

IBM WebSphere Partner Gateway Enterprise e Advanced
Editions



Guida alla configurazione hub

Versione 6.0

IBM WebSphere Partner Gateway Enterprise e Advanced
Editions



Guida alla configurazione hub

Versione 6.0

Nota!

Prima di utilizzare queste informazioni e il relativo prodotto, leggere le informazioni presenti in Appendice E, "Informazioni particolari", a pagina 299.

28 giugno 2005

Questa edizione si applica a WebSphere Partner Gateway Enterprise Edition (5724-L69), versione 6.0, e Advanced Edition (5724-L68), versione 6.0 e a tutti i successivi rilasci e modifiche, fino a quando non diversamente indicato nelle nuove edizioni.

Per inviare commenti relativi a questa documentazione, inviare un e-mail a: doc-comments@us.ibm.com.
Attendiamo le vostre domande.

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

© Copyright International Business Machines Corporation 2004, 2005. Tutti i diritti riservati.

Indice

Informazioni sul presente manuale	xi
Destinatari	xi
Convezioni tipografiche	xi
Documenti correlati	xii
Novità di questo rilascio	xiii
Novità nel rilascio 6.0.	xiii
Novità in questo rilascio 4.2.2	xiii
Capitolo 1. Introduzione	1
Panoramica	1
Informazioni necessarie per l'impostazione dell'hub	2
Panoramica dei trasporti	2
Panoramica delle definizioni del flusso di documenti	3
Panoramica sull'elaborazione del documento	7
Configurazione dei componenti di elaborazione del documento con i gestori	9
Destinazioni	9
Gestore documenti	10
Gateway	14
Panoramica della configurazione dell'hub	15
Configurazione dell'hub	15
Creazione partecipanti	16
Come stabilire le connessioni del documento	16
Capitolo 2. Preparazione alla configurazione dell'hub	17
Creazione di una directory per un gateway della directory del file	17
Configurazione del server FTP per la ricezione dei documenti	17
Configurazione della struttura di directory richiesta sul server FTP	18
Modalità di elaborazione dei file inviati su FTP	19
Configurazione del server FTP aggiuntiva	20
Considerazioni di protezione per il server FTPS	20
Configurazione dell'hub per il protocollo di trasporto JMS	21
Creazione di una directory per JMS	21
Modifica della configurazione JMS predefinita	21
Creazione delle code e del canale	21
Aggiunta di un runtime Java ^(TM) all'ambiente	22
Definizione della configurazione JMS	22
Utilizzo di script FTP per le destinazioni e i gateway dello script FTP	23
Utilizzo di mappe dal client Data Interchange Services	24
Capitolo 3. Avvio del server e visualizzazione della Console comunità	25
Avvio di WebSphere MQ	25
Avvio dei componenti di WebSphere Partner Gateway	25
Collegamento alla Console comunità	26
Capitolo 4. Configurazione di Console comunità	27
Specifiche delle informazioni locali e del marchio della console	27
Marchi della console	27
Modifica del foglio di calcolo	28
Localizzazione dei dati sulla console	28
Impostazione della politica della password	29
Configurazione delle autorizzazioni	30
Modalità di concessione dei permessi agli utenti	30
Abilitazione e disabilitazione permessi	30

Capitolo 5. Definizione delle destinazioni	31
Panoramica	31
Caricamento dei gestori definiti dall'utente	32
Impostazione di valori di trasporto globale	33
Impostazione di una destinazione HTTP/S	33
Dettagli di destinazione	34
Configurazione della destinazione	34
Gestori	34
Impostazione di una destinazione FTP	34
Dettagli di destinazione	35
Configurazione della destinazione	35
Gestori	35
Impostazione di una destinazione SMTP	36
Dettagli di destinazione	36
Configurazione della destinazione	36
Pianificazione	36
Impostazione di una destinazione JMS	37
Dettagli di destinazione	37
Configurazione della destinazione	37
Gestori	38
Impostazione di una destinazione di sistema di file	38
Dettagli di destinazione	39
Configurazione della destinazione	39
Gestori	39
Impostazione di una destinazione Script FTP	39
Creazione dello script FTP	40
Comandi di script FTP	40
Dettagli di destinazione	41
Configurazione della destinazione	42
Attributi definiti dall'utente	42
Pianifica	43
Gestori	43
Impostazione di una destinazione per un trasporto definito dall'utente	43
Modifica dei punti di configurazione	44
Preprocesso	44
SyncCheck	47
Postprocesso	48
Modifica dell'elenco Configurati	48
Capitolo 6. Configurazione delle procedure e delle azioni del flusso di lavoro fisso.	49
Caricamento dei gestori	49
Configurazione dei flussi di lavoro fissi	50
Flussi di lavori fissi	50
Flusso di lavoro in uscita	51
Configurazione azioni	51
Modifica di un'azione definita dall'utente	52
Creazione di azioni	52
Capitolo 7. Configurazione dei flussi di documenti.	55
Panoramica	55
Passaggio 1: Assicurarsi che la definizione di flusso di documenti sia disponibile	55
Passaggio 2: Creare le interazioni	56
Passaggio 3: Creare profili partecipante, gateway e funzioni B2B	56
Passaggio 4: Attivare le connessioni	56
Un esempio di flusso	57
Documenti binari	58
Documenti EDI con azione Pass-Through	59
Creazione delle definizioni di flusso di documenti	59
Creazione interazioni	60
Documenti RosettaNet	60

Panoramica	60
RNIF e pacchetti di flusso dei documenti PIP	61
Creazione di definizioni di flusso di documenti	63
Configurazione dei valori dell'attributo	65
Creazione di interazioni	66
Servizi Web	68
Identificazione dei partecipanti per un servizio Web	69
Creazione di definizioni di flusso di documenti	69
Creazione interazioni	73
Restrizioni e limitazioni del supporto del servizio web	73
documenti cXML	73
Panoramica	74
Creazione delle definizioni del flusso di documenti	77
Creazione interazioni	78
Documenti XML personalizzati	78
Panoramica	78
Creazione del formato di definizione di un protocollo	78
Creazione di un flusso di definizione di documenti	79
Creazione di un formato XML	80
Utilizzo delle mappe di convalida	80
Aggiunta mappe di convalida	80
Associazione delle mappe alle definizioni di flusso di documenti	81
Visualizzazione dei documenti	81
Capitolo 8. Configurazione dei flussi di documenti EDI	83
Panoramica su EDI	83
Struttura dell'interscambio EDI	83
Mappe	85
Panoramica dei documenti XML e ROD	86
Documenti XML	86
Documenti ROD	86
Separatori e più documenti	86
Panoramica sulla creazione di flussi di documenti ed impostazione degli attributi	87
Passaggio 1: Assicurarsi che la definizione di flusso di documenti sia disponibile	87
Passaggio 2: Creare le interazioni	88
Passaggio 3: Creare profili partecipante, gateway e funzioni B2B.	88
Passaggio 4: Attivare le connessioni	89
Panoramica sui flussi possibili	89
Flusso EDI in EDI	89
Flusso EDI in XML o ROD	90
Flusso XML o ROD in EDI	91
Flusso di più documenti XML o ROD in scambio EDI	91
Flusso XML in ROD o ROD in XML	92
Flusso XML in XML o ROD in ROD	93
Modalità di elaborazione degli interscambi EDI	94
Modalità di elaborazione dei documenti XML o ROD	97
Impostazione dell'ambiente EDI	97
Envelope	98
Profili busta	99
Profili connessione	104
Numeri di controllo	106
Inizializzazione numeri di controllo	109
Numeri di controllo correnti	109
Passaggi generali per la definizione di scambio di documenti	110
Importazione delle mappe	110
Impostazione di un flusso EDI in EDI	112
Impostazione di un flusso EDI in XML o ROD	114
Impostazione del flusso XML o ROD in EDI	116
Impostazione di più documenti XML o ROD in un file in un flusso EDI.	117
Impostazione di un flusso di documenti XML in ROD o ROD in XML	118
Impostazione di un flusso di documenti XML in XML o ROD in ROD	119

Impostazione dei riconoscimenti	120
Aggiunta di una notifica al flusso di documenti	121
Visualizzazione di interscambi e transazioni EDI	122

Capitolo 9. Creazione del profilo Gestore comunità e delle funzioni B2B 123

Creazione del profilo Gestore comunità.	123
Impostazione delle capacità B2B	124

Capitolo 10. Creazione gateway 127

Panoramica	127
Impostazione dei valori globali di trasporto	128
Configurazione di un proxy di inoltro	129
Configurazione di un gateway HTTP	129
Dettagli del gateway	130
Configurazione del gateway	130
Configurazione di un gateway HTTPS	131
Dettagli del gateway	131
Configurazione del gateway	131
Configurazione di un gateway FTP	132
Dettagli del gateway	132
Configurazione del gateway	133
Configurazione di un gateway SMTP	133
Dettagli del gateway	134
Configurazione del gateway	134
Configurazione di un gateway JMS	134
Dettagli del gateway	135
Configurazione del gateway	135
Configurazione di un gateway della directory del file	136
Dettagli del gateway	137
Configurazione del gateway	137
Configurazione di un gateway FTPS.	138
Dettagli del gateway	138
Configurazione del gateway	138
Configurazione di un gateway script FTP	139
Creazione dello script FTP	139
Comandi script FTP	139
Gateway script FTP	140
Dettagli del gateway	140
Configurazione del gateway	141
Attributi definiti dall'utente	141
Pianifica	142
Configurazione dei gestori	142
Configurazione di un gateway per il trasporto definito dall'utente.	143
Specifica di un gateway predefinito	143

Capitolo 11. Creazione dei partecipanti e delle funzioni B2B 145

Creazione dei profili dei partecipanti	145
Impostazione delle funzioni B2B	146

Capitolo 12. Gestione delle connessioni 149

Panoramica	149
Attivazione delle connessioni del partecipante	149
Specifica e modifica di attributi	150

Capitolo 13. Impostazione di sicurezza per gli scambi in arrivo e in uscita 153

Termini e concetti di protezione	153
Meccanismi di protezione e protocolli utilizzati in WebSphere Partner Gateway	153
L'utilità iKeyman	154
Console comunità	154
Keystore e truststore	155

Catene di certificati	156
Certificati principali e secondari	156
Modifica dell'intensità della codifica	156
Creazione e installazione dei certificati SSL	157
Handshake SSL.	157
Certificati SSL in entrata.	158
Certificato SSL in uscita	160
Aggiunta di un CRL (Certificate Revocation List)	162
Abilitazione dell'accesso ai punti di distribuzione CRL	163
Creazione e installazione dei certificati di firma	164
Certificato di firma in entrata	164
Certificato di firma in uscita	165
Creazione e installazione di certificati di codifica	166
Certificato di codifica in entrata	166
Certificato di codifica in uscita	167
Configurazione di SSL in entrata per la Console e il Destinatario	169
Panoramica certificati.	169
Capitolo 14. Ultimazione della configurazione	173
Abilitazione all'utilizzo degli API.	173
Specifiche delle code utilizzate per gli eventi	173
Specifiche degli eventi notificabili	174
Aggiornamento di un trasposto definito dall'utente.	175
Appendice A. Esempi di base	177
Configurazione di base – Scambio di documenti EDI autorizzati	177
Configurazione hub	177
Creazione dei partecipanti e delle connessioni del partecipante.	179
Configurazione di base - Configurazione della protezione per documenti in entrata e in uscita	183
Impostazione dell'autenticazione SSL per i documenti in entrata	183
Impostazione della codifica.	185
Impostazione della firma del documento	186
Come estendere la configurazione di base	188
Creazione di una destinazione FTP	188
Impostazione dell'hub per la ricezione di file binari	188
Impostazione dell'hub per i documenti XML personalizzati	190
Appendice B. Esempi EDI	193
Esempio EDI in ROD.	193
Sbustamento e trasformazione di un interscambio EDI	193
Aggiunta di un TA1 ad uno scambio	199
Aggiunta di una mappa FA	202
Esempio EDI in XML.	206
Importazione della mappa di trasformazione.	207
Verifica della mappa di trasformazione e delle definizioni di flusso di documenti	207
Configurazione della destinazione	207
Creazione delle interazioni	208
Creazione di partecipanti	208
Creazione dei gateway	209
Impostazione delle funzioni B2B	210
Attivazione delle connessioni	211
Esempio da XML a EDI	212
Importazione della mappa di trasformazione.	212
Verifica della mappa di trasformazione e delle definizioni di flusso di documenti	212
Configurazione della destinazione	213
Creazione delle interazioni	213
Creazione di partecipanti	214
Creazione dei gateway	214
Impostazione delle funzioni B2B	215
Creazione del profilo busta.	217

Creazione del formato XML	217
Attivazione delle connessioni	217
Configurazione di attributi	218
Esempio ROD in EDI.	219
Importazione della mappa di trasformazione	219
Verifica della mappa di trasformazione e delle definizioni di flusso di documenti	219
Configurazione della destinazione	220
Creazione delle interazioni	221
Creazione di partecipanti	221
Creazione dei gateway	222
Impostazione delle funzioni B2B	223
Creazione del profilo busta	224
Attivazione delle connessioni	224
Configurazione di attributi	225

Appendice C. Informazioni su RosettaNet aggiuntive 227

Disattivazione dei PIP	227
Come fornire la notifica dell'errore	227
PIP 0A1	227
Aggiornamento delle informazioni sul contatto	228
Modifica dei valori degli attributi di RosettaNet	228
Creazione di pacchetti di flusso di documenti PIP	229
Creazione di file XSD.	230
Creazione del file XML	236
Creazione del pacchetto	239
Convalida	239
Cardinalità	239
Formato	240
Enumerazione	240
Contenuti del pacchetto del flusso di documenti PIP	241
0A1 Notification of Failure V1.0	241
0A1 Notification of Failure V02.00	241
2A1 Distribute New Product Information	242
2A12 Distribute Product Master	243
3A1 Request Quote	244
3A2 Request Price and Availability	245
3A4 Request Purchase Order V02.00.	245
3A4 Request Purchase Order V02.02.	247
3A5 Query Order Status.	248
3A6 Distribute Order Status	249
3A7 Notify of Purchase Order Update	250
3A8 Request Purchase Order Change V01.02	252
3A8 Request Purchase Order Change V01.03	253
3A9 Request Purchase Order Cancellation.	254
3B2 Notify of Advance Shipment.	255
3B3 Distribute Shipment Status	256
3B11 Notify of Shipping Order	257
3B12 Request Shipping Order	258
3B13 Notify of Shipping Order Confirmation.	259
3B14 Request Shipping Order Cancellation	259
3B18 Notify of Shipping Documentation	260
3C1 Return Product	261
3C3 Notify of Invoice.	262
3C4 Notify of Invoice Reject	263
3C6 Notify of Remittance Advice.	264
3C7 Notify of Self-Billing Invoice.	265
3D8 Distribute Work in Process	266
4A1 Notify of Strategic Forecast	266
4A3 Notify of Threshold Release Forecast	267
4A4 Notify of Planning Release Forecast	268
4A5 Notify of Forecast Reply	269

4B2 Notify of Shipment Receipt	270
4B3 Notify of Consumption	271
4C1 Distribute Inventory Report V02.01	272
4C1 Distribute Inventory Report V02.03	272
5C1 Distribute Product List.	273
5C2 Request Design Registration	274
5C4 Distribute Registration Status	275
5D1 Request Ship From Stock And Debit Authorization	275
6C1 Query Service Entitlement	276
6C2 Request Warranty Claim	277
7B1 Distribute Work in Process	278
7B5 Notify Of Manufacturing Work Order.	279
7B6 Notify Of Manufacturing Work Order Reply	280
Appendice D. Attributi.	281
Attributi EDI	281
attributi profilo busta.	281
Attributi definizione flusso di documenti e connessione	285
Proprietà del client Data Interchange Services	292
Attributi AS	293
Attributi RosettaNet	296
Attributo integrazione di backend	298
Appendice E. Informazioni particolari	299
Informazioni interfaccia di programmazione	301
Marchi commerciali e marchi di servizio	301
Indice analitico.	303

Informazioni sul presente manuale

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

Destinatari

Questo documento è indirizzato alla persona responsabile per la configurazione del server di WebSphere Partner Gateway, meglio noto come hub. Per configurare l'hub, è necessario essere l'Ammin hub. L'Ammin Hub ha la capacità di utilizzare tutte le funzioni della Console comunità di WebSphere Partner Gateway per configurare e far funzionare l'hub.

Convezioni tipografiche

Questo documento utilizza le seguenti convenzioni.

Tabella 1. Convenzioni tipografiche

Convenzione	Descrizione
Font a spaziatura fissa	Questo tipo di testo indica il testo che si digita, i valori degli argomenti o le opzioni di comando, gli esempi e gli esempi di codice oppure le informazioni che il sistema stampa nella 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 di menu) e le intestazioni delle colonne nelle tabelle e il testo.
<i>corsivo</i>	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.
<i>Font a spaziatura fissa corsivo</i>	Questo tipo di testo indica nomi variabili nel testo a spaziatura fissa.
<i>ProductDir</i>	<i>ProductDir</i> rappresenta la directory in cui è installato il prodotto. Tutti i nomi del percorso IBM WebSphere Partner Gateway sono relativi alla directory in cui il prodotto WebSphere Partner Gateway viene installato sul sistema.
<i>%text%</i> e <i>\$text</i>	Il testo fra segni di percentuale (%) indica il valore della variabile di testo del sistema Windows ^(R) o la variabile dell'utente. La notazione equivalente in un ambiente ^(R) è <i>\$testo</i> , che indica il valore della variabile di ambiente UNIX <i>testo</i> .
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) La sottolineatura indica un riferimento incrociato. Fare clic su questo tipo di testo 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 circondano i riferimenti incrociati ad altre sezioni del documento.

Tabella 1. Convenzioni tipografiche (Continua)

Convenzione	Descrizione
{ }	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 circondano un parametro opzionale.
< >	Le parentesi angolari circondano gli elementi variabili di un nome per distinguerli l'uno dall'altro. Ad esempio, <nome_server><nome_connettore>tmp.log.
/, \	Le barre inverse (\) vengono utilizzate come separatori nei percorsi di directory delle installazioni di Windows. Per le installazioni UNIX, sostituire le barre (/) con quelle all'indietro.

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 e Advanced Editions.

E' possibile eseguire il download di questa documentazione o leggerla direttamente online al seguente sito web:

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

Nota: Le informazioni importanti su questo prodotto sono disponibili nelle Note tecniche di supporto tecnico e Immagini pubblicate dopo questo documento. Tali informazioni possono essere trovati al sito web di supporto per WebSphere Business Integration, al seguente indirizzo

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

Selezionare l'area d'interesse relativa al componente ed esaminare le sezioni Technotes e Flashes.

Novità di questo rilascio

Novità nel rilascio 6.0

WebSphere Partner Gateway (noto come WebSphere Business Integration Connect nei rilasci precedenti) presenta le seguenti nuove funzioni:

- La capacità di eseguire lo sbustamento delle transazioni EDI e convalidarle e trasformarle in quelle buste
- La capacità di imbustare le singole transazioni EDI prima che siano recapitate.
- La capacità di ricevere più ROD (record-oriented-data) e documenti XML o interscambi EDI in un solo file e separarli in singoli documenti o in interscambi
- La capacità di trasformare qualsiasi combinazione di documenti ROD, XML e EDI
- L'introduzione di un nuovo script FTP di trasporto che può essere utilizzato su entrambe le destinazioni e sui gateway per comunicare con le VAN (value added networks), nonché con altri server FTP
- La capacità di supportare più di un certificato per certe funzioni, in modo che, se il certificato principale dovesse scadere, può essere utilizzato quello secondario
- La capacità di inviare documenti da un gateway HTTP o HTTPS mediante un server proxy ai partecipanti

WebSphere Partner Gateway versione 6.0 non supporta l'algoritmo RC5.

Novità in questo rilascio 4.2.2

La versione 4.2.2 è il primo rilascio della *Guida alla configurazione hub* .

Capitolo 1. Introduzione

Dopo aver installato WebSphere Partner Gateway e prima dello scambio di qualsiasi tipo di documento tra il Gestore comunità e i partecipanti, è necessario configurare il server WebSphere Partner Gateway (l'hub).

In questo capitolo, vengono descritti i seguenti argomenti:

- "Panoramica"
- "Informazioni necessarie per l'impostazione dell'hub" a pagina 2
- "Panoramica sull'elaborazione del documento" a pagina 7
- "Configurazione dei componenti di elaborazione del documento con i gestori" a pagina 9
- "Panoramica della configurazione dell'hub" a pagina 15

Panoramica

L'obiettivo è abilitare il Gestore comunità all'invio di un documento o di una serie di documenti (elettronicamente) a un partecipante o alla ricezione di un documento o di una serie di documenti da parte di un partecipante. L'hub gestisce la ricezione dei documenti, la trasformazione 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 scambiati tra l'hub e i partecipanti sono, di solito, in formato standard e rappresentano un'interazione aziendale specifica. Ad esempio, al partecipante potrebbe essere inviata una richiesta di ordine di acquisto come documento RosettaNet 3A4 PIP, cXML OrderRequest o un interscambio EDI-X12 con una transazione 850. L'hub trasforma il documento in un formato che può essere utilizzato da un'applicazione sul Gestore comunità. In modo simile, un'applicazione back-end del Gestore comunità potrebbe inviare una risposta ad un ordine di acquisto in un formato personalizzato trasformato in un formato standard. Il documento trasformato viene, quindi, inviato al partecipante.

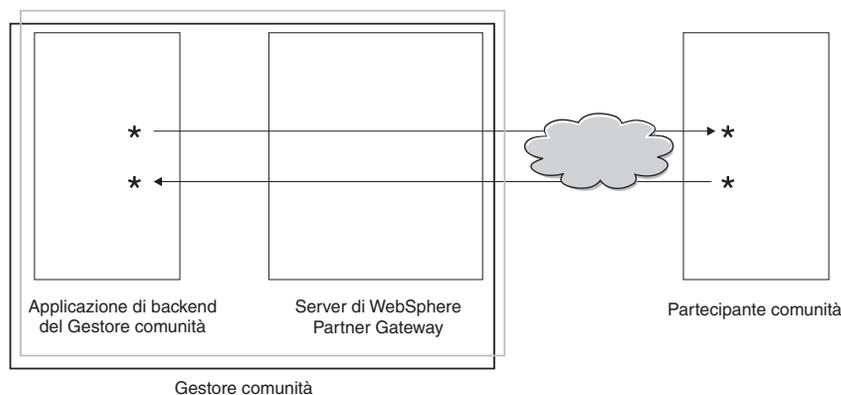


Figura 1. Flusso dei documenti nell'hub

In questo documento, viene illustrato in che modo configurare l'hub e quindi i partecipanti. È inoltre possibile imparare a configurare la protezione per l'hub.

Si noti in Figura 1 a pagina 1 che il server WebSphere Partner Gateway e l'applicazione back-end del Gestore comunità siano tutti di proprietà del Gestore comunità. Il Gestore comunità corrisponde alla società che possiede l'hub, ma corrisponde anche ad un partecipante dell'hub. Come descritto nei capitoli successivi, si definisce un profilo nel Gestore comunità come per i partecipanti.

Nota: In questo documento, viene mostrato come creare le connessioni che fluiscono dall'applicazione back-end del Gestore comunità ad un gateway del partecipante e da un partecipante al gateway del Gestore comunità. Dopo che il documento arriva sul gateway del Gestore comunità, si desidererà forse integrarlo con un'applicazione back-end, come ad esempio WebSphere InterChange Server o WebSphere MQ Broker. Le attività richieste per l'integrazione tra WebSphere Partner Gateway e le applicazioni di back-end sono definite nella Guida *Enterprise Integration*.

Informazioni necessarie per l'impostazione dell'hub

È necessario disporre di alcune informazioni sui tipi di scambi dei quali il Gestore comunità partecipa per impostare l'hub. Ad esempio, sono necessarie le seguenti informazioni:

- Quali tipi di documenti (ad esempio, EDI-X12 o XML personalizzato) il Gestore comunità e i suoi partecipanti inviano mediante hub?
- Quali tipi di trasporti (ad esempio, HTTP o FTP) il Gestore comunità e i suoi partecipanti utilizzano 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 trasformati prima di essere recapitati?
- I documenti vengono convalidati prima di essere recapitati?
- 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.

Dopo aver definito l'hub, è possibile definire i partecipanti, utilizzando informazioni (come l'indirizzo IP e i numeri DUNS) fornite dai partecipanti. Come descritto in precedenza, si definisce anche il Gestore comunità come un tipo speciale di partecipante dell'hub.

Panoramica dei trasporti

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

Nota: Quando viene utilizzato il trasporto della directory di file tra un partecipante e l'hub, è necessario che l'amministratore verifichi tutte le problematiche relative alla protezione.

In modo simile, 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 e directory di file.

Figura 2 illustra i vari trasporti che possono essere utilizzati.

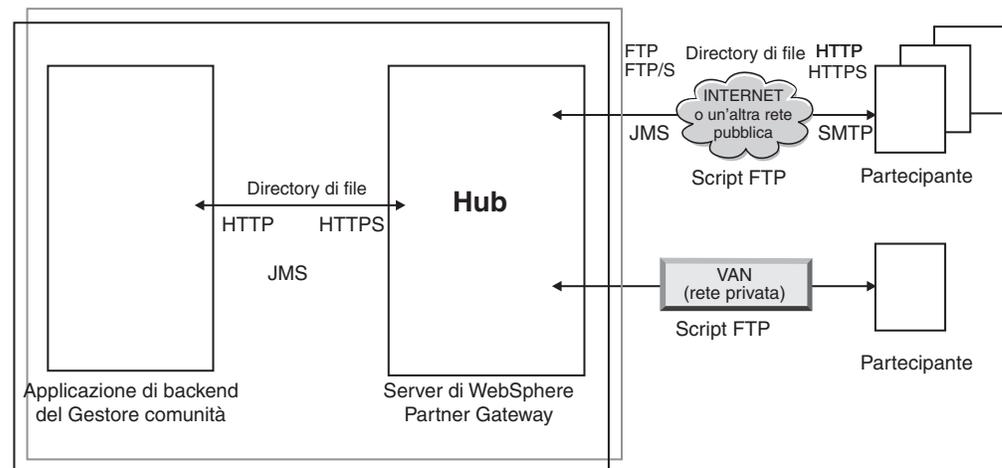


Figura 2. I trasporti supportati da WebSphere Partner Gateway

Il tipo di trasporto utilizzato per inviare e ricevere documenti riguarda l'impostazione di destinazioni e gateway. Una destinazione è un punto d'entrata nell'hub, un luogo dove i documenti inviati dai partecipanti o da applicazioni back-end vengono ricevuti sull'hub. Un gateway è un punto d'entrata nel computer del partecipante o nel sistema back-end, luogo dove 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 2, "Preparazione alla configurazione dell'hub", a pagina 17.

Panoramica delle definizioni del flusso di documenti

Quando si configura l'interscambio di documenti tra i partecipanti e il Gestore comunità, vengono specificati molti elementi sul documento:

- L'impacchettamento del documento
- Il protocollo aziendale che definisce il documento
- Il tipo di flusso del documento

L'impacchettamento, il protocollo e il flusso di un documento costituiscono la *definizione di flusso di documenti*. La definizione del flusso di documenti fornisce informazioni sull'hub relative all'elaborazione del documento. Ad esempio, si supponga di utilizzare la definizione di flusso dei documenti fornita dal sistema di:

- Impacchettamento: AS
- Protocollo: EDI-X12
- Flusso di documenti: ISA

L'hub estrae le informazioni sull'intestazione AS (e le utilizza per stabilire l'origine e la destinazione del documento). Sa dove trovare, nel documento, certe informazioni, in base a dove sono posizionate nel documento stesso. Le tre parti della definizione di flusso di documenti hanno attributi ad esse assegnati. È possibile modificare o aggiungerli a quelli definiti dal sistema.

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 partecipante invia un PIP RosettaNet al Gestore comunità, il PIP viene impacchettato come RNIF.

Figura 3 illustra i tipi di impacchettamento che possono essere impostati per i documenti scambiati tra l'hub e un partecipante della comunità e tra l'hub e un'applicazione di backend.

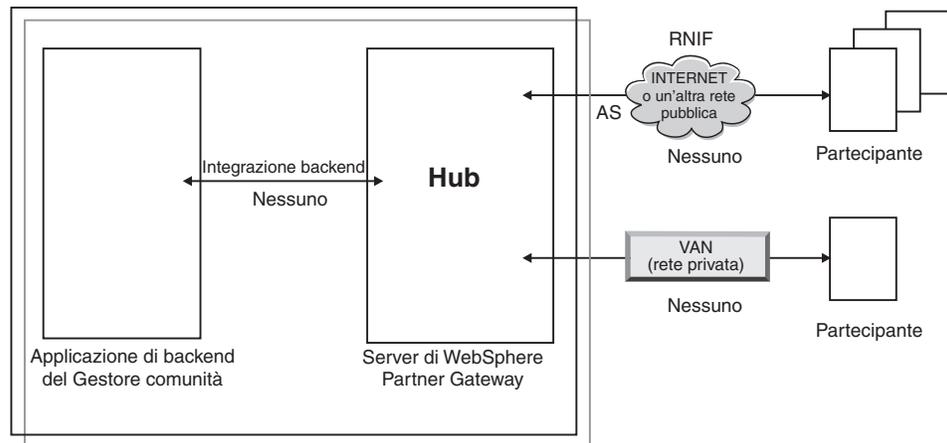


Figura 3. Tipi di impacchettamento del documento

I pacchetti sono associati a protocolli specifici. Ad esempio, un partecipante deve specificare l'impacchettamento RNIF quando invia RosettaNet all'hub.

Integrazione backend: Come descritto in Figura 3, l'integrazione backend è disponibile solo tra l'hub e l'applicazione 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 un impacchettamento di integrazione backend all'hub, è necessario aggiungere informazioni sull'intestazione. Il pacchetto di integrazione di backend e i requisiti per le informazioni di intestazione vengono descritti nella guida *Enterprise Integration*.

AS: Il pacchetto AS è disponibile solo tra partecipanti e hub. Il pacchetto AS può essere utilizzato per i documenti che aderiscono agli standard AS1 o AS2. 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. I documenti inviati da un partecipante con impacchettamento AS hanno sia informazioni sull'intestazione AS1 che sull'intestazione AS2. I documenti inviati ad un partecipante che prevede intestazioni AS1 o AS2 devono essere impacchettati (sull'hub) come AS.

Nessuno: Il pacchetto Nessuno può essere utilizzato per inviare e ricevere documenti tra l'hub e i partecipanti e tra l'hub e un'applicazione back-end. Non viene aggiunta alcuna informazione sull'intestazione (o prevista) quando un documento viene impacchettato come Nessuno.

RNIF: Il pacchetto RNIF viene fornito sul supporto di installazione. Si carica il pacchetto RNIF (insieme ai PIP che si desidera scambiare), come descritto in "Documenti RosettaNet" a pagina 60. Il pacchetto RNIF viene utilizzato per inviare documenti RosettaNet dal partecipante all'hub o dall'hub al partecipante.

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

Per la maggior parte delle trasmissioni monodirezionali tra il partecipante e il Gestore comunità (o viceversa), WebSphere Partner Gateway riceve un documento da un partecipante e lo invia al Gestore comunità. In WebSphere Partner Gateway, quando si crea una connessione del partecipante, specificare l'impacchettamento in cui WebSphere Partner Gateway riceverà il documento e l'impacchettamento che WebSphere Partner Gateway utilizzerà per inviare il documento. In Figura 4, un documento impacchettato come AS fluisce da un partecipante al back-end del Gestore comunità. Il documento viene recapitato al gateway del Gestore comunità senza intestazioni di trasposto. In Figura 4, un'azione è associata allo scambio di documenti.

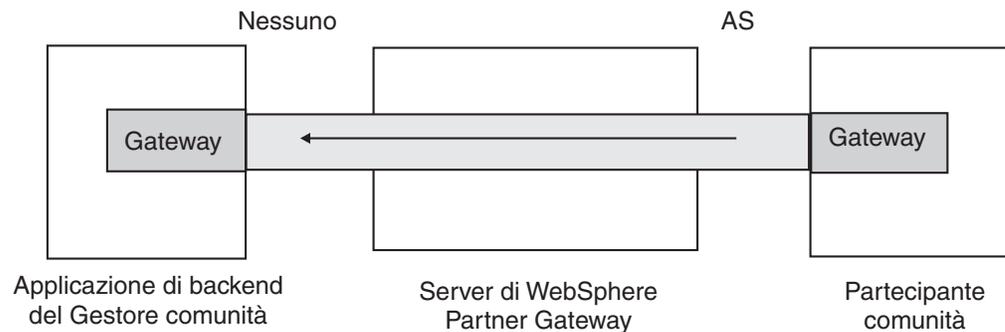


Figura 4. connessione monodirezionale tipica

Tuttavia, alcuni protocolli richiedono più attività, (come ad esempio lo sbustamento e la trasformazione) alcune delle quali si verificano come parti dello scambio globale. Se, ad esempio, un partecipante invia uno scambio EDI all'hub, per l'eventuale consegna al Gestore comunità, lo scambio viene sbustato e le singole transazioni EDI elaborate. Lo scambio EDI originale ha un pacchetto associato quando viene inviato dal partecipante. Tuttavia, poiché lo scambio non viene consegnato al Gestore comunità (viene sbustato nell'hub e non si verifica alcuna elaborazione dello scambio), non viene applicato l'impacchettamento dello scambio. Quando si configura l'interazione per lo sbustamento, di conseguenza, si immette un pacchetto sul lato dell'invio ma si specifica N/D per il lato della ricezione.

Il processo di configurazione delle definizioni di flusso di documenti richiesto per uno scambio EDI viene descritto in Capitolo 8, "Configurazione dei flussi di documenti EDI", a pagina 83.

Protocolli

I protocolli forniti con il sistema sono:

- Binary

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

- EDI-X12, EDI-Consent, EDI-EDIFACT

Questi protocolli EDI possono essere utilizzati con pacchetti AS o Nessuno. Come descritto in “N/D” a pagina 5, se la transazione EDI o l’interscambio che nasce dall’hub o termina all’hub, specificare N/D per il pacchetto. X12 e EDIFACT sono standard EDI utilizzati per lo scambio dei dati. EDI-Consent si riferisce a tipi di contenuto diversi da X12 o EDIFACT.

- servizio Web
Le richieste del servizio Web possono essere utilizzate solo con il pacchetto Nessuno.
- cXML
I documenti cXML possono essere utilizzati solo con il pacchetto Nessuno.
- XMLEvent
XMLEvent è un protocollo speciale utilizzato per fornire la notifica dell’evento per i documenti che fluiscono a e dall’applicazione back-end. Può essere utilizzato solo con il pacchetto Integrazione backend. Questo protocollo è descritto nella Guida *Enterprise Integration*.

Quando si caricano pacchetti RNIF, si ottengono anche i protocolli associati (RosettaNet e RNSC). RosettaNet (protocollo utilizzato tra il partecipante e l’hub) è associato al pacchetto RNIF. RNSC (protocollo utilizzato tra l’hub e l’applicazione back-end del Gestore comunità) è associato al pacchetto Integrazione Backend.

Per le transazioni EDI o i documenti XML o ROD che verranno trasformati, si importa una mappa di trasformazione dal client Data Interchange Services. Nel client Data Interchange Services, i dizionari sono definiti per il protocollo associato a questa trasformazione. Un dizionario contiene informazioni su tutte le definizioni dei documenti EDI, i segmenti, gli elementi dei dati composti e gli elementi di dati che costituiscono uno standard EDI. Per informazioni dettagliate su un determinato standard EDI, fare riferimento ai manuali degli standard EDI appropriati. Per informazioni sul client Data Interchange Services, fare riferimento alla *Guida alla mappatura* o alla guida in linea fornita con il client Data Interchange Services.

Nota: Gli ID mittente e destinatario devono essere parte della definizione di documento ROD associata alla mappa di trasformazione. Le informazioni necessarie per stabilire il tipo di documento e 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 trasformazione.

E’ 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 XLM, come descritto in “Documenti XML personalizzati” a pagina 78.

Flusso di documenti

Il documento può avere vari formati. Di seguito sono riportati i flussi di documenti forniti dal sistema e protocolli associati:

- Binario, che può essere utilizzato con il protocollo binario.
- ISA, che rappresenta l’interscambio 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 inoltre possibile creare propri flussi di documenti, come descritto in "Documenti XML personalizzati" a pagina 78.

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.

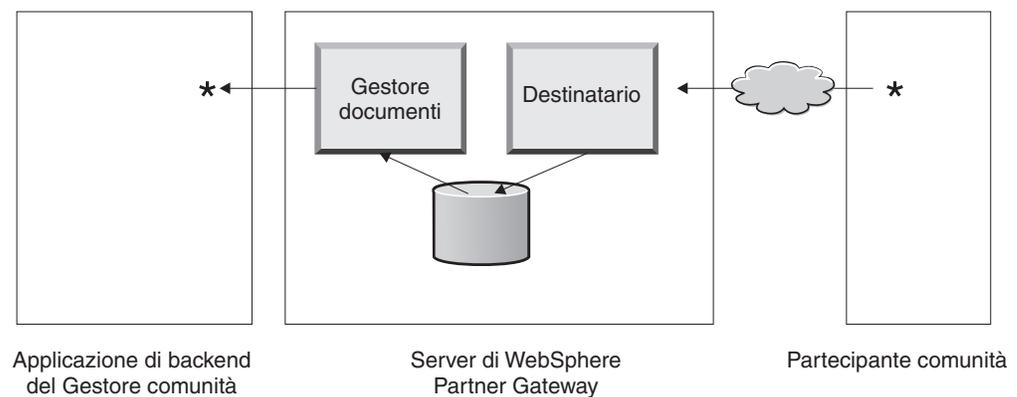


Figura 5. I componenti del Destinatarario e del Gestore documenti

Figura 5 è un esempio del modo in cui un documento viene inviato da un partecipante, ricevuto ed elaborato dall'hub e inviato all'applicazione di backend del Gestore comunità.

Nota: A scopo illustrativo, le figure in questo documento mostrano un Destinatarario 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 tipologie utilizzabile per configurare, consultare il manuale *Guida all'installazione*.

