qualificatore mittente scambio
IchgSndrId	ID mittente scambio
IchgRcvrQl	Qualificatore destinatario scambio
IchgRcvrId	ID destinatario scambio
IchgDate	Data scambio
IchgTime	Ora scambio
IchgPswd	Password scambio
IchgUsgInd	Indicatore utilizzo scambio
IchgAppRef	Riferimento applicazione scambio
IchgVerRel	Versione e release scambio
IchgGrpCnt	Numero dei gruppi nello scambio
IchgCtlTotal	Controllo totale dal segmento di coda dello scambio
IchgTrxCnt	Numero di documenti nello scambio
GrpCtlNum	Numero di controllo gruppo
GrpFuncGrpId	ID gruppo funzionale
GrpAppSndrId	ID mittente applicazione gruppo
GrpAppRcvrId	ID destinatario applicazione gruppo
GrpDate	Data gruppo

Tabella 108. Proprietà del client Data Interchange Services ed attributi associati (Continua)

Proprietà del client Data Interchange Services	Sostituisce l'attributo WebSphere Partner Gateway
GrpTime	Ora gruppo
GrpPswd	Password gruppo
GrpVer Versione gruppo.	Versione gruppo
GrpRel Release gruppo.	Release gruppo
GrpTrxCnt	Numero di documenti nel gruppo
TrxCtlNum	Numero di controllo transazione
TrxCode	Codice transazione
TrxVer	Versione transazione
TrxRel	Release transazione
TrxSegCnt	Numero di segmenti EDI nel documento

Attributi AS

La sezione descrive gli attributi AS.

Tabella 109. Attributi AS

Attributo	Richiesto	Descrizione	Limitazioni	Val. predef.
Ora per riconoscere in min	No	L'intervallo di attesa per un riconoscimento MDN prima di inviare nuovamente la richiesta di origine. Questo attributo funziona insieme al Conteggio tentativi. Le unità sono espresse in minuti.	Limitato al package o alla connessione	30
conteggio tentativi	No	Il numero di volte in base al quale viene inviata una richiesta se non è stato ricevuto MDN. Questo attributo funziona insieme all'attributo Ora per riconoscere. Ad esempio, se questo attributo è stato impostato su 3, la richiesta può essere inviata potenzialmente per quattro volte (la prima volta più tre tentativi).	Limitato al package o alla connessione	3
Comprimi AS prima della firma	No	Indica se la compressione AS deve essere applicata sia al payload sia alla firma o solo al payload. Se si seleziona Sì, il payload viene compresso prima che il messaggio sia stato firmato. Questo attributo funziona insieme all'attributo AS Compresso.	Limitato al package o alla connessione	Sì
AS Compresso	No	Comprime i dati. Questo attributo funziona insieme all'attributo Comprimi AS prima della firma.	Limitato al package o alla connessione	No

Tabella 109. Attributi AS (Continua)

Attributo	Richiesto	Descrizione	Limitazioni	Val. predef.
AS Codificato	No	Questo attributo si applica ad AS2 e consente di specificare l'indirizzo URL a cui un partner dovrebbe inviare un MDN asincrono. Questo attributo funziona insieme all'attributo AS MDN Asincrono ed un valore è stato richiesto anche per MDN sincroni.	Limitato al package o alla connessione	No
AS MDN Url Http	Sì se l'attributo ″AS MDN asincrono″ è Sì e si utilizza AS2.	Questo attributo si applica ad AS2 e consente di specificare l'indirizzo URL a cui un partner dovrebbe inviare un MDN asincrono. Questo attributo funziona insieme all'attributo AS MDN Asincrono ed un valore è stato richiesto anche per MDN sincroni.	Limitato al package o alla connessione	
AS MDN Indirizzo e-mail	Sì se l'attributo ″AS MDN asincrono″ è Sì e si utilizza AS1.	Specifica l'indirizzo e-mail utilizzato dal partner durante l'invio di MDN asincroni. Questo attributo è utilizzato insieme all'attributo AS MDN Richiesto. Il valore dell'attributo AS MDN Indirizzo e-mail viene utilizzato nel campo "Disposition-notification-to". Per AS1, questo attributo funziona insieme all'attributo AS MDN Asincrono nel formato mailto:xxx@company.com. Per AS2 questo attributo richiede ancora un valore sebbene l'indirizzo email non sia stato utilizzato.	Limitato al package o alla connessione	
AS MDN Asincrono	No	Specifica se è necessario restituire MDN in modo sincrono o asincrono. Il valore di questo attributo influenza l'utilizzo degli attributi AS MDN URL HTTP o AS MDN Indirizzo e-mail. I valori validi sono Sì e No. **Sì** Asincrono **No** Sincrono Se questo attributo è stato impostato su Sì, il campo ″receipt-delivery-option″ viene compilato in base all'attributo AS MDN URL HTTP (per AS2) o l'attributo AS MDN Indirizzo e-mail (per AS1).	Limitato al package o alla connessione	Sì

Tabella 109. Attributi AS (Continua)