Un documento viene ricevuto in WebSphere Partner Gateway dal componente Destinatarario. Il Destinatarario è responsabile del monitoraggio dei trasporti per i

documenti in entrata, il recupero dei documenti che arrivano, l'esecuzione di alcune elaborazioni di base e le relative code, in modo che il Gestore documenti possa richiamarli.

I Destinatari sono specifici del trasporto. Le istanze dei destinatari specifici del trasporto sono note come *destinazioni*. Si imposta una destinazione per ogni tipo di trasporto che l'hub supporta. Ad esempio, se i partecipanti inviano i documenti su HTTP, si imposta una destinazione HTTP per riceverli.

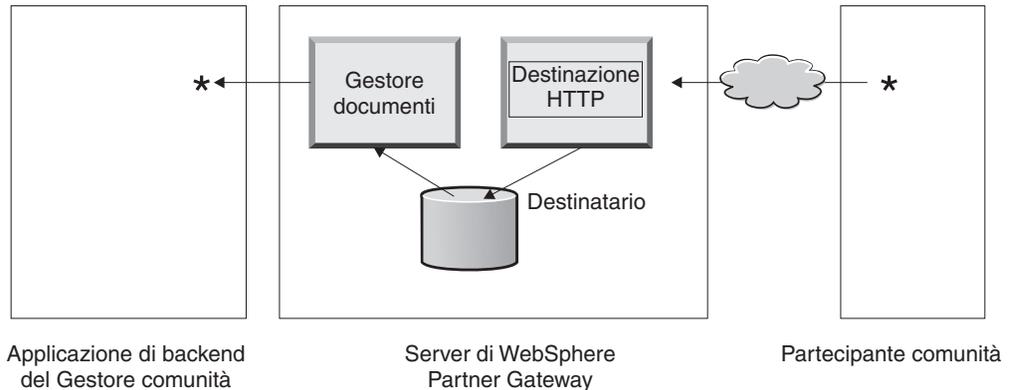


Figura 6. Una destinazione HTTP

Se l'applicazione back-end del Gestore comunità invia i documenti su JMS, si imposta una destinazione JMS per riceverli.

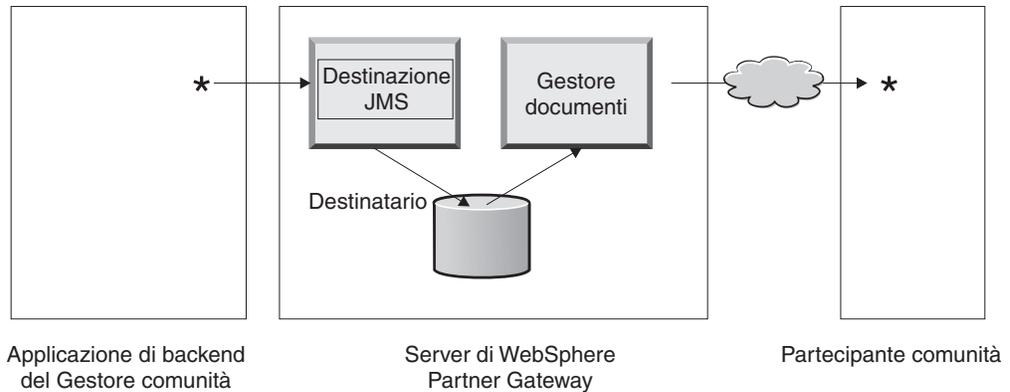


Figura 7. Una destinazione JMS

Come descritto in "Panoramica dei trasporti" a pagina 2, WebSphere Partner Gateway supporta una varietà di trasporti, ma è possibile caricare anche i trasporti definiti dall'utente per definire una destinazione normale (come descritto in "Impostazione di una destinazione per un trasporto definito dall'utente" a pagina 43).

Il Destinatario invia il documento ad un sistema di file condiviso. Per più documenti contenuti in un singolo file (ad esempio, documenti XML o ROD o scambi EDI inviati insieme), la destinazione divide i documenti o gli interscambi prima di inviarli al file system condiviso. Il componente del Gestore documenti recupera il documento dal sistema di file e determina le informazioni di instradamento e le eventuali trasformazioni necessarie.

Ad esempio, il Gestore comunità può inviare un documento EDI-X12 senza alcun impacchettamento all'hub per il recapito ad un partecipante che attende il documento EDI-X12 con impacchettamento AS2. Il partecipante fornisce l'URL HTTP in cui dovrebbe essere recapitato il documento impacchettato come AS2 e il Gestore documenti lo impacchetta come previsto dal partecipante. Il gestore documenti utilizza la configurazione del gateway per quel partecipante (che deve essere stato configurato per l'URL HTTP in cui il partecipante prevede di ricevere i documenti AS2) per inviare il documento al partecipante.

Configurazione dei componenti di elaborazione del documento con i gestori

In questa sezione, vengono descritti più dettagliatamente i componenti di WebSphere Partner Gateway e mostrati i vari punti in cui è possibile (o necessario) cambiare il funzionamento fornito dal sistema dei componenti per l'elaborazione di un documento aziendale.

Si utilizza *gestori* per modificare il comportamento delle destinazioni fornite dal sistema delle destinazioni, procedure del flusso di lavoro fisse e azioni. Ci sono due tipi di gestori, quelli forniti da WebSphere Partner Gateway e quelli che sono definiti dall'utente. Vedere la *Guida del programmatore* se si desiderano informazioni sulla creazione dei gestori.

Una volta creato un gestore, viene caricato per renderlo disponibile. Si caricano solo i gestori definiti dall'utente. I gestori forniti da WebSphere Partner Gateway sono già disponibili.

Le sezioni che seguono descrivono i punti di elaborazione nei quali è possibile specificare i gestori.

Destinazioni

Le destinazioni presentano tre *punti di configurazione* per i quali è possibile specificare i gestori--Preprocesso, SyncCheck e Postprocesso.

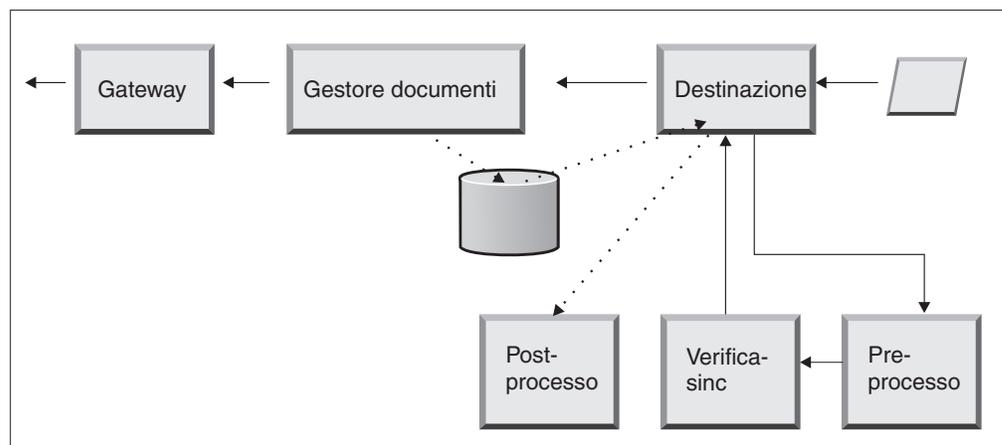


Figura 8. Punti di configurazioni di destinazione

L'elaborazione ha luogo nel seguente ordine:

1. Il Destinatario riceve i passaggi Preprocesso e SyncCheck, dopo aver ricevuto il documento.

- Viene quindi chiamato il Gestore documenti per elaborare il documento.
- In caso di flussi sincroni, il Gestore documenti fornisce una risposta sinc. Il destinatario chiama quindi il Postprocesso con la risposta restituita dal Gestore documenti.

I passaggi vengono descritti nelle seguenti sezioni:

- Preprocesso

Il preprocesso viene generalmente utilizzato per eventuali elaborazioni sul documento che devono essere effettuate prima che il documento venga elaborato dal Gestore documenti. Ad esempio, se si ricevono più documenti ROD in un singolo file, configurare il gestore splitter ROD quando si definisce la destinazione. Lo splitter ROD, insieme ai due splitter forniti dal sistema, sono disponibili per essere utilizzati quando si configura una destinazione. Se si creano gestori aggiuntivi per il preprocesso, anche questi gestori diventano disponibili.

Per informazioni sulla configurazione del punto di configurazione del preprocesso, consultare "Preprocesso" a pagina 44.

- SyncCheck

SyncCheck viene utilizzato per determinare se WebSphere Partner Gateway deve elaborare il documento in modo sincronico o asincrono. Ad esempio, in caso di documenti AS2 ricevuti su HTTP, determina se un MDN (message disposition notification) deve essere restituito in modo sincronico sulla stessa connessione HTTP. WebSphere Partner Gateway fornisce una varietà di gestori per la verifica sincrona. L'elenco di gestori varia a seconda del trasporto associato alla destinazione.

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

Nota: Per documenti AS2, cXML, RNIF o SOAP che verranno utilizzati in scambi sincroni, specificare il gestore SyncCheck sulla destinazione HTTP o HTTPS.

Per informazioni sulla configurazione del punto di configurazione SyncCheck, fare riferimento a "SyncCheck" a pagina 47.

- Postprocesso

Il postprocesso viene utilizzato per l'elaborazione del documento di risposta che viene inviato dall'hub come risultato di una transazione sincrona.

Per informazioni sulla configurazione del punto di configurazione del Postprocesso, fare riferimento a "Postprocesso" a pagina 48.

Gestore documenti

I documenti ricevuti dalle destinazioni vengono raccolti dal Gestore documenti dal file system comune per ulteriore elaborazione. Il Gestore documenti utilizza connessioni del partecipante per instradare i documenti. Tutti i documenti che passano mediante 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 di un flusso di lavoro in entrata, viene determinata la connessione del partecipante. La connessione del partecipante specifica l'azione da eseguire su questo documento. Una volta eseguito il flusso di lavoro della variabile, il Gestore documenti esegue il flusso di lavoro in uscita fisso su questo documento.

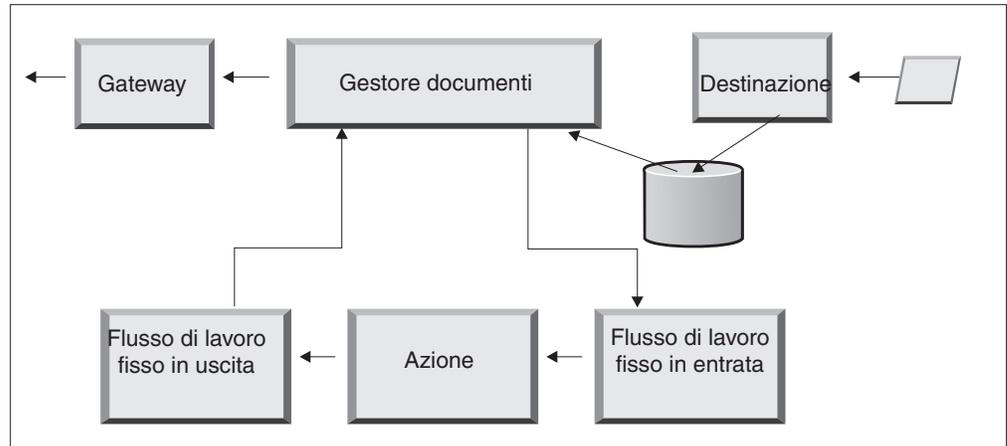


Figura 9. Flussi di lavoro fissi e azioni

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 sbustare l'insieme di singole transazioni. Ciascuna di queste transazioni viene quindi reintrodotta ed elaborata in un flusso configurato.

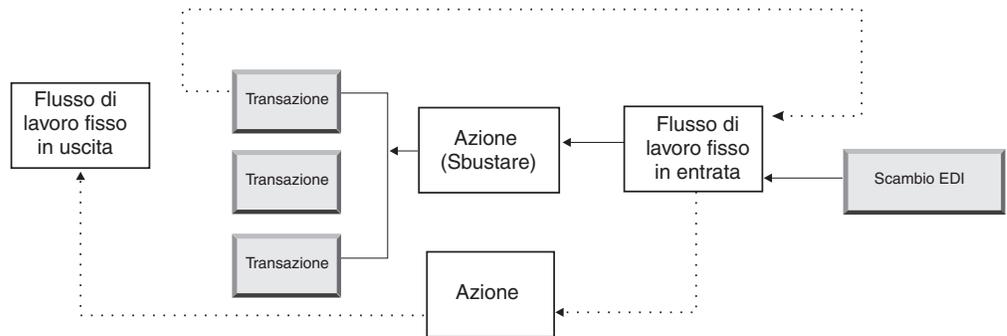


Figura 10. Flussi di lavoro fissi ed azioni per uno scambio EDI

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 gestori personalizzati per l'elaborazione di questi passaggi: lo spaccettamento del protocollo e l'elaborazione del protocollo. L'ultimo passaggio di un flusso di lavoro in entrata esegue la ricerca della connessione del partecipante, che stabilisce il flusso di lavoro variabile che viene eseguito per questo documento aziendale.

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.

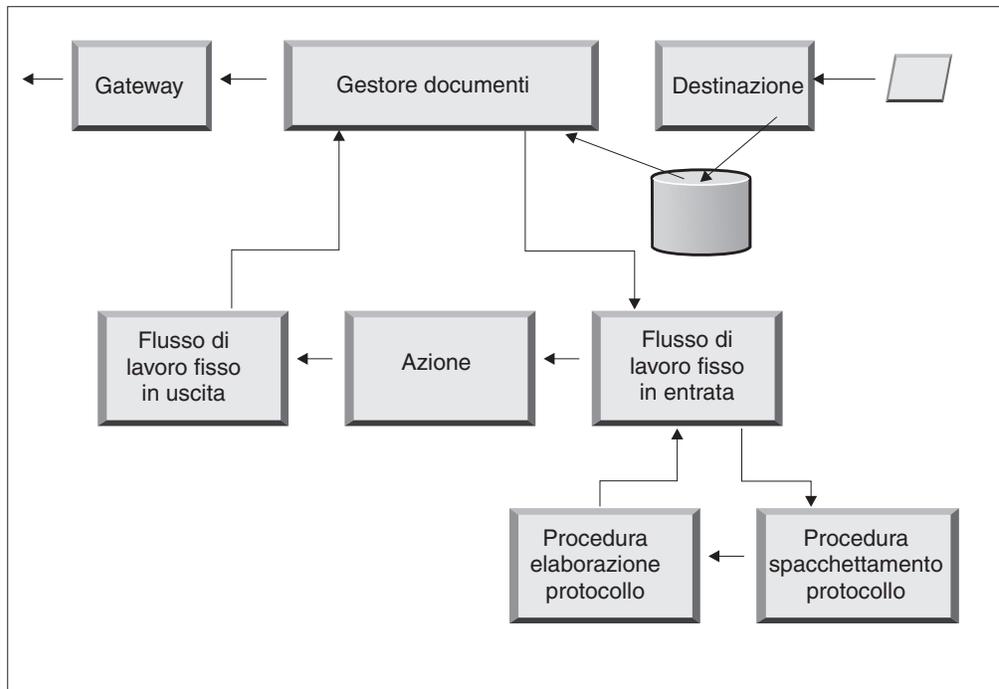


Figura 11. Procedure del flusso di lavoro fisso in entrata

Spaccettamento del protocollo: Durante lo spaccettamento del protocollo, un documento viene spaccettato 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 i gestori per l'impacchettamento RNIF, AS, Integrazione backend e Nessuno. Se sono necessari gestori per altri tipi di pacchetto, possono essere sviluppati come user exit. Per informazioni sulla scrittura delle uscite utente, fare riferimento al manuale *Guida per il programmatore*.

Non è possibile modificare la procedura di impacchettamento del protocollo, tuttavia è possibile aggiungere una logica aziendale al passo aggiungendo i gestori.

Per informazioni sulla configurazione di questo passo, consultare "Configurazione dei flussi di lavoro fissi" a pagina 50.

Passo di elaborazione del protocollo: L'elaborazione del protocollo coinvolge le informazioni specifiche del protocollo, che potrebbero includere l'analisi del messaggio per stabilire le informazioni di instradamento (come ad esempio l'ID mittente e l'ID destinatario), le informazioni sul protocollo e le informazioni sul flusso di documenti. WebSphere Partner Gateway fornisce l'elaborazione di una varietà di protocolli, come descritto in "Gestori per l'elaborazione del protocollo" a pagina 51. L'elaborazione di altri protocolli—ad esempio, CSV (valore separato da virgola)—può essere fornita con un user exit.

Non è possibile modificare l'elaborazione del protocollo; tuttavia, è possibile aggiungere una logica aziendale aggiungendo i gestori.

Per informazioni sulla configurazione di questo passo, consultare "Configurazione dei flussi di lavoro fissi" a pagina 50.

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

Azioni

La procedura 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 trasformazione del documento nel formato richiesto dal destinatario.

Se il documento non ha procedure specifiche necessarie, può utilizzare l'azione di Passaggio autorizzato fornita dal sistema, il che non effettua modifiche al documento.

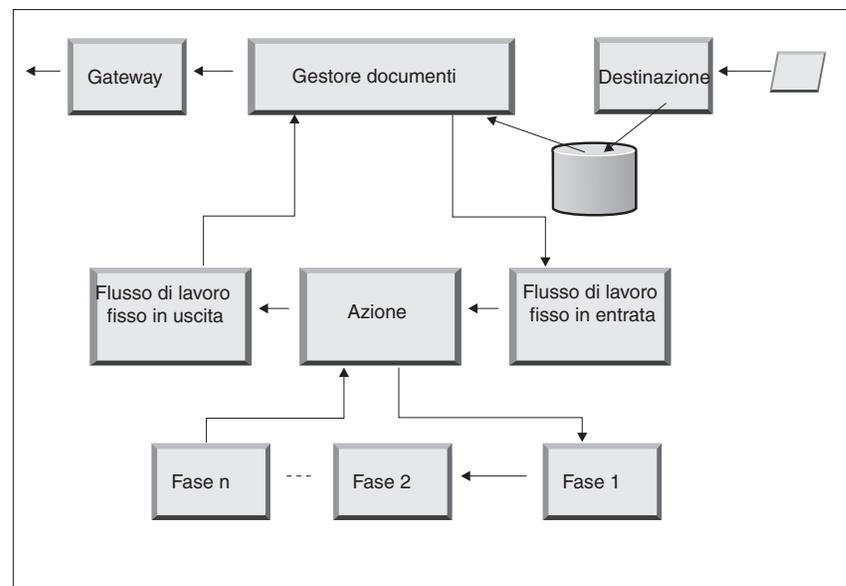


Figura 12. Procedure Azione

Non è possibile modificare un'azione fornita dal sistema. Si può tuttavia creare un'azione (ed aggiungere gestori all'elenco Configurati) o copiare un'azione fornita dal sistema e modificare l'elenco dei gestori.

Per informazioni sulla creazione o la copia di un'azione fornita dal sistema o la configurazione di un'azione definita dall'utente, fare riferimento a "Configurazione azioni" a pagina 51.

Flusso di lavoro fisso in uscita

Il Flusso di lavoro fisso in uscita è formato da una procedura —lo spaccettamento del documento con le informazioni del protocollo. Ad esempio, se un documento è stato impostato per essere ricevuto da un'applicazione back-end mediante il pacchetto Integrazione backend, determinate informazioni di intestazione vengono aggiunte al documento prima di passare nel gateway.

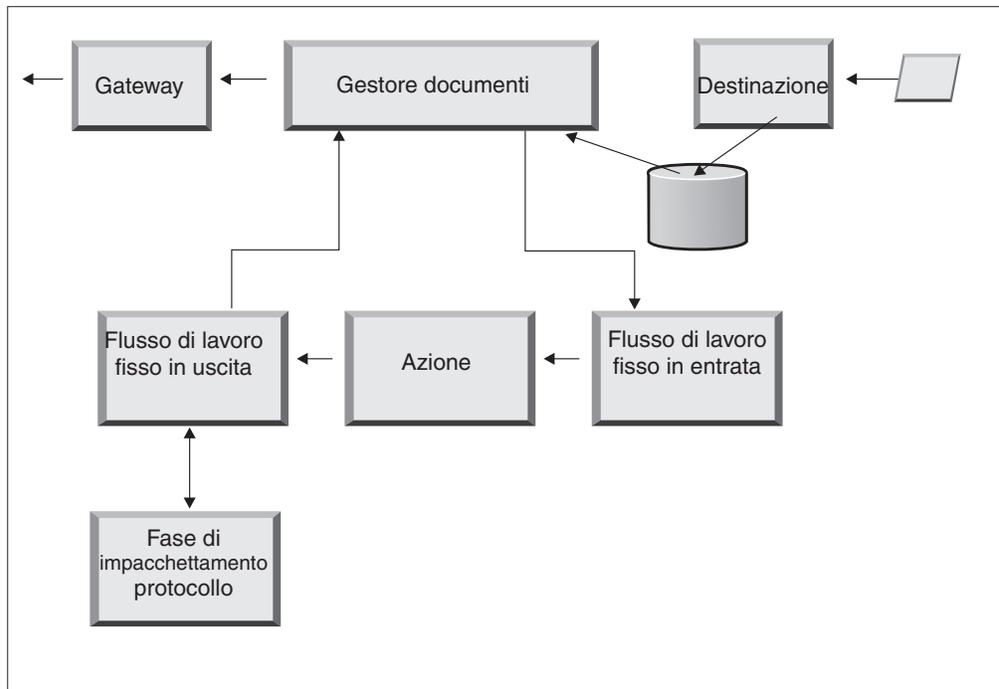


Figura 13. Procedure del flusso di lavoro fisso in uscita

WebSphere Partner Gateway fornisce gestori per una varietà di pacchetti e protocolli, come descritto in “Flusso di lavoro in uscita” a pagina 51. Se sono necessari gestori per altri tipi di pacchetto, possono essere sviluppati come user exit. 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 aziendale

Non è possibile modificare la procedura di Impacchettamento del protocollo, tuttavia è possibile aggiungere una logica aziendale alla procedura aggiungendo i gestori.

Per informazioni sulla configurazione di questa procedura del flusso di lavoro, fare riferimento a “Configurazione dei flussi di lavoro fissi” a pagina 50.

Gateway

Dopo che il documento abbandona il Gestore documenti, viene inviato dal gateway al destinatario previsto. Il gateway dispone di due punti di configurazione —Preprocesso e Postprocesso.

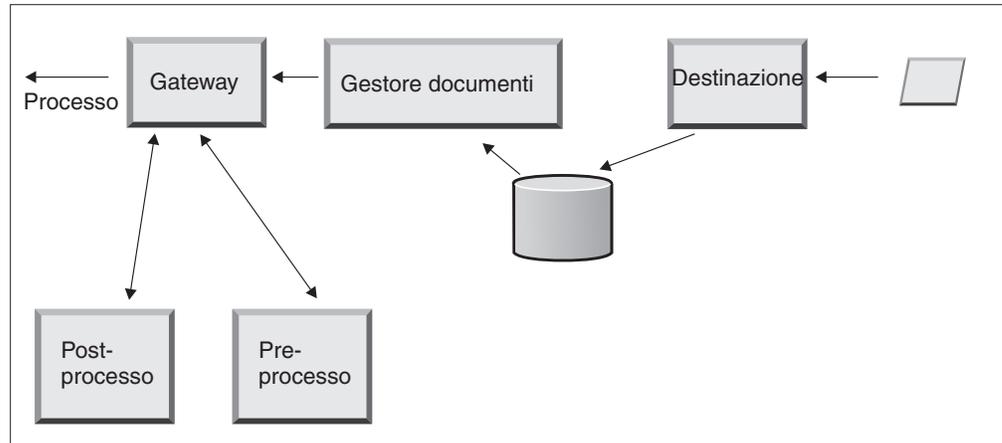


Figura 14. Punti di configurazione gateway

- Preprocesso
Il preprocesso compromette l'elaborazione di un documento prima di essere inviato al destinatario. Il processo è l'effettivo invio del documento. Non viene fornito alcun gestore dal sistema per configurare il passaggio di preprocesso; tuttavia, è possibile caricare un gestore definito dall'utente.
- Postprocesso
Il postprocesso agisce sui risultati della trasmissione del documento (ad esempio, sulla risposta che riceve dal destinatario durante una trasmissione sincrona). Non viene fornito alcun gestore dal sistema per configurare il passaggio di postprocesso; tuttavia, è possibile caricare un gestore definito dall'utente.

Per informazioni sulla configurazione delle procedure di Preprocesso e Postprocesso, fare riferimento a "Configurazione dei gestori" a pagina 142.

Panoramica della configurazione dell'hub

Dopo aver analizzato le necessità aziendali, come descritto in "Informazioni necessarie per l'impostazione dell'hub" a pagina 2, si configura l'hub e si creano i profili del partecipante. In questa sezione, viene fornita una panoramica di livello superiore delle attività coinvolte.

Nota: Una volta configurato l'hub, fare riferimento al manuale *Guida per l'amministratore* Per informazioni su i codici degli eventi e sui suggerimenti per la risoluzione dei problemi.

Configurazione dell'hub

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 2, "Preparazione alla configurazione dell'hub", a pagina 17.
2. Facoltativamente, personalizzare la console e modificare la password predefinita ed i criteri delle autorizzazioni. Queste attività vengono descritte in Capitolo 4, "Configurazione di Console comunità", a pagina 27.
3. Creare destinazioni per i tipi di trasporto che verranno utilizzati per ricevere i documenti sull'hub (dal Gestore comunità e dai partecipanti). La creazione delle destinazioni viene descritta in Capitolo 5, "Definizione delle destinazioni", a pagina 31.

Nota: Se si configura la destinazione con gestori definiti dall'utente, caricare i gestori prima di creare la destinazione. Il caricamento dei gestori viene descritto in "Caricamento dei gestori definiti dall'utente" a pagina 32.

4. Configurare i passaggi o le azioni del flusso di lavoro in entrata. Si tratta di un passaggio *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 funzionamento fornito dal sistema o i flussi di lavoro o le azioni, ignorare questo passo. La configurazione dei passaggi e delle azioni del flusso di lavoro viene descritta in Capitolo 6, "Configurazione delle procedure e delle azioni del flusso di lavoro fisso", a pagina 49.

Nota: Caricare i gestori definiti dall'utente prima di configurare flussi di lavoro ed azioni. Il caricamento dei gestori definiti dall'utente viene descritto in "Caricamento dei gestori" a pagina 49.

5. Creare le definizioni del flusso di documenti (o verificare che quelli di cui si ha necessità siano già disponibili) per definire i tipi di documenti che è possibile inviare e ricevere sull'hub.
6. Creare le interazioni per indicare la combinazione valida di due definizioni di flusso di documenti.

La creazione di definizioni di flusso di documenti e la creazione di interazioni vengono descritte in Capitolo 7, "Configurazione dei flussi di documenti", a pagina 55 e in Capitolo 8, "Configurazione dei flussi di documenti EDI", a pagina 83.

7. Creare un profilo per Gestore comunità, fornendo le informazioni sul Gestore comunità e stabilendo i tipi di documenti che il Gestore comunità può inviare e ricevere (le funzioni B2B del Gestore comunità). La creazione del profilo viene descritta in Capitolo 9, "Creazione del profilo Gestore comunità e delle funzioni B2B", a pagina 123.

Creazione partecipanti

Dopo aver configurato l'hub, si crea un profilo per ciascun partecipante che scambierà documenti con il Gestore comunità. Solo l'Ammin hub può creare partecipanti.

Come Ammin hub, è possibile impostare le funzioni B2B dei partecipanti, stabilirne i gateway e configurarne i profili di protezione. Questi passaggi possono essere eseguiti alternativamente dai partecipanti stessi.

La creazione dei partecipanti viene descritta in Capitolo 11, "Creazione dei partecipanti e delle funzioni B2B", a pagina 145. La creazione dei gateway viene descritta in Capitolo 10, "Creazione gateway", a pagina 127. La configurazione dei profili viene descritta in Capitolo 13, "Impostazione di sicurezza per gli scambi in arrivo e in uscita", a pagina 153.

Come stabilire le connessioni del documento

Dopo aver configurato l'hub e creato i profili del partecipante, si è pronti per 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 in Capitolo 12, "Gestione delle connessioni", a pagina 149.

Capitolo 2. Preparazione alla configurazione dell'hub

Nei successivi ultimi capitoli, si impostano le destinazioni e i gateway descritti in Capitolo 1, "Introduzione". A seconda dei tipi di trasporto che si utilizzano per ricevere i documenti nelle destinazioni e per inviarli dai gateway, è necessario fare un lavoro di impostazione.

In questo capitolo, vengono descritti i seguenti argomenti:

- "Creazione di una directory per un gateway della directory del file"
- "Configurazione del server FTP per la ricezione dei documenti"
- "Configurazione dell'hub per il protocollo di trasporto JMS" a pagina 21

Viene fornita anche una breve panoramica degli script FTP necessari per le destinazioni e i gateway dello script FTP e viene descritto il client Data Interchange Services, che può essere utilizzato per creare trasformazione, convalida e mappe di riconoscimento funzionale per documenti EDI, XML e ROD (record-oriented-data).

- "Utilizzo di script FTP per le destinazioni e i gateway dello script FTP" a pagina 23
- "Utilizzo di mappe dal client Data Interchange Services" a pagina 24

Se si pensa di non dover impostare nessuno di questi tipi di destinazioni o gateway, saltare questo capitolo e passare direttamente a Capitolo 3, "Avvio del server e visualizzazione della Console comunità".

Creazione di una directory per un gateway della directory del file

Se si pensa di utilizzare un gateway della directory del file per inviare i documenti al Gestore documenti, è per prima cosa necessario creare una directory sul sistema di file utilizzato dal Gestore documenti.

Ad esempio, supporre di voler creare una directory denominata FileSystemGateway nella directory c:\temp di un'installazione Windows. Questi sono i passaggi che si desidera effettuare:

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

Configurazione del server FTP per la ricezione dei documenti

Nota: Questa sezione si applica solo alla ricezione dei documenti su FTP o FTPS dai partecipanti. L'invio di documenti ai partecipanti viene descritto in "Configurazione di un gateway FTP" a pagina 132 e "Configurazione di un gateway FTPS" a pagina 138.

Se si pensa di utilizzare FTP o FTPS come trasporto per i documenti in entrata, è necessario disporre di un server FTP installato. Se si pensa di utilizzare l'FTP e di non disporre attualmente di un server installato, procedere come segue prima di continuare. 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

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 particolare struttura di directory in modo tale che i componenti del Destinatario e del Gestore documenti possono correttamente identificare il partecipante che invia il documento in entrata. La struttura è descritta in Figura 15.

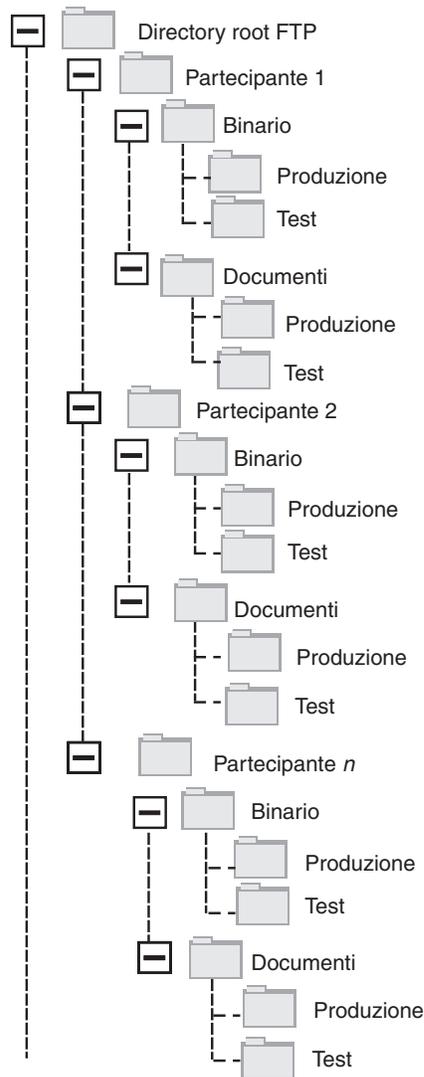


Figura 15. Struttura directory FTP

Ciascuna directory del partecipante contiene una directory Binary e una directory Documents. Entrambe le directory contengono una Directory Production e una directory Test.

La directory dei documenti viene utilizzata quando un partecipante invia un documento XML che contiene le informazioni di instradamento complete (utilizzando l'FTP) in un hub. E' necessaria la creazione di una definizione XML personalizzata.

La directory Binaria viene utilizzata quando un partecipante invia altri documenti (utilizzando l'FTP) nell'hub.

Per ogni partecipante che utilizza l'FTP per inviare e ricevere i documenti, creare le seguenti cartelle dalla directory root del server FTP:

1. Creare una cartella per il partecipante.

Nota: Il nome della cartella dovrebbe corrispondere al nome specificato per **Nome accesso società** quando si crea il partecipante. La creazione dei partecipanti viene descritta in "Creazione dei profili dei partecipanti" a pagina 145.

2. Creare le cartelle secondarie nella cartella del partecipante denominata Binary e Documents.
3. Creare le cartelle secondarie nelle cartelle Binary e Documents denominate Production e Test.

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_ParticipantID><Unique_Filename>*

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

Il nome della directory nel quale il file è stato rilevato viene utilizzato per valutare Da nome partecipante e la prima parte del nome del file viene utilizzata per valutare A nome partecipante. La posizione della directory nella struttura della directory viene utilizzata per valutare se la transazione è una transazione Production o Test.

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

- Da nome partecipante è partnerdue (perché il file è stato trovato nella parte di partnerdue dell'albero della directory).
- A nome partecipante è partneruno (perché la prima parte del nome del file è 123456789, che è l'ID DUNS per partneruno)

Nota: Qui e in tutto il manuale, i numeri DUNS sono solo esempi.

- Il tipo di transazione è Production.

Il Gestore documenti cerca una connessione del partecipante di produzione da partner2 a partner1 per:

- Pacchetto: Nessuno (N/D)

- Protocollo: Binario (1.0)
- Flusso di documenti: Binario (1.0)

Quindi, il Gestore documenti elabora il file.

File XML

Un file XML non ha alcun requisito del nome di file dato che il file viene ispezionato dal Gestore documenti e le informazioni di instradamento vengono estratte dal documento stesso.

Quando un file XML viene rilevato dal Destinatario, viene scritto nella memoria condivisa e passato nel 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 "Documenti XML personalizzati" a pagina 78.) Le informazioni A nome partecipante, Da nome partecipante e Instradamento vengono estratte dal file XML.

La posizione della directory nella struttura della directory viene utilizzata per valutare se la transazione è una transazione Production o Test.

Il Gestore documenti utilizza, quindi, queste informazioni per localizzare la connessione corretta del partecipante prima di elaborare il file.

Configurazione del server FTP aggiuntiva

Una volta creata la struttura di directory richiesta, è possibile configurare il server FTP per ciascuno dei partecipanti nella comunità di 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, Partecipanti).
2. Aggiungere un utente ad un gruppo recentemente creato per ogni partecipante che invia o riceve i documenti sull'FTP.
3. Per ogni partecipante, impostare il server FTP per mappare il partecipante in entrata nella rispettiva struttura della directory creato per il partecipante nella sezione precedente "Configurazione della struttura di directory richiesta sul server FTP" a pagina 18. 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 di protezione per le sessioni SSL vengono gestite solo dal server FTPS e dal client che il partecipante sta utilizzando. Non c'è nessuna configurazione di protezione specifica per WebSphere Partner Gateway sui documenti FTPS in entrata. WebSphere Partner Gateway recupera i documenti dalla destinazione FTP (che viene descritta in "Impostazione di una destinazione FTP" a pagina 34) dopo che il server ha negoziato correttamente i canali protetti e ha ricevuto il documento. Per determinare quali certificati sono necessari (e dove sono necessari) e configurare correttamente un canale protetto che il partecipante può contattare, fare riferimento alla documentazione del server FTPS.

Per l'autenticazione del server, fornire il certificato del Destinatario ai partecipanti. 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 supportata dal server FTPS, è necessario specificare i certificati di autenticazione

del client dei partecipanti nel server FTP. 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.

Nelle sezioni successive di questo documento, si apprenderà come configurare le destinazioni JMS o i gateway (o entrambi). Queste attività vengono descritte in "Impostazione di una destinazione JMS" a pagina 37 e in "Configurazione di un gateway JMS" a pagina 134.

Creazione di una directory per JMS

Si crea prima una directory per JMS. Ad esempio, si vorrebbe 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

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 Notepad 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". Se, ad esempio, di imposta la directory c:/temp/JMS, la riga appare in questo modo:
`PROVIDER_URL=file:/c:/temp/JMS`
6. Salvare il file.

Creazione delle 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. E' necessario immettere il nome del Gestore al posto di `<queue_manager_name>` nei seguenti passi. Si presume, inoltre, che un listener per questo gestore 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 JavaTM all'ambiente

Inserire il seguente comando per aggiungere un runtime Java nel percorso del sistema:

```
set PATH=%PATH%;<ProductDir>\_jvm\jre\bin
```

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

Definizione della configurazione JMS

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

```

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 21. 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 delle code e del canale" a pagina 21. 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.

Utilizzo di script FTP per le destinazioni e i gateway dello 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.

Si specifica questo script quando si crea la destinazione o il gateway Script FTP. WebSphere Partner Gateway sostituisce i valori reali immessi quando si crea la destinazione o il gateway per i segnaposti 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 riempita in fase di runtime.

Per informazioni sulla creazione di uno script FTP per una destinazione Script FTP, vedere "Impostazione di una destinazione Script FTP" a pagina 39. Per informazioni sulla creazione di uno script FTP per un gateway di script FTP, consultare "Configurazione di un gateway script FTP" a pagina 139.

Utilizzo di mappe dal client Data Interchange Services

Per eseguire lo sbustamento, la trasformazione e la convalida o per effettuare trasformazioni 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 trasformati e convalidati. Ad esempio, si potrebbe avere un ordine di acquisto creato da un'applicazione di back-end che si desidera trasformare ed inviare ad un partecipante della comunità come 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 trasformare 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 delle mappe" a pagina 110.

Capitolo 3. 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 inclusi i seguenti argomenti:

- “Avvio di WebSphere MQ”
- “Avvio dei componenti di WebSphere Partner Gateway”
- “Collegamento alla Console comunità” a pagina 26

Avvio di WebSphere MQ

Se non si è ancora avviato WebSphere MQ, seguire una delle seguenti procedure:

- Per i sistemi UNIX:
 1. Inserire:
`su mqm`
 2. Inserire:
`strmqm bcg.queue.manager`
 3. Inserire:
`runmqtsr -t tcp -p 9999 -m bcg.queue.manager &`
 4. Attendere 10 secondi e premere Invio per ritornare al prompt dei comandi.
 5. Inserire:
`strmqbrk -m bcg.queue.manager`
- Per i sistemi basati su Windows:
 1. Inserire:
`strmqm bcg.queue.manager`
 2. Inserire:
`runmqtsr -t tcp -p 9999 -m bcg.queue.manager`
Listener viene eseguito in questa finestra, lasciarla quindi aperta.
 3. Aprire una nuova finestra e avviare il broker JMS (il broker pubblicazione e iscrizione) con il seguente comando:
`strmqbrk -m -bcg.queue.manager`

Avvio dei componenti di WebSphere Partner Gateway

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 `\<ProductDir\bin`.
2. Digitare il seguente comando per avviare la Console:
 - Per i sistemi UNIX:
`./bcgStartServer.sh bcgconsole`
 - Per i sistemi basati su Windows:
`bcgStartServer bcgconsole`
3. Digitare il seguente comando per avviare Destinatario:
`./bcgStartServer.sh bcgreceiver`

o
bcgStartServer bcgreceiver

4. Digitare il seguente comando per avviare Gestore documenti:

./bcgStartServer.sh bcgdocmgr

o
bcgStartServer bcgdocmgr

Una volta avviati i componenti, avviare il sistema di guida. Per avviare il sistema di guida, immettere il seguente comando:

./bcgStartHelp.sh

o
bcgStartHelp.bat

Una volta avviati i componenti, collegarsi alla Console comunità, come descritto in "Collegamento alla Console comunità".

Per informazioni sull'avvio del client di Data Interchange Services, fare riferimento alla *Guida alla mappatura*.

Collegamento alla Console comunità

La Console comunità è il punto di accesso per WebSphere Partner Gateway. La maggior parte delle attività eseguite nell'impostazione dell'hub richiede l'accesso come Amministratore hub. (ammin hub), che è il superutente del sistema.

Accertarsi di conoscere l'indirizzo IP del computer sul quale il componente della Console è in esecuzione. Si inserisce questo indirizzo nel comando HTTP.

1. Da un browser, digitare il seguente URL:
http://<IP_address>:58080/console
2. Inserire le seguenti informazioni:
 - a. Come **Nome utente**, immettere hubadmin
 - b. Come **Password**, immettere Pa55word

Nota: Se si è già firmato in Console comunità e modificato la password predefinita di Pa55word, inserire la nuova password nel campo **Password**.

- c. Come **Nome accesso società**, immettere Operatore

Viene visualizzata la pagina Ricerca partecipante, che è sempre la prima visualizzata quando si accede nella Console comunità.

Si utilizza questa pagine successivamente in questo manuale per definire i partecipanti.

Se si fa clic su **Cerca** adesso, si nota che un partecipante, l'Operatore comunità, viene elencato. L'operatore comunità viene definito automaticamente da WebSphere Partner Gateway.

Nota: Se la password non è stata modificata da quella predefinita Pa55word, si richiede di fare ciò prima che viene visualizzata la pagina Ricerca partecipante.

Capitolo 4. Configurazione di Console comunità

In questo capitolo, viene descritto in che modo configurare la Console comunità in modo da specificare i partecipanti, come accedono alla console e che tipo di accesso hanno alle varie attività della console. In questo capitolo, sono contenuti i seguenti argomenti:

- “Specificazione delle informazioni locali e del marchio della console”
- “Impostazione della politica della password” a pagina 29
- “Configurazione delle autorizzazioni” a pagina 30

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

Specificazione delle informazioni locali e del marchio della console

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 locali, 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 **Ammin 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

Marchi della console

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.
- Il logo della società viene visualizzato in alto a destra della Console comunità.

Le immagini devono essere file in formato .JPG conformi a determinate specifiche, in modo da adattarsi 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**, digitare il percorso e il nome del file di immagine che si desidera utilizzare per l'intestazione/banner.
 - Fare clic su **Sfoggia** 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**, digitare il percorso e il nome del file che si desidera utilizzare per il logo aziendale.
 - Fare clic su **Sfoggia** 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 calcolo

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**, digitare il percorso e il nome del file che contiene il foglio di stile personalizzato.
 - Fare clic su **Sfoggia** per navigare nel file che contiene il foglio di stile e selezionarlo.
2. Fare clic su **Carica**.

Localizzazione dei dati sulla console

Se si ricevono i bundle di risorse o gli altri file locali 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 locale:

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

Impostazione della politica della 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 partecipante 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 partecipante 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'login utente o nel nome completo. Questo campo viene selezionato per impostazione predefinita.

Per modificare i valori predefiniti:

1. Fare clic su **Ammin 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 dei permessi agli utenti

Prima di configurare i permessi, è utile comprendere in che modo i permessi vengono concessi ai singoli. Tutti e tre i tipi di entità nella comunità hub, l'Operatore comunità, il Gestore comunità e i partecipanti hanno un utente Ammin. Quando si crea un Gestore partecipante o un Gestore comunità, si crea effettivamente un utente Ammin per quell'entità. (Nel caso dell'Operatore comunità, l'Ammin hub viene creato automaticamente, lo stesso vale per l'utente ammin per l'hub).

Quando si crea il partecipante (come definito in "Creazione dei profili dei partecipanti" a pagina 145), si fornisce il partecipante con le informazioni di accesso (come il nome e la password da utilizzare per accedere). Dopo che il partecipante ha avuto accesso, questo crea gli utenti aggiuntivi nell'organizzazione. Il partecipante crea inoltre i gruppi e assegna gli utenti a tali gruppi. Ad esempio, un'organizzazione potrebbe voler avere un gruppo per le persone che controllano il volume di documenti. Il partecipante crea un gruppo volume e aggiunge gli utenti ad esso.

Nota: Come utente Ammin hub, è inoltre possibile definire gli utenti e i gruppi per un partecipante.

L'utente Ammin per il partecipante assegna le autorizzazioni al gruppo di eventi. Ad esempio, l'utente Ammin potrebbe decidere che il gruppo Volume vede solo il Volume documento e i report di Analisi documento. L'utente Ammin, utilizzando la pagina Dettagli gruppo, abilita il modulo dei report dei documenti, ma disabilita tutti gli altri moduli per il gruppo Volume.

L'impostazione, come Ammin hub, si esegue sulla pagina Permessi determina se un modulo viene elencato sulla pagina Dettagli gruppo.

Alcuni moduli vengono limitati a determinati membri della comunità hub (ad esempio, l'Ammin hub). Di conseguenza, anche se si abilita uno di questi moduli per l'uso da parte di un partecipante, il modulo non viene visualizzato nella pagina Dettagli gruppo per il partecipante.

Abilitazione e disabilitazione permessi

Dalla pagina Elenco autorizzazioni, è possibile determinare quali autorizzazioni saranno disponibili per assegnarle ai gruppi di utenti abilitandole o disabilitandole. In caso contrario, tuttavia, definire le nuove autorizzazioni.

Per modificare le autorizzazioni predefinite:

1. Fare clic su **Ammin 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 5. Definizione delle destinazioni

In questo capitolo, viene descritto come impostare le destinazioni in WebSphere Partner Gateway. Sono inclusi i seguenti argomenti:

- “Panoramica”
- “Caricamento dei gestori definiti dall’utente” a pagina 32
- “Impostazione di valori di trasporto globale” a pagina 33
- “Impostazione di una destinazione HTTP/S” a pagina 33
- “Impostazione di una destinazione FTP” a pagina 34
- “Impostazione di una destinazione SMTP” a pagina 36
- “Impostazione di una destinazione JMS” a pagina 37
- “Impostazione di una destinazione di sistema di file” a pagina 38
- “Impostazione di una destinazione Script FTP” a pagina 39
- “Impostazione di una destinazione per un trasporto definito dall’utente” a pagina 43
- “Modifica dei punti di configurazione” a pagina 44

Panoramica

Come descritto in “Panoramica sull’elaborazione del documento” a pagina 7, Il destinatario è responsabile dell’accettazione di documenti in entrata da un trasporto specifico. La destinazione è un’istanza Destinatario configurato per una distribuzione in particolare.

I documenti ricevuti su una destinazione possono venire dai partecipanti della comunità (per eventuale consegna al Gestore comunità) o dall’applicazione back-end del Gestore comunità (per eventuale consegna ai partecipanti).

In Figura 16 a pagina 32 viene mostrato un server WebSphere Partner Gateway con quattro destinazioni impostate. Due delle destinazioni (HTTP/S e FTP/S) sono per i documenti che vengono dai partecipanti. Queste due destinazioni rappresentano un URI HTTP e una directory FTP. Vengono fornite informazioni su queste destinazioni ai partecipanti per indicare dove devono inviare i documenti all’utente. Le altre due richieste (JMS e directory di file) sono per i documenti che provengono dall’applicazione back-end del Gestore comunità. Queste destinazioni rappresentano una coda ed una directory.

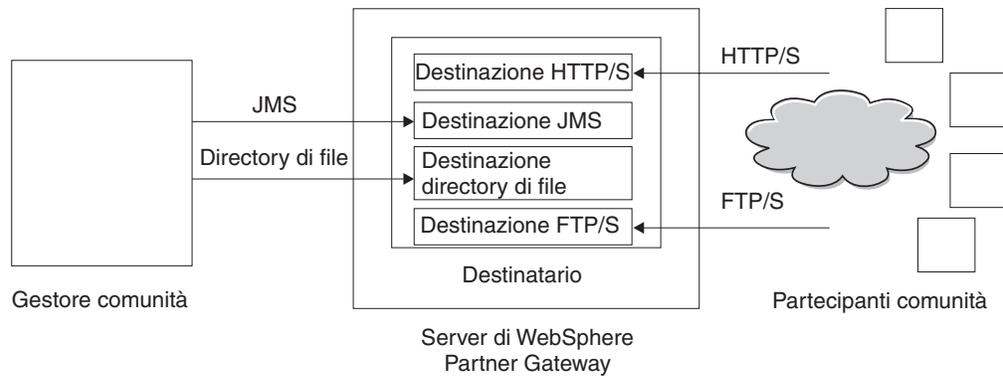


Figura 16. Trasporti a destinazioni associate

Si imposta almeno una destinazione per ogni tipo di trasporto sul quale i documenti vengono inviati all'hub. Ad esempio, si dispone di una destinazione HTTP per ricevere i documenti inviati sull'HTTP o il trasporto HTTPS. Se i partecipanti della comunità inviano i documenti sull'FTP, si imposta una destinazione FTP.

Il componente Destinatario rileva quando arriva un messaggio sulle destinazioni. Alcune destinazioni rilevano messaggi effettuando il polling dei trasporti ad intervalli regolari o su base pianificata, per stabilire se sono arrivati nuovi messaggi. Le destinazioni WebSphere Partner Gateway che si basano sull'effettuazione del polling sono: JMS, FTP, SMTP, File e Script FTP. La destinazione HTTP/S si basa sul callback, vale a dire che riceve la notifica dal trasporto quando arriva un messaggio. I trasporti definiti dall'utente possono essere sia su base polling che su base callback.

Caricamento dei gestori definiti dall'utente

È possibile modificare i punti di configurazione per le destinazioni specificando un gestore per la destinazione. Il gestore può essere fornito da WebSphere Partner Gateway o definito dall'utente. In questa sezione, viene descritto come caricare un gestore definito dall'utente. Utilizzare questa sezione solo per i gestori definiti dall'utente. I gestori forniti da WebSphere Partner Gateway sono già disponibili.

Per caricare un gestore, effettuare le seguenti procedure:

1. Dal menu principale, fare clic su **Ammin hub > Configurazione hub > Gestori**.
2. Selezionare **Destinazione**.
Viene visualizzato l'elenco di gestori attualmente definiti per le destinazioni. Si noti che i gestori forniti da WebPShere Partner Gateway presentano un ID fornitore di **Prodotto**.
3. Dalla pagina Elenco gestore, fare clic su **Importa**.
4. Nella pagina Importa gestore, specificare il percorso al file XML che rappresenta il gestore o utilizzare **Sfoggia** per cercare quel file XML.

Dopo il caricamento del gestore, è possibile utilizzarlo per personalizzare i punti di configurazione delle destinazioni.

Impostazione di valori di trasporto globale

Si impostano gli attributi di trasporto globale che si applicano tutti alle destinazioni HTTP/S e Script FTP. Se non si desidera definire le destinazioni HTTPS e Script FTP, saltare questa sezione.

1. Fare clic su **Ammin hub > Configurazione hub > Destinazioni** per visualizzare l'elenco delle destinazioni.
2. Selezionare **Attributi di trasporto globale** dall'elenco Destinazione.
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** accanto a **Attributi globali elencati per categoria**.
5. Esaminare e, se necessario, modificare i valori di **Trasporto di script FTP e Script FTP - Origini e gateway**.

Il trasporto Script FTP utilizza un meccanismo di blocco che evita che più di un'istanza Script FTP acceda alla stessa destinazione nello stesso momento. Quando un trasporto FTP è pronto per inviare documenti, richiede questo blocco. I valori predefiniti vengono forniti per esprimere, ad esempio, per quanto tempo l'istanza di destinazione ottiene il blocco e quante volte può tentare di recuperarlo, se il blocco è in uso. È, inoltre, possibile utilizzare i valori predefiniti o modificarli. Per modificare uno o più valori, immettere il nuovo o i nuovi valori. È possibile modificare:

- **Valori Trasporto Script FTP**
 - **Numero tentativi blocco**, che indica quante volte la destinazione tenterà 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 - Destinazioni e gateway**
 - **Tempo max di blocco (secondi)**, che indica per quanto tempo la destinazione può tenere il blocco. Il valore predefinito è 240 secondi.
 - **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.
6. Esaminare, e, se necessario, modificare i valori di **Trasporto HTTP/S**. È possibile modificare:
 - **Timeout max sincrono (secondi)**, per indicare il numero di secondi in cui può restare aperta una connessione sincrona. Il valore predefinito è 300 secondi.
 - **Numero max di connessione sincrone contemporanee**, per indicare quante connessioni sincrone sono consentite dal sistema. Il valore predefinito è 100 connessioni.
 7. Fare clic su **Salva**

Impostazione di una destinazione HTTP/S

Il componente Destinatarario ha un servlet bcgreceiver predefinito che viene utilizzato per ricevere messaggi POST HTTP/S. Si creano una o più destinazioni HTTP per accedere ai messaggi ricevuti dal servlet.

I seguenti passaggi descrivono cosa è necessario specificare per una destinazione HTTP/S.

1. Fare clic su **Ammin hub > Configurazione hub > Destinazioni** per visualizzare la pagina dell'elenco delle destinazioni.
2. Dalla pagina Elenco destinazione, fare clic su **Crea destinazione**.

Dettagli di destinazione

Nella sezione **Dettagli di destinazione**, eseguire questi passaggi:

1. Digitare un nome per la destinazione. Ad esempio, è possibile chiamare la destinazione HttpTarget1. Questo è un campo obbligatorio. Il nome che viene inserito sarà visualizzato nell'elenco destinazioni.
2. Facoltativamente, indicare lo stato della destinazione. **Abilitato** è quello predefinito. Una destinazione che viene abilitata è pronta per accettare i documenti. Una destinazione che viene disabilitata non può accettare i documenti.
3. Facoltativamente, inserire una descrizione della destinazione.
4. Selezionare **HTTP/S** dall'elenco **Trasporto**.

Configurazione della destinazione

Nella sezione **Configurazione della destinazione**, eseguire questi passaggi:

1. Facoltativamente, indicare il tipo di gateway. Il tipo di gateway 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'URI per la destinazione HTTP/S. Il nome deve iniziare con **bcgreceiver**. Ad esempio, è possibile inserire bcgreceiver/inoltra. I documenti che arrivano nel server su HTTP/S vengono ricevuti in bcgreceiver/submit.

Nota: I valori di **Instradamento sincrono** 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 di valori di trasporto globale" a pagina 33.

Gestori

Se si ricevono file contenenti più scambi EDI o documenti XML o ROD che devono essere divisi, configurare il gestore splitter appropriato nel punto di configurazione Preprocesso.

Se si desidera inviare o ricevere certi tipi di documenti aziendali (RosettaNet, cXML, SOAP e AS2) tramite uno scambio sincrono, specificare un gestore per il protocollo associato nel punto di configurazione SyncCheck. Inoltre, è possibile modificare i punti di configurazione di postprocesso per la destinazione.

Per modificare un punto di configurazione, andare a "Modifica dei punti di configurazione" a pagina 44. Altrimenti, fare clic su **Salva**.

Impostazione di una destinazione FTP

Una destinazione FTP esegue il polling del server FTP ad un intervallo fisso per ricercare nuovi documenti.

I seguenti passaggi descrivono cosa è necessario specificare per una destinazione FTP.

1. Fare clic su **Ammin hub > Configurazione hub > Destinazioni** per visualizzare l'elenco delle destinazioni.
2. Dalla pagina Elenco destinazione, fare clic su **Crea destinazione**.

Dettagli di destinazione

Nella sezione **Dettagli di destinazione**, eseguire questi passaggi:

1. Digitare un nome per la destinazione. Ad esempio, si potrebbe chiamare la destinazione FTPTarget1. Questo è un campo obbligatorio. Il nome che viene inserito sarà visualizzato nell'elenco destinazioni.
2. Facoltativamente indicare lo stato della destinazione. **Abilitato** è quello predefinito. Una destinazione che viene abilitata è pronta per accettare i documenti. Una destinazione che viene disabilitata non può accettare i documenti.
3. Facoltativamente inserire una descrizione della destinazione.
4. Selezionare **Directory FTP** dall'elenco **Trasporto**.

Configurazione della destinazione

Nella sezione **Configurazione della destinazione**, eseguire questi passaggi:

1. Nel campo **Directory root FTP**, inserire la directory root del server FTP. Il Gestore documenti effettua il polling delle directory secondarie del partecipante nella directory root FTP per l'instradamento del documento. Questo campo è obbligatorio. Per informazioni sull'impostazione della directory per un server FTP, fare riferimento a "Configurazione del server FTP per la ricezione dei documenti" a pagina 17.

Nota: Immettere il percorso della directory che termina sulla directory FTP. Non includere le directory secondarie del partecipante.

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 **Num thread**, per indicare il numero di documenti che Gestore documenti elabora simultaneamente. Si consiglia come valore predefinito 1.
4. Facoltativamente, inserire un valore per **Escludi est file** per indicare i tipi di documenti che il gestore documenti deve ignorare (escludere dall'elaborazione), se trova 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 di file (ad esempio: .exe o .txt). Utilizzare solo i caratteri che denotano l'estensione file.

Gestori

Se si ricevono file contenenti più scambi EDI o documenti XML o ROD che devono essere divisi, configurare il gestore splitter appropriato nel punto di configurazione Preprocesso.

Per modificare il punto di configurazione del preprocesso, andare al passo "Modifica dei punti di configurazione" a pagina 44. Altrimenti, fare clic su **Salva**.

Impostazione di una destinazione SMTP

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

I seguenti passaggi descrivono cosa è necessario specificare per una destinazione SMTP (POP3).

1. Fare clic su **Ammin hub > Configurazione hub > Destinazioni** per visualizzare la pagina dell'elenco delle destinazioni.
2. Dalla pagina Elenco destinazione, fare clic su **Crea destinazione**.

Dettagli di destinazione

Nella sezione **Dettagli di destinazione**, eseguire questi passaggi:

1. Digitare un nome per la destinazione. Ad esempio, è possibile chiamare la destinazione POP3Target1. Questo è un campo obbligatorio. Il nome che viene inserito sarà visualizzato nell'elenco destinazioni.
2. Facoltativamente, indicare lo stato della destinazione. **Abilitato** è quello predefinito. Una destinazione che viene abilitata è pronta per accettare i documenti. Una destinazione che viene disabilitata non può accettare i documenti.
3. Facoltativamente, inserire una descrizione della destinazione.
4. Selezionare **POP3** dall'elenco **Trasporto**.

Configurazione della destinazione

Nella sezione **Configurazione del gateway** della pagina, eseguire questi passaggi:

1. Facoltativamente, indicare il tipo di gateway. Il tipo di gateway 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 **Num thread**, per indicare il numero di documenti che Gestore documenti elabora simultaneamente. Il valore predefinito di 1 è quello consigliato.

Pianificazione

Nella sezione **Pianifica** della pagina, eseguire questi passaggi:

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 una destinazione JMS

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

I seguenti passaggi descrivono cosa è necessario specificare per una destinazione JMS.

1. Fare clic su **Ammin hub > Configurazione hub > Destinazioni** per visualizzare l'elenco delle destinazioni.
2. Dalla pagina Elenco destinazione, fare clic su **Crea destinazione**.

Dettagli di destinazione

Nella sezione **Dettagli di destinazione**, eseguire questi passaggi:

1. Digitare un nome per la destinazione. Ad esempio, si potrebbe chiamare la destinazione JMSTarget1. Questo è un campo obbligatorio. Il nome che viene inserito sarà visualizzato nell'elenco destinazioni.
2. Facoltativamente indicare lo stato della destinazione. **Abilitato** è quello predefinito. Una destinazione che viene abilitata è pronta per accettare i documenti. Una destinazione che viene disabilitata non può accettare i documenti.
3. Facoltativamente inserire una descrizione della destinazione.
4. Selezionare **JMS** dall'elenco **Trasporto**.

Configurazione della destinazione

Nella sezione **Configurazione del gateway** della pagina, eseguire questi passaggi:

1. Facoltativamente indicare il tipo di gateway. Il tipo di gateway 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 21). 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. Si tratta di 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 23).
Se viene immessa la cartella secondaria per il contesto JMS al passo 2 a pagina 37, 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. Si tratta di 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 23).
Se viene immessa la cartella secondaria per il contesto JMS al passo 2 a pagina 37, 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 pacchetto dell'URL del provider.
7. Inserire un nome `factory` JNDI. Se non si inserisce nulla, viene utilizzato il valore `com.sun.jndi.fscontext.RefFSContextFactory`. Questo è un campo obbligatorio.
8. Facoltativamente, inserire un valore per **Timeout**, per indicare quanti secondi la destinazione controlla la coda JMS per i documenti. Questo campo è facoltativo.
9. Facoltativamente, inserire un valore per **Num thread**, per indicare il numero di documenti che il Gestore documenti elabora simultaneamente. Il valore predefinito di 1 è consigliato.

Ad esempio, se si desidera impostare una destinazione JMS per far corrispondere l'esempio di configurazione JMS in "Configurazione dell'hub per il protocollo di trasporto JMS" a pagina 21, è preferibile:

1. Inserire il valore **JMSTarget** in **Nome destinazione** box.
2. Immettere il valore **file:/C:/TEMP/JMS/JMS** nella casella **URL provider JMS**.
3. Inserire il valore **inQ** in **Nome coda JMS** box.
4. Inserire il valore **Hub** in **Nome factory JMS**.

Gestori

Se si ricevono file contenenti più scambi EDI o documenti XML o ROD che devono essere divisi, configurare il gestore splitter appropriato nel punto di configurazione Preprocesso.

Per modificare un punto di configurazione per questa destinazione, andare a "Modifica dei punti di configurazione" a pagina 44. Altrimenti, fare clic su **Salva**.

Impostazione di una destinazione di sistema di file

Una destinazione del file-system esegue il polling in base ad un intervallo fissato per la ricerca di nuovi documenti.

I seguenti passaggi descrivono cosa è necessario specificare per una destinazione di sistema di file.

1. Fare clic su **Ammin hub > Configurazione hub > Destinazioni** per visualizzare la pagina dell'elenco delle destinazioni.
2. Dalla pagina **Elenco destinazione**, fare clic su **Crea destinazione**.

Dettagli di destinazione

Nella sezione **Dettagli di destinazione**, eseguire questi passaggi:

1. Digitare un nome per la destinazione. Ad esempio, è possibile chiamare la destinazione FileTarget1. Questo è un campo obbligatorio. Il nome che viene inserito sarà visualizzato nell'elenco destinazioni.
2. Facoltativamente, indicare lo stato della destinazione. **Abilitato** è quello predefinito. Una destinazione che viene abilitata è pronta per accettare i documenti. Una destinazione che viene disabilitata non può accettare i documenti.
3. Facoltativamente, inserire una descrizione della destinazione.
4. Selezionare **Directory file** dall'elenco **Trasporto**.

Configurazione della destinazione

Nella sezione **Configurazione del gateway** della pagina, eseguire questi passaggi:

1. Facoltativamente, indicare il tipo di gateway. Il tipo di gateway 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 un valore per **Percorso root documento** per indicare la directory in cui i documenti vengono ricevuti.
3. Facoltativamente, inserire un valore per **Intervallo polling**, per indicare la frequenza con la quale effettuare il polling della directory per i nuovi documenti. Se non viene inserito nulla, il polling della directory viene effettuato ogni 5 secondi.
4. 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 di 3 secondi.
5. Facoltativamente, inserire un valore per **Num thread**, per indicare il numero di documenti che Gestore documenti elabora simultaneamente. Si consiglia come valore predefinito 1.

Gestori

Se si ricevono file contenenti più scambi EDI o documenti XML o ROD che devono essere divisi, configurare il gestore splitter appropriato nel punto di configurazione Preprocesso.

Per modificare il punto di configurazione del preprocesso, andare al passo "Modifica dei punti di configurazione" a pagina 44. Altrimenti, fare clic su **Salva**.

Impostazione di una destinazione Script FTP

Un gateway script FTP esegue il polling della destinazione che viene eseguita secondo la pianificazione impostata. Il funzionamento di una destinazione script FTP è governato da uno script di comandi FTP.

A differenza della destinazione FTP, che effettua il polling di una directory sul server FTP, la destinazione Script FTP effettua il polling delle directory su un altro server (ad esempio, una VAN).

Creazione dello script FTP

I server FTP possono avere requisiti specifici per i comandi che accettano. Per utilizzare una destinazione script FTP, viene creato un file che include tutti i comandi FTP necessari richiesti dal server FTP a cui ci si connette. (Ricevere queste informazioni dall'amministratore del server FTP),

1. Creare uno script per le destinazioni, per indicare le azioni da 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 segnaposti (ad esempio, %BCGSERVERIP%) vengono posizionati quando la destinazione viene messa in servizio dai valori immessi al momento della creazione di un'istanza specifica di una destinazione di script FTP. In questo esempio, %BCGOPTION% è il nome della directory nel comando cd. I parametri dello script e i campi di destinazione di script FTP associati vengono descritti in Tabella 2:

Tabella 2. Come i parametri dello script mappano alle voci del campo Destinazione script FTP

Parametro dello script	Voce del campo Destinazione script FTP
%BCGSERVERIP%	IP server
%BCGUSERID%	ID utente
%BCGPASSWORD%	Password
%BCGOPTIONx%	Opzione <i>x</i> in Attributi definiti dall'utente

2. Salvare il file.

Comandi di script FTP

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

- `ascii`, binario, passivo

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.

- **open**

Questo comando fa riferimento a 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 dello script FTP deve essere:

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

- **quit, bye**

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 di destinazione

I seguenti passaggi descrivono cosa è necessario specificare per una destinazione Script FTP.

1. Fare clic su **Ammin hub > Configurazione hub > Destinazioni** per visualizzare l'elenco delle destinazioni.
2. Dalla pagina Elenco destinazione, fare clic su **Crea destinazione**.

Nella sezione **Dettagli di destinazione**, eseguire questi passaggi:

1. Digitare un nome per la destinazione. Ad esempio, si potrebbe chiamare la destinazione FTPScriptingTarget1. Questo è un campo obbligatorio. Il nome che viene inserito sarà visualizzato nell'elenco destinazioni.
2. Facoltativamente indicare lo stato della destinazione. **Abilitato** è quello predefinito. Una destinazione che viene abilitata è pronta per accettare i documenti. Una destinazione che viene disabilitata non può accettare i documenti.
3. Facoltativamente inserire una descrizione della destinazione.
4. Selezionare **Script FTP** dall'elenco Trasporto.

Configurazione della destinazione

Nella sezione **Configurazione del gateway** della pagina, eseguire questi passaggi:

1. Facoltativamente indicare il tipo di gateway. Il tipo di gateway 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 la destinazione funziona in modalità SSL protetta. In tal caso, sarà necessario scambiare certificati con i partecipanti, come descritto in Capitolo 13, "Impostazione di sicurezza per gli scambi in arrivo e in uscita", a pagina 153.
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. Fare clic su **Carica file** per caricare il file di script nella casella di testo **File di script al momento caricato**.
 - d. Se il file di script è quello che si desidera utilizzare, fare clic su **Salva**.
 - e. Fare clic su **Chiudi finestra**.
6. Nel campo **Timeout connessione**, inserire il numero di secondi in cui un socket rimane aperto senza traffico.
7. Nel campo **Utente blocco**, specificare se la destinazione richiederà un blocco, in modo che nessuna altra istanza di una destinazione script FTP possa avere accesso alla stessa directory del server FTP nello stesso momento.

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 di valori di trasporto globale" a pagina 33.

Attributi definiti dall'utente

Se si desidera specificare attributi aggiuntivi, eseguire questi passaggi. Il valore immesso per l'opzione sostituisce *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.

Pianifica

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.

Gestori

Se si ricevono file contenenti più scambi EDI o documenti XML o ROD che devono essere divisi, configurare il gestore splitter appropriato nel punto di configurazione Preprocesso.

Per modificare il punto di configurazione del preprocesso, andare al passo "Modifica dei punti di configurazione" a pagina 44. Altrimenti, fare clic su **Salva**.

Impostazione di una destinazione per un trasporto definito dall'utente

Se si definisce una destinazione per un trasporto definito dall'utente, i nomi di campo e le altre informazioni vengono definite nel file che descrive il trasporto.

Eeguire quindi questi passaggi:

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

Nota: Nella pagina dell'elenco delle destinazioni, è possibile anche 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 dopo che è stato utilizzato per la creazione di una destinazione.

5. Fare clic su **Crea destinazione**.
6. Digitare un nome per la destinazione. Questo è un campo obbligatorio. Il nome che viene inserito sarà visualizzato nell'elenco destinazioni.
7. Facoltativamente, indicare lo stato della destinazione. **Abilitato** è quello predefinito. Una destinazione che viene abilitata è pronta per accettare i documenti. Una destinazione che viene disabilitata non può accettare i documenti.

8. Facoltativamente, inserire una descrizione della destinazione.
9. Selezionare il trasporto definito dall'utente dall'elenco.
10. Compilare i campi (che saranno univoci per ciascun trasporto definito dall'utente).
11. Se si desidera modificare i punti di configurazione per questa destinazione, fare riferimento a "Modifica dei punti di configurazione". Altrimenti, fare clic su **Salva**.

Modifica dei punti di configurazione

Il numero dei punti di configurazione disponibili e il numero dei gestori associati per questi punti di configurazione variano, a seconda del tipo di destinazione che si imposta. Ad esempio, il punto di configurazione SyncCheck è disponibile solo con destinazioni HTTP/S e JMS.

Per determinati protocolli aziendali (RosettaNet, cXML, SOAP, e AS2) che vengono coinvolti negli scambi sincroni, è necessario specificare un gestore per il punto di configurazione SyncCheck. Inoltre, è possibile modificare il modo in cui le destinazioni elaborano i documenti applicando un gestore definito dall'utente caricato (o un processo fornito dal sistema) ai punti di preprocesso e postprocesso della destinazione.

Per applicare un gestore scritto dall'utente per questi punti di configurazione, è per prima cosa necessario caricare il gestore, come descritto in "Caricamento dei gestori definiti dall'utente" a pagina 32. È, inoltre, possibile utilizzare un gestore fornito dal sistema che è già disponibile e non deve essere caricato.

Preprocesso

Il gestore della configurazione del preprocesso è disponibile su tutti i tipi di destinazioni ma non è applicabile alle destinazioni SMTP.

Attributi preprocesso

Tabella 3 descrive gli attributi da impostare per un gestore di preprocesso ed elenca i gestori splitter cui si applicano gli attributi.

Gli attributi ROD utilizzati come esempio in questa tabella corrispondono a quelli utilizzati in "Esempio ROD in EDI" a pagina 219. In questo esempio, gli attributi ROD sono contenuti in map S_DT_ROD_TO_EDI.eif, che comprende la seguente definizione di flusso dei documenti:

- Pacchetto: Nessuno (versione N/D)
- Protocollo: ROD_TO_EDI_DICT (versione TUTTE)
- Flusso di documenti: DTROD-TO-EDI_ROD (versione TUTTE)

Il metadizionario ROD e i metadocumenti associati a questo flusso sono ROD_TO_EDI_DICT e DTROD-TO-EDI_ROD.

Tabella 3. Attributi gestore splitter

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

Tabella 3. Attributi gestore splitter (Continua)

Attributo	Descrizione	Gestore splitter
BATCHDOCS	Quando BCG_BATCHDOCS è attivo, lo splitter aggiunge ID di batch al documento quando i documenti vengono separati. Se i documenti vengono trasformati in transazioni EDI da imbustare, l'utilità Enveloper utilizza ID di batch per assicurarsi che le transazioni siano posizionate nello stesso interscambio EDI (se possibile) prima di essere recapitate. Si noti che l'utilità Enveloper deve disporre dell'attributo di batch impostato su On (valore predefinito). Vedere "Modalità batch" a pagina 98.	ROD Generico XML
Da nome impacchettamento	L'impacchettamento associato al documento. Questo valore deve corrispondere all'impacchettamento specificato nella definizione del flusso di documenti. Ad esempio, per un documento che dispone di un impacchettamento impostato su Nessuno, questo valore deve essere Nessuno .	ROD Generico
Da versione impacchettamento	La versione dell'impacchettamento specificata in Da nome impacchettamento. Ad esempio, se il documento dispone di un impacchettamento impostato su Nessuno, questo valore deve essere N/D .	ROD Generico
Da nome protocollo	Il protocollo associato al documento. Il valore deve corrispondere al protocollo specificato nella definizione del flusso di documenti. Ad esempio, per un documento ROD, questo valore può essere ROD-TO-EDI_DICT .	ROD Generico
Da versione protocollo	La versione del protocollo specificato in Da nome protocollo. Ad esempio per il protocollo ROD-TO-EDI_DICT, il valore deve essere TUTTI .	ROD Generico
Da codice processo	Il processo (flusso di documenti) associato al documento. Il valore deve corrispondere al flusso di documenti indicato nella definizione del flusso di documenti. Ad esempio, per un documento ROD, questo valore può essere DTROD-TO-EDI_ROD .	ROD Generico
Da versione processo	La versione del processo specificato in Da coda processo. Ad esempio, per DTROD-TO-EDI_ROD, questo valore deve essere TUTTI .	ROD Generico
Metadizionario	Il metadizionario fornisce 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 Generico
Metadocumento	Il metadocumento fornisce 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 Generico
Metasintassi	La metasintassi descrive il formato del documento che sta per essere separato. Il valore predefinito è rod .	ROD Generico

Note:

1. E' supportato un solo tipo di documento ROD per istanza di destinazione.
2. Se una destinazione dispone di più di un gestore splitter configurato (ad esempio, se dispone di gestori splitter EDI, ROD e XML configurati), il gestore splitter ROD deve essere l'ultimo nell'**Elenco configurati**.

Modifica del punto di configurazione del preprocesso

Per modificare il punto di configurazione del preprocesso, eseguire i passi indicati:

1. Selezionare **Preprocesso** dall'elenco **Gestori del punto di configurazione**.

Vengono forniti quattro gestori di preprocesso (per impostazione predefinita) e mostrati 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

Nota: I gestori del preprocesso non si applicano alle destinazioni SMTP.

2. Se si ricevono più interscambi EDI o documenti XML o ROD da separare, assicurarsi di selezionare il gestore splitter appropriato. Per configurare il passo del preprocesso:

- a. Selezionare un gestore dall'**elenco Disponibili** e fare clic su **Aggiungi**. Si noti che il gestore si sposta dall'**elenco Disponibili** all'**elenco Configurati**, come descritto in Figura 17:

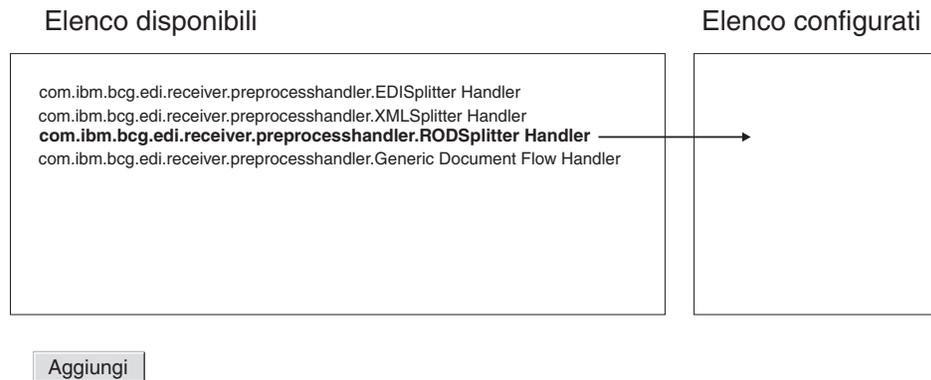


Figura 17. Configurazione del passaggio di preprocesso per una destinazione

- b. Ripetere questo passaggio per ciascun gestore che si desidera aggiungere all'elenco Configurati.

Ricordare che per le destinazioni, i gestori vengono chiamati nell'ordine nel quale vengono visualizzati in **Elenco configurati**. Il primo gestore disponibile elabora la richiesta e gli altri gestori nell'elenco non vengono chiamati.

- c. Configurare il gestore 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 attributo-BCGBATCHDOC. Il valore predefinito è ON. Per informazioni su questo attributo, consultare "Attributi preprocesso" a pagina 44.
- Se è stato aggiunto RODSplitterHandler, è possibile modificare i valori di 11 attributi. La codifica, BATCHDOCS e la metasintassi dispongono di valori predefiniti. Per gli altri attributi, è necessario immettere un valore per Da nome impacchettamento, Da versione impacchettamento, Da nome protocollo, Da versione protocollo, Da codice processo, Da versione processo, Metadizionario e Metadocumento. Per informazioni su tali attributi, consultare "Attributi preprocesso" a pagina 44.

- Se è stato aggiunto GenericDocumentFlowHandler, è possibile specificare i valori di 11 attributi. La codifica e BATCHDOCS hanno valori predefiniti. Per gli altri attributi, digitare un valore per Dal nome impacchettamento, Dalla versione impacchettamento, Dal nome protocollo, Dalla versione protocollo, Dal codice processo, Dalla versione processo, Metadizionario, Metadocumento e Metasintassi. Per informazioni su tali attributi, consultare “Attributi preprocesso” a pagina 44.

SyncCheck

Il punto di configurazione SyncCheck è disponibile solo con destinazioni HTTP/S e JMS.

Per specificare un gestore per un protocollo aziendale coinvolto in uno scambio sincrono, eseguire questi passaggi:

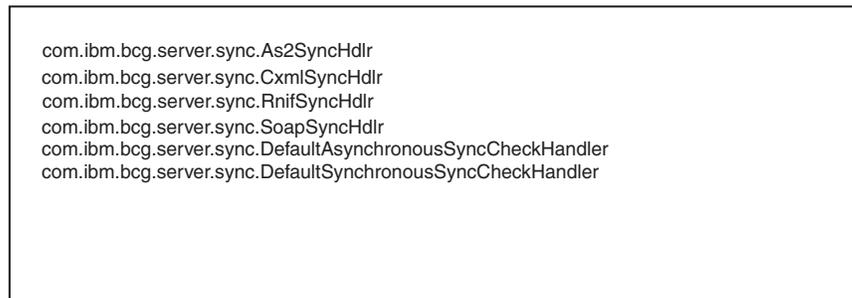
1. Selezionare **SyncCheck** dall’elenco **Gestori del punto di configurazione**.

Vengono forniti sei gestori SyncCheck (per impostazione predefinita) per una destinazione HTTP/S. Questi gestori vengono mostrati nell’**elenco Disponibili**:

- 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

Se, ad esempio, si configura una destinazione HTTP/S, l’elenco Disponibili appare come segue:

Elenco disponibili



Aggiungi

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

Come è possibile notare dalla convenzione di denominazione, i primi quattro gestori sono specifici di 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.

DefaultAsynchronousSyncCheckHandler e DefaultSynchronousSyncCheckHandler possono essere utilizzati con altre destinazioni (come ad esempio una destinazione JMS).

2. Verranno ricevuti documenti sincroni su questa destinazione, effettuare questi passaggi:
 - a. Selezionare uno o più gestori dall'**elenco Disponibili** e fare clic su **Aggiungi**.
 - b. Ripetere questa procedura, se si desidera aggiungere altri gestori all'elenco. Ricordare che per le destinazioni, i gestori vengono chiamati nell'ordine nel quale vengono visualizzati in **Elenco configurati**. Il primo gestore disponibile elabora la richiesta e gli altri gestori nell'elenco non vengono chiamati.

Per le destinazioni HTTP e HTTPS, è opportuno elencare il gestore SyncCheck specifico (ad esempio, com.ibm.bcg.server.sync.As2SyncHdlr per le transazioni AS2), prima di elencare i gestori predefiniti SyncCheck.

Postprocesso

Non viene fornito alcun gestore per impostazione predefinita per il preprocesso e, di conseguenza, nessun gestore viene elencato nell'**elenco Disponibili**. Si può, tuttavia, caricare un gestore per questo punto di configurazione per tutti i tipi di destinazione che supportano la comunicazione sincrona. I tipi di gestore disponibili per il postprocesso sono:

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

Aggiungere un gestore di postprocesso caricando un gestore conforme ad uno di questi tipi di gestore. Si utilizza la scelta **Importa** della pagina Elenco gestori per caricare un gestore definito dall'utente. Quando si carica un gestore di destinazione definito dall'utente, il gestore viene aggiunto all'Elenco gestori. Viene inoltre visualizzato nell'Elenco disponibili per il tipo di punto di configurazione al quale appartiene.

Per modificare il punto di configurazione del postprocesso, eseguire i passi indicati:

1. Selezionare **Postprocesso** dall'elenco **Gestori del punto di configurazione**.
2. Selezionare un gestore definito dall'utente dall'**elenco Disponibili** e fare clic su **Aggiungi**. Si noti che il gestore si sposta dall'**elenco Disponibili** all'**elenco Configurati**

Modifica dell'elenco Configurati

Se è necessario modificare l'ordine dei gestori, eliminare un gestore, o configurare gli attributi del gestore, eseguire il passaggio appropriato:

- Rimuovere un gestore selezionandolo dall'**elenco Configurati** e facendo clic su **Rimuovi**. Il gestore viene spostato nell'**elenco Disponibili**.
- Riorganizzare l'ordine nel quale il gestore viene utilizzato selezionando il gestore e facendo clic su **Sposta su** o **Sposta giù**.
- Configurare il gestore selezionandolo dall'**elenco Configurati** e facendo clic su **Configura**. Viene visualizzato l'elenco di attributi configurabili.

Capitolo 6. Configurazione delle procedure e delle azioni 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 funzionamento fornito dal sistema di flussi di lavoro ed azioni, saltare questo capitolo.

In questo capitolo, sono contenuti i seguenti argomenti:

- “Caricamento dei gestori”
- “Configurazione dei flussi di lavoro fissi” a pagina 50
- “Configurazione azioni” a pagina 51

Caricamento dei gestori

Se si modificano i componenti, caricare prima i gestori per quei componenti prima di creare o configurare i componenti. È necessario caricare solo i gestori definiti dall'utente per i componenti necessari. Ad esempio, se si aggiunge una procedura di convalida, è necessario caricare il gestore dalla pagina Azioni dei **Gestori** (come descritto nei passi da 1 a 4).