Attributo	Richiesto	Descrizione	Limitazioni	Val. predef.
AS MDN Richiesto	No	Specifica se è stata richiesta una riposta MDN. Se è stato impostato su Sì, questo attributo consente la compilazione dell'intestazione "transport Disposition-notification-to" con il valore dell'attributo AS MDN Indirizzo e-mail. I valori validi sono Sì e No. **Sì** È richiesto MDN. **No** Non è richiesto MDN.	Limitato al package o alla connessione	Sì
AS Algoritmo message digest	No	L'algoritmo message digest da utilizzare durante la firma. Questo attributo viene utilizzato insieme agli attributi AS Firmato e AS MDN Firmato. Per MDN firmati, questo valore consente di compilare l'intestazione "Disposition-notification-options: signed-receipt-micalg".	Limitato al package o alla connessione	sha1
AS MDN Firmato	No	Indica se è necessario restituire un MSN firmato alla richiesta. Questo attributo funziona insieme a AS MDN Richiesto. Se il valore è stato impostato su Sì, viene compilato il campo "Disposition-notification-options: signed-receipt-protocol". I valori validi sono Sì e No. **Sì** È richiesto MDN Firmato **No** Non è richiesto MDN Firmato Se l'attributo è stato impostato su Sì, l'MDN inviato dal partner deve essere firmato. Se questo attributo è stato impostato su No, l'MDN può essere firmato o non firmato.	Limitato al package o alla connessione	No

Tabella 109. Attributi AS (Continua)

Attributo	Richiesto	Descrizione	Limitazioni	Val. predef.
AS Firmato	No	Specifica se firmare il documento. Per TO dello scambio (quando si inviano documenti ad un partner), specifica se firmare o meno il documento. Per FROM dello scambio (quando si ricevono documenti da un partner), se l'attributo è stato impostato su Sì, è necessario firmare una richiesta AS inviata dal partner. Se l'attributo è stato impostato su No, il documento proveniente dal partner può essere firmato o non firmato. **Sì** Firmare il documento **No** Il documento firmato non è richiesto	Limitato al package o alla connessione	No
Non-rifiuto richiesto	No	Indica se è necessario salvare questo documento nella memoria di non-rifiuto. Sarà applicato al documento come origine o destinazione. Sì – Salvare il documento nella memoria di non-rifiuto. No – Non salvare il documento nella memoria di non-rifiuto.	Limitato al package o alla connessione	Sì
Memorizzazione messaggio richiesta	No	Indica se è necessario salvare questo documento nella memorizzazione messaggio. Verrà applicato a entrambi i documenti di origine e di destinazione. Sì – Salvare il documento nella memorizzazione messaggio. No – Non salvare il documento nella memorizzazione messaggio.	Limitato al package o alla connessione	Sì
AS ID di business	No	L'attributo AS ID di business da utilizzare nell'intestazione "AS2-To" o "AS3-To". Se un valore non è stato fornito, WebSphere Partner Gateway utilizza l'ID di business del destinatario utilizzato nel documento di origine. **Nota:** l'intestazione "AS2-From" o "AS3-From" sarà impostata dall'attributo "AS ID di business" dalla definizione del documento di origine oppure, se non è stata definita, dal documento di origine originale, che passa in WebSphere Partner Gateway e che viene inviato come AS.	Limitato al package o alla connessione	

Tabella 109. Attributi AS (Continua)

Attributo	Richiesto	Descrizione	Limitazioni	Val. predef.
AS MDN Indirizzo FTP	Sì per AS3 quando l'attributo ″AS MDN Richiesto″ è impostato su Sì.	L'attributo AS MDN Indirizzo FTP da utilizzare durante la richiesta di MDN. Questo attributo viene utilizzato insieme all'attributo ″AS MDN Richiesto″. Il valore dell'attributo AS MDN Indirizzo FTP viene utilizzato nel campo "Disposition-notification-to". È necessario che il formato sia: `ftp://username:pwd@host.com:port/folder-name`.	Limitato al package o alla connessione	No

Attributi RosettaNet

In questa sezione vengono descritti gli attributi RosettaNet.

Tabella 110. Attributi RosettaNet

Attributo	Richiesto	Descrizione	Limitazioni	Val. predef.
Ora per riconoscere	Sì	L'intervallo di attesa per una notifica di ricezione prima di inviare nuovamente la richiesta originale. Questo attributo funziona insieme al Conteggio tentativi. Le unità sono espresse in minuti. Il valore predefinito è desunto dal documento di specifica PIP RosettaNet.	Limitato al package o alla connessione	120
Ora per eseguire	Sì	L'intervallo di attesa di una risposta ad un'azione di richiesta prima di inviare un messaggio di notifica errori.	Limitato al package o alla connessione	
Conteggio tentativi	Sì	Il numero di volte in base al quale viene inviata una richiesta se non si ottiene una notifica di ricezione. Questo attributo funziona insieme all'attributo Ora per riconoscere. Ad esempio, con un impostazione pari a 3, la richiesta può essere inviata potenzialmente per 4 volte (la prima volta più altri tre tentativi). Il valore predefinito è desunto dal documento di specifica PIP RosettaNet.	Limitato al package o alla connessione	3
Firma digitale obbligatoria	No	Indica se il messaggio PIP richiede una firma digitale. Il valore predefinito è desunto dal documento di specifica PIP RosettaNet.	Limitato al package o alla connessione	Sì

Tabella 110. Attributi RosettaNet (Continua)

Attributo	Richiesto	Descrizione	Limitazioni	Val. predef.
non-rifiuto richiesto	No	Indica se è necessario salvare questo documento nella memoria di non-rifiuto. Sarà applicato al documento come origine o destinazione. Sì – Salvare il documento nella memoria di non-rifiuto. No – Non salvare il documento nella memoria di non-rifiuto.	Limitato al package o alla connessione	Sì
Memorizzazione messaggio richiesta	No	Indica se è necessario salvare questo documento nella memorizzazione messaggio. Verrà applicato a entrambi i documenti di origine e di destinazione. Sì – Salvare il documento nella memorizzazione messaggio. No – Non salvare il documento nella memorizzazione messaggio.	Limitato al package o alla connessione	Sì
Non-rifiuto di ricevuta richiesto	No	Indica se memorizzare il documento per la notifica di ricezione nella memoria di non-rifiuto. Il valore predefinito è desunto dal documento di specifica PIP RosettaNet.	Limitato al package o alla connessione	Sì
sinc supportata		Indica se PIP supporta la comunicazione sincrona. Il valore predefinito è stato fornito in base alla specifica PIP.	Limitato al package o alla connessione. Questo attributo è disponibile solo per RNIF 2.0.	
ric sinc richiesto		Indica se PIP richiede una notifica di ricezione sincrona. Il valore predefinito è stato fornito in base alla specifica PIP.	Limitato al package o alla connessione. Questo attributo è disponibile solo per RNIF 2.0.	
Codice della catena di fornitura globale	Richiesto per RNIF 1.1	Il codice che identifica la catena di fornitura per la funzione del partner. I valori possibili sono: • Componenti elettronici • Tecnologia delle informazioni • Tecnologia del semiconduttore	Limitato al package o alla connessione	

Tabella 110. Attributi RosettaNet (Continua)

Attributo	Richiesto	Descrizione	Limitazioni	Val. predef.
Codifica		Questo attributo indica se è necessario eseguire la codifica. **Nota:** non coincide con la codifica SSL. Per TO dello scambio (quando si inviano documenti ad un partner), specifica se codificare o meno il documento. Per FROM dello scambio (quando si ricevono documenti da un partner), se l'attributo è stato impostato su Sì, è necessario codificare una richiesta RNIF inviata dal partner. Se l'attributo è stato impostato su No, il documento proveniente dal partner può essere codificato o decodificato. I valori possibili sono: **Nessuno** La codifica non è richiesta. **Payload** Codificare solo il contenuto del servizio di RosettaNet. **Payload e contenitore** Codificare il contenuto del servizio di RosettaNet insieme all'intestazione del servizio.	Limitato al package o alla connessione. Questo attributo è disponibile solo per RNIF 2.0.	Nessuno
Testo standard del messaggio	No	Lo standard in base al quale il contenuto del servizio deve essere compatibile. È necessario che sia impostato soltanto nel caso in cui un attributo, diverso da RosettaNet, abbia specificato un messaggio di contenuto del servizio.		Nessun valore predefinito
Versione standard del messaggio	No	La versione dello standard in base al quale il contenuto del servizio deve essere compatibile. È necessario che sia impostato soltanto nel caso in cui un attributo, diverso da RosettaNet, abbia specificato un messaggio di contenuto del servizio.		Nessun valore predefinito
Identificativo collegamento payload PIP	No	Indica l'identificativo di collegamento PIP definito dal partner, che risulta univoco tra i partner commerciali. Questo attributo è impostato soltanto nel caso di un contenuto del servizio diverso da RosettaNet.		Nessun valore predefinito
FromGlobalPartner ClassificationCode	Sì per gli schemi di RNIF 1.1	Il codice che identifica una funzione del partner della catena di fornitura. È richiesto solo quando si utilizza RNIF 1.1 per PIP basati sullo schema. Questo valore deve essere specificato anche per PIP 0A1, quando sono utilizzati i PIP basati sullo schema.		Nessun valore predefinito

Tabella 110. Attributi RosettaNet (Continua)

Attributo	Richiesto	Descrizione	Limitazioni	Val. predef.
ToGlobalPartner ClassificationCode	Sì per gli schemi di RNIF 1.1	Il codice che identifica una funzione del partner della catena di fornitura. È richiesto solo quando si utilizza RNIF 1.1 per PIP basati sullo schema. Questo valore deve essere specificato anche per PIP 0A1, quando sono utilizzati i PIP basati sullo schema.		Nessun valore predefinito
Algoritmo message digest RN	No	Questo attributo è utilizzato solo quando l'attributo "Firma digitale obbligatoria" è stata impostata su Sì. Determina l'algoritmo digest da utilizzare per la firma digitale. I valori consentiti sono SHA1 e MD5.		SHA1
Algoritmo codifica RN	No	Questo attributo viene utilizzato solo quando l'attributo "Codifica" è stato impostato su "Payload" o "Payload e contenitore". I valori consentiti sono "DES triplo" e "RC2-40".		DES triplo

Attributo Integrazione di backend

La sezione descrive l'attributo associato all'impacchettamento integrazione di backend.

Tabella 111. Attributo Integrazione di backend

Attributo	Descrizione	Val. predef.
Indicatore busta	Questo attributo indica se adattare il documento in una busta XML. I valori validi sono Sì e No.	No

Attributi ebMS

Questa sezione descrive gli attributi ebMS.