Nota: Come menzionato in “Configurazione dei componenti di elaborazione del documento con i gestori” a pagina 9, si caricano solo i gestori definiti dall'utente. I gestori 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 dai gestori che si associano ad essi.

Nota: È possibile elencare i tipi di gestori validi per le azioni e i flussi di lavoro fissi facendo clic su **Gestione hub > Configurazione hub > Gestori > Azioni > Tipi di gestore** o **Gestione hub > Configurazione hub > Gestori > Flusso di lavoro fisso > Tipi di gestori**. Utilizzare questo elenco per confermare che il gestore è un tipo valido prima di caricarlo. Deve essere uno dei tipi consentiti o non si carica con esito positivo.

Per caricare un gestore, effettuare le seguenti procedure:

1. Dal menu principale, fare clic su **Ammin hub > Configurazione hub > Gestori**.
2. Selezionare il tipo di gestore (**Azione** o **Flusso di lavoro fisso**).
Viene visualizzato l'elenco di gestori attualmente definiti per quel componente in particolare. Si noti che vengono elencati i gestori forniti da WebSphere Partner Gateway. Presentano un ID fornitore di **Prodotto**.
3. Dalla pagina Elenco gestore, fare clic su **Importa**.
4. Nella pagina Importa gestore, specificare il percorso al file XML che descrive il gestore o utilizzare **Sfoggia** per cercare quel file XML.
5. Fare clic su **Carica**.

Dopo il caricamento del gestore, è possibile utilizzarlo per creare nuove azioni e flussi di lavoro.

Nota: È possibile aggiornare i gestori definiti dall'utente caricando il file XML modificato. Per un gestore di azione, ad esempio, è preferibile fare clic su **Ammin hub > Configurazione hub > Gestori > Azione**, quindi fare clic su **Importa**.

Non è possibile modificare o eliminare i gestori forniti da WebSphere Partner Gateway.

Configurazione dei flussi di lavoro fissi

Capitolo 1, "Introduzione" descritto nei due passi relativi al flusso di lavoro in entrata fisso che è possibile configurare - una per decomprimere un protocollo e una per analizzare quest'ultimo. Per i flussi di lavoro in uscita, c'è una procedura per lo spaccettamento del protocollo.

Se si utilizza un gestore definito dall'utente per configurare una procedura del flusso di lavoro, caricare il gestore come descritto in "Caricamento dei gestori" a pagina 49.

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

1. Fare clic su **Ammin 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 procedura che si desidera configurare.
Viene visualizzata la procedura, insieme all'elenco di gestori già configurati per questa procedura. Per un elenco dei gestori predefiniti, vedere "Flussi di lavori fissi" e "Flusso di lavoro in uscita" a pagina 51.
4. Fare clic sull'icona **Modifica** per modificare l'elenco dei gestori.
5. Eseguire una o più delle seguenti attività per ciascuna procedura si desidera modificare.
 - a. Aggiungere un gestore selezionandolo dall'**elenco Disponibili** e facendo clic su **Aggiungi**. (Potrebbe essere visualizzato un gestore in **Disponibili**, se è stato caricato un gestore definito dall'utente o se è stato precedentemente rimosso un gestore dall'elenco **Configurati**). Il gestore viene spostato nell'elenco **Configurati**.
 - b. Rimuovere un gestore selezionandolo dall'elenco **Configurati** e facendo clic su **Aggiungi**. Il gestore viene spostato nell'elenco **Disponibili**.
 - c. Riorganizzare l'ordine nel quale i gestori vengono chiamati selezionando il gestore e facendo clic su **Sposta su** o su **Sposta giù**.
I gestori vengono chiamati nell'ordine nel quale sono elencati nell'elenco **Configurati**. Il primo gestore 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, documento ROD), è possibile spostare il gestore associato a quel tipo di documento (in questo esempio, com.ibm.bcg.edi.business.process.RODScannerHandler) in alto nell'elenco.
6. Fare clic su **Salva**.

Flussi di lavori fissi

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

Gestori per lo spaccettamento del protocollo

Per impostazione predefinita, la fase di decompressione del protocollo dispone dei seguenti gestori configurati:

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

Gestori per l'elaborazione del protocollo

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

- com.ibm.bcg.server.RNOChannelParseHandler
- com.ibm.bcg.server.RNSignalChannelParseHandler
- com.ibm.bcg.server.RNSCChannelParseHandler
- com.ibm.bcg.server.BinaryChannelParseHandler
- com.ibm.bcg.xml.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

Flusso di lavoro in uscita

Per impostazione predefinita, la procedura per l'impacchettamento del protocollo dispone dei seguenti gestori 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.xml.cXMLPackagingHandler
- com.ibm.bcg.soap.SOAPPackagingHandler
- com.ibm.bcg.eai.EAIPackagingHandler

Configurazione azioni

Capitolo 1, "Introduzione" ha descritto che le azioni possono essere effettuate da una o più procedure. WebSphere Partner Gateway fornisce una serie di azioni predefinite. È possibile aggiungere all'elenco di azioni caricando uno o più gestori di azioni (che sono procedure nell'azione), che è possibile utilizzare in un'azione. È, inoltre, possibile creare nuove azioni come descritto in "Creazione di azioni" a pagina 52.

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 53.

Se si utilizza un gestore definito dall'utente per configurare un'azione, caricare il gestore come descritto in "Caricamento dei gestori" a pagina 49.

Modifica di un'azione definita dall'utente

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

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.
L'azione, insieme all'elenco di gestori (procedure azione) già configurati per questa azione, viene elencata.
3. Effettuare una delle seguenti procedure per ogni azione che si desidera modificare.
 - a. Aggiungere una procedura selezionando il gestore associato dall'**elenco Disponibili** e facendo clic su **Aggiungi**. Il gestore viene spostato nell'elenco **Configurati**.
 - b. Rimuovere un gestore selezionandolo dall'elenco **Configurati** e facendo clic su **Aggiungi**. Il gestore viene spostato nell'elenco **Disponibili**.
 - c. Riorganizzare l'ordine nel quale i gestori vengono chiamati selezionando il gestore e facendo clic su **Sposta su** o su **Sposta giù**.
 - d. In tal modo, un gestore deve essere elaborato più di una volta selezionandolo e facendo clic su **Ripeti**.
Ricordare che tutti i gestori configurati per un'azione vengono chiamati e le procedure che i gestori rappresentano vengono effettuate nell'ordine nel quale vengono visualizzate nell'elenco **Configurati**.
 - e. Configurare il gestore selezionandolo dall'**elenco configurati** e facendo clic su **Configura**. Viene visualizzato l'elenco di attributi configurabili.
4. Fare clic su **Salva**.

Creazione di azioni

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

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

Creazione di una nuova azione

Per creare una nuova azione, effettuare le seguenti procedure:

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 procedura che viene richiamata come parte dell'azione, aggiungere il gestore selezionandolo dall'**elenco Disponibili** e fare clic su **Aggiungi**. Il gestore viene spostato nell'elenco **Configurati**.
Ricordare che i gestori vengono chiamati dall'azione nell'ordine nel quale sono elencati nell'elenco **Configurati**. Assicurarsi di posizionare i gestori nell'ordine corretto. È possibile utilizzare **Sposta su** o **Sposta giù** per disporre di nuovo l'ordine dei gestori o **Ripeti** per fare in modo che il gestore debba essere elaborato più di una volta.
7. Configurare un gestore selezionandolo dall'**elenco Configurati** e facendo clic su **Configura**. Viene visualizzato l'elenco di attributi configurabili.
8. Fare clic su **Salva**.

Copia di un'azione

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

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 procedure si trovano già nell'**Elenco configurati**. Queste sono le procedure associate all'azione che si desidera effettuare: Ad esempio, se si clona l'annullamento di gestore comunità fornito dal sistema dell'azione del processo RosettaNet, viene visualizzato il seguente elenco di gestori configurati e disponibili:

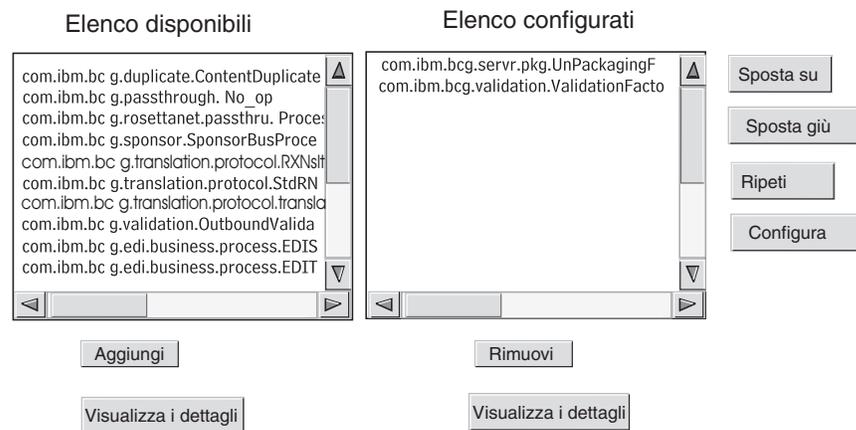


Figura 19. Clonazione di un'azione

Per modificare l'**elenco Configurati**, eseguire una o più delle seguenti procedure:

- a. Aggiungere una procedura selezionando il gestore associato dall'**elenco Disponibili** e facendo clic su **Aggiungi**. Il gestore viene spostato nell'**elenco Configurati**.
 - b. Rimuovere un gestore selezionando quello associato dall'**elenco Configurati** e facendo clic su **Aggiungi**. Il gestore viene spostato nell'**elenco Disponibili**.
 - c. Riorganizzare l'ordine nel quale i gestori vengono chiamati selezionando il gestore e facendo clic su **Sposta su** o su **Sposta giù**.
Ricordare che tutti i gestori configurati per un'azione vengono chiamati e le procedure associate ai gestori vengono effettuate nell'ordine nel quale vengono visualizzate nell'**elenco Configurati**.
 - d. Configurare il gestore selezionandolo dall'**elenco Configurati** e facendo clic su **Configura**. Viene visualizzato l'elenco di attributi configurabili.
7. Fare clic su **Salva**.

Capitolo 7. Configurazione dei flussi di documenti

In questo capitolo, viene descritto come configurare i documenti non EDI che verranno scambiati con i partecipanti della comunità e con le applicazioni back-end. La configurazione dei flussi di documenti e delle interazioni per i documenti EDI (con l'eccezione dei documenti EDI trasmessi) viene descritta in Capitolo 8, "Configurazione dei flussi di documenti EDI", a pagina 83. Inoltre, Capitolo 8 descrive il modo in cui configurare il flusso dei documenti e le interazioni per i documenti XML e ROD (record-oriented-data).

In questo capitolo, vengono descritti i seguenti argomenti:

- "Panoramica"
- "Documenti binari" a pagina 58
- "Documenti EDI con azione Pass-Through" a pagina 59
- "Documenti RosettaNet" a pagina 60
- "Servizi Web" a pagina 68
- "documenti cXML" a pagina 73
- "Documenti XML personalizzati" a pagina 78

Panoramica

Una definizione di flusso di documenti è costituita, al minimo, di un pacchetto, di un protocollo e di un flusso di documenti. Per determinati protocolli, è possibile specificare un'azione, un'attività e un segnale. Le definizioni di flusso di documenti specificano i tipi di documento che verranno elaborati da WebSphere Partner Gateway.

L'impacchettamento fa riferimento alla logica richiesta per assemblare 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 flusso di documenti descrive come deve essere il documento.

Le sezioni successive vengono illustrati i passaggi in generale per l'impostazione di un flusso di documenti tra Gestore comunità ed un partecipante.

Passaggio 1: Assicurarsi che la definizione di flusso di documenti sia disponibile

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

Come parte di come stabilire una definizione di flusso di documenti, è possibile modificare alcuni 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 di definizione di flusso di documenti forniscono un'impostazione globale per il pacchetto, protocollo o flusso di documenti associato. Gli attributi disponibili variano, a seconda della definizione di flusso di documenti. Ad esempio, gli

attributi per le definizioni del flusso di documenti EDI dispongono di diversi attributi delle definizioni del flusso di documenti RosettaNet.

Ad esempio, se si specifica un valore per **Ora di notifica** sul pacchetto AS, quest'ultimo viene applicato a tutti i documenti impacchettati con AS. (**Ora di notifica** specifica l'intervallo di tempo di attesa di una notifica MDN (message disposition notification) prima di inviare di nuovo la richiesta di origine.) Se, in seguito si imposta l'attributo **Ora di notifica** a livello delle funzioni B2B, questa impostazione sovrascrive quella impostata a livello di definizione del flusso di documenti.

Per gli attributi impostati su tutti i livelli della definizione di flusso di documenti, i valori impostati del flusso di documenti hanno la precedenza su quelli impostati sul livello del protocollo, e quest'ultimi hanno la precedenza su quelli impostati sul livello di pacchetto.

È necessario avere il flusso di documenti elencato nella pagina Gestisci le definizioni del flusso di documenti prima di poter creare le interazioni.

Passaggio 2: Creare le interazioni

Creare le interazioni per i flussi 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 partecipante o Gestore comunità) e l'altro che descrive il documento inviato dall'hub (al partecipante o Gestore comunità). 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.

Passaggio 3: Creare profili partecipante, gateway e funzioni B2B

Creare profili di partecipante per Gestore comunità e per i partecipanti della comunità. Definire i gateway (che stabiliscono dove verranno inviati i documenti) e le funzioni B2B, che specificano i documenti che il Gestore comunità e i partecipanti sono in grado di inviare e ricevere. Nella pagina Funzioni B2B sono elencati tutti i flussi di documenti definiti.

È possibile impostare attributi sul livello delle funzioni B2B. Gli attributi impostati su questo livello sostituiscono quelli impostati sul livello della definizione di documenti. Ad esempio, se si imposta **Ora di notifica** su 30 a livello di definizione del flusso di documenti per un pacchetto AS, ma poi si imposta su 60 a livello di funzioni B2B, viene utilizzato il valore 60. L'impostazione di un attributo sul livello delle funzioni B2B consente di personalizzare l'attributo per uno specifico partecipante.

È necessario disporre di profili e di funzioni B2B del Gestore comunità e dei partecipanti definiti prima di poter creare connessioni tra loro.

Passaggio 4: Attivare le connessioni

Attivare le connessioni tra Gestore comunità e partecipanti. Le connessioni disponibili si basano sulle funzioni B2B dei partecipanti. Le funzioni B2B si basano sulle interazioni create. Le interazioni dipendono dalle definizioni di flusso di documenti disponibili.

Per alcuni scambi, viene richiesta una sola connessione. Se, ad esempio, un partecipante invia un documento binario ad un'applicazione back-end del Gestore comunità, è necessaria una sola connessione. Per lo scambio di scambi EDI in cui lo scambio viene sbustato e le singole transazioni trasformate, vengono impostate più connessioni.

Nota: Per gli scambi EDI trasmessi come tali, viene 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 **Ora di notifica** su 60 per il pacchetto AS2 a livello delle funzioni B2B, ma poi lo si imposta su 120, il valore utilizzato è 120. L'impostazione del valore di un attributo a livello di connessione consente di personalizzare ulteriormente l'attributo, in base ai requisiti di routing dei partecipanti e delle applicazioni coinvolte.

Un esempio di flusso

Per impostazione predefinita, sono abilitati molti metodi di impacchettamento. Per illustrare la procedura in generale per stabilire le definizioni di flusso di documenti, considerare il caso in cui si ha un accordo con un partecipante della comunità per ricevere uno scambio EDI che aderisca allo standard EDI-X12. Il partecipante invia il documento nell'impacchettamento AS2. Si specifica che lo scambio venga inviato senza trasformazione ad un'applicazione back-end, senza alcun impacchettamento.

1. Nella pagina Gestisci definizioni del flusso di documenti, verificare che la definizione del flusso dei documenti (che descrive il tipo di documento inviato nell'hub dal partecipante della comunità) sia abilitata.
 - a. Fare clic su **Ammin hub > Configurazione hub > Definizione di flusso di documenti**.
 - b. Fare clic sull'icona **Espandi** accanto a **Pacchetto: AS**. Si noti che **EDI-X12** è già elencato.
 - c. Fare clic sull'icona **Espandi** accanto a **Protocollo: EDI-X12**. Si noti che **Flusso di documenti: ISA** è già elencato.
2. Con la pagina Gestisci definizione di flusso di documenti ancora visualizzata, verificare che la seconda definizione di flusso di documenti (che descrive il tipo di documento che fluirà nell'applicazione back-end) sia abilitata.
 - a. Fare clic sull'icona **Espandi** accanto a **Pacchetto: Nessuno**. Si noti che **EDI-X12** è già elencato.
 - b. Fare clic sull'icona **Espandi** accanto a **Protocollo: EDI-X12**. Si noti che **Flusso di documenti: ISA** è già elencato.
3. Creare un'interazione che descrive se il flusso di documenti sarà un flusso di origine o un flusso di destinazione.
 - a. Con la pagina Gestisci definizione di flusso di documenti ancora visualizzata, fare clic su **Gestisci interazioni**.
 - b. Fare clic su **Crea interazione**.
 - c. Nella colonna Origine, espandere **Pacchetto: AS, Protocollo: EDI-X12 (TUTTI)**, quindi fare clic su **Flusso di documenti: ISA**.
 - d. Nella colonna Destinazione, espandere **Pacchetto: Nessuno, Protocollo: EDI-X12 (TUTTI)**, quindi fare clic su **Flusso di documenti: ISA**.
 - e. In questo esempio, non ha luogo alcuna trasformazione. Non selezionare, di conseguenza, nulla dall'elenco **Mappa di trasformazione**.
 - f. Dall'elenco **Azione**, selezionare **Passaggio autorizzato**.

g. Fare clic su **Salva**.

A questo punto, si specifica che l'hub è in grado di accettare scambi EDI-X12 (standard ISA) impacchettati con 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 trasformazione con lo scambio; si verifica il passaggio all'applicazione back-end (dopo aver rimosso le intestazioni AS).

Non è stato specificato il partecipante della comunità che è in grado di inviare questo tipo di scambio all'hub. Si definisce che viene impostato il profilo del partecipante e le funzioni B2B del partecipante. (Si definisce inoltre un profilo e le funzioni B2B per il sistema back-end di Gestore Comunità). Dopo aver eseguito queste attività, si crea una connessione tra il partecipante della comunità e l'applicazione back-end. In Figura 20 viene mostrata la connessione tra il partecipante e l'applicazione back-end del Gestore comunità per questo esempio.

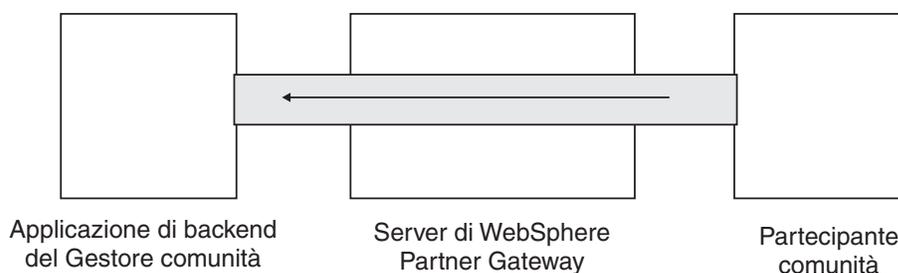


Figura 20. Una connessione monodirezionale da un partecipante al Gestore comunità

Si verifica che esiste una connessione mediante la pagina Gestisci connessioni (**Gestione account > Connessioni partecipante**). Nella pagina Gestisci connessioni, selezionare il partecipante dall'elenco **Origine**, Gestore comunità dall'elenco **Destinazione**, quindi fare clic su **Ricerca**. 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 flusso di documenti - quelle fornite con il sistema che è possibile selezionare dalla console, quelle già definite ma non definite nella Console comunità (è possibile caricare queste definizioni mediante l'installazione di WebSphere Partner Gateway o da un'altra posizione) e quelle create dall'utente. Per ogni tipo di definizione di flusso di documenti, è possibile (a volte è necessario) specificare attributi o caricare mappe che definiscano maggiormente il flusso di documenti.

Documenti binari

I documenti binari vengono trasmessi tramite l'hub come essi sono e, di conseguenza, lo scambio di documenti binari tra un partecipante della comunità ed un'applicazione back-end è un processo lineare. Il protocollo binario è già disponibile per i pacchetti AS, Nessuno e Integrazione backend; di conseguenza, "Passaggio 1: Assicurarsi che la definizione di flusso di documenti sia disponibile" a pagina 55 è già stato realizzato.

Nota: Si possono aggiungere attributi su qualsiasi livello (Pacchetto, Protocollo o Flusso di documenti) per modificare l'elaborazione predefinita facendo clic sull'icona **Modifica i valori dell'attributo**. Nessun attributo viene associato per impostazione predefinita al protocollo binario o al flusso di documenti.

Similmente, per impostazione predefinita vengono fornite quattro interazioni che coinvolgono documenti binari e per queste interazioni non è necessario che vengano eseguite. Passaggio 2: Creare le interazioni. Le interazioni vengono fornite per i seguenti scambi:

Tabella 4. Interazioni fornite dal sistema

Flusso di documenti del pacchetto/protocollo/documento di origine	Flusso di documenti del pacchetto/protocollo/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:

- Passaggio 3: Creare profili partecipante, gateway e funzioni B2B, che viene descritto in Capitolo 9, “Creazione del profilo Gestore comunità e delle funzioni B2B”, a pagina 123, Capitolo 11, “Creazione dei partecipanti e delle funzioni B2B”, a pagina 145 e Capitolo 10, “Creazione gateway”, a pagina 127.
- Passaggio 4: Attivare le connessioni, che viene descritto in Capitolo 12, “Gestione delle connessioni”, a pagina 149.

Documenti EDI con azione Pass-Through

WebSphere Partner Gateway fornisce la funzione di sbustare e trasformare gli scambi EDI, un processo descritto in Capitolo 8, “Configurazione dei flussi di documenti EDI”, a pagina 83.

In Figura 21 viene mostrato il flusso di uno scambio EDI trasmesso da un partecipante al Gestore comunità.

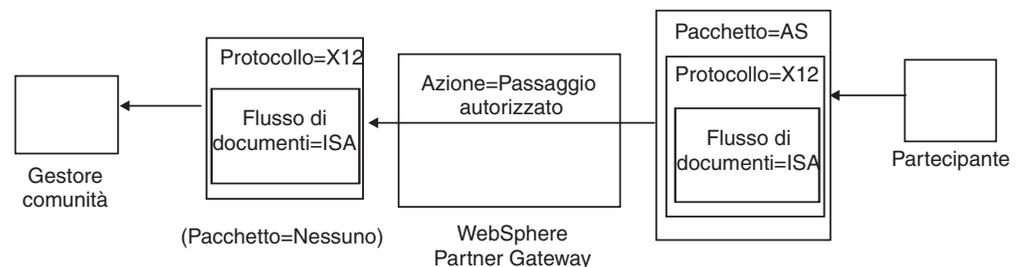


Figura 21. Interscambio EDI in entrata con azione Pass-Through

In questo esempio, vengono rimosse le intestazioni, altrimenti lo scambio viene lasciato intatto e fluisce attraverso il sistema al gateway del Gestore comunità.

Creazione delle definizioni di flusso di documenti

Il flusso di documenti per gli scambi passthrough EDI viene già fornito per impostazione predefinita nella pagina Gestisci definizioni di flusso di documenti, come descritto in “Un esempio di flusso” a pagina 57. Se si desidera modificare qualcuno degli attributi con i valori predefiniti o impostare un attributo che non dispone di un valore assegnato, è possibile utilizzare la pagina Gestisci definizioni del flusso di documenti per eseguire questa attività.

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 **Ammin hub > Configurazione hub > Definizione di flusso di documenti**.
2. Fare clic sull'icona **Modifica valori dell'attributo** accanto a **Pacchetto: AS**.
3. Scorrere verso il basso fino alla sezione della pagina intitolata **Attributi del contesto del flusso di documenti**.
4. Nella riga **ora per riconoscere**, digitare un valore differente nella colonna **Aggiorna**.
5. Fare clic su **Salva**.

In questo esempio, è stato modificato un attributo. Gli attributi del protocollo (ad esempio, EDI-X12) e flusso di documenti (ad esempio, ISA) non sono rilevanti per un'azione Pass Through. Questo attributo si applica a tutti i documenti compresi nell'impacchettamento AS.

Creazione interazioni

Per creare l'interazione per un interscambio EDI con l'azione Pass-Through, eseguire questi passi:

1. Fare clic su **Ammin hub > Configurazione hub > Definizione di flusso di documenti**.
2. Con la pagina Gestisci definizioni del flusso di documenti ancora visualizzata, fare clic su **Gestisci interazioni**.
3. Fare clic su **Crea interazione**.
4. In **Origine**, espandere **Pacchetto: AS** e **Protocollo: EDI-X12**, quindi selezionare **Flusso di documenti: ISA**.
5. In **Destinazione**, espandere **Pacchetto: Nessuno** e **Protocollo: EDI-X12**, quindi selezionare **Flusso di documenti: ISA**.
6. Dall'elenco **Azione**, selezionare **Passaggio autorizzato**.

I passaggi compresi tra 1 e 6 hanno abilitato WebSphere Partner Gateway ad accettare uno scambio EDI-X12 impacchettato come AS da un partecipante di origine, per inviare uno scambio EDI-X12 senza alcun impacchettamento al partecipante di destinazione e per far sì che avvenga il passaggio autorizzato dello scambio dall'origine alla destinazione.

Se si desidera impostare un'interazione che ha il documento di origine impacchettato come Nessuno/EDI-X12/ISA e quello di destinazione impacchettato come AS/EDI-X12/ISA, espandere **Pacchetto: Nessuno** nel passaggio 4 (nella colonna **Origine**) ed espandere **Pacchetto: AS** nel passaggio 5 (nella colonna **Destinazione**).

Documenti RosettaNet

In questa sezione, viene fornita una panoramica di documenti RosettaNet e mostrato come impostare le definizioni di flusso di documenti e le interazioni per quei documenti.

Panoramica

RosettaNet un'organizzazione che fornisce standard aperti per supportare lo scambio di messaggi aziendali tra partner commerciali. 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 in che modo i partner commerciali si scambiano i messaggi fornendo un framework di pacchetti di messaggi, protocolli di trasferimento e sicurezza. Ci sono due versioni emesse: 1.1 e 2.0. Un PIP definisce un processo aziendale 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 trasforma il messaggio da inviare al sistema di back-end appropriato. WebSphere Partner Gateway fornisce un protocollo per l'impacchettamento del messaggio trasformato 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 la Guida *Enterprise Integration*.

L'hub può inoltre ricevere i messaggi RNSC dai sistemi di back-end e creare il messaggio PIP appropriato e inviare il messaggio al partner commerciale appropriato (un partecipante). Fornire le definizioni del flusso di documenti per la versione RNIF e PIP da utilizzare.

Oltre a fornire la capacità di instradamento per i messaggi RosettaNet, WebSphere Partner Gateway conserva uno stato per ogni messaggio che gestisce. Questo lo abilita a reinviare i messaggi che hanno esito negativo fino a che il numero di tentativi raggiunge una soglia specificata. Il meccanismo di Notifica dell'evento avvisa i sistemi di back-end se un messaggio PIP non può essere recapitato. Inoltre, l'hub può automaticamente generare 0A1 PIP per inviare i partecipanti appropriati se riceve determinati messaggi di Notifica di eventi dai sistemi di back-end. Per ulteriori informazioni sulla notifica degli eventi, consultare la guida *Enterprise Integration*.

RNIF e pacchetti di flusso dei documenti PIP

Per supportare la messaggistica RosettaNet, WebSphere Partner Gateway fornisce due gruppi di file compressi denominati pacchetti. I *pacchetti RNIF* sono costituiti da definizioni del flusso di documenti richiesti per supportare il protocollo RNIF. Questi pacchetti sono nella directory B2BIntegrate.

Per RNIF V1.1, i pacchetti sono:

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

Per RNIF V02.00, i pacchetti sono:

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

Il primo pacchetto in ogni coppia fornisce le Definizioni di flusso di documenti necessarie per supportare le comunicazioni di RosettaNet con i partecipanti e il secondo pacchetto fornisce le Definizioni di flusso di documenti necessarie per supportare le comunicazioni di RosettaNet con i sistemi di back-end.

Il secondo gruppo di pacchetti comprende i pacchetti del flusso di documenti PIP. Ogni pacchetto del flusso di documenti PIP presenta una directory Packages che contiene un file XML e una directory GuidelineMaps che contiene i file XSD. Il file XML specifica le definizioni del flusso di documenti che definiscono in che modo WebSphere Partner Gateway gestisce il PIP e definisce i messaggi e i segnali

scambiati. I file XSD specificano il formato dei messaggi PIP e definiscono i valori accettabili per gli elementi XML nei messaggi. I file compressi per PIP 0A1 presentano anche un file XML che l'hub utilizza come modello per creare i documenti 0A1.

I PIP per i quali WebSphere Partner Gateway fornisce i pacchetti del flusso di documenti PIP sono:

- PIP 0A1 Notification of Failure v1.0
- PIP 0A1 Notification of Failure V02.00.00
- PIP 2A1 Distribute New Product Information V02.00.00
- PIP 2A12 Distribute Product Master V01.03.00
- PIP 3A1 Request Quote V02.00.00
- PIP 3A2 Request Price and Availability R02.01.00
- PIP 3A4 Request Purchase Order V02.02.00
- PIP 3A4 Request Purchase Order V02.00
- PIP 3A5 Query Order Status R02.00.00
- PIP 3A6 Distribute Order Status V02.02.00
- PIP 3A7 Notify of Purchase OrderUpdate V02.02.00
- PIP 3A8 Request Purchase Order Change V01.02.00
- PIP 3A8 Request Purchase Order Change V01.03.00
- PIP 3A9 Request Purchase Order Cancellation V01.01.00
- PIP 3B2 Notify of Advance Shipment V01.01.00
- PIP 3B3 Distribute Shipment Status R01.00.00
- PIP 3B11 Notify of Shipping Order R01.00.00A
- PIP 3B12 Request Shipping Order V01.01.00
- PIP 3B13 Notify of Shipping Order Confirmation V01.01.00
- PIP 3B14 Request Shipping Order Cancellation V01.00.00
- PIP 3B18 Notify of Shipping Documentation V01.00.00
- PIP 3C1 Return Product V01.00.00
- PIP 3C3 Notify of Invoice V01.01.00
- PIP 3C4 Notify of Invoice Reject V01.00.00
- PIP 3C6 Notify of Remittance Advice V01.00.00
- PIP 3C7 Notify of Self-Billing Invoice V01.00.00
- PIP 3D8 Distribute Work in Process V01.00.00
- PIP 4A1 Notify of Strategic Forecast V02.00.00
- PIP 4A3 Notify of Threshold Release Forecast V02.00.00
- PIP 4A4 Notify of Planning Release Forecast R02.00.00A
- PIP 4A5 Notify of Forecast Reply V02.00.00
- PIP 4B2 Notify of Shipment Receipt V01.00.00
- PIP 4B3 Notify of Consumption V01.00.00
- PIP 4C1 Distribute Inventory Report V02.03.00
- PIP 4C1 Distribute Inventory Report V02.01
- PIP 5C1 Distribute Product List V01.00.00
- PIP 5C2 Request Design Registration V01.00.00
- PIP 5C4 Distribute Registration Status V01.02.00
- PIP 5D1 Request Ship From Stock And Debit Authorization V01.00.00

- PIP 6C1 Query Service Entitlement V01.00.00
- PIP 6C2 Request Warranty Claim V01.00.00
- PIP 7B1 Distribute Work in Process V01.00.00
- PIP 7B5 Notify of Manufacturing Work Order V01.00.00
- PIP 7B6 Notify of Manufacturing Work Order Reply V01.00.00

Per ogni PIP, ci sono quattro Pacchetti di flusso di documenti PIP

- Per RNIF 1.1 messaggistica con i partecipanti
- Per RNIF 1.1 messaggistica con i sistemi di back-end
- Per RNIF 2.0 messaggistica con i partecipanti
- Per RNIF 2.0 messaggistica con i sistemi di back-end

Ogni pacchetto del flusso di documenti PIP segue una convenzione di denominazione specifica in modo che sia possibile identificare se il pacchetto è per i messaggi tra WebSphere Partner Gateway e i partecipanti o tra WebSphere Partner Gateway e i sistemi di back-end. La convenzione di denominazione identifica inoltre la versione RNIF, PIP, e la versione PIP che il pacchetto supporta. Per i pacchetti del flusso di documenti PIP utilizzati per la messaggistica tra WebSphere Partner Gateway e i partecipanti, il formato è:

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

Per i pacchetti del flusso di documenti PIP utilizzati per la messaggistica tra WebSphere Partner Gateway e i sistemi di back-end, il formato è:

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

Ad esempio, BCG_Package_RNIF1.1_3A4V02.02.zip è per la convalida dei documenti per la versione 02.02 del 3A4 PIP inviato tra i partecipanti e WebSphere Partner Gateway mediante il protocollo RNIF 1.1. Per i pacchetti del flusso di documenti PIP per la comunicazione con i sistemi di back-end, il nome del pacchetto deve inoltre identificare il protocollo utilizzato per inviare il contenuto di RosettaNet nei sistemi di back-end. Per ulteriori informazioni sull'impacchettamento utilizzato per questi messaggi, consultare la Guida *Enterprise Integration Guide*.

Creazione di definizioni di flusso di documenti

Per la messaggistica RosettaNet, WebSphere Partner Gateway richiede i pacchetti RNIF per la versione di RNIF utilizzata per inviare i messaggi. Per ciascun PIP che WebSphere Partner Gateway supporta, sono richiesti i due pacchetti di flusso dei documenti PIP per la versione RNIF. Ad esempio, per supportare il PIP 3A4 sul RNIF 2.0, WebSphere Partner Gateway richiede i seguenti pacchetti:

- 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 pacchetto supporta la messaggistica RosettaNet con i partecipanti e il secondo pacchetto supporta la messaggistica RosettaNet con i sistemi di back end. Il terzo e il quarto pacchetto abilitano WebSphere Partner Gateway a passare i messaggi 3A4 tra i partecipanti e i sistemi di back-end utilizzando RNIF 2.0.

Per caricare un pacchetto RosettaNet:

1. Fare clic su **Ammin hub > Configurazione hub > Definizione di flusso di documenti.**
2. Fare clic su **Carica/Scarica pacchetti.**
3. Selezionare **No** per **Pacchetto WSDL.**
4. Fare clic su **Sfoggia** e selezionare il pacchetto RNIF per la comunicazione con i partecipanti.
I pacchetti RNIF sono ubicati, per impostazione predefinita, nella directory B2BIntegrate/Rosettanet sul supporto di installazione. Se, ad esempio si stava caricando la versione RNIF del pacchetto 2.00, si dovrebbe sfogliare la directory B2BIntegrate/Rosettanet e scegliere: Package_RNIF_V0200.zip.
5. Accertarsi che **Salva nel database** sia impostato su **Sì.**
6. Fare clic su **Carica.**
7. Fare clic su **Sfoggia** di nuovo e selezionare il pacchetto RNIF per la comunicazione con le applicazioni back-end.
Se, ad esempio si stava caricando la versione 2.00 del pacchetto RNIF, si dovrebbe sfogliare la directory B2BIntegrate/Rosettanet e scegliere: Package_RNSC_V02.00.zip.
8. Fare clic su **Carica.**
I pacchetti necessari per comunicare con i partecipanti o con i sistemi di back-end sono ora installati nel sistema. Controllando la pagina Gestisci definizioni documento, viene visualizzata una voce **Pacchetto: RNIF/Protocollo: RosettaNet**, che rappresenta il pacchetto per comunicare con i partecipanti e **Pacchetto: Backend Integration/Protocollo: RNSC**, che rappresenta il pacchetto per comunicare con le applicazioni di back-end.
9. Per ciascun PIP che si desidera supportare, caricare il pacchetto del flusso di documenti PIP per il PIP e per la versione RNIF che si supporta. Ad esempio, per caricare il PIP 3A6 (Notify of Remittance Advice) da inviare ad un partecipante, eseguire questi passi:
 - a. Fare clic su **Sfoggia** e selezionare BCG_Package_RNIFV02.00_3C6V02.02 dalla directory B2BIntegrate/Rosettanet.
 - b. Accertarsi che **Salva nel database** sia impostato su **Sì.**
 - c. Fare clic su **Carica.**

Il PIP 3C6V02.02 ora appare come flusso di documenti sotto **Pacchetto:RNIF/Protocol:RosettaNet** nella pagina Gestisci definizioni 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 back-end, eseguire questi passaggi:

 - a. Fare clic su **Sfoggia** e selezionare BCG_Package_RNSC1.0_RNIFV02.00_3C6V02.02.zip.
 - b. Accertarsi che **Salva nel database** sia impostato su **Sì.**
 - c. Fare clic su **Carica.**

Il PIP 3C6V02.02 ora appare come flusso di documenti sotto **Pacchetto:Integrazione Backend:RNSC** nella pagina Gestisci definizioni documento. Se WebSphere Partner Gateway non fornisce un pacchetto per il PIP o la versione PIP che si desidera utilizzare, è possibile creare la propria e caricarla. Per ulteriori informazioni, vedere "Creazione di pacchetti di flusso di documenti PIP" a pagina 229.

Configurazione dei valori dell'attributo

Per le definizioni di flusso di documenti PIP, la maggior parte dei valori degli attributi è già impostata e non deve essere configurata. Tuttavia, non è necessario impostare i seguenti attributi:

Pacchetto RNIF (1.0)

- **GlobalSupplyChainCode** - Identificare il tipo di catena di fornitura utilizzata dal partecipante. I tipi sono produttori di Componenti elettronici, Information Technology e semiconduttori. Questo attributo non presenta un valore predefinito.

Pacchetto 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** - Impostare su sì se il partecipante desidera ricevere il riconoscimento di ricevuta. Impostare su No se è richiesto 200.
- **Sinc supportata** - Impostare se il PIP supporta gli scambi di messaggi sincroni. Il valore predefinito è No.

Si noti che i PIP per i quali WebSphere Partner Gateway fornisce i pacchetti del flusso di documenti PIP sono sincroni. Come risultato, non è necessario modificare gli attributi Ric sinc richiesto e Sinc supportato per questi PIP.

Nota: Il comportamento dell'attributo Ric sinc richiesto si differenzia dai PIP di 1 tipo e 2 tipi. Per un PIP a 2 modi, quando Ric sinc richiesto è impostato su No, questa impostazione ha la precedenza su NonRif dell'impostazione Ric di Sì. 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, si riceve un messaggio di errore sul documento in arrivo. Su un PIP di 1 tipo, tuttavia, si trova il documento in arrivo sulla console e un OKB 200 viene restituito al partecipante.

Per impostare gli attributi, effettuare questi passaggi:

1. Fare clic su **Ammin hub > Configurazione hub > Definizione di flusso di documenti**.
2. Fare clic sulle icone **Espandi** per espandere singolarmente un nodo a livello di flusso di definizione documenti appropriato o selezionare **Tutti** per espandere tutti i nodi delle definizioni del flusso documenti visualizzati.
3. Nella colonna **Azioni**, fare clic sull'icona **Modifica valori attributo** per il pacchetto (ad esempio, Pacchetto: RNIF (1.1) o Pacchetto: RNIF (V02.00)) che si desidera modificare.
4. Nella sezione **Attributi del contesto del flusso di documenti**, passare alla colonna **Aggiorna** dell'attributo da impostare e selezionare o immettere il nuovo valore. Ripetere per ogni attributo che si desidera impostare.
5. Fare clic su **Salva**.

Nota: È possibile anche aggiornare gli attributi RosettaNet sul livello della connessione facendo clic su **Attributi** per l'origine e la destinazione ed inserendo o modificando i valori nella colonna **Aggiornare**. Fare riferimento a "Specifica e modifica di attributi" a pagina 150.

Creazione di interazioni

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

Prima di iniziare, verificare che siano state caricate le definizioni del flusso di documenti appropriate, oltre ai pacchetti per il PIP da utilizzare. Se si desidera generare un PIP 0A1 (Notification of Failure), verificare di aver caricato quel PIP, come descritto al passo 9 a pagina 64.

Per creare un'interazione per un PIP in particolare, eseguire questi passaggi:

1. Fare clic su **Ammin hub > Configurazione hub > Definizione di flusso di documenti**.
2. Fare clic su **Gestisci interazioni**.
3. Fare clic su **Crea interazione**.
4. Espandere l'albero **Origine** al livello **Azione** ed espandere l'albero **Destinazione** al livello **Azione**.
5. Negli alberi, selezionare le definizioni di flusso di documenti da utilizzare per il contesto di origine e quello di destinazione. Se, ad esempio, il partecipante è l'iniziatore di un PIP 3C6 (un'unica azione PIP), selezionare la seguente definizione di flusso di documenti:

Tabella 5. 3C6 PIP iniziato da un partecipante

Origine	Destinazione
Pacchetto: RNIF (V02.00)	Pacchetto: Integrazione Backend (1.0)
Protocollo: RosettaNet (V02.00)	Protocollo: RNSC (1.0)
Flusso di documenti: 3C6 (V01.00)	Flusso di documenti: 3C6 (V01.00)
Attività: Notifica dell'avviso di rimessa	Attività: Notifica dell'avviso di rimessa
Azione: Azione della notifica dell'azione di rimessa	Azione: Remittance Advice Notification Action

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

Tabella 6. 3C6 PIP iniziato da un sistema di back-end

Origine	Destinazione
Pacchetto: Integrazione Backend (1.0)	Pacchetto: RNIF (V02.00)
Protocollo: RNSC (1.0)	Protocollo: RosettaNet (V02.00)
Flusso di documenti: 3C6 (V01.00)	Flusso di documenti: 3C6 (V01.00)
Attività: Notify of Remittance Advice	Attività: Notifica dell'avviso di rimessa
Azione: Azione della notifica dell'azione di rimessa	Azione: Azione della notifica dell'avviso di rimessa

Per un PIP a due azioni come 3A4 inizializzato da un partecipante, selezionare le seguenti definizioni di flusso di documenti per la prima azione:

Tabella 7. PIP 3A4 inizializzato da un partecipante

Origine	Destinazione
Pacchetto: RNIF (V02.00)	Pacchetto: Integrazione Backend (1.0)
Protocollo: RosettaNet (V02.00)	Protocollo: RNSC (1.0)
Flusso di documenti: 3A4 (V02.02)	Flusso di documenti: 3A4 (V02.02)
Attività: Richiesta di ordine di acquisto	Attività: Richiesta di ordine di acquisto
Azione: Azione della richiesta dell'ordine di acquisto	Azione: Azione della richiesta dell'ordine di acquisto

Se un sistema di back-end inizia le due azioni PIP 3A4, selezionare le seguenti definizioni di flusso di documenti per la prima azione:

Tabella 8. PIP 3A4 inizializzato da un sistema di back-end

Origine	Destinazione
Pacchetto: Integrazione Backend (1.0)	Pacchetto: RNIF (V02.00)
Protocollo: RNSC (1.0)	Protocollo: RosettaNet (V02.00)
Flusso di documenti: 3A4 (V02.02)	Flusso di documenti: 3A4 (V02.02)
Attività: Richiesta di ordine di acquisto	Attività: Richiesta di ordine di acquisto
Azione: Azione della richiesta dell'ordine di acquisto	Azione: Azione della richiesta dell'ordine di acquisto

6. Nel campo Azione, selezionare **Traslazione bidirezionale di RosettaNet e contenuto del servizio di RosettaNet con convalida**.

7. Fare clic su **Salva**.

8. Se si imposta un PIP di due azioni, ripetere i passaggi necessari per creare l'interazione per la seconda azione. Selezionare, ad esempio, le seguenti definizioni di flusso di documenti per la seconda azione per un PIP 3A4 inizializzato da un partecipante. Questa è l'azione nella quale il sistema di back-end invia la risposta.

Tabella 9. 3A4 PIP inizializzato da un partecipante (seconda azione)

Origine	Destinazione
Pacchetto: Integrazione Backend (1.0)	Pacchetto: RNIF (V02.00)
Protocollo: RNSC (1.0)	Protocollo: RosettaNet (V02.00)
Flusso di documenti: 3A4 (V02.02)	Flusso di documenti: 3A4 (V02.02)
Attività: Richiesta di ordine di acquisto	Attività: Richiesta di ordine di acquisto
Azione: Azione di conferma dell'ordine di acquisto	Azione: Azione di conferma dell'ordine di acquisto

Per la seconda azione per un sistema di back-end inizializzato PIP 3A4, selezionare le seguenti definizioni del flusso di documenti:

Tabella 10. PIP 3A4 inizializzato da un sistema di back-end (seconda azione)

Origine	Destinazione
Pacchetto: RNIF (V02.00)	Pacchetto: Integrazione Backend (1.0)
Protocollo: RosettaNet (V02.00)	Protocollo: RNSC (1.0)
Flusso di documenti: 3A4 (V02.02)	Flusso di documenti: 3A4 (V02.02)
Attività: Richiesta di ordine di acquisto	Attività: Richiesta di ordine di acquisto

Tabella 10. PIP 3A4 inizializzato da un sistema di back-end (seconda azione) (Continua)

Origine	Destinazione
Azione: Azione di conferma dell'ordine di acquisto	Azione: Azione di conferma dell'ordine di acquisto

9. Se si desidera generare una notifica di errore 0A1, creare un'interazione per XMLEvent.
 - a. Fare clic su **Ammin hub > Configurazione hub > Definizione di flusso di documenti**.
 - b. Fare clic su **Gestisci interazioni**.
 - c. Fare clic su **Crea interazione**.
 - d. Espandere l'albero **Origine** al livello **Flusso di documenti** ed espandere l'albero **Destinazione** al livello **Flusso di documenti**.
 - e. Selezionare le seguenti definizioni di flusso di documenti:

Tabella 11. Definizione di flusso di documenti XML Event

Origine	Destinazione
Pacchetto: Integrazione Backend (1.0)	Pacchetto: Integrazione Backend (1.0)
Protocollo: XMLEvent (1.0)	Protocollo: XMLEvent (1.0)
Flusso di documenti: XMLEvent (1.0)	Flusso di documenti: XMLEvent (1.0)

- f. Nel campo Azione, selezionare **Pass Through**.
 - g. Fare clic su **Salva**.
10. Creare un'interazione per XMLEvent per 0A1 RNSC.
 - a. Fare clic su **Ammin hub > Configurazione hub > Definizione di flusso di documenti**.
 - b. Fare clic su **Gestisci interazioni**.
 - c. Fare clic su **Crea interazione**.
 - d. Espandere l'albero **Origine** al livello **Flusso di documenti** ed espandere l'albero **Destinazione** al livello **Attività**.
 - e. Selezionare le seguenti definizioni di flusso di documenti:

Tabella 12. Definizione di flusso di documenti fXML Event per 0A1

Origine	Destinazione
Pacchetto: Integrazione Backend (1.0)	Pacchetto: Integrazione Backend (1.0)
Protocollo: XMLEvent (1.0)	Protocollo: RNSC (1.0)
Flusso di documenti: XMLEvent (1.0)	Flusso di documenti: 0A1 (V02.00)
	Attività: Notifica di errore di distribuzione.

- f. Nel campo Azione, selezionare **Traslazione bidirezionale di RosettaNet con convalida XML**.
 - g. Fare clic su **Salva**.

Servizi Web

Un partecipante può richiedere un servizio Web fornito dal Gestore comunità. Allo stesso modo, il Gestore comunità può richiedere un servizio Web fornito da un partecipante. Il partecipante o il Gestore comunità richiama il server WebSphere Partner Gateway per ottenere il servizio Web. 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 l'impostazione di un servizio Web per l'utilizzo da parte di un partecipante o un Gestore comunità:

- Identificazione dei partecipanti per il servizio web
- Impostazione di una definizione del flusso di documenti per un servizio web.
- Aggiunta delle definizioni del flusso di documenti per le funzioni B2B del partecipante
- Restrizioni e limitazioni del supporto del servizio Web

Identificazione dei partecipanti per un servizio Web

Quando un servizio Web viene fornito dal Gestore comunità per essere utilizzato dai partecipanti, WebSphere Partner Gateway richiede l'identificazione di un partecipante. Quando si invia la richiesta del servizio Web, impostare l'identità in uno dei seguenti modi:

1. Utilizzare l'autenticazione di base HTTP con l'ID utente in formato `<participant's_business_ID>/<console_user_name>` (ad esempio, `123456789/joesmith`) e una password uguale alla password del nome utente della console.
2. Presentare un certificato client SSL che è stato precedentemente caricato in WebSphere Partner Gateway per il partecipante

Quando viene fornito un servizio web da un partecipante, per l'utilizzo mediante il Gestore comunità, l'URL pubblico utilizzato dal Gestore comunità per richiamare il servizio web deve contenere la stringa di query `?to=<participant's_business_ID>`. Un esempio è:

```
http://<IP_address>/bcgreceiver/Receiver?to=123456789
```

Ciò indica a WebSphere Partner Gateway che il provider del servizio web è il partecipante con l'ID aziendale 123456789.

Creazione di definizioni di flusso di documenti

Per impostare la definizione di flusso di documenti, si caricano i file WSDL (Web Service Definition Language) che definiscono il servizio Web, oppure si immettono le definizioni di flusso di documenti manualmente tramite la Console comunità.

Caricamento dei file WSDL per un servizio Web

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"/>
```

E si supponga che il file WSDL importato `bindingRPC.wsdl` contenga il seguente elemento di importazione:

```
<import namespace="http://www.helloworld.com/wsdl/helloRPC.wsdl" location="port/porttypeRPC.wsdl"/>
```

Il file deve contenere quanto segue:

Nome	Percorso
<code>helloworldRPC.wsdl</code>	
<code>bindingRPC.wsdl</code>	
<code>porttypeRPC.wsdl</code>	<code>porta\</code>

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 da WebSphere Partner Gateway. Vengono passati direttamente, con l'URL di endpoint del servizio originale). Questo viene chiamato WSDL *privato*.

Inoltre, un WSDL viene salvato con l'URL privato sostituito dall'URL di destinazione specificato nella pagina Carica/scarica pacchetti. Il WSDL pubblico viene fornito agli utenti del servizio Web che invocano il servizio Web sull'URL di destinazione (URL pubblico). WebSphere Partner Gateway instrada quindi la richiesta del servizio Web in un gateway che è l'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: I 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 **Ammin hub > Configurazione hub > Definizione flusso di documenti**.
2. Fare clic su **Carica/Scarica pacchetti**.
3. Per **Pacchetto WSDL** fare clic su **Sì**.
4. Per **URL pubblico del servizio Web**, eseguire uno di seguenti passaggi:
 - Per un servizio Web fornito da Gestore comunità (che viene richiamato da un partecipante), inserire 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 un partecipante (che viene richiamato dal Gestore comunità), inserire l'URL pubblico del partecipante con una stringa della query. Ad esempio:
`https://<target_host:port>/bcgreceiver/Receiver?to=<participant_business_ID>`
5. Fare clic su **Sfoggia** 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 pacchetti 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`, `ewsdsoap.xsd`, che contengono lo schema che descrive il file di WSDL (Web Service Definition Language).

I file vengono posizionati in: `B2BIntegrate\packagingSchemas`

Creazione della definizione di flusso di documenti manualmente

Per immettere manualmente le definizioni del flusso di documenti, seguire le procedure illustrate in questa sezione. Inoltre, è necessario creare le voci Flusso di documenti, 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 di gerarchia di Pacchetto/Protocollo/Flusso di documenti/Attività/Azione delle Definizioni del flusso di documenti, viene rappresentato un servizio Web supportato come:

- **Pacchetto: Nessuno**
- **Protocollo: servizio web (1.0)**

- **Flusso di documenti:** {<Web_service_namespace>:<Web_service_name>} (nome e codice), ce è richiesto come univoco tra i flussi di documenti per il protocollo del 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 = first_child_of_soap:body>:
<name_of_identifying_xml_element = 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 partecipante definita. Lo spazio dei nomi e il nome del primo elemento XML child dell'elemento del messaggio SOAP ricevuto soap:body deve corrispondere al uno spazio dei nomi e nome dell'Azione nota nelle definizioni del flusso di documenti 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 interazioni

Per creare un'interazione per un servizio Web, si utilizza la stessa azione del flusso di documenti del servizio Web per l'origine e la destinazione.

Per creare le interazioni, utilizzare la seguente procedura.

1. Fare clic su **Ammin hub > Configurazione hub > Definizione flusso di documenti**.
2. Fare clic su **Gestisci interazioni**.
3. Fare clic su **Crea interazione**.
4. In **Origine**, espandere **Pacchetto: Nessuno > Protocollo: servizio web > Flusso di documenti: <flusso di documenti>** > **Azione: <azione>**. Ripetere questo 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:

- 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).
- Soap con allegati non è supportato.

documenti cXML

In questa sezione, è contenuta una panoramica sul supporto cXML e le informazioni sulla creazione di definizioni di flusso di documenti per gli scambi cXML.

Panoramica

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 la versione cXML 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. Dopo aver caricato il DTD, associarlo al flusso di documenti cXML. Fare riferimento a "Associazione delle mappe alle definizioni di flusso di documenti" a pagina 81 per ulteriori informazioni sull'associazione del DTD con il flusso di documenti cXML.

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: Qui e 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 aziendale 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 Flusso di documenti in WebSphere Partner Gateway. Gli elementi tipici della richiesta sono:

- OrderRequest
- ProfileRequest
- PunchOutSetupRequest
- StatusUpdateRequest
- GetPendingRequest
- ConfirmationRequest
- ShipNoticeRequest

La seguente tabella mostra la relazione tra gli elementi in un documento di richiesta cXML e le definizioni di flusso di documenti in WebSphere Partner Gateway:

Elemento cXML	Definizione del flusso di documenti
cXML DOCTYPE	Protocollo
Versione DTD	Versione del protocollo
Richiesta (tipo) Ad esempio, OrderRequest	Flusso di documenti

Risposta: Il partecipante di destinazione invia a una risposta cXML per informare il partecipante 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 mostra la relazione tra gli elementi in un documento di richiesta cXML e le definizioni di flusso di documenti in WebSphere Partner Gateway:

Elemento cXML	Definizione del flusso di documenti
cXML DOCTYPE	Protocollo
Versione DTD	Versione del protocollo
Risposta (tipo) Ad esempio, ProfileResponse	Flusso di documenti

Messaggio: Un messaggio cXML contiene le informazioni sul flusso di documenti di WebSphere Partner Gateway nell'elemento Messaggio cXML. Può contenere un elemento Stato facoltativo identico a quello trovato nell'elemento Risposta. Può essere utilizzato nei messaggi che sono risposte ai messaggi di richiesta.

Il contenuto del messaggio è personale e definito dalle esigenze commerciali dell'utente. L'elemento direttamente in basso all'elemento <Messaggio> corrisponde