Tabella 112. Attributi ebMS

Attributo	Richiesto	Descrizione	Limitazioni	Val. predef.
Ora per riconoscere in min	No	L'intervallo di attesa per un riconoscimento prima di inviare nuovamente la richiesta di origine. Questo attributo funziona insieme al Conteggio tentativi. Le unità sono espresse in minuti.	Limitato al package o alla connessione	30
conteggio tentativi	No	Il numero di volte in base al quale viene inviata una richiesta se non è stato ricevuto un riconoscimento. Questo attributo funziona insieme all'attributo Ora per riconoscere. Ad esempio, se questo attributo è stato impostato su 3, la richiesta può essere inviata potenzialmente per quattro volte (la prima volta più tre tentativi).	Limitato al package o alla connessione	3

Tabella 112. Attributi ebMS (Continua)

Attributo	Richiesto	Descrizione	Limitazioni	Val. predef.
Non-rifiuto richiesto	No	Indica se è necessario salvare questo documento nella memoria di non-rifiuto. Sarà applicato al documento come origine o destinazione. Sì – Salvare il documento nella memoria di non-rifiuto. No – Non salvare il documento nella memoria di non-rifiuto.	Limitato al package o alla connessione	Sì
Memorizzazione messaggio richiesta	No	Indica se è necessario salvare questo documento nella memorizzazione messaggio. Verrà applicato a entrambi i documenti di origine e di destinazione. Sì – Salvare il documento nella memorizzazione messaggio. No – Non salvare il documento nella memorizzazione messaggio.	Limitato al package o alla connessione	Sì
Non-rifiuto di ricevuta richiesto	No	Indica se memorizzare il documento per la notifica di ricezione nella memoria di non-rifiuto.	Limitato al package o alla connessione	Sì
Riconoscimento obbligatorio	No	I valori possibili sono sempre, perMessage e mai. Se è stato impostato su “sempre”, durante l’invio di un documento ebMS sarà eseguita una richiesta per un riconoscimento inserendo l’elemento acknowledgmentRequested nel documento SOAP ebMS. Per il mittente, “perMessage” e “mai” significano “No.” Durante la ricezione di un documento ebMS, se il valore è stato impostato su “sempre”, il documento in arrivo deve richiedere il riconoscimento anche in caso di esito negativo. Se il valore è stato impostato su “perMessage” sull’hub del destinatario, il documento non ha esito negativo se il richiede un riconoscimento. Se il valore è stato impostato su “mai” il documento ebMS in arrivo non deve mai richiedere un riconoscimento.		mai

Tabella 112. Attributi ebMS (Continua)

Attributo	Richiesto	Descrizione	Limitazioni	Val. predef.
Firma di riconoscimento obbligatoria	No	I valori possibili sono sempre, perMessage e mai. "sempre" indica la richiesta per un riconoscimento firmato. "perMessage" e "mai" implicano l'esecuzione di una richiesta per un riconoscimento non firmato. Funziona insieme all'attributo "AcknowledgementRequested". Se il valore dell'attributo AcknowledgmentRequested è stato impostato su "perMessage" o "mai", questo attributo non sarà preso in considerazione. . Se non esiste alcun valore, sarà utilizzato "mai". Questo attributo viene utilizzato solo durante l'invio di un documento. Questo attributo non viene utilizzato per un documento ricevuto.		mai
Attore	No	L'attributo non deve essere impostato necessariamente durante l'implementazione ebMS 2.0. L'attributo Attore è necessario quando viene richiesto un riconoscimento della sincronizzazione. Viene inserito nel documento SOAP ebMS. Per questo attributo, la specifica ebMS 2.0 consiglia un valore costante http://schemas.xmlsoap.org/soap/actor/next (valore predefinito). Viene utilizzato questo attributo e in ogni caso l'utente non deve impostare il valore di tale attributo. Sarà utilizzato nella successiva implementazione.		http://schemas.xmlsoap.org/soap/actor/next
compressione obbligatoria	No	I valori possibili sono "Sì" e "No." Se i payload ebMS devono essere compressi, il valore deve essere impostato su "Sì." Se la compressione non è obbligatoria, non impostare alcun attributo o impostarla su "No."		No

Tabella 112. Attributi ebMS (Continua)

Attributo	Richiesto	Descrizione	Limitazioni	Val. predef.
Eliminazione duplicata	No	Per inviare un messaggio ebMS, se questo valore di attributo è stato impostato su "sempre", nel documento SOAP ebMS sarà inserito un elemento DuplicateElimination. La presenza di questo elemento nel documento SOAP ebMS significa che l'hub di ricezione non deve distribuire i payload ebMS sul backend se il documento ebMS risulta essere un duplicato. I valori "perMessage" e "mai" non inseriscono l'elemento DuplicateElimination nel documento SOAP. Per ricevere un documento ebMS, se il valore è stato impostato su "sempre", l'elemento DuplicateElimination deve essere presente nel documento SOAP ebMS anche se il documento ha esito negativo. Se il valore è "perMessage", il documento non avrà mai esito negativo indipendentemente dalla presenza dell'elemento DuplicateElimination nel documento SOAP. Per il valore "mai", l'elemento DuplicateElimination non deve esistere nel documento SOAP anche in caso di esito negativo del documento. Se non esiste alcun valore, sarà utilizzato "mai". Per un documento ebMS ricevuto, se il valore di attributo è "sempre e se l'elemento DuplicateElimination risulta presente, il documento sarà verificato per controllare se si tratti di un duplicato. Se il documento è un duplicato, esso avrà esito negativo.		mai
Costituente codifica	No	Il valore di questo attributo deve essere un elenco di tipo di contenuto separato dal punto e virgola per i payload, ad esempio application/xml;text/xml; application/binary:application/edi causa la codifica dei payload con questi tipi di contenuto. Questo attributo viene utilizzato solo se il valore di attributo "Codifica obbligatoria" è stato impostato su "Sì." **Nota:** se il valore "Codifica obbligatoria" è stato impostato su "Sì" e non sono stati configurati i tipi di contenuto per "Costituente codifica", non sarà codificato alcun attributo.		application/xml;text/xml; application/EDI-X12; application/EDI-CONSENT; application/EDIFACT; application/binary; application/octet-stream
Parametro Mime di codifica	No	Un attributo facoltativo è utilizzato per inserire i parametri aggiuntivi come intestazioni MimeMultipart nel documento codificato. Sarà applicato ad ogni payload codificato. Valore di esempio: smime-type="enveloped-data" o type="text/xml" version="1.0." Questo attributo viene utilizzato solo se il valore di attributo "Codifica obbligatoria" è stato impostato su "Sì."		Nessun valore predefinito

Tabella 112. Attributi ebMS (Continua)

Attributo	Richiesto	Descrizione	Limitazioni	Val. predef.
Tipo Mime di codifica	No	Non è utilizzato nell'implementazione corrente.		Nessun valore predefinito
codifica obbligatoria	No	I valori possibili sono "Sì" e "No." Se impostato su "Sì," i payload verranno codificati. Questo attributo funziona insieme all'attributo "Costituente codifica." **Nota:** se il valore "Codifica obbligatoria" è stato impostato su "Sì" e non sono stati configurati i tipi di contenuto per "Costituente codifica", non sarà codificato alcun attributo.		
Conversione codifica	No	Non è utilizzato nell'implementazione corrente.		Nessun valore predefinito
Escludi da firma	No	Il valore di questo attributo sarà un elenco di tipi di contenuto separato dal punto e virgola, ad esempio: `application/binary;application/octet-stream`. I payload dotati di questo tipo di contenuto non saranno inclusi nella firma. Questo attributo viene utilizzato solo se il valore di attributo "Firma digitale obbligatoria" è "Sì."		Nessuna immissione, la firma sarà applicata a tutti i payload.
funzione hash	No	L'algoritmo hash, che deve essere utilizzato nella firma XML quando si esegue l'hashing dei payload durante la firma. Questo attributo viene utilizzato solo se il valore di attributo "Firma digitale obbligatoria" è "Sì."		SHA1
Semantica ordine del messaggio	No	I valori possibili sono "Garantito" e "Non garantito". Durante l'invio di un documento, se il valore è stato impostato su "Garantito", un elemento Ordine del messaggio sarà inserito nel documento SOAP. Durante l'identificazione di questo elemento nel documento SOAP, l'hub di ricezione verifica che i payload siano stati distribuiti al backend in sequenza. Per un documento ricevuto, se questo attributo è stato impostato su "Garantito", il documento ebMS in entrata deve includere l'elemento Ordine del messaggio e se il documento risultasse mancante si verificherà l'esito negativo ed un messaggio di errore con codice di "Non coerente" sarà inviato al partner.		Non garantito
ruolo	No	Durante l'invio di un documento ebMS, questo valore di attributo è come un valore di elemento Ruolo nel documento SOAP ebMS. Durante la ricezione di un documento ebMS, questo valore di attributo viene confrontato con il valore di elemento Ruolo nel documento SOAP ebMS e, se i valori non corrispondono (anche se il valore di attributo è vuoto), il documento ha esito negativo ed un messaggio di errore con codice di errore "Non coerente" viene inviato al partner.		Nessun valore predefinito

Tabella 112. Attributi ebMS (Continua)

Attributo	Richiesto	Descrizione	Limitazioni	Val. predef.
continua durata	No	Il tempo espresso in minuti per cui il documento deve essere continuato, ad esempio 1440 per 24 ore. Durante l'invio di un documento, l'attributo Continua durata consente di calcolare TimeToLive mediante la formula: TimeToLive = Continua durata + (numero di Tentativi * Intervallo tentativi). Durante la ricezione di un documento, l'attributo Continua durata consente di effettuare un'eliminazione duplicata. Se un documento con l'IDMessaggio duplicato è stato ricevuto, esso viene verificato se è stato trasferito l'attributo Continua durata per il documento precedente. Se Continua durata non è stato trasferito, il documento viene contrassegnato come duplicato anche se il documento non è indicato come duplicato. Se non viene inserito alcun valore, risulta valido il valore predefinito 0.		0
costituente impacchettamento	No	Non è utilizzato nell'implementazione corrente.		Nessun valore predefinito
Parametro Mime del package	No	Non è utilizzato nell'implementazione corrente.		Nessun valore predefinito
Algoritmo codifica	Sì quando il valore di attributo "Codifica obbligatoria" è stato impostato su "Sì"	L'algoritmo utilizzato per codificare i payload ebMS. Questo valore funziona insieme all'attributo ″Protocollo codifica″. Questo attributo viene utilizzato solo se il valore di attributo "Codifica obbligatoria" è stato impostato su "Sì."		AES-128
protocollo codifica	No	Il protocollo utilizzato per codificare i payload ebMS. I valori possibili sono Codifica XML e SMIME. Questo attributo viene utilizzato solo se il valore di attributo "Codifica obbligatoria" è stato impostato su "Sì." Se l'attributo Codifica obbligatoria è stata impostata su ″sì″ e nessun valore è stato fornito per tale attributo, il documento ha esito negativo.		Codifica XML

Tabella 112. Attributi ebMS (Continua)