al flusso di documenti creato in WebSphere Partner Gateway. Nel seguente esempio, SubscriptionChangeMessage è il flusso di documenti:

```
<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 la relazione tra gli elementi in un messaggio cXML e le definizioni di flusso di documenti in WebSphere Partner Gateway:

Elemento cXML	Definizione del flusso di documenti
cXML DOCTYPE	Protocollo
Versione DTD	Versione del protocollo
Messaggio	Flusso di documenti

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 Messaggio invece di un elemento di richiesta o risposta.

Un messaggio può avere i seguenti attributi:

- deploymentMode, che indica 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 di definizione di flusso di documenti cXML:

- Dal partecipante al Gestore comunità: da Nessuno/cXML a Nessuno/cXML con Pass-Through e convalida
- Da Gestore comunità al partecipante:
 - Nessuno/cXML a Nessuno/cXML con Pass Through e convalida
 - Nessuno/XML a Nessuno/cXML con Pass Through, convalida e trasformazione

Creazione delle definizioni del flusso di documenti

Utilizzare il seguente processo per creare una nuova definizione di flusso di documenti per un documento cXML.

Nota: Accertarsi che la versione corretta del cXML sia definita prima di creare una definizione di flusso di documenti cXML. Quella predefinita è la versione 1.2.009.

1. Fare clic su **Ammin hub > Configurazione hub > Definizione flusso di documenti**.
 2. Fare clic su **Crea definizione di flusso di documenti**. Viene visualizzata la pagina Crea le definizioni del flusso di documenti.
 3. Selezionare **Flusso di documenti** per il tipo di flusso di documenti.
 4. Eseguire una delle attività riportate, in base al tipo di documento:
 - Per le richieste, immettere il tipo di richiesta (ad esempio, OrderRequest) nei campi **Codice** e **Nome**.
 - Per le risposte, se la Risposta non dispone di tag child diverse da <Stato>, immettere Risposta. Altrimenti, immettere il nome del tag successivo rispetto a <Stato>. Nel seguente esempio, immettere Risposta per il primo elemento di Risposta e Riposta profilo 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 **Pacchetto: Nessuno** per espandere le opzioni di selezione del pacchetto.
  11. Selezionare **Protocollo: cXML (1.2.009): cXML**.
  12. Fare clic su **Salva**.

## Creazione interazioni

Dopo aver creato la definizione di flusso di documenti, impostare un'interazione per il documento cXML.

Per creare le interazioni, utilizzare la seguente procedura.

1. Fare clic su **Ammin hub > Configurazione hub > Definizione flusso di documenti**.
2. Fare clic su **Gestisci interazioni**.
3. Fare clic su **Crea interazione**.
4. Se un documento cXML è l'origine, in **Origine**, espandere **Pacchetto: Nessuno e Protocollo: cXML**, quindi selezionare **Flusso di documenti: <document\_flow>**. Se il documento cXML è la destinazione, espandere **Pacchetto: Nessuno e Protocollo: cXML**, quindi selezionare **Flusso di documenti: <document\_flow>** nella colonna **Destinazione**.
5. Espandere la colonna origine o destinazione per l'altra metà dell'interazione (il documento che verrà convertito in cXML o il documento che verrà trasformato da cXML) ed espandere il pacchetto e il protocollo e selezionare il flusso di documenti.
6. Selezionare **Pass Through** dall'elenco **Azione** in basso nella pagina. (**Pass Through** è l'unica opzione valida supportata per i documenti cXML).

---

## Documenti XML personalizzati

In questa sezione, viene descritto come creare documenti XML personalizzati.

### Panoramica

XML (Extensible Markup Language) è il formato universale per i documenti strutturati e i dati sul Web. Utilizzando la pagina Gestisci protocolli XML, è possibile creare e gestire formati XML personalizzati che è possibile aggiungere all'elenco di definizioni del flusso di documenti disponibili.

Un formato XML definisce i percorsi in un gruppo di documenti XML. Questo consente al Gestore documenti di recuperare i valori che unicamente identificano un documento in entrata e accedono alle informazioni in gestore documenti necessarie per un corretto instradamento ed elaborazione.

La creazione di un formato XML è un processo multifase. È necessario:

1. Creare un protocollo per il formato e associarlo ad uno o più pacchetti
2. Creare un flusso di documenti per il formato e associarlo al protocollo recentemente creato
3. Creare il formato

Si crea quindi una valida interazione per il formato recentemente creato.

Queste procedure vengono descritte nelle sezioni che seguono. È possibile trovare un esempio di queste procedure in "Impostazione dell'hub per i documenti XML personalizzati" a pagina 190.

### Creazione del formato di definizione di un protocollo

I seguenti passaggi descrivono come creare un formato di definizione del protocollo XML:

1. Fare clic su **Admin hub > Configurazione hub > Definizione flusso documenti > Crea definizione flusso documenti**.
2. Per **Tipo di flusso di documenti**, selezionare **Protocollo**.
3. Per **Codice**, immettere il valore per il tipo di oggetto selezionato al passo precedente. Ad esempio, è possibile inserire l'XML.
4. Per **Nome**, inserire un identificativo per la definizione del flusso di documenti. Ad esempio, per un protocollo XML personalizzato, è possibile inserire un XML\_personalizzato. Questo campo è obbligatorio.
5. Per **Versione**, inserire **1.0**.
6. Inserire una descrizione facoltativa del protocollo.
7. Impostare **Livello documento** su **No**, poiché si definisce un protocollo, piuttosto che un flusso di documenti (che verrà definito nella sezione successiva).
8. Impostare **Stato** su **Abilitato**.
9. Impostare **Visibilità** per questo protocollo. Si desidera probabilmente essere visibile a tutti i partecipanti.
10. Selezionare i pacchetti nei quali questo nuovo protocollo viene incluso. Ad esempio, se si desidera associare questo protocollo con i pacchetti AS, Nessuno e Integrazione di back-end, selezionare **Pacchetto: AS, Pacchetto: Nessuno, Pacchetto: Integrazione di back-end**.
11. Fare clic su **Salva**.

## Creazione di un flusso di definizione di documenti

In seguito, utilizzare la pagina Crea definizione di flusso di documenti per creare nuovamente un flusso di documenti.

1. Fare clic su **Admin hub > Configurazione hub > Definizione flusso documenti > Crea definizione flusso documenti**.
2. Per **tipo flusso di documenti**, selezionare **Flusso di documenti**.
3. Per **Codice**, immettere il valore per il tipo di oggetto (flusso di documenti) selezionato nel passaggio precedente.
4. Per **Nome**, inserire un identificativo per la definizione del flusso di documenti. Ad esempio, è possibile inserire XML\_Tester come un nome per il flusso di documenti. Questo campo è obbligatorio.
5. Per **Versione**, inserire **1.0**.
6. Inserire una descrizione facoltativa del protocollo.
7. Impostare **Livello documento** su **Sì** (poiché si definisce un livello di documento).
8. Impostare **Stato** in **Abilitato**.
9. Impostare **Visibilità** per questo flusso. Probabilmente si vuole renderlo visibile a tutti i partecipanti.
10. Fare clic sull'icona **Espandi** per espandere ciascun pacchetto selezionato al passo 10. Ingrandire la cartella e selezionare il nome del protocollo creato nella sezione precedente (ad esempio, Protocollo: CustomXML.).
11. Fare clic su **Salva**.

Nella pagina Gestisci definizioni del flusso di documenti ora sono contenuti un flusso di documenti di XML\_Tester e un protocollo di CustomXML sotto pacchetti AS, Nessuno e Integrazione Backend.

## Creazione di un formato XML

Dopo la creazione di un protocollo XML personalizzato (e l'associazione con un pacchetto o una serie di pacchetti) e la creazione di un flusso di documento associato, si è pronti per creare il formato XML.

Per creare un formato XML, utilizzare la seguente procedura.

1. Fare clic su **Ammin hub > Configurazione hub >Formati XML**.
2. Fare clic su **Crea formato XML**.
3. Per **Formato di instradamento**, selezionare la definizione del flusso di documenti con il quale questo formato viene associato.
4. Per **Tipo di file**, selezionare **XML**.

**Nota:** L'XML è l'unica opzione disponibile per il tipo di file.

5. Per **Tipo identificativo**, selezionare l'elemento utilizzato per identificare il tipo di documento in arrivo. Le scelte sono **DTD**, **Spazio nome**, o **Tag root**.
6. Per ogni campo per il quale una scelta dei tipi viene offerta, selezionare **Percorso elemento**, che è il percorso nel valore nel documento o **Costante**, che il valore effettivo nel documento. Quindi fornire un valore.
  - a. Per **ID aziendale origine/destinazione**, inserire il percorso dell'ID aziendale. Questo campo è obbligatorio.
  - b. Per **Flusso di documenti di origine & Versione**, inserire un'espressione che definisce il percorso nel Flusso di documenti e il valore della versione nel documento XML. Questo campo è obbligatorio.
  - c. Per **Identificativo documento**, inserire il percorso per il numero ID del documento.
  - d. Per **Data e ora documento**, inserire il percorso per la data e ora di creazione del documento.
  - e. Per **Chiave di verifica duplicata 1-5**, inserire i percorsi utilizzati per identificare l'instradamento di un documento duplicato.
7. Fare clic su **Salva**.

---

## 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".

## Aggiunta mappe di convalida

Un'azione può avere una mappa di convalida associata per garantire che il partecipante di destinazione o il sistema di back-end possano 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 la mappa di convalida a una definizione di flusso di documenti, non è possibile dissociarli.

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 **Ammin 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 flusso di documenti

Per associare una mappa di convalida ad una definizione di flusso di documenti, utilizzare la seguente procedura.

1. Fare clic su **Ammin hub > configurazione hub > Mappe > Mappe di convalida**.
2. Fare clic sull'icona **Visualizza i dettagli** accanto alla mappa di convalida che si desidera associare alla definizione di flusso di documenti.
3. Fare clic sull'icona **Espandi** accanto a un pacchetto per espanderlo singolarmente al livello appropriato (ad esempio **Azione** per un documento RosettaNet).
4. Selezionare la definizione di flusso di documenti che si desidera associare alla mappa di convalida.
5. Fare clic su **Salva**.

---

## Visualizzazione dei documenti

Il visualizzatore di documenti visualizza informazioni sui documenti che costituiscono un flusso di documenti. E' possibile visualizzare i documenti raw e i dettagli e gli eventi di elaborazione associati utilizzando criteri di ricerca specifici. Queste informazioni sono utili se si prova a determinare se un documento è stato recapitato correttamente o determinare la causa di un eventuale problema.

Per visualizzare il Visualizzatore di documenti, fare clic su **Visualizzatori > Visualizzatore di documenti**. Per informazioni sull'utilizzo del Visualizzatore di documenti, consultare il manuale *Administrator Guide*.



---

## Capitolo 8. Configurazione dei flussi di documenti EDI

In questo capitolo, viene descritto come configurare le definizioni di flusso di documenti e le interazioni per gli scambi EDI standard. In questo capitolo sono incluse le descrizioni di ricezione e la trasformazione dei documenti ROD (record-oriented-data). In questo capitolo, vengono descritti i seguenti argomenti:

- “Panoramica su EDI”
- “Panoramica dei documenti XML e ROD” a pagina 86
- “Panoramica sulla creazione di flussi di documenti ed impostazione degli attributi” a pagina 87
- “Panoramica sui flussi possibili” a pagina 89
- “Modalità di elaborazione degli interscambi EDI” a pagina 94
- “Modalità di elaborazione dei documenti XML o ROD” a pagina 97
- “Impostazione dell’ambiente EDI” a pagina 97
- “Passaggi generali per la definizione di scambio di documenti” a pagina 110
- “Visualizzazione di interscambi e transazioni EDI” a pagina 122

È, inoltre, possibile disporre di uno scambio EDI trasmesso senza alcun sbustamento o trasformazione. I passaggi per la creazione delle interazioni per questo tipo di scambio vengono rappresentati in “Documenti EDI con azione Pass-Through” a pagina 59.

---

### 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 lo sbustamento, la trasformazione e l’imbustamento 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 trasformati i documenti XML e ROD e gli interscambi EDI.

### Struttura dell’interscambio EDI

Uno scambio EDI contiene una o più transazioni aziendali. 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 aziendale* 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.

Un interscambio dispone sempre di un segmento di intestazione dell'interscambio 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 aziendale, come ad esempio un ordine di acquisto. Il contenuto del documento aziendale 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 13. 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
Fine transazione	SE	SE	UNT

In Figura 22 a pagina 85 viene mostrato un esempio di uno scambio X12 e i segmenti che costituiscono lo scambio.

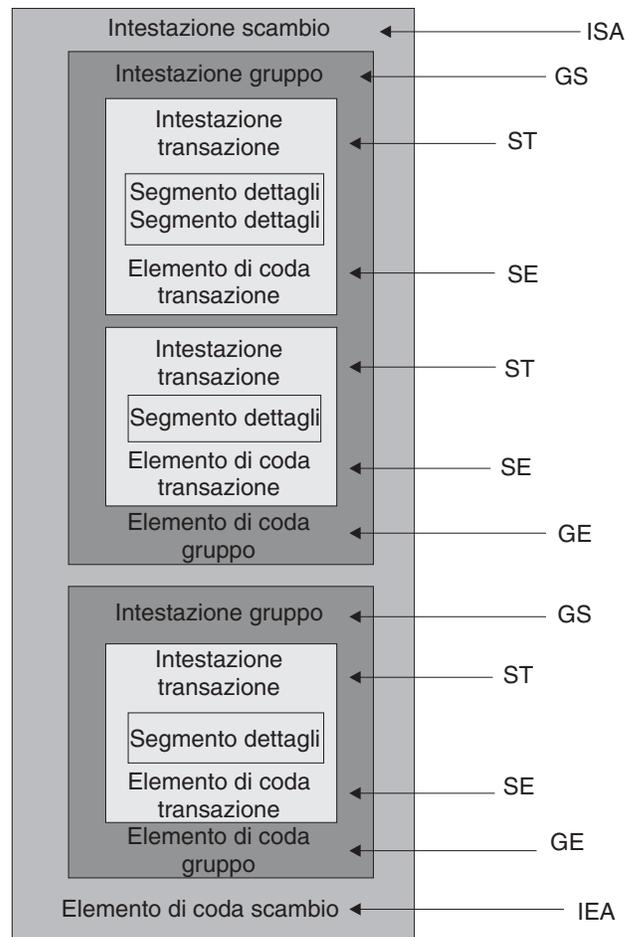


Figura 22. Una busta dello scambio

## Mappe

Lo specialista della mappa del client Data Interchange Services crea mappe di trasformazione che descrivono come modificare un documento di un formato in un altro documento di un formato differente. E' possibile, ad esempio, disporre di una mappa di trasformazione che modifica una transazione X12 in un messaggio EDIFACT. È possibile anche trasformare una transazione EDI in un documento XML o in un documento dati ROD (record-oriented data).

La mappa di trasformazione 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 "Riconoscimenti funzionali" a pagina 120. Le mappe di riconoscimento funzionale possono essere create dallo specialista della mappatura del client Data Interchange Services. WebSphere Partner Gateway genera una notifica funzionale quando viene convalidata una transazione EDI e quando tale transazione dispone di una mappa di notifica 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 una notifica funzionale utilizza la mappa di notifica funzionale e i risultati della convalida del documento EDI. La mappa di notifica 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 trasformazione 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 trasformazione 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 trasformazione basata sulla definizione DTD o sullo schema che descrive come convertire il documento XML in un altro formato. Un documento XML può essere trasformato 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 trasformare il documento ROD in un altro documento ROD, un documento XML o una transazione EDI.

### Separatori e più documenti

I documenti XML o ROD possono inserire l'hub come documento singolo o come gruppo di documenti nello stesso file. Più documenti potrebbero essere inseriti nello stesso file quando, ad esempio, un lavoro pianificato sul partecipante o Gestore comunità carica periodicamente i documenti inviati. Se più documenti XML o ROD arrivano in un solo file, il Destinatario chiama il gestore splitter associato (XMLSplitterHandler o RODSplitterHandler) per dividere il gruppo di documenti. (I gestori splitter vengono configurati quando si crea una destinazione). Per informazioni, vedere "Preprocesso" a pagina 44). 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 trasformazione. Le informazioni necessarie per stabilire il tipo di documento e 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 trasformazione.

Inoltre, è possibile inviare più interscambi EDI in un singolo file. Se arrivano più interscambi EDI in un file, il Destinatario richiama EDISplitterHandler per separare la serie di interscambi. Gli interscambi vengono reintrodotti nel Gestore documenti per essere elaborati singolarmente.

**Nota:** La separazione viene eseguita sull'interscambio, non sulle singole transazioni all'interno dell'interscambio. Le transazioni all'interno dell'interscambio vengono sbustate.

---

## **Panoramica sulla creazione di flussi di documenti ed impostazione degli attributi**

Una definizione di flusso di documenti è formata al minimo, di un pacchetto, di un protocollo e di un flusso di documenti. Le definizioni di flusso di documenti specificano i tipi di documenti che verranno elaborati da WebSphere Partner Gateway.

L'impacchettamento fa riferimento alla logica richiesta per assemblare 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 flusso di documenti descrive come deve essere il documento.

Nelle sezioni successive vengono illustrati i passaggi, in generale, per l'impostazione di un flusso di documenti tra Gestore comunità ed un partecipante. Inoltre, in queste sezioni vengono descritti i punti in cui è possibile impostare gli attributi.

### **Passaggio 1: Assicurarsi che la definizione di flusso di documenti sia disponibile**

Prima di poter inviare o ricevere un documento, è necessario definire una definizione di flusso di documenti per il documento. WebSphere Partner Gateway fornisce molte definizioni di flusso di documenti, incluse quelle che rappresentano i riconoscimenti funzionali. Quando si importano mappe di trasformazione per le transazioni EDI o i documenti XML ROD, le definizioni del flusso di documenti associate vengono visualizzate nella pagina Definizioni di flusso di documenti. Similmente, se si importa una mappa di riconoscimento funzionale che non è stata definita, la definizione di flusso di documenti per il riconoscimento appare nella pagina Definizioni di flussi di documenti. È, inoltre, possibile creare definizioni di flusso di documenti.

Come parte di come stabilire una definizione di flusso di documenti, è possibile modificare alcuni attributi. Gli attributi utilizzati per eseguire varie funzioni di elaborazione e routing dei documenti, come ad esempio la convalida, la verifica della codifica e il conteggio tentativi. Gli attributi impostati sul livello di definizione di flusso di documenti forniscono un'impostazione globale per il pacchetto, protocollo o flusso di documenti associato. Gli attributi disponibili

variano, a seconda della definizione di flusso di documenti. Gli attributi per le definizioni del documento EDI hanno attributi differenti per le definizioni di flusso di documento RosettaNet.

Ad esempio, se si specifica un valore per l'attributo **consenti una richiesta TA1** a livello di flusso del documento ISA, l'impostazione si applica a tutti i documenti ISA. Se, in seguito si imposta **Consenti un attributo TA1** livello delle funzioni B2B, quell'impostazione sostituisce quella impostata sul livello del flusso di documenti.

Per gli attributi che è possibile impostare su più livelli della definizione di flusso di documenti, i valori impostati del flusso di documenti hanno la precedenza su quelli impostati sul livello del protocollo, e quest'ultimi hanno la precedenza su quelli impostati sul livello di pacchetto. Se, ad esempio, si specifica un profilo busta sul livello di protocollo &X44TA1 ma si specifica un profilo busta differente sul livello di flusso di documenti TA1, si utilizza il profilo busta specificato sul livello di flusso di documenti TA1.

È necessario avere il flusso di documenti elencato nella pagina Gestisci le definizioni del flusso di documenti prima di poter creare le interazioni.

## Passaggio 2: Creare le interazioni

Quindi, vengono configurate le interazioni, ovvero maschere per la creazione di connessioni del partecipante. 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 partecipante o Gestore comunità) e l'altro che descrive il documento inviato dall'hub (al partecipante o Gestore comunità). Se, tuttavia, l'hub invia o riceve uno scambio EDI che verrà sbustato in singole transazioni o in cui sono richiesti i riconoscimenti, verranno create effettivamente più interazioni. Ad esempio, se si riceve un interscambio EDI all'hub, l'interazione descrive il modo in cui l'interscambio 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 interscambi EDI che lasciano l'hub, l'interazione descrive il modo in cui la busta dell'interscambio viene inviata al destinatario.

## Passaggio 3: Creare profili partecipante, gateway e funzioni B2B

Creare, in seguito, profili di partecipante per Gestore comunità e per i partecipanti della comunità. Si definiscono i gateway (che stabiliscono dove verranno inviati i documenti) e le funzioni B2B, che specificano i documenti che il Gestore comunità o i partecipanti sono in grado di inviare e ricevere. Nella pagina Funzioni B2B sono elencati tutti i flussi di documenti definiti.

È possibile impostare attributi sul livello delle funzioni B2B. Gli attributi impostati su questo livello sostituiscono quelli impostati sul livello della definizione di documenti. Ad esempio, se si imposta **Consenti richiesta TA1** su **No** a livello di destinazione del flusso di documenti per i documenti ISA, ma poi si imposta su **Sì** a livello di funzioni B2B, viene utilizzato il valore **Sì**. L'impostazione di un attributo sul livello delle funzioni B2B consente di personalizzare l'attributo per uno specifico partecipante.

Se si imposta il profilo busta sul livello di protocollo o di flusso di documenti (nella pagina Gestisci le definizioni del flusso di documenti) e quindi si imposta su un valore differente nella pagina Funzioni B2B, si utilizza l'ultimo valore.

È necessario disporre di profili e di funzioni B2B del Gestore comunità e dei partecipanti definiti prima di poter creare connessioni tra loro.

## Passaggio 4: Attivare le connessioni

Attivare, infine, le connessioni tra Gestore comunità e partecipanti. Le connessioni disponibili si basano sulle funzioni B2B dei partecipanti sulle interazioni create. Le interazioni dipendono dalle definizioni di flusso di documenti disponibili.

Per alcuni scambi, viene richiesta una sola connessione. Se, ad esempio, un partecipante invia un documento binario ad un'applicazione back-end del Gestore comunità, è necessaria una sola connessione. Per lo scambio di scambi EDI in cui lo scambio viene sbustato e le singole transazioni trasformate, vengono impostate più connessioni.

**Nota:** Per gli scambi EDI trasmessi come tali, viene 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 **Sk** a livello delle funzioni B2B, ma poi si imposta su **No** a livello di connessione, il valore utilizzato è **No**. L'impostazione del valore di un attributo a livello di connessione consente di personalizzare ulteriormente l'attributo, in base ai requisiti di routing dei partecipanti e delle applicazioni coinvolte.

---

## Panoramica sui flussi possibili

In questa sezione, viene fornita una breve panoramica dei tipi di trasformazione che WebSphere Partner Gateway può eseguire. I dettagli di queste trasformazioni e ciò che è necessario per configurarle vengono descritti in "Passaggi generali per la definizione di scambio di documenti" a pagina 110.

### Flusso EDI in EDI

WebSphere Partner Gateway può accettare uno scambio EDI da un partecipante o dal Gestore comunità, trasformarlo in un tipo differente (ad esempio, EDI-X12 in EDIFACT), ed inviare il documento al Gestore comunità o al partecipante. I passaggi seguenti hanno luogo quando uno scambio EDI viene trasformato in un altro scambio EDI:

1. Lo scambio EDI ricevuto sull'hub viene sbustato.
2. Le singole transazioni in uno scambio EDI vengono trasformate nel formato EDI del partecipante.
3. Le transazioni EDI trasformate vengono imbustate ed inviate al destinatario.

In Figura 23 a pagina 90 viene mostrato uno scambio X12 che consiste di tre transazioni da sbustare. Le transazioni vengono trasformate in formato EDIFACT e quindi imbustate ed inviate al partecipante.

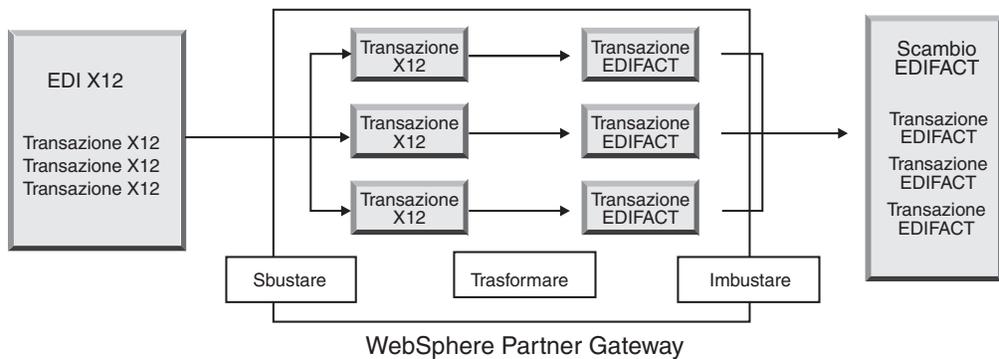


Figura 23. Flusso scambio EDI in scambio EDI

Ciascuna delle transazioni ha una mappa di trasformazione associata che specifica come viene trasformata la transazione. La transazione può essere trasformata in una transazione singola oppure, se è stato il concatenamento di mappe per la creazione della mappa, più transazioni. Se il batch dell'Envelope è attivo, le transazioni che entrano nell'hub in una busta lasciano l'hub in una busta. Tuttavia, se sono presenti breakpoint della busta (ad esempio, valori diversi per gli attributi EDI o un profilo di busta diverso) o se il batch è disattivato, le transazioni lasciano l'hub in buste diverse. Per una descrizione generale dell'Envelope (ovvero il componente che raccoglie una serie di transazioni da inviare ad un partecipante, le imbusta e le invia), consultare "Envelope" a pagina 98. Per ulteriori informazioni sul batch, consultare "Modalità batch" a pagina 98.

La transazione potrebbe anche avere una mappa di convalida ad essa associata.

## Flusso EDI in XML o ROD

WebSphere Partner Gateway può accettare uno scambio EDI da un partecipante o dal Gestore comunità, sbustare lo scambio e trasformare le transazioni EDI risultanti in documenti XML o ROD.

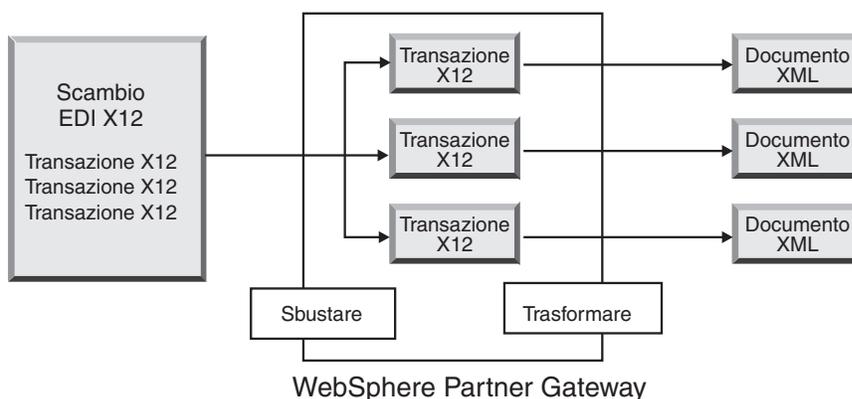


Figura 24. Interscambio EDI nel flusso di documenti XML

La transazione può essere trasformata in un singolo documento oppure se è stato utilizzato il concatenamento della mappa, più documenti.

## Flusso XML o ROD in EDI

WebSphere Partner Gateway può ricevere documenti XML o ROD da un partecipante o dal Gestore comunità, trasformare i documenti in transazioni EDI, imbustare le transazioni ed inviarle al Gestore comunità o al partecipante.

Figura 25 illustra i documenti XML che sono trasformati in transazioni X12 e quindi imbustati.

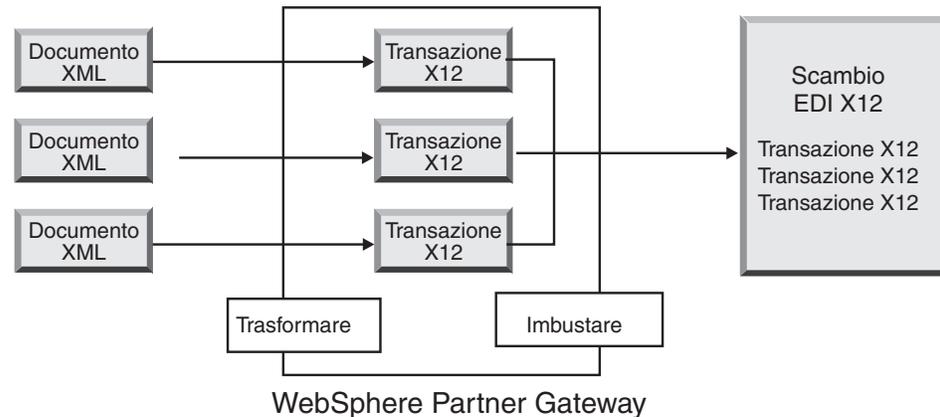


Figura 25. Flusso documento XML in scambio EDI

Un documento può essere trasformato in più transazioni (se è stato utilizzato il concatenamento di mappe per creare la mappa) e le transazioni imbustate in scambi differenti. In Figura 26 viene mostrato un documento XML trasformato in tre transazioni X12. Due delle transazioni vengono imbustate insieme. Una di esse viene inserita in una busta separata.

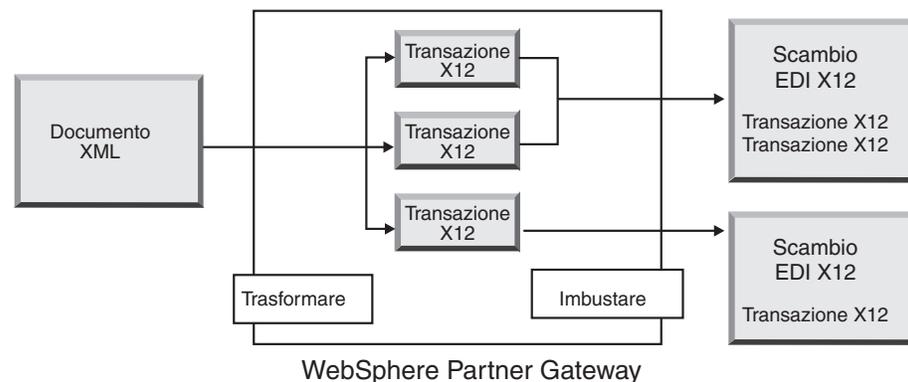


Figura 26. Flusso di documenti XML in più transazioni EDI

## Flusso di più documenti XML o ROD in scambio EDI

WebSphere Partner Gateway può ricevere un file costituito da uno o più documenti XML o ROD da un partecipante o un Gestore comunità, trasformare il documento o documenti in transazioni EDI e imbustarle in più buste e inviarle al Gestore comunità o al partecipante.

Ciascun documento può essere trasformato in una singola transazione o se è stato utilizzato il concatenamento della mappa, più transazioni.

**Note:**

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 illustra una serie di documenti XML da separare in documenti XML singoli. I documenti XML vengono trasformati in transazioni X12 e le transazioni vengono imbustate.

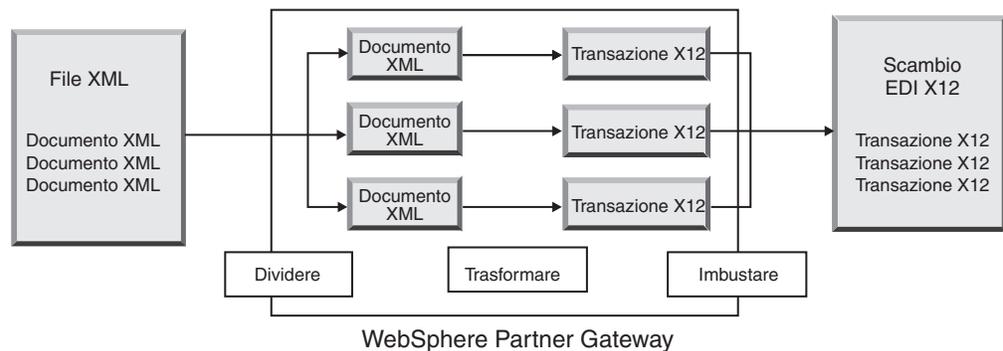


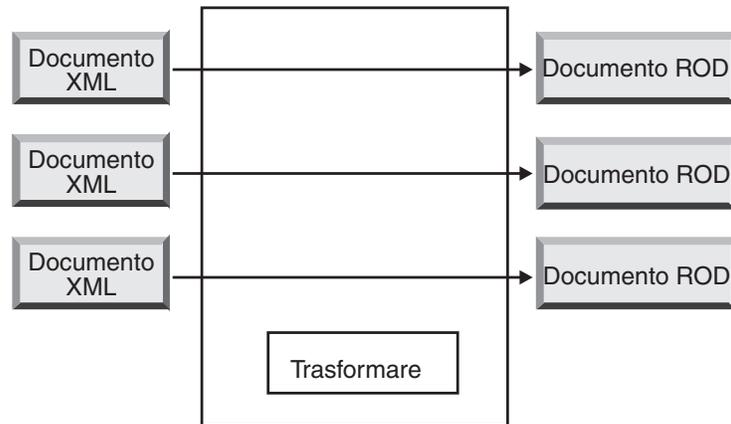
Figura 27. Flusso di più documenti XML in scambio EDI

In Figura 27, i documenti vengono divisi (mediante il gestore splitter XML) e le transazioni trasformate vengono imbustate insieme. Il gestore splitter XML deve disporre dell'opzione BCG\_BATCHDOCS impostata su on (valore predefinito) affinché si verifichi questo scenario. Se BCG\_BATCHDOCS è impostato su on ed è attivo il modo batch dell'Envelope, queste transazioni possono essere imbustate nella stessa busta EDI. L'attributo per il modo batch dell'Envelope viene descritto in "Modalità batch" a pagina 98.

## Flusso XML in ROD o ROD in XML

WebSphere Partner Gateway può ricevere un documento XML o ROD da un partecipante o Gestore comunità, trasformare il documento in un altro tipo (XML in ROD o ROD in XML), ed inviare il documento al partecipante o Gestore comunità.

In Figura 28 a pagina 93 viene mostrata una serie di documenti XML trasformati in documenti ROD.



### WebSphere Partner Gateway

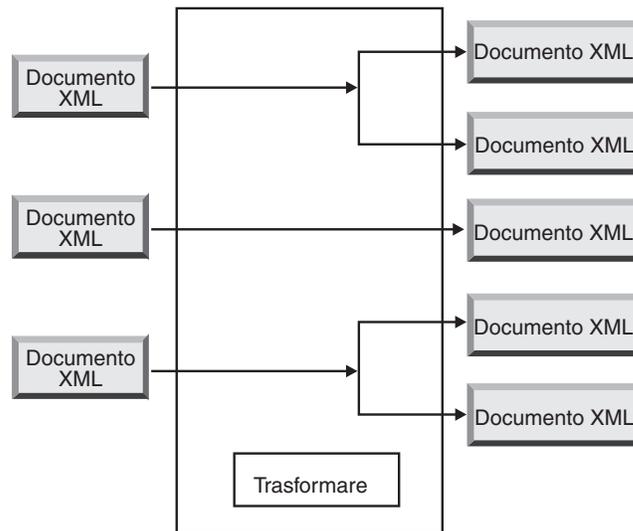
Figura 28. Flusso di documenti XML in documenti ROD

Il documento può essere trasformato in un singolo documento oppure se è stato utilizzato il concatenamento delle mappe, in più documenti.

### Flusso XML in XML o ROD in ROD

WebSphere Partner Gateway può ricevere un documento XML o ROD da un partecipante o Gestore comunità, trasformarlo in un documento dello stesso tipo (XML in XML o ROD in ROD), ed inviare il documento al partecipante o Gestore comunità.

In Figura 29 vengono mostrati documenti XML trasformati in documenti XML di un formato differente.



### WebSphere Partner Gateway

Figura 29. Flusso di documenti XML in documenti XML

Il documento può essere trasformato in un singolo documento oppure se è stato utilizzato il concatenamento delle mappe, in più documenti.

---

## Modalità di elaborazione degli interscambi EDI

Uno scambio EDI ricevuto sull'hub è, di solito, sbustato e le singole transazioni elaborate. Spesso, le transazioni EDI (come ad esempio X12 850 o EDIFACT ORDERS, che rappresenta un ordine di acquisto) vengono trasformate in un formato che può essere compreso da un'applicazione back-end. Inoltre, un riconoscimento funzionale viene spesso inviato al partecipante per indicare che lo scambio è stato ricevuto. Lo scambio di scambi EDI, di conseguenza, richiede più azioni (quali lo sbustamento, la conversione e la convalida EDI). Se, ad esempio, lo scambio contiene due transazioni e non viene richiesto alcun riconoscimento, WebSphere Partner Gateway esegue le seguenti azioni:

1. Sbusta lo scambio

WebSphere Partner Gateway estrae le informazioni sullo scambio dall'intestazione della busta e i segmenti dell'elemento di coda sullo scambio, sul gruppo e sui livelli di transazione. Le informazioni includono:

- Sul livello dello scambio, gli identificativi aziendali dei partecipanti che inviano e ricevono, l'indicatore di utilizzo che specifica se lo scambio indica un ambiente di produzione o di verifica e la data e l'ora in cui è stato preparato lo scambio
- Sul livello di gruppo, gli identificativi dell'applicazione del mittente e del destinatario e l'ora e la data in cui è stato preparato il gruppo
- Sul livello della transazione, il tipo di transazione (come ad esempio X12 850 o EDIFACT ORDERS)

2. Trasforma la prima transazione secondo la mappa associata.

3. Trasforma la seconda transazione secondo la mappa associata.

4. Consegna i documenti trasformati all'applicazione back-end.

Similmente, quando l'hub invia un documento o documenti che sono originati sull'applicazione back-end del Gestore comunità, i documenti vengono trasformati in transazioni EDI standard. Le transazioni EDI risultanti vengono imbustate prima di essere inviate al partecipante. Come nel caso di ricezione di uno scambio EDI, vengono richieste più azioni per creare, imbustare 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 106.

Nella seguente figura viene rappresentato come uno scambio EDI, impacchettato come AS, viene inviato dal partecipante, con l'eventuale obiettivo di consegnare due documenti XML trasformati in due gateway differenti sul sistema back-end del Gestore comunità. In questo esempio, le transazioni 850 vengono trasformate in ordini di acquisto che possono essere elaborati da un'applicazione di back-end. Le transazioni 890 vengono trasformate in ordini di spedizione di magazzino che possono essere elaborati dall'applicazione di back-end.

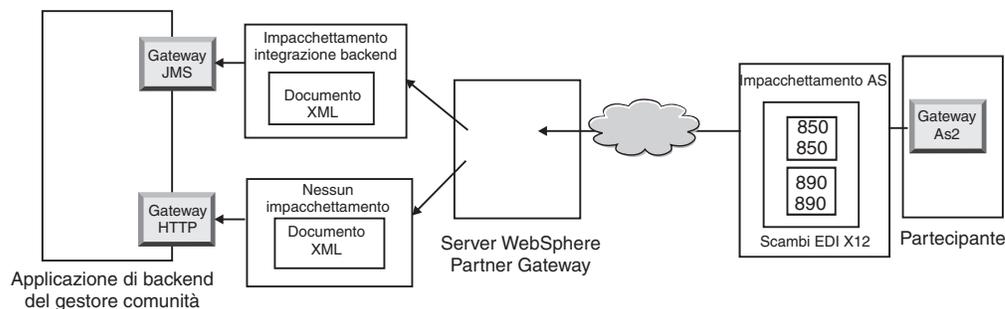


Figura 30. Flusso generale da un partecipante al Gestore comunità

Invece che richiedere una connessione dal partecipante al Gestore comunità, questo scambio richiede tre connessioni:

- Una dal partecipante all'hub per sbustare lo scambio. Poiché questo è un passo intermedio (l'interscambio viene sbustato, ma non recapitato al partecipante), la parte di destinazione della connessione del partecipante è N/D (non disponibile).

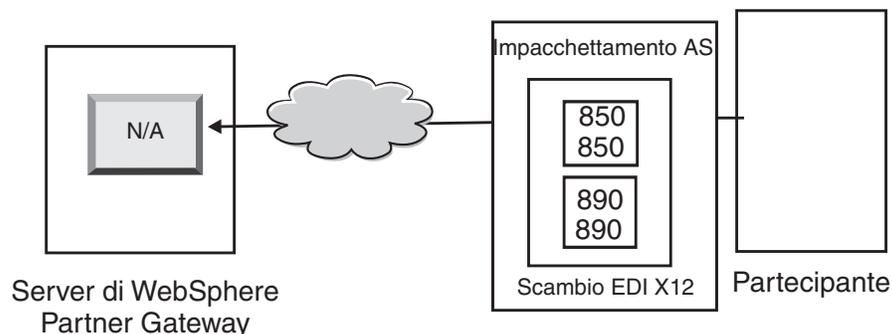


Figura 31. Connessione di sbustamento

- Una per la prima transazione da trasformare e consegnare al gateway JMS del Gestore comunità e l'altra per la seconda transazione da trasformare ed inviare al gateway HTTP del Gestore comunità.

Per le transazioni, l'impacchettamento di origine non è disponibile, poiché le transazioni entrano nell'interscambio di origine che era stato sbustato dal sistema. Pertanto, la parte di origine delle transazioni, deve disporre del seguente parametro **Impacchettamento: N/D** specificato nella connessione del partecipante.

Per la transazione che viene trasformata in XML e che passa all'applicazione di backend attraverso JMS, è necessario specificare il gateway di destinazione sulla connessione del partecipante della transazione come gateway del Gestore comunità. Per la transazione trasformata in XML e che passa all'applicazione di back-end sull'HTTP, è necessario specificare il gateway di destinazione sulla connessione del partecipante di questa transazione come gateway HTTP.

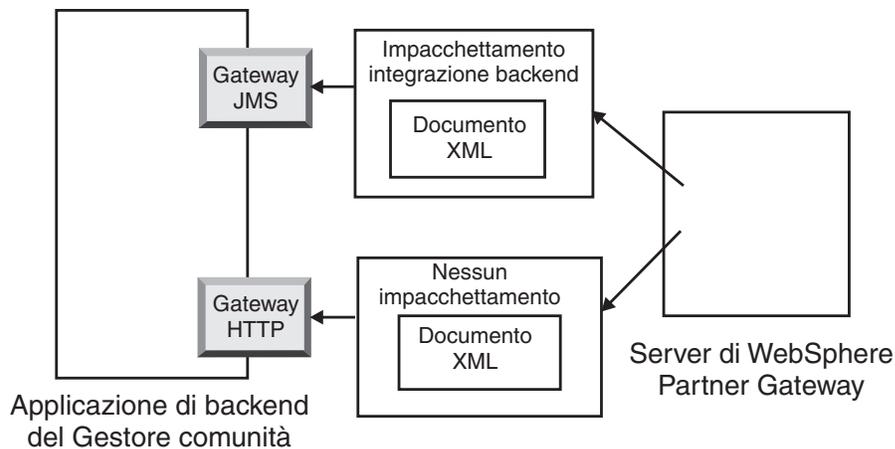


Figura 32. Connessioni per singole transazioni

È possibile utilizzare il visualizzatore di documenti per visualizzare l'interscambio e le transazioni individuali, che nei termini del visualizzatore documenti, sono i *child* dell'interscambio. Utilizzando il visualizzatore di documenti, è possibile visualizzare i *child* associati all'interscambio di origine o di destinazione ed è possibile visualizzare gli eventi associati. Il visualizzatore di documenti è descritto nella sezione "Visualizzazione di eventi e documenti" del manuale *Guida dell'amministratore*.

Se il mittente richiede riconoscimenti, sono necessarie connessioni aggiuntive:

- Una per ciascuno dei riconoscimenti inviati indietro al partecipante. Le notifiche funzionali vengono generate dal sistema, pertanto la parte di origine della connessione del partecipante deve disporre di **Impacchettamento: N/D** specificato. Le notifiche funzionali vengono imbustate prima di essere recapitate, pertanto la parte di destinazione della connessione del partecipante deve disporre di **Impacchettamento: N/D** specificato. Enveloper raccoglie questi riconoscimenti secondo la pianificazione impostata. Per informazioni sull'impostazione della pianificazione, vedere "Enveloper" a pagina 98.
- Una per imbustare i riconoscimenti prima che vengano inviati di nuovo al partecipante. La busta viene generata dal sistema, pertanto la parte di origine della connessione del partecipante deve disporre di **Impacchettamento: ND** specificato. La parte di destinazione della connessione del partecipante deve disporre del gateway di destinazione impostato sul gateway del partecipante e, in questo caso, con **Impacchettamento: AS specificato**. Si può utilizzare una busta predefinita per lo standard EDI, oppure si possono personalizzare le buste. Per informazioni sulla personalizzazione delle buste, vedere "Profili busta" a pagina 99.

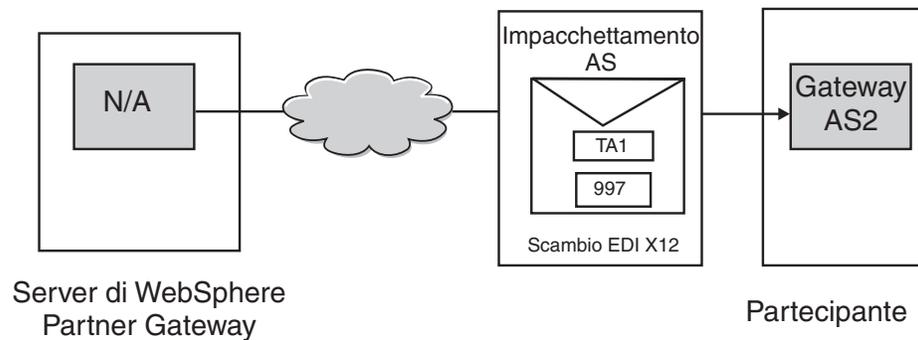


Figura 33. Imbustamento ed invio di riconoscimenti all'originator

---

## Modalità di elaborazione dei 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. Trasforma ogni documento secondo la mappa associata.
3. Se i documenti vengono trasformati in transazioni EDI, impacchetta le transazioni e le consegna all'applicazione back-end. Se i documenti vengono trasformati in documenti XML o ROD, vengono consegnati trasformati all'applicazione back-end.

Se il documento XML o ROD arriva come singolo documento, WebSphere Partner Gateway esegue le seguenti azioni:

1. Trasforma il documento secondo la mappa associata.
2. Se il documento viene trasformato in una transazione EDI, impacchetta la transazione e la consegna all'applicazione back-end. Se il documento viene trasformato in un documento XML o ROD, il documento viene consegnato all'applicazione back-end.

Similmente, quando l'hub invia un documento o documenti che sono originati sull'applicazione back-end del Gestore comunità, i documenti vengono trasformati in documenti XML o ROD o in transazioni EDI. Le transazioni EDI risultanti vengono imbustate prima di essere inviate al partecipante. Come nel caso di ricezione di uno scambio EDI, vengono richieste più azioni per trasformare il documento o i documenti, imbustare le transazioni risultanti ed inviare lo scambio EDI.

---

## 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 per le buste forniti dal sistema, definire buste specifiche da utilizzare per alcune connessioni, configurare numeri di controllo assegnati alle varie parti di un interscambio e impostare profili di connessione in modo che lo stesso interscambio possa essere recapitato in un modo diverso. Queste attività vengono descritte in questa sezione.

## Enveloper

L'utilità Enveloper è il componente che raccoglie una serie di transazioni da inviare a un partecipante, le racchiude in una busta e le invia. Si pianifica l'Enveloper (o si accetta la pianificazione predefinita) per indicare a WebSphere Partner Gateway quando si desidera che Enveloper cerchi le transazioni in attesa di essere inviate. Si può anche 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 non si modifica nessuno dei valori per Enveloper, si utilizzano i valori predefiniti.

### 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 imbustate. 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 al gestore splitter configurato per quel tipo di documento. (La configurazione dei gestori splitter, che è parte della definizione delle destinazioni, è descritta in "Modifica dei punti di configurazione" a pagina 44.) Uno degli attributi del gestore splitter è BCG\_BATCHDOCS. Quando BCG\_BATCHDOCS è 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 insieme nello stesso file siano elaborati prima di imbustarli e inviarli, in modo che le transazioni siano imbustate insieme. Ad esempio, si supponga che cinque documenti XML arrivino nello stesso file. I documenti XML vengono trasformati in transazioni EDI e consegnati allo stesso destinatario. Dopo che solo tre documenti vengono trasformati, Enveloper inizia il polling pianificato per le transazioni. Se si seleziona la modalità batch, Enveloper non elabora (busta) le tre transazioni pronte. Al contrario, attende finché non termina l'elaborazione delle cinque transazioni prima che vengano imbustate ed inviate. Le transazioni vengono posizionate nella stessa busta, a meno che lo standard EDI non lo eviti.

### Modifica dei valori predefiniti

Per modificare i valori predefiniti per l'Enveloper, effettuare i passi di seguito riportati:

1. Fare clic su **Ammin 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. Si assegna il profilo della busta alle transazioni EDI nella definizione di flusso di documenti per l'attributo **Profilo busta**. 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. I passaggi per la modifica o creazione di un profilo busta vengono descritti in "Modifica dei valori predefiniti" a pagina 100.

I profili busta hanno un campo per ogni elemento nello standard della busta. I profili forniscono dati letterali e costanti per la generazione di segmenti di intestazione e dell'elemento di coda per gli insiemi di transazioni, per i messaggi, i gruppi funzionali e gli scambi. Si forniscono solo i valori necessari da popolare e per i quali non viene fornito un 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 in “Attributi busta”, l’insieme di attributi dovunque ha la precedenza sui valori impostati nel profilo busta. Alcuni attributi possono essere sostituiti negli attributi o mappe correlate alla definizione di flusso di documenti.

### **Attributi busta**

Gli attributi della busta possono essere impostati in molti punti differenti durante il processo di configurazione e possono essere impostati anche nella mappa di trasformazione 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 trasformazione possono sostituire i valori correlati impostati sulla Console comunità. Ad esempio, se CtlNumFlag è impostato nella mappa della trasformazione come N (no) e viene immesso un valore S (si) nel campo **Numeri di controllo per ID della transazione**, il valore N è quello utilizzato.

Altri profili busta possono essere impostati sul livello di protocollo (dalla pagina Gestisci le definizioni del flusso di documenti o dalla Funzioni B2B associate ad un partecipante), oppure possono essere impostati come parte della connessione. L’ordine della precedenza viene sottolineato nel seguente elenco:

1. Le proprietà impostate nella mappa di trasformazione 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 funzioni B2B.
3. Gli attributi impostati sul livello delle funzioni B2B hanno la precedenza sugli attributi impostati sul livello della definizione di flusso di documenti.
4. Gli attributi impostati dovunque (sia nella mappa di trasformazione che sul livello della definizione di flusso di documenti, delle funzioni B2B o della connessione) hanno la precedenza sui valori impostati nel profilo busta.

Per un elenco delle proprietà della mappa di trasformazione e gli attributi del Gestore comunità appropriati, consultare “Proprietà del client Data Interchange Services” a pagina 292.

### **Modifica dei valori predefiniti**

In “attributi profilo busta” a pagina 281 viene fornita 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 **Ammin hub > Configurazione hub > EDI > Profilo busta**.
2. Eseguire uno dei seguenti gruppi di passaggi:
  - Creare una busta
    - a. Fare clic su **Crea**.
    - b. Immettere il nome per il profilo. Si tratta del nome che apparirà nell’elenco dei profili busta.
    - c. Facoltativamente, immettere una descrizione del profilo.
    - d. Fare clic sullo standard EDI cui si riferisce 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 a pagina 100.
- Si possono aggiungere valori per i seguenti campi:
- **Lunghezza del numero di controllo dello scambio**, per indicare quanti caratteri devono essere utilizzati quando viene assegnato un numero di controllo ad uno scambio nella busta.
  - **Lunghezza del numero di controllo del gruppo**, per indicare quanti caratteri devono essere utilizzati quando viene assegnato un numero di controllo ad un gruppo nella busta.
  - **Lunghezza del numero di controllo della transazione**, per indicare quanti caratteri devono essere utilizzati quando viene assegnato un numero di controllo ad una transazione nella busta.
  - **Numero max di transazioni**, per indicare il numero massimo di transazioni consentite in questa busta.
  - **Numeri di controllo per ID transazione**, che indicano se si desidera utilizzare l'ID della transazione (come parte della chiave) quando i numeri impostati 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 interscambio.
      - **ISA03: Qualificatore informazioni di sicurezza**, ovvero un codice per il tipo di informazioni in ISA04. I valori possibili sono:
 

<b>00</b>	ISA04 non è significativo
<b>01</b>	ISA04 contiene una password
      - **ISA04: Informazioni sulla sicurezza**, ovvero informazioni sulla sicurezza per il mittente o i dati di interscambio. il codice in ISA03 definisce il tipo di informazioni.
      - **ISA11: ID standard di interscambio**, ovvero un codice per l'agenzia che controlla l'interscambio. 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 interscambio**, ovvero il numero di versione della sintassi utilizzata nei segmenti di interscambio e di controllo del gruppo funzionale.

- **ISA14: notifica richiesta**, ovvero il codice del mittente per richiedere una notifica. I valori possibili sono:
  - 0 Non richiedere notifica
  - 1 Richiedi una notifica per il ricevimento e il riconoscimento dei segmenti ISA e IEA
- **ISA15: Indicatore di prova**, ovvero un'indicazione che l'interscambio 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**, ovvero una password che il destinatario assegna da utilizzare come accettazione da parte dei partecipanti.
- 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**, ovvero una password assegnata dal destinatario da utilizzare come accettazione da parte dei partecipanti.
  - **UNB0602: Qualificatore ricevimento/password destinatari**, ovvero un qualificatore per la password di un destinatario da utilizzare come accettazione da parte dei partecipanti.
  - **UNB07: Riferimento applicazione**, ovvero l'identificativo del mittente dell'area funzionale cui sono correlati i messaggi di interscambio.
  - **UNB08: Priorità**, ovvero il codice del mittente per la priorità di elaborazione, come accettazione con i partecipanti. Il codice A è la massima priorità.
  - **UNB09: Richiesta di notifica**, ovvero il codice del mittente per la richiesta di una notifica.
  - **UNB10: ID accettazione comunicazioni**, ovvero il nome o il codice per il tipo di accettazione utilizzato per questo interscambio, come d'accordo con il partecipante.
  - **UNB11: Indicatore di prova (Indicatore di utilizzo)**, ovvero un indicatore del fatto che l'interscambio è per prova. 1 indica un interscambio 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, rilascio 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: Rilascio messaggio**, ovvero il numero di rilascio 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: Rilascio messaggio**, ovvero il numero di rilascio 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 assegnata**, 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 partecipanti possono concordare sull'utilizzo una chiave fatta dai componenti, ma non è possibile utilizzare separatori dell'elemento secondario.

Se si sono apportate modifiche alla pagina Transazione, fare clic su **Salva**.

7. Fare clic su **Salva**.
8. Ripetere i passi da 2 a pagina 100 a 7 per altri eventuali profili di busta da definire o modificare.

Dopo che viene definito un profilo busta, appare nell'elenco dei profili busta. Dall'elenco, è possibile selezionare il profilo e si fa clic sull'icona **Dove utilizzato** per stabilire le connessioni mediante il profilo.

## Profili connessione

Si utilizzano profili della connessione con transazioni sbustate e scambi EDI create da Enveloper. Per le transazioni, il profilo della connessione determina il modo in cui la transazione viene elaborata una volta sbustata. Per gli scambi, il profilo della connessione stabilisce come viene consegnato lo scambio.

Nella seguente tabella vengono mostrati gli attributi del profilo connessione, i nomi di campo corrispondenti nella pagina Dettagli del profilo connessione, e se vengono applicati agli scambi o transazioni:

Tabella 14. Attributi profilo connessione

Attributo	Nome campo	Scambio EDI	Transazione EDI
Qualificatore profilo connessione 1	Qualificatore1	X	
Indicatore utilizzo scambio	Tipo di utilizzo EDI		X
Identificativo mittente applicazione gruppo	ID mittente applicazione		X
Identificativo destinatario applicazione gruppo	ID destinatario applicazione		X
Password applicazione gruppo	Password		X

## Transazioni

Quando uno scambio EDI va a finire in WebSphere Partner Gateway, la prima azione server, di solito, per sbustare lo scambio in singole transazioni. Quando vengono create le transazioni, l'azione di sbustamento imposta l'**indicatore utilizzo interscambio** 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 altrimenti le stesse (hanno lo stesso partecipante, pacchetto, protocollo e tipo di documento di origine e di destinazione), 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 interscambio**, 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 interscambi, 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 (impacchettamento Nessuno) o di Internet (impacchettamento AS2). Si desidera transazioni 840 (Richiesta di quotazione) per utilizzare VAN e transazioni 850 (Ordine di acquisto) per utilizzare Internet. Si configurano due connessioni di partecipante, entrambe con lo stesso scambio di origine con destinazioni differenti (una con impacchettamento Nessuno 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 **Qualifier1 profilo di connessione** impostati al passo 1 (ConNone e ConAS2).
3. Creare due connessioni per lo scambio. Ciascuna connessione ha un impacchettamento della stessa origine (N/D) di differente destinazione (Nessuno e AS2). La connessione del partecipante con il profilo di connessione CPNone disporrà di un gateway di destinazione impostato sul gateway di script FTP che può connettersi a VAN. La connessione del partecipante con il profilo di connessione CPAS2 disporrà di un impacchettamento di destinazione impostato su AS.
4. Associare il profilo connessione appropriato l'uno con l'altro.

L'Enveloper utilizza l'attributo **Qualificatore 1 profilo di connessione** nella parte "A" della connessione del partecipante come punto di interruzione della busta. Pertanto, le transazioni con valori diversi per l'attributo **Qualificatore profilo di connessione 1** verranno imbustate in buste diverse. Quando si impostano valori diversi per le transazioni, l'Enveloper non imbusterà mai le transazioni 840 e 850 nello stesso interscambio.

Quando Gestore documenti cerca la connessione, vengono trovate le due possibili connessioni, ma si utilizza quella con profilo corrispondente.

## Impostazione dei profili connessione

L'impostazione di profili connessione è facoltativa. Se si non ha la necessità di disporre di una connessione per ogni tipo di documento che si scambierà con un partecipante, saltare questa sezione.

Per impostare un profilo connessione:

1. Fare clic su **Ammin 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 un valore che stabilisce la connessione da utilizzare per uno scambio EDI. Consultare "Scambi" a pagina 105 per un esempio di utilizzo del **Qualificatore 1**.
6. Facoltativamente, immettere un valore per **Tipo di utilizzo EDI** per indicare se si tratta di uno scambio di prova, di produzione o di informazioni. Consultare "Transazioni" a pagina 104 per un esempio di utilizzo del **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 quelle transazioni da inserire nelle buste di interscambio, è possibile specificare il valore dell'attributo **Qualificatore profilo di connessione 1** corrispondente al profilo di connessione con gli stessi valori per l'attributo **Qualificatore 1**. L'attributo **Qualificatore del profilo di connessione 1** può essere impostato a livello di protocollo di una definizione del flusso di documenti (ad esempio, è possibile modificare gli attributi del protocollo X12V5R1 nel pannello Gestisci definizione del flusso di documenti per indicare il profilo di connessione da utilizzare facendo clic sul valore dell'attributo **Qualificatore del profilo di connessione 1**). Quindi, quando si attiva la connessione dell'interscambio, 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 vengono stabiliti per il Gestore comunità e i partecipanti. Quando si verifica lo scambio dei documenti, anche i numeri di controllo vengono generati per la *coppia* di partecipanti.

Per ciascun partecipante con funzioni EDI B2B è presente una serie di valori di inizializzazione per i numeri di controllo. Questi valori vengono utilizzati la prima volta che viene creato uno scambio EDI ed inviato tra una coppia di partecipanti. I valori di inizializzazione vengono applicati al partecipante cui è inviato lo scambio. Dopo che un documento viene inviato da un partecipante ad un altro, gli ultimi numeri utilizzati possono essere visualizzati nella pagina Numeri di controllo. Possono essere presenti varie voci per una determinata coppia di partecipanti se **Numeri di controllo per ID transazione** viene impostato su Y. Quando esiste una voce, viene utilizzata per generare 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 15.

Tabella 15. 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.
Gn	Transazione	<i>n</i> 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 restanti byte nel campo del numero di controllo del gruppo o transazione vengono utilizzati per mantenere un numero di controllo per questo partecipante.
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.
Vn	Transazione	Si utilizza un valore di incremento pari a <i>n</i> byte in modo che la prima transazione abbia un valore di 1, la seconda un valore pari a 2 e così via.
GnC	Transazione	<i>n</i> 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.
GnV	Transazione	<i>n</i> 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.

Tabella 15. Maschere del numero di controllo (Continua)

Codice	Numero di controllo	Descrizione
$GnVm$	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 dello scambio. Solo un gruppo è consentito per lo scambio e solo una transazione è consentita per il gruppo o scambio.
$In$	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.
$InC$	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 di controllo va dal valore massimo fino a 1.
$InV$	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.
$InVm$	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.
$InGm$	Transazione	$n$ byte vengono presi dal numero di controllo dello 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
$InGmC$	Transazione	$n$ byte vengono presi dal numero di controllo dello 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 di controllo va dal valore massimo fino a 1.

Tabella 15. Maschere del numero di controllo (Continua)

Codice	Numero di controllo	Descrizione
InGmV	Transazione	$n$ byte vengono presi dal numero di controllo dello 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.
InGmVo	Transazione	$n$ byte vengono presi dal numero di controllo dello scambio e $m$ byte dal numero di controllo del gruppo. Per $i$ byte restanti, fino a $o$ 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 numeri di controllo

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. Immettere il nome di un partecipante e fare clic su **Cerca** senza immettere un nome per visualizzare tutti i partecipanti. Se **Compatibile EDI** è selezionato, la ricerca è limitata ai partecipanti che con funzioni B2B del documento EDI. Se si deselegna questa casella, si ricercano tutti partecipanti.
3. Fare clic sull'icona **Visualizza i dettagli** accanto al partecipante.
4. Gli assignment del numero di controllo del partecipante (se ve ne sono) sono elencati 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 di partecipanti che dispone già dei dati nella tabella di controllo, è possibile modificare la generazione del numero di controllo. È possibile:

- Ripristinare la generazione del numero di controllo per la coppia ad uno stato iniziale.
- Modificare il numero di interscambio, 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 quali partecipanti abbiano numeri di controllo assegnati (e per stabilire quali numeri siano), si utilizza la funzione Numeri di controllo correnti.

1. Fare clic su **Ammin hub > Configurazione hub > EDI > Numeri di controllo correnti**.
2. Eseguire uno dei seguenti gruppi di passaggi:
  - Se si desidera visualizzare lo stato corrente di tutti i partecipanti, lasciare **Qualsiasi partecipante** selezionato negli elenchi dei partecipanti, quindi fare clic su **Visualizza stato corrente**.
  - Se si desidera visualizzare lo stato dei partecipanti selezionati, eseguire questi passaggi:
    - a. Immettere il nome dei partecipanti di origine e di destinazione e fare clic su **Cerca**. Se si desidera limitare i risultati della ricerca solo a quei partecipanti che stanno scambiando documenti EDI, lasciare **Trova compatibile EDI** selezionato.
    - b. Dagli elenchi dei risultati, selezionare uno o più partecipanti da ogni elenco, e fare clic su **Visualizza stato corrente**.

---

## Passaggi generali per la definizione di scambio di 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 trasformate 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. I passaggi generali per l'abilitazione delle funzioni B2B per i partecipanti (per tutti i tipi di scambi dei documenti) vengono descritti in "Impostazione delle funzioni B2B" a pagina 146. I passaggi generali per la gestione delle connessioni (per tutti i tipi di scambi dei documenti) vengono descritti in Capitolo 12, "Gestione delle connessioni", a pagina 149. Se si desidera visualizzare un esempio completo di uno scambio EDI dall'importazione delle mappe fino alla gestione delle connessioni, fare riferimento a Appendice B, "Esempi EDI", a pagina 193. Nell'appendice sono inclusi questi esempi specifici:

- "Esempio EDI in ROD" a pagina 193
- "Esempio EDI in XML" a pagina 206
- "Esempio ROD in EDI" a pagina 219
- "Esempio da XML a EDI" a pagina 212

## Importazione delle mappe

Le mappe di trasformazione 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.

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*.

Quando la mappa di trasformazione viene importata in WebSphere Partner Gateway, le definizioni del documento create in Data Interchange Services vengono visualizzate come definizioni di flusso di documenti (pacchetto, protocollo e flusso di documenti) nella pagina Mappa di trasformazione e Gestisci le definizioni del flusso di documenti.

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 trasformazione 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 richiederli 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:

```
<ProductDir>/bin/bcgDISImport.sh <database_user_ID>
<password> <control_string_map>
```
  - In un sistema Windows:

```
<ProductDir>\bin\bcgDISImport.bat <database_user_ID>
<password> <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 trasformazione, verificare sia importata che la definizione del flusso di documenti.
  - a. Fare clic su **Ammin hub > Configurazione hub > Mappe > Mappe di trasformazione**.
  - b. Nella pagina Mappe di trasformazione, fare clic sull'icona **Visualizza i dettagli** accanto alla mappa da Data Interchange Services. Si noterà che vengono visualizzate le definizioni del flusso di documenti per l'origine e la destinazione indicanti il formato in cui il documento verrà ricevuto sull'hub e quello in cui verrà consegnato dall'hub.

- c. Fare clic su **Ammin hub > Configurazione hub > Definizioni di flusso di documenti**.
- d. Espandere i pacchetti e i protocolli associati alle definizioni del documento visualizzate nella pagina Mappe di trasformazione per verificare che i flussi di documenti vengano visualizzati nella pagina Gestisci le definizioni del flusso di documenti.

È possibile utilizzare le mappe di convalida insieme alle mappe di trasformazione 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 trasformazione 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.

## Impostazione di un flusso EDI in EDI

In questa sezione, vengono descritte le interazioni necessarie a ricevere uno scambio EDI, sbustare lo scambio, trasformare una transazione da un formato EDI ad un altro, imbustare la transazione e consegnarla.

1. Verificare che esista una definizione di flusso di documenti per lo scambio EDI ricevuto sull'hub. Una volta sbustato l'interscambio, la busta di origine non continua ad essere elaborata. In altre parole, non c'è un punto di consegna. Pertanto, si utilizza **N/D** per il pacchetto sull'interazione di destinazione.
  - a. Fare clic su **Ammin hub > Configurazione hub > Definizione di flusso di documenti**.
  - b. Verificare se un documento o definizione di flusso di documenti già esista. Se, ad esempio, un partecipante invierà un impacchettamento AS, un protocollo EDI-X12 e un flusso di documenti ISA, la definizione è già disponibile. Similmente, la definizione di documenti N/D/EDI-X12/ISA già esiste.
  - c. Immettere un valore (o selezionarlo dall'elenco) per un attributo da associare al profilo. Se, ad esempio, si specifica che la busta deve essere eliminata e se se verificano errori con alcune transazioni, fare clic sull'icona **Modifica i valori dell'attributo** accanto a **Flusso di documenti**. Nella riga **Elimina busta in caso di errori**, selezionare **Sì** dall'elenco.
  - d. Se la definizione del documento non esiste, crearne una selezionando Pacchetto, Protocollo e Flusso di documenti.
2. Creare un'interazione per lo scambio.
  - a. Fare clic su **Ammin hub > Configurazione hub > Definizioni di flusso di documenti > Gestisci interazioni**.
  - b. Selezionare **Crea interazione**.
  - c. Selezionare le definizioni del flusso di documenti di origine e di destinazione. Escluso l'impacchettamento (che sarà **N/D** per la destinazione) le definizioni del flusso di documenti saranno uguali.
  - d. Selezionare **Sbustamento EDI** dall'elenco delle azioni.
3. Importare la mappa di trasformazione che fornisce le definizioni del documento delle transazioni EDI e che descrive come la transazione viene trasformata da un formato EDI all'altro. Vedere "Importazione delle mappe" a pagina 110.

- 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 **Ammin hub > Configurazione hub > Definizione di flusso di documenti**.
    - 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 valori dell'attributo** accanto al flusso di documenti. In genere, viene visualizzato un piccolo elenco di attributi rispetto a quelli associati al protocollo.
    - e. Immettere un valore (o selezionarne uno dall'elenco) per un attributo da associare al flusso di documenti. Ad esempio, è possibile modificare la **Mappa di convalida** associata al flusso di documenti.  
Verificare di selezionare un profilo di busta per la transazione.
  5. Creare un'interazione per la mappa importata.
    - a. Fare clic su **Ammin hub > Configurazione hub > Definizioni di flusso di documenti > Gestisci interazioni**.
    - b. Fare clic su **Crea interazione**.
    - c. Sotto **Origine**, selezionare il flusso di documenti associato alla transazione. Espandere il pacchetto e il protocollo e selezionare il flusso di documenti. Sarà di solito **N/D** poiché la transazione non proviene da un partecipante), il protocollo definito nella mappa (ad esempio, **X12V4R1**) e il documento EDI effettivo definito nella mappa (ad esempio, **850**).
    - d. In **Destinazione**, selezionare la definizione del flusso di documenti per il documento trasformato. Espandere il pacchetto e il protocollo e selezionare il flusso di documenti. Poiché la transazione verrà imbustata (e, di conseguenza, non verrà consegnata direttamente ad un partecipante), l'impacchettamento sarà di nuovo **N/D**.
    - e. Dall'elenco delle mappe di trasformazione, selezionare la mappa che definisce come trasformare questo documento.
    - f. Dall'elenco delle azioni, selezionare **Convalida EDI e conversione EDI**.
  6. Verificare che la definizione di flusso di documenti esiste per lo scambio EDI inviato dall'hub ed impostare gli attributi che si desidera associare allo scambio.
    - a. Fare clic su **Ammin hub > Configurazione hub > Definizione di flusso di documenti**.
    - b. Verificare se una definizione di flusso di documenti già esiste. L'origine sarà **N/D**, con il protocollo e il flusso di documenti che corrisponde al protocollo e al flusso di documenti utilizzati per consegnare lo scambio. Se, ad esempio lo scambio verrà consegnato come **AS/EDI-X12/ISA**, l'origine sarà **N/D/EDI-X12/ISA**.
    - c. Modificare gli attributi che vengono applicati allo scambio consegnato.
    - d. Se la definizione del documento non esiste, crearne una selezionando **Pacchetto, Protocollo e Flusso di documenti**.
  7. Creare un'interazione per lo scambio EDI che viene inviato dall'hub dopo che la transazione viene trasformata.

- a. Fare clic su **Ammin hub > Configurazione hub > Definizioni di flusso di documenti > Gestisci interazioni**.
- b. Fare clic su **Crea interazione**.
- c. Selezionare i documenti di origine e di destinazione. Escluso l'impacchettamento (che sarà **N/D** per il documento di origine) le definizioni del flusso di documenti saranno uguali.
- d. Selezionare **Pass Through** dall'elenco **Azione**.

Per aggiungere un riconoscimento al flusso, consultare "Impostazione dei riconoscimenti" a pagina 120.

Dopo aver impostato le interazioni, creare le funzioni B2B per i partecipanti.

- Per ciascun partecipante di origine, abilitare tre definizioni del flusso di documenti (in **Imposta origine**) - una per il flusso di documenti di origine, una per la transazione EDI e una per la busta.
- Per ciascun partecipante di destinazione, abilitare tre definizioni del flusso di documenti (in **Imposta destinazione**) - una per il flusso di documenti per lo sbustamento, una per la transazione EDI trasformata e una per la busta EDI.

I passi dettagliati per la creazione delle funzioni B2B sono descritti in "Impostazione delle funzioni B2B" a pagina 146.

Una volta impostate le funzioni B2B per i partecipanti, creare le connessioni. Sono necessarie tre connessioni:

- Una per la busta dal partecipante di origine all'hub.
- Una per la transazione EDI di origine alla transazione EDI di destinazione.
- Una per la busta dall'hub al partecipante di destinazione.

I passi dettagliati per la creazione delle connessioni sono descritti in Capitolo 12, "Gestione delle connessioni", a pagina 149.

## Impostazione di un flusso EDI in XML o ROD

In questa sezione, vengono descritte le interazioni necessarie a ricevere uno scambio EDI, sbustare lo scambio, trasformare 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 EDI in XML" a pagina 206. Per un esempio completo del flusso EDI in ROD, vedere "Esempio EDI in ROD" a pagina 193.

1. Verificare che esista una definizione di flusso di documenti per lo scambio EDI ricevuto sull'hub. Si ricordi che dopo che lo scambio viene sbustato, la busta non continua ad essere elaborata. In altre parole, non c'è un punto di consegna. Pertanto, si utilizza **N/D** per il pacchetto sull'interazione di destinazione.
  - a. Fare clic su **Ammin hub > Configurazione hub > Definizione di flusso di documenti**.
  - b. Verificare se un documento o definizione di flusso di documenti già esista. Se, ad esempio, un partecipante invierà un impacchettamento AS, un protocollo EDI-X12 e un flusso di documenti ISA, la definizione è già disponibile. Similmente, la definizione di documenti **N/D/EDI-X12/ISA** già esiste.
  - c. Se la definizione del documento non esiste, crearne una.
2. Creare un'interazione per lo scambio EDI ricevuto sull'hub.

- a. Fare clic su **Ammin hub > Configurazione hub > Definizioni di flusso di documenti> Gestisci interazioni**.
  - b. Selezionare **Crea interazione**.
  - c. Selezionare i documenti di origine e di destinazione. Escluso l'impacchettamento (che sarà **N/D** per la destinazione) le definizioni del flusso di documenti saranno uguali.
  - d. Selezionare **Sbustamento EDI** dall'elenco delle azioni.
3. Importare la mappa di trasformazione che fornisce le definizioni del documento della transazione EDI e il documento XML e ROD e che descrive come la transazione viene trasformata in un documento XML o ROD. Vedere "Importazione delle mappe" a pagina 110.
- Se lo scambio contiene più di una transazione, ripetere questo passaggio per ciascuna transazione.
4. Creare un'interazione per la mappa appena importata.
- a. Fare clic su **Ammin hub > Configurazione hub > Definizioni di flusso di documenti> Gestisci interazioni**.
  - b. Fare clic su **Crea interazione**.
  - c. Sotto **Origine**, selezionare il flusso di documenti associato alla transazione. Espandere il pacchetto e il protocollo e selezionare il flusso di documenti. Sarà di solito **N/D** poiché la transazione non proviene da un partecipante), il protocollo definito nella mappa (ad esempio, **X12V4R1**) e il documento EDI effettivo definito nella mappa (ad esempio, **850**).
  - d. In **Destinazione**, selezionare la definizione del flusso di documenti per il documento (XML o ROD trasformato). Espandere il pacchetto e il protocollo e selezionare il flusso di documenti.
  - e. Dall'elenco delle mappe di trasformazione, selezionare la mappa che definisce come trasformare questo documento.
  - f. Dall'elenco delle azioni, selezionare **Convalida EDI e conversione EDI**.

Per aggiungere un riconoscimento al flusso, consultare "Impostazione dei riconoscimenti" a pagina 120.

Dopo aver impostato le interazioni, creare le funzioni B2B per i partecipanti.

- Per ciascun partecipante di origine, abilitare due definizioni del flusso di documenti (in **Imposta origine**) - una per la busta e una per la transazione EDI.
- Per il partecipante di destinazione, abilitare due definizioni del flusso di documenti (in **Imposta destinazione**) - una per la busta EDI e una per il documento XLM o ROD.

I passi dettagliati per la creazione delle funzioni B2B sono descritti in "Impostazione delle funzioni B2B" a pagina 146.

Una volta impostate le funzioni B2B per i partecipanti, creare le connessioni. Sono necessarie due connessioni:

- Una per la busta dal partecipante di origine all'hub.
- Una per la transazione EDI di origine al documento XML o ROD.

I passi dettagliati per la creazione delle connessioni sono descritti in Capitolo 12, "Gestione delle connessioni", a pagina 149.

## Impostazione del flusso XML o ROD in EDI

In questa sezione, vengono descritte le interazioni necessarie per ricevere un documento XML o ROD, trasformarlo in una transazione EDI, imbustare la transazione e consegnarla.

**Nota:** Per un esempio completo del flusso XML o in ROD, vedere “Esempio da XML a EDI” a pagina 212. Per un esempio completo del flusso ROD in EDI, vedere “Esempio ROD in EDI” a pagina 219.

1. Importare la mappa di trasformazione che fornisce le definizioni del documento XML o ROD e della transazione EDI e che descrive come il documento venga trasformato in una transazione EDI. Vedere “Importazione delle mappe” a pagina 110.
2. Creare un’interazione per la mappa importata.
  - a. Fare clic su **Ammin hub > Configurazione hub > Definizioni di flusso di documenti > Gestisci interazioni**.
  - b. Fare clic su **Crea interazione**.
  - c. In **Destinazione**, selezionare la definizione del flusso di documenti associata al documento XML o ROD. Espandere il pacchetto e il protocollo e selezionare il flusso di documenti.
  - d. In **Destinazione**, selezionare il flusso di documenti associato alla transazione EDI. Espandere il pacchetto e il protocollo e selezionare il flusso di documenti. Poiché la transazione non verrà recapitata direttamente (verrà imbustata prima di essere recapitata), per il pacchetto verrà indicato **N/D**.
  - e. Dall’elenco delle mappe di trasformazione, selezionare la mappa che definisce come trasformare questo documento.
  - f. Dall’elenco Azione, selezionare **Conversione XML e convalida EDI o Conversione ROD e convalida EDI**.
3. Verificare che la definizione di flusso di documenti esista per lo scambio EDI inviato dall’hub ed impostare gli attributi che si desidera associare allo scambio.
  - a. Fare clic su **Ammin hub > Configurazione hub > Definizione di flusso di documenti**.
  - b. Verificare se una definizione di flusso di documenti già esiste. Per il pacchetto per il documento di origine dovrebbe essere indicato **N/D** (essendo l’interscambio inviato dall’hub).
  - c. Modificare gli attributi che vengono applicati allo scambio consegnato.
  - d. Se la definizione del documento non esiste, crearne una selezionando Pacchetto, Protocollo e Flusso di documenti.
4. Creare un’interazione per lo scambio EDI che viene inviato dall’hub dopo che il documento è stato trasformato.
  - a. Fare clic su **Ammin hub > Configurazione hub > Definizioni di flusso di documenti > Gestisci interazioni**.
  - b. Fare clic su **Crea interazione**.
  - c. Selezionare i documenti di origine e di destinazione. I documenti di origine e di destinazione dispongono di diversi impacchettamenti (il documento di origine dispone di un pacchetto N/D), ma il protocollo (ad esempio EDI-X12) e il flusso di documenti (ad esempio ISA) dovrebbero essere uguali.
  - d. Selezionare **Pass through** dall’elenco delle azioni.

Dopo aver impostato le interazioni, creare le funzioni B2B per i partecipanti.

- Per il partecipante di origine, il numero di definizioni del flusso di documenti che è necessario impostare (in **Imposta origine**) varia in base al tipo di flusso di documenti.
  - Ad esempio, per un documento XML in cui il flusso documenti è ICGPO e la transazione EDI convertita è MX12V3R1, abilitare tre definizioni del flusso di documenti (in **Imposta origine**) - una per il documento XML (ICGPO), una per la transazione EDI (MX12V3R1) e una per la busta inviata dall'hub.
  - Per altri documenti XML e ROD, abilitare due definizioni del flusso di documenti (in **Imposta origine**) - una per il documento XML o ROD e una per la busta inviata dall'hub.
- Per il partecipante di destinazione, abilitare due definizioni del flusso di documenti (in **Imposta origine**) - una per la transazione EDI e 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.

I passi dettagliati per la creazione delle funzioni B2B sono descritti in "Impostazione delle funzioni B2B" a pagina 146.

Una volta impostate le funzioni B2B per i partecipanti, 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 partecipante.

I passi dettagliati per la creazione delle connessioni sono descritti in Capitolo 12, "Gestione delle connessioni", a pagina 149.

## Impostazione di più documenti XML o ROD in un file in un flusso EDI

In questa sezione vengono descritte le interazioni per ricevere più documenti XML o ROD in un file, trasformare i documenti in transazioni EDI, imbustare le transazioni e consegnare lo scambio EDI.

1. Importare la mappa di trasformazione che fornisce le definizioni del documento dei documenti XML o ROD e delle transazioni EDI e che descrive la trasformazione. Vedere "Importazione delle mappe" a pagina 110.
2. Creare un'interazione per documenti di origine e di destinazione.
  - a. Fare clic su **Ammin hub > Configurazione hub > Definizioni di flusso di documenti > Gestisci interazioni**.
  - b. Fare clic su **Crea interazione**.
  - c. Dall'elenco Azione, selezionare i documenti di origine e di destinazione, quindi selezionare **Conversione XML e convalida EDI** o **Conversione ROD e convalida EDI**.
3. Ripetere il passaggio 2 per il documento di origine e ciascun documento di destinazione dalla mappa di trasformazione.
4. Verificare che la definizione di flusso di documenti esista per lo scambio EDI inviato dall'hub ed impostare gli attributi che si desidera associare allo scambio.
  - a. Fare clic su **Ammin hub > Configurazione hub > Definizione di flusso di documenti**.
  - b. Verificare se un documento o definizione di flusso di documenti già esista. L'origine sarà N/D, con il protocollo e il flusso di documenti che corrisponde al protocollo e al flusso di documenti utilizzati per consegnare

- lo scambio. Se, ad esempio, lo scambio verrà consegnato come AS/EDI-X12/ISA, l'origine sarà N/D/EDI-X12/ISA.
- c. Modificare gli attributi che vengono applicati allo scambio consegnato.
  - d. Se la definizione del documento non esiste, crearne una selezionando Pacchetto, Protocollo e Flusso di documenti.
5. Creare un'interazione per lo scambio EDI che viene inviato dall'hub dopo che la transazione viene trasformata.
    - a. Fare clic su **Ammin hub > Configurazione hub > Definizioni di flusso di documenti > Gestisci interazioni**.
    - b. Fare clic su **Crea interazione**.
    - c. Selezionare i documenti di origine e di destinazione. I documenti di origine e di destinazione dispongono di diversi impacchettamenti (il documento di origine dispone di un pacchetto N/D), ma il protocollo (ad esempio EDI-X12) e il flusso di documenti (ad esempio ISA) dovrebbero essere uguali.
    - d. Selezionare **Pass through** dall'elenco delle azioni.

Dopo aver impostato le interazioni, creare le funzioni B2B per i partecipanti.

- Per il partecipante di origine, il numero di definizioni del flusso di documenti che è necessario impostare (in **Imposta origine**) varia in base al tipo di flusso di documenti.
  - Ad esempio, per un documento XML in cui il flusso documenti è ICGPO e la transazione EDI convertita è MX12V3R1, abilitare tre definizioni del flusso di documenti (in **Imposta origine**) - una per il documento XML (ICGPO), una per la transazione EDI (MX12V3R1) e una per la busta inviata dall'hub.
  - Per altri documenti XML e ROD, abilitare due definizioni del flusso di documenti (in **Imposta origine**) - una per il documento XML o ROD e una per la busta inviata dall'hub.

I passi dettagliati per la creazione delle funzioni B2B sono descritti in "Impostazione delle funzioni B2B" a pagina 146.

Una volta impostate le funzioni B2B per i partecipanti, creare le connessioni. Sono necessari varie connessioni:

- Una per ciascun documento XML o ROD trasformato in una transazione EDI.
- Una per la busta dall'hub al partecipante.

I passi dettagliati per la creazione delle connessioni sono descritti in Capitolo 12, "Gestione delle connessioni", a pagina 149.

## Impostazione di un flusso di documenti XML in ROD o ROD in XML

In questa sezione, vengono descritte le interazioni necessarie per ricevere un documento XML o ROD, trasformarlo in un altro tipo di documento (XML in ROD o ROD in XML) e consegnarlo.

1. Importare la mappa di trasformazione che fornisce le definizioni dei documenti XML o ROD e che descrive in che modo i documenti vengono trasformati. Vedere "Importazione delle mappe" a pagina 110.
2. Fare clic su **Ammin hub > Configurazione hub > Mappe > Mappe di trasformazione**, quindi fare clic sull'icona **Visualizza dettagli** accanto alla mappa importata.
3. Creare un'interazione per la mappa appena importata.

- a. Fare clic su **Ammin hub > Configurazione hub > Definizioni di flusso di documenti> Gestisci interazioni.**
  - b. Fare clic su **Crea interazione.**
4. Dall'elenco Azione, selezionare i documenti di origine e di destinazione, quindi selezionare **Conversione XML e convalida EDI** o **Conversione ROD e convalida EDI.** .

Dopo aver impostato le interazioni, creare le funzioni B2B per i partecipanti.

- Per il partecipante di origine, abilitare le definizioni del flusso di documenti (in **Imposta origine**) per il documento XML o ROD.
- Per il partecipante di destinazione, abilitare le definizioni del flusso di documenti (in **Imposta destinazione**) per il documento XML o ROD.

I passi dettagliati per la creazione delle funzioni B2B sono descritti in "Impostazione delle funzioni B2B" a pagina 146.

Una volta impostate le funzioni B2B per i partecipanti, creare le connessioni. E' necessaria una connessione - per il flusso da XML a ROD o da ROD a XML. I passi dettagliati per la creazione delle connessioni sono descritti in Capitolo 12, "Gestione delle connessioni", a pagina 149.

## Impostazione di un flusso di documenti XML in XML o ROD in ROD

In questa sezione, vengono descritte le interazioni necessarie per ricevere un documento XML o ROD, trasformarlo in un documento dello stesso tipo (XML in XML o ROD in ROD) e consegnarlo.

1. Importare la mappa di trasformazione che fornisce le definizioni dei documenti XML o ROD e che descrive in che modo i documenti vengono trasformati. Vedere "Importazione delle mappe" a pagina 110.
2. Fare clic su **Ammin hub > Configurazione hub > Mappe > Mappe di trasformazione**, quindi fare clic sull'icona **Visualizza dettagli** accanto alla mappa importata.
3. Creare un'interazione per la mappa importata.
  - a. Fare clic su **Ammin hub > Configurazione hub > Definizioni di flusso di documenti> Gestisci interazioni.**
  - b. Fare clic su **Crea interazione.**
  - c. Selezionare i documenti di origine e di destinazione.
  - d. Selezionare **Conversione XML e convalida EDI** oppure **Conversione ROD e convalida EDI** dall'elenco Azione.

Dopo aver impostato le interazioni, creare le funzioni B2B per i partecipanti.

- Per il partecipante di origine, abilitare una definizione del flusso di documenti (in **Imposta origine**) per il documento XML o ROD.
- Per il partecipante di destinazione, abilitare una definizione del flusso di documenti (in **Imposta destinazione**) per il documento XML o ROD.

I passi dettagliati per la creazione delle funzioni B2B sono descritti in "Impostazione delle funzioni B2B" a pagina 146.

Una volta impostate le funzioni B2B per i partecipanti, creare le connessioni. E' necessaria una connessione - per il flusso da XML a XML o da ROD a ROD. I passi dettagliati per la creazione delle connessioni sono descritti in Capitolo 12, "Gestione delle connessioni", a pagina 149.

## 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 vengono utilizzate per fornire la generazione di riconoscimenti funzionali quando si risponde ai documenti EDI ricevuti da un partecipante. 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 sotto **Pacchetto:Nessuno** nella pagina Definizioni di flusso di documenti. &FUNC\_ACK\_META è la definizione del documento di origine per tutte le mappe di riconoscimento funzionale. Questa mappa fornisce la struttura di una notifica funzionale. Una notifica funzionale passa ai partecipanti e la relativa mappa indica al sistema il modo in cui generare la notifica. 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 vengono installate con WebSphere Partner Gateway e appaiono nella pagina Gestisci le definizioni del flusso di documenti in **Pacchetto: N/D**:

Tabella 16. Mappe di riconoscimento funzionale fornite dal sistema

Protocollo	Flusso di documenti	Descrizione
&DTCTL21	CONTRL	Riconoscimento funzionale CONTRL – UN/EDIFACT Versione 2 rilascio 1 (D94B)
&DTCTL	CONTRL	Riconoscimento funzionale CONTRL – UN/EDIFACT prima del D94B
&DT99933	999	Riconoscimento funzionale 999 – UCS Versione 3 rilascio 3
&DT99737	997	Riconoscimento funzionale 997 – X12 Versione 3 rilascio 7
&DT99735	997	Riconoscimento funzionale 997 – X12 Versione 3 rilascio 5
&DT99724	997	Riconoscimento funzionale 997 – X12 Versione 2 rilascio 4

Inoltre, il protocollo &X44TA1 (con flusso di documenti TA1 associato) viene elencato sotto **Pacchetto: N/D**. Questa mappa viene utilizzata per generare un TA1. TA1 è un riconoscimento funzionale generato per gli scambi X12 in entrata.

Anche il protocollo &WDIEVAL (con X12ENV associato) viene fornito sotto **Pacchetto: N/D**.

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 dell'interscambio di un TA1 corrisponde ad uno scambio X12 trasmesso in precedenza con lo stesso numero di controllo per completare il processo di notifica.

Al pari delle transazioni EDI e dei riconoscimenti, i TA1 sono sempre inseriti in uno scambio prima di essere consegnati.

## **Aggiunta di una notifica al flusso di documenti**

Per aggiungere una notifica ad un flusso, eseguire i passi indicati:

1. Se la mappa di notifica funzionale non è fornita da WebSphere Partner Gateway, importare la mappa dal client Data Interchange Services. Vedere "Importazione delle mappe" a pagina 110.
2. Associare la mappa FA ad una definizione del flusso di documenti:
  - a. Fare clic su **Ammin hub > Configurazione hub > Mappe > Mappe FA EDI**.
  - b. Fare clic sull'icona **Visualizza i dettagli** accanto alla mappa.
  - c. Fare clic sull'icona **Espandi** accanto al pacchetto per espandere fino al livello appropriato (ad esempio, espandere le cartelle **Pacchetto** e **Protocollo**, quindi selezionare la transazione).
  - d. Fare clic su **Salva**.
3. Creare un'interazione per la mappa appena importata.
  - a. Fare clic su **Ammin hub > Configurazione hub > Definizione del flusso di documenti > Gestisci interazioni**.
  - b. Fare clic su **Crea interazione**.
  - c. Sotto **Origine**, selezionare il flusso di documenti associato al riconoscimento funzionale. Espandere il pacchetto e il protocollo e selezionare il flusso di documenti.
  - d. Sotto **Destinazione**, selezionare gli stessi valori.
  - e. Dall'elenco Azione, selezionare **Pass Through**.
4. Verificare che la definizione di flusso di documenti esista per lo scambio EDI inviato dall'hub ed impostare gli attributi che si desidera associare allo scambio.
  - a. Fare clic su **Ammin hub > Configurazione hub > Definizione di flusso di documenti**.
  - b. Verificare se una definizione di flusso di documenti già esiste. L'origine sarà N/D, con il protocollo e il flusso di documenti che corrisponde al protocollo

- e al flusso di documenti utilizzati per consegnare lo scambio. Se, ad esempio lo scambio verrà consegnato come AS/EDI-X12/ISA, l'origine sarà N/D/EDI-X12/ISA.
- c. Modificare gli attributi che vengono applicati allo scambio consegnato.
  - d. Se la definizione del documento non esiste, crearne una selezionando Pacchetto, Protocollo e Flusso di documenti.
5. Creare un'interazione per lo scambio EDI che viene inviato dall'hub dopo che il documento è stato trasformato.
- a. Fare clic su **Ammin hub > Configurazione hub > Definizioni di flusso di documenti > Gestisci interazioni**.
  - b. Fare clic su **Crea interazione**.
  - c. Selezionare i documenti di origine e di destinazione.
  - d. Selezionare **Pass Through** dall'elenco **Azione**.