Attributo	Richiesto	Descrizione	Limitazioni	Val. predef.
intervallo tentativi	No	Per un documento inviato, è l'intervallo di tempo espresso in minuti per un riconoscimento prima di inviare nuovamente il documento ebMS. I documenti ebMS sono inviati nuovamente solo quando un riconoscimento è stato richiesto, ma un riconoscimento non è stato ricevuto dal partner entro l'intervallo tentativi. Un valore pari a 0 indica che non sono eseguiti tentativi. Questo attributo funziona insieme all'attributo "Conteggio tentativi".		270
algoritmo firma	Sì se la ″Firma digitale obbligatoria″ è impostata su Sì	L'algoritmo utilizzato per firmare il documento ebMS. Questo attributo viene utilizzato solo se il valore di attributo "Firma digitale obbligatoria" è "Sì."		dsa-sha1
Conversione firma	No	L'algoritmo di conversione utilizzato per convertire i payload prima di creare la firma XML. Questo attributo viene utilizzato solo se il valore di attributo "Firma digitale obbligatoria" è "Sì."		Nessun valore predefinito
modalità di risposta sincronizzata	No	Il tipo di risposta sincrona è stato richiesto per il documento inviato. Se il valore è stato impostato su: • **MSHSignalsOnly** - solo i documenti di errore/notifica MSH saranno inviati mediante una connessione sincrona. I documenti di segnale e di risposta di business saranno restituiti in maniera asincrona. • **signalsOnly** – solo i documenti MSH ed i documenti di segnale di business saranno inviati mediante una connessione sincrona. I documenti di risposta di business saranno restituiti in maniera asincrona. • **responseOnly** – solo i documenti MSH ed i documenti di risposta di business saranno inviati mediante una connessione sincrona. I documenti di segnale di business saranno restituiti in maniera asincrona. • **signalsAndResponse** - I documenti di segnale e di risposta di business saranno inviati mediante una connessione sincrona. • **none** – Nessun documento di risposta sincrona dal destinatario.		none

Tabella 112. Attributi ebMS (Continua)

Attributo	Richiesto	Descrizione	Limitazioni	Val. predef.
Verifica intelligibile obbligatoria	No	Il valore di questo attributo è stato inviato al backend come valore di intestazione "x-aux-IntelligibleCheckRequired". I valori possibili sono "sì" e "no." L'obiettivo è indicare al backend che è necessario inviare solo ReceiptAcknowledgement se il documento ebXML con i payload non contiene errori. È gestito sul backend per interpretare questo valore.		No
Metodo di canonicalizzazione	No	L'algoritmo di canonicalizzazione utilizzato prima di eseguire la firma XML. Questo attributo viene utilizzato solo se il valore di attributo "Firma digitale obbligatoria" è "Sì."		INCLUSIVE_ WITH_ COMMENTS
Costituente compressione	No	L'elenco del tipo di contenuto separato dal punto e virgola dei payload, che devono essere compressi. Ad esempio, se i payload con contentType "text/xml" e "application/edi" devono essere compressi, il valore di questo attributo sarà "text/xml;application/edi". Nessuna immissione indica che non sarà compresso alcun payload anche se "Compressione obbligatoria" è stato impostato su "Sì." Questo attributo viene utilizzato solo se il valore di attributo "Compressione obbligatoria" è "Sì."		application/xml; text/ xml;application/ EDI-X12; application/ EDI-CONSENT; application/ EDIFACT
tipo di servizio	Sì se il valore di elemento Servizio (Tipo di documento) non è un indirizzo URI	Durante l'invio di un documento ebMS, il valore di elemento ebMSService del messaggio SOAP ebMS deve essere un indirizzo URI o un'altra stringa. Nel caso in cui sia una stringa, questo attributo Tipo è obbligatorio. Se il valore Servizio (Tipo di documento) non è un indirizzo URI, questo valore di attributo Tipo di servizio viene utilizzato come un valore di attributo Tipo nel documento ebMS.		Nessun valore predefinito

attributi generali

Questa sezione descrive gli attributi generali.

Tabella 113. attributi generali

Attributo	Richiesto	Descrizione	Limitazioni	Val. predef.
Mappa di convalida	No	La mappa di convalida che consente di convalidare questo documento. L'Azione, utilizzata in runtime, non deve includere una fase di convalida che utilizza questo attributo. Solo le mappe di convalida, caricate ed associate a questo Tipo di documento, saranno selezionabili.	Limitato al package o alla connessione	Nessun valore predefinito

Tabella 113. attributi generali (Continua)

Attributo	Richiesto	Descrizione	Limitazioni	Val. predef.
Attributo utente 1	No	Utilizzato nelle uscite definite dall'utente. Il valore è stato determinato dal creatore dell'uscita definita dall'utente. Esso sarà impostato in BDO (Business Document Object) con l'attributo bcg.ro.user.User01 come un prefisso From (Documento di origine) o To (Documento di destinazione).		Nessun valore predefinito
attributo utente 2	No	Utilizzato nelle uscite definite dall'utente. Il valore è stato determinato dal creatore dell'uscita definita dall'utente. Esso sarà impostato in BDO (Business Document Object) con l'attributo bcg.ro.user.User02 come un prefisso From (Documento di origine) o To (Documento di destinazione).		Nessun valore predefinito
attributo utente 3	No	Utilizzato nelle uscite definite dall'utente. Il valore è stato determinato dal creatore dell'uscita definita dall'utente. Esso sarà impostato in BDO (Business Document Object) con l'attributo bcg.ro.user.User03 come un prefisso From (Documento di origine) o To (Documento di destinazione).		Nessun valore predefinito
attributo utente 4	No	Utilizzato nelle uscite definite dall'utente. Il valore è stato determinato dal creatore dell'uscita definita dall'utente. Esso sarà impostato in BDO (Business Document Object) con l'attributo bcg.ro.user.User04 come un prefisso From (Documento di origine) o To (Documento di destinazione).		Nessun valore predefinito
attributo utente 5	No	Utilizzato nelle uscite definite dall'utente. Il valore è stato determinato dal creatore dell'uscita definita dall'utente. Esso sarà impostato in BDO (Business Document Object) con l'attributo bcg.ro.user.User05 come un prefisso From (Documento di origine) o To (Documento di destinazione).		Nessun valore predefinito
attributo utente 6	No	Utilizzato nelle uscite definite dall'utente. Il valore è stato determinato dal creatore dell'uscita definita dall'utente. Esso sarà impostato in BDO (Business Document Object) con l'attributo bcg.ro.user.User06 come un prefisso From (Documento di origine) o To (Documento di destinazione).		Nessun valore predefinito
attributo utente 7	No	Utilizzato nelle uscite definite dall'utente. Il valore è stato determinato dal creatore dell'uscita definita dall'utente. Esso sarà impostato in BDO (Business Document Object) con l'attributo bcg.ro.user.User07 come un prefisso From (Documento di origine) o To (Documento di destinazione).		Nessun valore predefinito

Tabella 113. attributi generali (Continua)

Attributo	Richiesto	Descrizione	Limitazioni	Val. predef.
attributo utente 8	No	Utilizzato nelle uscite definite dall'utente. Il valore è stato determinato dal creatore dell'uscita definita dall'utente. Esso sarà impostato in BDO (Business Document Object) con l'attributo bcg.ro.user.User08 come un prefisso From (Documento di origine) o To (Documento di destinazione).		Nessun valore predefinito
attributo utente 9	No	Utilizzato nelle uscite definite dall'utente. Il valore è stato determinato dal creatore dell'uscita definita dall'utente. Esso sarà impostato in BDO (Business Document Object) con l'attributo bcg.ro.user.User09 come un prefisso From (Documento di origine) o To (Documento di destinazione).		Nessun valore predefinito
attributo utente 10	No	Utilizzato nelle uscite definite dall'utente. Il valore è stato determinato dal creatore dell'uscita definita dall'utente. Esso sarà impostato in BDO (Business Document Object) con l'attributo bcg.ro.user.User10 come un prefisso From (Documento di origine) o To (Documento di destinazione).		Nessun valore predefinito

Informazioni particolari

Queste informazioni sono state sviluppate per prodotti e servizi offerti negli Stati Uniti.

È possibile che negli altri paesi IBM non offra i prodotti, i servizi o le funzioni illustrati in questo documento. Rivolgersi al rappresentante IBM locale per informazioni sui prodotti e i servizi disponibili nel proprio paese. Qualunque riferimento relativo a prodotti, programmi o servizi IBM non implica che solo quei prodotti, programmi o servizi IBM possano essere utilizzati. In sostituzione a quelli forniti da IBM, possono essere usati prodotti, programmi o servizi funzionalmente equivalenti che non comportino la violazione dei diritti di proprietà intellettuale o di altri diritti di IBM. È comunque responsabilità dell'utente valutare e verificare la possibilità di utilizzare altri programmi e/o prodotti, fatta eccezione per quelli espressamente indicati da IBM.

IBM può avere brevetti o domande di brevetto in corso relativi a quanto trattato nella presente pubblicazione. La fornitura del presente documento non concede alcuna licenza a tali brevetti. Chi desiderasse ricevere informazioni relative a licenze può rivolgersi per iscritto a:

IBM Director of Commercial Relations
IBM Europe
Schoenaicher Str. 220
D-7030 Boeblingen
Deutschland

Per richieste di licenze relative ad informazioni double-byte (DBCS), contattare il Dipartimento di Proprietà Intellettuale IBM nel proprio paese o inviare richieste per iscritto a:

IBM World Trade Asia Corporation Licensing
2-31 Roppongi 3-chome, Minato-ku
Tokyo 106-0032, Japan.

Il seguente paragrafo non si applica al Regno Unito o a qualunque altro paese in cui tali dichiarazioni sono incompatibili con le norme locali:IBM (INTERNATIONAL BUSINESS MACHINES CORPORATION) FORNISCE LA PRESENTE PUBBLICAZIONE ″NELLO STATO IN CUI SI TROVA″ SENZA GARANZIE DI ALCUN TIPO, ESPRESSE O IMPLICITE, IVI INCLUSE, A TITOLO DI ESEMPIO,GARANZIE IMPLICITE DI NON VIOLAZIONE, DI COMMERCIABILITÀ E DI IDONEITÀ PER UNO SCOPO PARTICOLARE. Alcuni stati non consentono la rinuncia a garanzie esplicite o implicite in determinate transazioni, quindi, la presente dichiarazione potrebbe non essere a voi applicabile.

Questa pubblicazione potrebbe contenere imprecisioni tecniche o errori tipografici. Le informazioni incluse in questo documento vengono modificate su base periodica; tali modifiche verranno incorporate nelle nuove edizioni della pubblicazione. IBM si riserva il diritto di apportare miglioramenti e/o modifiche al prodotto o al programma descritto nel manuale in qualsiasi momento e senza preavviso.

Tutti i riferimenti a siti Web non IBM contenuti in questo documento sono forniti solo per consultazione. I materiali disponibili presso i siti Web non fanno parte di questo prodotto e l'utilizzo di questi è a discrezione dell'utente.

Tutti i commenti e i suggerimenti inviati potranno essere utilizzati liberamente da IBM e diventeranno esclusiva della stessa.

Coloro che detengono la licenza su questo programma e desiderano avere informazioni su di esso allo scopo di consentire (i) uno scambio di informazioni tra programmi indipendenti ed altri (compreso questo) e (ii) l'uso reciproco di tali informazioni, dovrebbero rivolgersi a:

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

Tali informazioni possono essere disponibili, in base ad appropriate clausole e condizioni, includendo in alcuni casi, il pagamento di una tassa.

Il programma concesso in licenza descritto nel presente documento e tutto il materiale concesso in licenza disponibile sono forniti da IBM in base alle clausole dell'Accordo per Clienti IBM (IBM Customer Agreement), dell'IBM IPLA (IBM International Program License Agreement) o qualsiasi altro accordo equivalente tra le parti.

Tutti i dati relativi alle prestazioni contenuti in questa pubblicazione sono stati determinati in ambiente controllato. Pertanto, i risultati ottenuti in ambienti operativi diversi possono variare in modo considerevole. Alcune misure potrebbero essere state fatte su sistemi di livelli di sviluppo per cui non si garantisce che queste saranno uguali su tutti i sistemi disponibili. Inoltre, alcune misurazioni possono essere state stimate tramite estrapolazione. I risultati reali possono variare. Gli utenti di questa pubblicazione devono verificare che i dati siano applicabili al loro specifico ambiente.

Le informazioni relative a prodotti non IBM sono state ottenute dai fornitori di tali prodotti. IBM non ha testato quei prodotti e non può confermarne l'accuratezza della prestazione, la compatibilità o qualsiasi altro reclamo relativo ai prodotti non IBM. Eventuali commenti relativi alle prestazioni dei prodotti non IBM devono essere indirizzati ai fornitori di tali prodotti.

Tutte le dichiarazioni relative all'orientamento o alle intenzioni future di IBM sono soggette a modifica o a ritiro senza preavviso e rappresentano solo mete e obiettivi.

Tutti i prezzi IBM mostrati sono i prezzi al dettaglio suggeriti da IBM, sono attuali e soggetti a modifica senza preavviso. I prezzi al fornitore possono variare.

Queste informazioni sono solo per scopi di pianificazione. Le presenti informazioni sono soggette a modifiche prima che i prodotti descritti siano resi disponibili.

Questa pubblicazione contiene esempi di dati e report utilizzati quotidianamente nelle operazioni di business. Per illustrarli nel modo più completo possibile, gli esempi includono i nomi di individui, società, marchi e prodotti. Tutti i nomi contenuti nel manuale sono fittizi e ogni riferimento a nomi ed indirizzi reali è puramente casuale.

LICENZA DI COPYRIGHT

Queste informazioni contengono programmi applicativi di esempio in linguaggio sorgente, che illustrano tecniche di programmazione su varie piattaforme operative. È possibile copiare, modificare e distribuire questi programmi di esempio sotto qualsiasi forma senza alcun pagamento a IBM, allo scopo di sviluppare, utilizzare, commercializzare o distribuire i programmi applicativi in conformità alle API (application programming interface) a seconda della piattaforma operativa per cui i programmi di esempio sono stati scritti. Questi esempi non sono stati testati approfonditamente tenendo conto di tutte le condizioni possibili. IBM, quindi, non può garantire o sottintendere l'affidabilità, l'utilità o il funzionamento di questi programmi.

Ogni copia o qualsiasi parte di questi programmi di esempio o qualsiasi lavoro derivato, devono contenere le seguenti informazioni relative alle leggi sul copyright:

Se si stanno visualizzando queste informazioni in formato elettronico, le fotografie e le illustrazioni a colori potrebbero non comparire.

Informazioni interfaccia di programmazione

Le informazioni di interfaccia di programmazione, se fornite, sono finalizzate alla creazione del software dell'applicazione mediante questo programma. Le interfacce di programmazione ad uso generale, consentono di scrivere il software dell'applicazione, ottenendo i servizi degli strumenti di questo programma. Tuttavia, queste informazioni potrebbero contenere informazioni di diagnosi, modifica e ottimizzazione. Le informazioni di diagnosi, modifica e ottimizzazione vengono fornite per eseguire il debug del software dell'applicazione.

Attenzione: Non utilizzare le informazioni di diagnosi, modifica e ottimizzazione come un'interfaccia di programmazione perché è soggetta a modifiche.

Marchi e marchi di servizio

I seguenti termini sono marchi della International Business Machines Corporation negli Stati Uniti e/o in altri paesi:

IBM	DB2	IMS	MQIntegrator	Tivoli
il logo IBM	DB2 Universal Database	Informix	MVS	WebSphere
AIX	Domino	iSeries	OS/400	z/OS
CICS	IBMLink	Lotus	Vantaggio passaporto	
CrossWorlds	i5/OS	Lotus Notes	SupportPac	

Microsoft, Windows, Windows NT e il logo Windows sono marchi di Microsoft Corporation negli Stati Uniti e/o in altri paesi.

MMX, Pentium e ProShare sono marchi di Intel Corporation negli Stati Uniti e/o in altri paesi.

Solaris, Java e tutti i marchi basati su Java sono marchi della Sun Microsystems, Inc. negli Stati Uniti e/o in altri paesi.

Linux è un marchio di Linus Torvalds negli Stati Uniti, in altri paesi o in entrambi.

Nomi di altre società, prodotti o servizi possono essere marchi di altre società.

WebSphere Partner Gateway Enterprise Edition e Advanced Edition includono del software sviluppato dal progetto Eclipse (www.eclipse.org)

Indice analitico

Caratteri speciali

Numerico

A

B

C

D

E

F

G

H

I

J

K

L

M

N

O

P

Q

R

S

T

U

V

W

X

Stampato in Italia