Dopo aver impostato le interazioni, creare le funzioni B2B per i partecipanti. Si noti che il partecipante di destinazione in una trasmissione di di notifica è il partecipante del documento EDI di origine.

- Per ciascun partecipante di origine, abilitare le definizioni del flusso di documenti (in **Imposta origine**) per la notifica funzionale. Inoltre, abilitare una definizione del flusso di documenti per la busta che sta per essere inviata dall'hub.
- Per il partecipante di destinazione, abilitare una definizione del flusso di documenti (in **Imposta destinazione**) per la notifica funzionale. Inoltre, abilitare una definizione del flusso di documenti per la busta EDI che viene ricevuta. Per la notifica funzionale, fare clic sull'icona **Modifica valori dell'attributo** accanto al protocollo, quindi specificare un profilo di busta.

I passi dettagliati per la creazione delle funzioni B2B sono descritti in "Impostazione delle funzioni B2B" a pagina 146.

Una volta impostate le funzioni B2B per i partecipanti, creare le connessioni. Sono necessarie due connessioni:

- Una per la notifica funzionale.
- Una per la busta dall'hub al partecipante.

I passi dettagliati per la creazione delle connessioni sono descritti in Capitolo 12, "Gestione delle connessioni", a pagina 149.

---

## Visualizzazione di interscambi e transazioni EDI

Come menzionato precedentemente in questo capitolo, il Visualizzatore documenti viene utilizzato per visualizzare informazioni sugli interscambi e sulle transazioni EDI che costituiscono un flusso di documenti. E' possibile visualizzare i documenti raw e i dettagli e gli eventi di elaborazione associati utilizzando criteri di ricerca specifici. Queste informazioni sono utili se si prova a determinare se un interscambio EDI è stato recapitato correttamente o determinare l'eventuale causa del problema.

Per visualizzare il Visualizzatore di documenti, fare clic su **Visualizzatori > Visualizzatore di documenti**. Per informazioni sull'utilizzo del Visualizzatore di documenti, consultare il manuale *Administrator Guide*.

---

## Capitolo 9. Creazione del profilo Gestore comunità e delle funzioni B2B

Dopo aver impostato l'hub, inclusi lo stabilire le destinazioni e l'impostazione delle definizioni di flusso di documenti e le interazioni, si è pronti per creare il Gestore comunità per la comunità hub. Si stabiliscono, quindi, le funzioni B2B del Gestore comunità. Dopo aver creato i partecipanti (come descritto in Capitolo 11, "Creazione dei partecipanti e delle funzioni B2B", a pagina 145), si attivano le connessioni effettive tra il Gestore comunità e i partecipanti, in modo che i documenti possano essere scambiati.

In questo capitolo, vengono descritti i seguenti argomenti:

- "Creazione del profilo Gestore comunità"
- "Impostazione delle capacità B2B" a pagina 124

---

### Creazione del profilo Gestore comunità

Il Gestore comunità, di solito, corrisponde alla società che possiede il server WebSphere Partner Gateway e che lo utilizza per comunicare con i partecipanti. Il Gestore comunità viene anche configurato come un partecipante dell'hub e, come tale, dispone di un profilo, di gateway e di funzioni B2B.

Per creare un profilo Gestore comunità, eseguire le seguenti procedure:

1. Fare clic su **Gestione account > Profili > Partecipante comunità**.
2. Fare clic su **Crea**.
3. Per **Nome accesso società**, immettere il nome che il Gestore comunità utilizzerà nel campo Società, quando accede all'hub. Ad esempio, è possibile immettere Gestore.
4. Per **Nome visualizzato partecipante**, immettere il nome della società o un altro nome descrittivo per il Gestore comunità. Si tratta del nome che appare nell'elenco **Ricerca partecipante**.
5. Dall'elenco Tipo partecipante, selezionare **Gestore comunità**.

**Nota:** WebSphere Partner Gateway supporta un solo Gestore comunità e un solo Operatore comunità. L'operatore comunità viene creato automaticamente quando si installa WebSphere Partner Gateway.

6. Selezionare lo stato per il Gestore comunità. Si desidera probabilmente utilizzare il valore predefinito di **Abilitato**.
7. Facoltativamente, inserire il tipo di azienda nel campo **Fornitore**.
8. Inserire facoltativamente il sito web del Gestore comunità.
9. Fare clic su **Nuovo** in **ID commerciale**.
10. Specificare un tipo dall'elenco ed immettere l'identificativo appropriato. WebSphere Partner Gateway utilizza il numero immesso qui per instradare i documenti al e dal Gestore comunità.

Osservare le seguenti direttive quando si digita l'identificativo:

- 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 di un ID aziendale al Gestore comunità. In alcuni casi, è necessario più di un ID aziendale. 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 Gestore comunità che i partecipanti coinvolti in questi tipi di flussi di documenti devono avere un ID DUNS e di Forma libera. L'ID in forma libera viene utilizzato per 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 in forma libera potrebbe essere specificato come ZZ-810810810.

11. Inserire facoltativamente un indirizzo IP per il Gestore comunità effettuando questi passaggi:
  - a. In **Indirizzo IP**, fare clic su **Nuovo**.
  - b. Specificare il tipo di gateway.
  - c. Immettere l'indirizzo IP del Gestore comunità.
12. Fare clic su **Salva**.
13. Verrà rappresentato con una password che il Gestore comunità utilizzerà per accedere sull'hub. Prendere nota della password. Verrà fornita all'utente Ammin Gestore comunità.

**Nota:** Quando si crea un profilo Gestore comunità, si crea effettivamente L'utente Admin per il gestore comunità. Gli utenti ammin creano quindi i singoli utenti nelle organizzazioni o, come Ammin hub, è possibile creare gli utenti per i partecipanti.

Dopo aver creato un profilo per il Gestore comunità, stabilire i gateway che l'hub utilizza per inviare i documenti al Gestore comunità. Per la configurazione dei gateway del Gestore comunità, fare riferimento alle seguenti sezioni:

- "Configurazione di un gateway HTTP" a pagina 129
- "Configurazione di un gateway HTTPS" a pagina 131
- "Configurazione di un gateway JMS" a pagina 134
- "Configurazione di un gateway della directory del file" a pagina 136

Dopo aver impostato i gateway per il Gestore comunità, si impostano le funzioni B2B del Gestore comunità.

---

## Impostazione delle capacità B2B

Il Gestore comunità dispone di Funzioni B2B che definiscono i tipi di documenti che possono essere inviati e ricevuti dal Gestore comunità.

Utilizzare Funzioni B2B per associare le funzioni B2B del Gestore comunità ad una definizione del flusso di documenti.

Attenersi alla seguente procedura per impostare le funzioni B2B del Gestore comunità.

1. Fare clic su **Ammin conto > Profili > Partecipante comunità**.

2. Inserire il criterio di ricerca e fare clic su **Cerca**, o fare clic su **Cerca** senza inserire alcun criterio di ricerca per visualizzare un elenco di tutti i partecipanti.
3. Fare clic sull'icona **Visualizza i dettagli** accanto al Gestore comunità.
4. Fare clic su **Capacità B2B**. Viene visualizzata la pagina Funzioni B2B. La parte destra illustra i pacchetti, i protocolli e i flussi dei documenti supportati dal sistema come definizioni del flusso di documenti.
5. Fare clic sull'icona **Il ruolo non è attivo** nella colonna **Imposta origine** per i Pacchetti a destra che contengono i documenti che il Gestore comunità invierà ai partecipanti.
6. Selezionare **Imposta destinazione** se si ricevono gli stessi documenti dai partecipanti. La console comunità visualizza un controllo se è abilitata la definizione del flusso di documenti.

**Nota:** La selezione di Imposta origine sarà uguale per tutte le azioni in un PIP in entrata e in uscita, indipendentemente dal fatto che la richiesta ha origine da un partecipante e la conferma corrispondente da un altro. Questo si applica a Imposta destinazione.

7. Fare clic sull'icona **Espandi** a livello di **Pacchetto** per espandere un nodo singolo al livello di definizione del flusso di documenti appropriato oppure selezionare un numero compreso tra **0 e 4** o **Tutti** per espandere tutte le definizioni del flusso di documenti al livello selezionato.
8. Di nuovo, selezionare **Imposta origine**, **Imposta destinazione** o entrambi i ruoli per i livelli inferiori **Protocollo** e **Flusso di documenti** per ciascuna definizione del flusso di documenti supportata dal sistema.  
Se è stata attivata una definizione a livello di **Flusso di documenti**, le definizioni **Azione** e **Attività** (se presenti) verranno attivate automaticamente.
9. Facoltativamente, fare clic su **Abilitato** nella colonna **Abilitato** per posizionare una Definizione di flusso di documenti fuori linea. (Quando si seleziona **Imposta origine** o **Imposta destinazione**, il record viene automaticamente abilitato). Fare clic su **Disabilitato** per metterlo in linea.

Se un pacchetto viene disabilitato, vengono disabilitate tutte le definizioni del flusso di documenti di livello inferiore nello stesso nodo, indipendentemente dal singolo stato in cui sono state precedentemente abilitate. Se una Definizione di flusso di documenti di livello inferiore viene disabilitata, tutte le definizioni di livello superiore nello stesso contesto rimangono abilitate. Quando una definizione di flusso di documenti viene disabilitata, tutte le connessioni preesistenti e gli attributi continuano a funzionare. La definizione di flusso di documenti disabilitata si vincola solo alla creazione di nuove connessioni.

10. Opzionalmente, fare clic sull'icona **Modifica**, se si desidera modificare uno degli attributi di un protocollo, pacchetto, flusso di documenti, azione, attività o segnale. Si visualizzano, quindi, le impostazioni per gli attributi (se disponibili). È possibile modificare gli attributi immettendo un valore o selezionandolo dalla colonna **Aggiorna** e facendo clic su **Salva**.

Come descritto in 10 a pagina 123, il Gestore comunità può (e in alcuni casi deve) disporre di più ID aziendali assegnati. Se il partecipante ha un requisito per ricevere un solo formato di ID, selezionare il valore appropriato per l'ID. Per selezionare l'ID:

- a. Fare clic sull'icona **Modifica** accanto a **Nessuno**.

Viene visualizzato l'attributo (**ID aziendale AS**) associato al pacchetto Nessuno.

- b. Dall'elenco **Aggiorna**, selezionare l'ID aziendale AS2 che è nel formato accettabile dal partecipante.
- c. Fare clic su **Salva**.

**Nota:** Se si imposta l'attributo nella pagina Funzioni B2B, viene applicato a tutti gli scambi che nascono dal Gestore comunità con il pacchetto Nessuno. Per rendere la selezione più specifica per una connessione, impostare il valore (o sovrascrivere il valore impostato qui) a livello di connessione. Fare riferimento a "Attivazione delle connessioni del partecipante" a pagina 149.

---

## Capitolo 10. Creazione gateway

Dopo aver creato i partecipanti, si definiscono i gateway per i partecipanti. I gateway definiscono i punti di entrata nel sistema del partecipante.

In questo capitolo, vengono descritti i seguenti argomenti:

- “Panoramica”
- “Impostazione dei valori globali di trasporto” a pagina 128
- “Configurazione di un proxy di inoltro” a pagina 129
- “Configurazione di un gateway HTTP” a pagina 129
- “Configurazione di un gateway HTTPS” a pagina 131
- “Configurazione di un gateway FTP” a pagina 132
- “Configurazione di un gateway SMTP” a pagina 133
- “Configurazione di un gateway JMS” a pagina 134
- “Configurazione di un gateway della directory del file” a pagina 136
- “Configurazione di un gateway FTPS” a pagina 138
- “Configurazione di un gateway script FTP” a pagina 139
- “Configurazione dei gestori” a pagina 142
- “Configurazione di un gateway per il trasporto definito dall’utente” a pagina 143
- “Specifiche di un gateway predefinito” a pagina 143

---

### Panoramica

WebSphere Partner Gateway utilizza i gateway per instradare i documenti nella destinazione corretta. Il destinatario può essere un partecipante della comunità o il Gestore comunità.

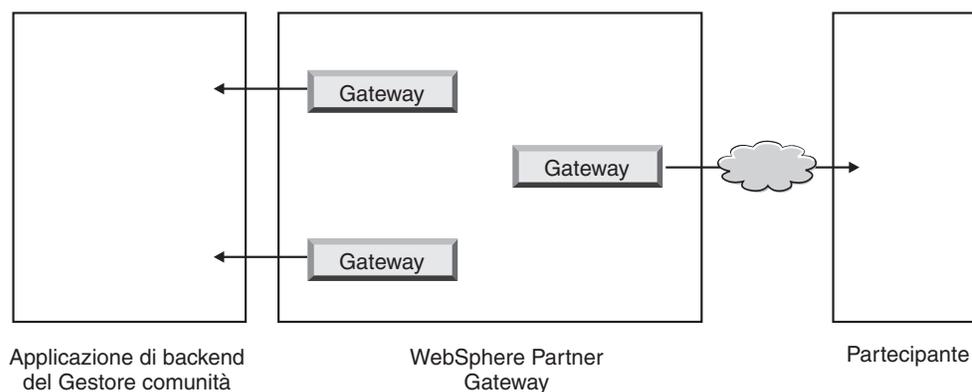


Figura 34. Gateway al Gestore comunità e partecipanti

Il protocollo di trasporto in uscita determina quali informazioni vengono utilizzate durante la configurazione del gateway.

I trasporti supportati (per impostazione predefinita) per i gateway del partecipante includono i seguenti:

- HTTP/1.1

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

**Nota:** È possibile definire un gateway SMTP solo per i partecipanti (non per il Gestore comunità).

- Directory file
- script FTP

È inoltre possibile specificare un trasporto definito dall'utente, che è possibile caricare durante la creazione del gateway.

Come Ammin hub, è possibile impostare i gateway per i partecipanti, o i partecipanti possono effettuare questa attività da soli. In questo capitolo, è possibile vedere in che modo effettuare l'attività per i partecipanti.

---

## Impostazione dei valori globali di trasporto

Si impostano gli attributi globali di trasporto che si applicano a tutti i gateway script FTP. Se non si desidera definire i gateway script FTP, saltare questa sezione.

Il trasporto di script FTP utilizza un meccanismo di blocco che impedisce a più di un'istanza di script FTP di accedere allo stesso gateway 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, inoltre, possibile utilizzare i valori predefiniti o modificarli.

1. Fare clic su **Gestione account > Profili > Partecipante comunità**.
2. Fare clic su **Gateway**.
3. Selezionare **Attributi globali di trasporto** dall'elenco Gateway.

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 corretti 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:
  - **Numero tentativi blocco**, che indica quante volte il gateway tenterà 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.
  - **Tempo max di blocco (secondi)**, che indica per quanto tempo il gateway può tenere 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

Per i trasporti HTTP e HTTPS, 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 HTTPS
- Supporto proxy su HTTPS con autenticazione
- Supporto proxy su SOCKS

Dopo aver impostato un proxy di inoltro, è possibile renderlo globale per il trasporto contrassegnandolo come gateway predefinito (ad esempio, tutti i gateway HTTP utilizzano il proxy di inoltro).

Per impostare un proxy di inoltro, attenersi alla seguente procedura:

1. Fare clic su **Gestione account > Profili > Partecipante comunità**.
2. Fare clic su **Gateway**.
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 del proxy e la relativa porta o l'host proxy socks e la porta proxy socks.
  - 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 dei sock**, immettere il server proxy SOCKS da utilizzare.
  - Per **Porta proxy dei sock**, immettere il numero della porta.
9. Selezionare la casella di controllo se si desidera che questo proxy sia quello predefinito (che può essere utilizzato da qualsiasi partecipante che abbia un supporto proxy specificato).
10. Fare clic su **Salva**.

---

## Configurazione di un gateway HTTP

Si configura un gateway HTTP in modo che i documenti possano essere inviati dall'hub all'indirizzo IP del partecipante. Quando si configura un gateway HTTP, è possibile anche specificare che i documenti vengano inviati tramite un server proxy configurato.

Per iniziare il processo di creazione di un gateway HTTP, attenersi alla seguente procedura.

1. Fare clic su **Gestione account > Profili > Partecipante comunità**.
2. Inserire il criterio di ricerca e fare clic su **Cerca**, o fare clic su **Cerca** senza inserire alcun criterio di ricerca per visualizzare un elenco di tutti i partecipanti.
3. Fare clic sull'icona **Visualizza i dettagli** per visualizzare il profilo del partecipante.
4. Fare clic su **Gateway**.
5. Fare clic su **Crea**.

## Dettagli del gateway

Nella pagina **Elenco gateway**, eseguire questi passaggi:

1. Digitare un nome per identificare il gateway. Si tratta di un campo obbligatorio. Questo è il nome che viene visualizzato nell'elenco dei gateway.
2. Facoltativamente, indicare lo stato del gateway. **Abilitato** è il valore predefinito. Un gateway che viene abilitato è pronto per inviare i documenti. Un gateway che viene disabilitato non può inviare i documenti.
3. Facoltativamente, indicare se il gateway è in linea o fuori linea. Il valore predefinito è **In linea**.
4. Facoltativamente, inserire una descrizione del gateway.

## Configurazione del gateway

Nella sezione **Configurazione del gateway** della pagina, eseguire questi passaggi:

1. Selezionare **HTTP/1.1** dall'elenco **Trasporto**.
2. 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 **Utilizza proxy di inoltro predefinito**. Se si desidera che il partecipante selezionato utilizzi un server proxy differente, selezionare quel server dall'elenco. Se non si desidera utilizzare questa funzione con il partecipante selezionato, scegliere **Non utilizzare proxy di inoltro**.
3. Nel campo **Indirizzo**, inserire l'URI in cui il documento viene recapitato. Questo campo è obbligatorio.  
Il formato è: `http://<server_name>:<optional_port>/<path>`  
Un esempio di questo formato è:  
`http://anotherserver.ibm.com:57080/bcgreceiver/Receiver`  
Quando si configura un gateway da utilizzare per un server Web, specificare l'URL privato fornito dal provider del servizio Web. Questo è dove WebSphere Partner Gateway richiama il servizio Web quando agisce come proxy per il provider del servizio Web.
4. Facoltativamente, inserire un nome utente e una password, se richiesti per accedere al server HTTP.
5. Nel campo **Conteggio tentativi**, inserire il numero di volte in cui si desidera che il gateway provi ad inviare un documento prima di non riuscire. Il valore predefinito è 3.
6. Nel campo **Intervallo tentativi**, inserire il tempo di attesa del gateway prima di provare a inviare di nuovo il documento. Il valore predefinito è 300 secondi.
7. Nel campo **Numero di thread**, inserire il numero di documenti che possono essere elaborati simultaneamente. Il valore predefinito è 3.

8. 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**.
9. Nel campo **Accodamento automatico**, selezionare **Sì** se si desidera che il gateway venga posizionato fuori linea (automaticamente), se un errore di recapito sta per verificarsi dato che il numero di tentativi è stato esaurito. Altrimenti, selezionare **No**. Il valore predefinito è **No**.  
Quando si seleziona **Accodamento automatico**, tutti i documenti rimangono in coda fino a che il gateway viene posizionato in linea manualmente.
10. Nel campo **Timeout 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 procedura di preprocesso o postprocesso per il gateway, andare a "Configurazione dei gestori" a pagina 142. Altrimenti, fare clic su **Salva**.

---

## Configurazione di un gateway HTTPS

Si configura un gateway HTTPS in modo che i documenti possano essere inviati dall'hub all'indirizzo IP del partecipante. Quando si configura un gateway HTTPS, è possibile anche specificare che i documenti vengano inviati tramite un server proxy configurato.

Per creare i gateway HTTPS, attenersi alla seguente procedura.

1. Fare clic su **Gestione account > Profili > Partecipante comunità**.
2. Inserire il criterio di ricerca e fare clic su **Cerca**, o fare clic su **Cerca** senza inserire alcun criterio di ricerca per visualizzare un elenco di tutti i partecipanti.
3. Fare clic sull'icona **Visualizza i dettagli** per visualizzare il profilo del partecipante.
4. Fare clic su **Gateway**.
5. Fare clic su **Crea**.

### Dettagli del gateway

Dalla pagina Elenco gateway, eseguire questi passaggi:

1. Digitare un nome per identificare il gateway. Questo è un campo obbligatorio.
2. Facoltativamente, indicare lo stato del gateway. **Abilitato** è il valore predefinito. Un gateway che viene abilitato è pronto per inviare i documenti. Un gateway che viene disabilitato non può inviare i documenti.
3. Facoltativamente, indicare se il gateway è in linea o fuori linea. Il valore predefinito è **In linea**.
4. Facoltativamente, inserire una descrizione del gateway.

### Configurazione del gateway

Nella sezione **Configurazione del gateway** della pagina, eseguire questi passaggi:

1. Selezionare **HTTPS/1.0** o **HTTPS/1.1** dall'elenco **Trasporto**.
2. 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 **Utilizza proxy di inoltro predefinito**. Se si desidera che il partecipante selezionato utilizzi un server proxy differente, selezionare quel server dall'elenco. Se non si desidera utilizzare questa funzione con il partecipante selezionato, scegliere **Non utilizzare proxy di inoltro**.

3. Nel campo **Indirizzo**, inserire l'URI in cui il documento viene recapitato. Questo campo è obbligatorio.  
Il formato è: `https://<server_name>:<optional_port>/<path>`  
Ad esempio:  
`https://anotherserver.ibm.com:57443/bcgreceiver/Receiver`
4. Facoltativamente, inserire un nome utente e una password, se richiedi per accedere al server HTTP protetto.
5. Nel campo **Conteggio tentativi**, inserire il numero di volte in cui si desidera che il gateway provi ad inviare un documento prima di non riuscire. Il valore predefinito è 3.
6. Nel campo **Intervallo tentativi**, inserire il tempo di attesa del gateway prima di provare a inviare di nuovo il documento. Il valore predefinito è 300 secondi.
7. Nel campo **Numero di thread**, inserire il numero di documenti che possono essere elaborati simultaneamente. Il valore predefinito è 3.
8. 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**.
9. Nel campo **Convalida Cert SSL client**, selezionare **Sì** se si desidera che il certificato digitale del partner di invio sia convalidato con l'ID aziendale associato al documento. Il valore predefinito è **No**.
10. Nel campo **Accodamento automatico**, selezionare **Sì** se si desidera che il gateway venga posizionato fuori linea (automaticamente), se un errore di recapito sta per verificarsi dato che il numero di tentativi è stato esaurito. Altrimenti, selezionare **No**. Il valore predefinito è **No**.  
Quando si seleziona **Accodamento automatico**, tutti i documenti rimangono in coda fino a che il gateway viene posizionato in linea manualmente.
11. Nel campo **Timeout connessione**, inserire il numero di secondi in cui un socket rimane aperto senza traffico. Il valore predefinito è 120 secondi.
12. Se si desidera configurare la procedura di preprocesso o postprocesso per il gateway, andare a "Configurazione dei gestori" a pagina 142. Altrimenti, fare clic su **Salva**.

---

## Configurazione di un gateway FTP

Per creare un gateway FTP, attenersi alla seguente procedura.

1. Fare clic su **Gestione account > Profili > Partecipante comunità**.
2. Inserire il criterio di ricerca e fare clic su **Cerca**, o fare clic su **Cerca** senza inserire alcun criterio di ricerca per visualizzare un elenco di tutti i partecipanti.
3. Fare clic sull'icona **Visualizza i dettagli** per visualizzare il profilo del partecipante.
4. Fare clic su **Gateway**.
5. Fare clic su **Crea**.

### Dettagli del gateway

Dalla pagina Dettagli del gateway, eseguire questi passaggi:

1. Digitare un nome per identificare il gateway. Questo è un campo obbligatorio.
2. Facoltativamente, indicare lo stato del gateway. **Abilitato** è il valore predefinito. Un gateway che viene abilitato è pronto per inviare i documenti. Un gateway che viene disabilitato non può inviare i documenti.

3. Facoltativamente, indicare se il gateway è in linea o fuori linea. Il valore predefinito è **In linea**.
4. Facoltativamente, inserire una descrizione del gateway.

## Configurazione del gateway

Nella sezione **Configurazione del gateway** della pagina, eseguire questi passaggi:

1. Selezionare **FTP** dall'elenco **Trasporto**.
2. Nel campo **Indirizzo**, inserire l'URI in cui il documento viene recapitato. Questo campo è obbligatorio.  
Il formato è: `ftp://<ftp_server_name>:<portno>`  
Ad esempio:  
`ftp://ftpsrvr1.ibm.com:2115`  
Se non si inserisce un numero di porta, si utilizza quella standard FTP.
3. Facoltativamente, inserire un nome utente e una password, se richiesti per accedere al server FTP.
4. Nel campo **Conteggio tentativi**, inserire il numero di volte in cui si desidera che il gateway provi ad inviare un documento prima di non riuscire. Il valore predefinito è 3.
5. Nel campo **Intervallo tentativi**, inserire il tempo di attesa del gateway prima di provare a inviare di nuovo 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 **Accodamento automatico**, selezionare **Sì** se si desidera che il gateway venga posizionato fuori linea (automaticamente), se un errore di recapito sta per verificarsi dato che il numero di tentativi è stato esaurito. Altrimenti, selezionare **No**. Il valore predefinito è **No**.  
Quando si seleziona **Accodamento automatico**, tutti i documenti rimangono in coda fino a che il gateway viene posizionato in linea manualmente.
9. Nel campo **Timeout connessione**, inserire il numero di secondi in cui un socket rimane aperto senza traffico. Il valore predefinito è 120 secondi.
10. Nel campo **Utilizza 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 tale casella di controllo; in questo caso WebSphere Partner Gateway assegnerà un nome al file.
11. Se si desidera configurare la procedura di preprocesso o postprocesso per il gateway, andare a "Configurazione dei gestori" a pagina 142. Altrimenti, fare clic su **Salva**.

---

## Configurazione di un gateway SMTP

Per creare un gateway SMTP, attenersi alla seguente procedura.

1. Fare clic su **Gestione account > Profili > Partecipante comunità**.
2. Inserire il criterio di ricerca e fare clic su **Cerca**, o fare clic su **Cerca** senza inserire alcun criterio di ricerca per visualizzare un elenco di tutti i partecipanti.
3. Fare clic sull'icona **Visualizza i dettagli** per visualizzare il profilo del partecipante.

4. Fare clic su **Gateway**.
5. Fare clic su **Crea**.

## Dettagli del gateway

Dalla pagina Elenco gateway, eseguire questi passaggi:

1. Digitare un nome per identificare il gateway. Questo è un campo obbligatorio.
2. Facoltativamente, indicare lo stato del gateway. **Abilitato** è il valore predefinito. Un gateway che viene abilitato è pronto per inviare i documenti. Un gateway che viene disabilitato non può inviare i documenti.
3. Facoltativamente, indicare se il gateway è in linea o fuori linea. Il valore predefinito è **In linea**.
4. Facoltativamente, inserire una descrizione del gateway.

## Configurazione del gateway

Nella sezione **Configurazione del gateway** della pagina, eseguire questi passaggi:

1. Selezionare **SMTP** dall'elenco **Trasporto**.
2. Nel campo **Indirizzo**, inserire l'URI in cui il documento viene recapitato. Questo campo è obbligatorio.  
Il formato è: `mailto:<user@server_name>`  
Ad esempio:  
`mailto:admin@anotherserver.ibm.com`
3. Facoltativamente, inserire un nome utente e una password, se richiedi per accedere al server SMTP.
4. Nel campo **Conteggio tentativi**, inserire il numero di volte in cui si desidera che il gateway provi ad inviare un documento prima di non riuscire. Il valore predefinito è 3.
5. Nel campo **Intervallo tentativi**, inserire il tempo di attesa del gateway prima di provare a inviare di nuovo 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 **Accodamento automatico**, selezionare **Sì** se si desidera che il gateway venga posizionato fuori linea (automaticamente), se un errore di recapito sta per verificarsi dato che il numero di tentativi è stato esaurito. Altrimenti, selezionare **No**. Il valore predefinito è **No**.  
Quando si seleziona **Accodamento automatico**, tutti i documenti rimangono in coda fino a che il gateway viene posizionato in linea manualmente.
9. Nel campo **Autenticazione richiesta**, indicare se un nome utente e password vengono forniti nel documento. Il valore predefinito è **No**.
10. Se si desidera configurare la procedura di preprocesso o postprocesso per il gateway, andare a "Configurazione dei gestori" a pagina 142. Altrimenti, fare clic su **Salva**.

---

## Configurazione di un gateway JMS

Per creare i gateway JMS, attenersi alla seguente procedura.

1. Fare clic su **Gestione account > Profili > Partecipante comunità**.

2. Inserire il criterio di ricerca e fare clic su **Cerca**, o fare clic su **Cerca** senza inserire alcun criterio di ricerca per visualizzare un elenco di tutti i partecipanti.
3. Fare clic sull'icona **Visualizza i dettagli** per visualizzare il profilo del partecipante.
4. Fare clic su **Gateway**.
5. Fare clic su **Crea**.

## Dettagli del gateway

Dalla pagina Elenco gateway, eseguire questi passaggi:

1. Digitare un nome per identificare il gateway. Questo è un campo obbligatorio.
2. Facoltativamente, indicare lo stato del gateway. **Abilitato** è il valore predefinito. Un gateway che viene abilitato è pronto per inviare i documenti. Un gateway che viene disabilitato non può inviare i documenti.
3. Facoltativamente, indicare se il gateway è in linea o fuori linea. Il valore predefinito è **In linea**.
4. Facoltativamente, inserire una descrizione del gateway.

## Configurazione del gateway

Nella sezione **Configurazione del gateway** della pagina, eseguire questi passaggi:

1. Selezionare **JMS** dall'elenco **Trasporto**.
2. Nel campo **Indirizzo**, inserire l'URI in cui il documento viene recapitato. Questo campo è obbligatorio.

Per WebSphere MQ JMS, il formato dell'URI di destinazione è il seguente:

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

Ad esempio:

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

La directory contiene il file ".bindings" per JNDI basato sul file. Questo file indica a WebSphere Partner Gateway in che modo instradare il documento nella destinazione prevista.

- Per un gateway JMS interno (ovvero, il gateway del sistema di back-end), dovrebbe corrispondere al valore immesso (il percorso del file system) al momento della configurazione di WebSphere Partner Gateway per JMS (passo 5 a pagina 21). 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 i gateway del partecipante, il partecipante fornisce probabilmente il file ".bindings".

Questo campo è obbligatorio.

3. Facoltativamente, inserire un nome utente e una password, se richiesti per accedere alla coda JMS.
4. Nel campo **Conteggio tentativi**, inserire il numero di volte in cui si desidera che il gateway provi ad inviare un documento prima di non riuscire. Il valore predefinito è 3.
5. Nel campo **Intervallo tentativi**, inserire il tempo di attesa del gateway prima di provare a inviare di nuovo 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 **Accodamento automatico**, selezionare **Sì** se si desidera che il gateway venga posizionato fuori linea (automaticamente), se un errore di recapito sta per verificarsi dato che il numero di tentativi è stato esaurito. Altrimenti, selezionare **No**. Il valore predefinito è **No**.  
Quando si seleziona **Accodamento automatico**, tutti i documenti rimangono in coda fino a che il gateway viene posizionato in linea manualmente.
9. Nel campo **Autenticazione richiesta**, indicare se un nome utente e password vengono forniti nel documento. Il valore predefinito è **No**.
10. 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 i gateway JMS interni, il nome deve corrispondere a quello specificato con il comando `define qcf` al momento della creazione del file di bind (passo 4 a pagina 23).  
Se viene immessa la cartella secondaria per il contesto JMS al passo 2 a pagina 135, 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).
11. Nel campo **Classe messaggio JMS**, inserire la classe messaggio. Le scelte sono tutte le classi messaggio JMS, come `TextMessage` o `BytesMessage`. Questo campo è obbligatorio.
12. Nel campo **Tipo messaggio JMS**, inserire il tipo di messaggio. Questo è un campo facoltativo.
13. Nel campo **Pacchetti URL provider**, inserire il nome delle classi (o file JAR) che Java utilizza per comprendere l'URL del contesto JMS. Questo campo è facoltativo. Se non si specifica un valore, viene utilizzato il percorso del sistema di file bindings.
14. Nel campo **Nome coda JMS**, inserire il nome della coda JMS in cui i documenti vengono inviati. Questo campo è obbligatorio.  
Per i gateway JMS interni, il nome deve corrispondere a quello specificato con il comando `define q` al momento della creazione del file di bind (passo 4 a pagina 23).  
Se viene immessa la cartella secondaria per il contesto JMS al passo 2 a pagina 135, 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`).
15. 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 come descritto in "Configurazione dell'hub per il protocollo di trasporto JMS" a pagina 21.
16. Se si desidera configurare la procedura di preprocesso o postprocesso per il gateway, andare a "Configurazione dei gestori" a pagina 142. Altrimenti, fare clic su **Salva**.

---

## Configurazione di un gateway della directory del file

Per creare i gateway della directory del file, attenersi alla seguente procedura.

1. Fare clic su **Gestione account > Profili > Partecipante comunità**.

2. Inserire il criterio di ricerca e fare clic su **Cerca**, o fare clic su **Cerca** senza inserire alcun criterio di ricerca per visualizzare un elenco di tutti i partecipanti.
3. Fare clic sull'icona **Visualizza i dettagli** per visualizzare il profilo del partecipante.
4. Fare clic su **Gateway**.
5. Fare clic su **Crea**.

## Dettagli del gateway

Dalla pagina Elenco gateway, eseguire questi passaggi:

1. Digitare un nome per identificare il gateway. Questo è un campo obbligatorio.
2. Facoltativamente, indicare lo stato del gateway. **Abilitato** è il valore predefinito. Un gateway che viene abilitato è pronto per inviare i documenti. Un gateway che viene disabilitato non può inviare i documenti.
3. Facoltativamente, indicare se il gateway è in linea o fuori linea. Il valore predefinito è **In linea**.
4. Facoltativamente, inserire una descrizione del gateway.

## Configurazione del gateway

Nella sezione **Configurazione del gateway** della pagina, eseguire questi passaggi:

1. Selezionare **Directory file** dall'elenco **Trasporto**.

2. Nel campo **Indirizzo**, inserire l'URI in cui il documento viene recapitato. Questo campo è obbligatorio.

Il formato per i sistemi UNIX e per i sistemi Windows in cui la directory del file si trova sulla stessa unità su cui è 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 del file è su un'unità a parte rispetto a quella in cui si trova WebSphere Partner Gateway, il formato è:  
`file:/// <drive_letter>:/ <path>`

3. Nel campo **Conteggio tentativi**, inserire il numero di volte in cui si desidera che il gateway provi ad inviare un documento prima di non riuscire. Il valore predefinito è 3.
4. Nel campo **Intervallo tentativi**, inserire il tempo di attesa del gateway prima di provare a inviare di nuovo 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 **Accodamento automatico**, selezionare **Sì** se si desidera che il gateway venga posizionato fuori linea (automaticamente), se un errore di recapito sta per verificarsi dato che il numero di tentativi è stato esaurito. Altrimenti, selezionare **No**. Il valore predefinito è **No**.  
 Quando si seleziona **Accodamento automatico**, tutti i documenti rimangono in coda fino a che il gateway viene posizionato in linea manualmente.
8. Nel campo **Utilizza nome file univoco**, lasciare la casella selezionata se si desidera che il documento disponga del nome di origine quando viene inviato

a destinazione. Altrimenti, deselectionarle tale casella di controllo; in questo caso WebSphere Partner Gateway assegnerà un nome al file.

9. Se si desidera configurare la procedura di preprocesso o postprocesso per il gateway, andare a "Configurazione dei gestori" a pagina 142. Altrimenti, fare clic su **Salva**.

---

## Configurazione di un gateway FTPS

Per creare i gateway FTPS, attenersi alla seguente procedura.

1. Fare clic su **Gestione account > Profili > Partecipante comunità**.
2. Inserire il criterio di ricerca e fare clic su **Cerca**, o fare clic su **Cerca** senza inserire alcun criterio di ricerca per visualizzare un elenco di tutti i partecipanti.
3. Fare clic sull'icona **Visualizza i dettagli** per visualizzare il profilo del partecipante.
4. Fare clic su **Gateway**.
5. Fare clic su **Crea**.

### Dettagli del gateway

Dalla pagina Elenco gateway, eseguire questi passaggi:

1. Digitare un nome per identificare il gateway. Questo è un campo obbligatorio.
2. Facoltativamente, indicare lo stato del gateway. **Abilitato** è il valore predefinito. Un gateway che viene abilitato è pronto per inviare i documenti. Un gateway che viene disabilitato non può inviare i documenti.
3. Facoltativamente, indicare se il gateway è in linea o fuori linea. Il valore predefinito è **In linea**.
4. Facoltativamente, inserire una descrizione del gateway.

### Configurazione del gateway

Nella sezione **Configurazione del gateway** della pagina, eseguire questi passaggi:

1. Selezionare **FTPS** dall'elenco **Trasporto**.
2. Nel campo **Indirizzo**, inserire l'URI in cui il documento viene recapitato. Questo campo è obbligatorio.  
Il formato è: `ftp://<ftp_server_name>:<portno>`  
Ad esempio:  
`ftp://ftpsrvr1.ibm.com:2115`  
Se non si inserisce un numero di porta, si utilizza quella standard FTP.
3. Facoltativamente, inserire un nome utente e una password, se richiesti per accedere al server FTP.
4. Nel campo **Conteggio tentativi**, inserire il numero di volte in cui si desidera che il gateway provi ad inviare un documento prima di non riuscire. Il valore predefinito è 3.
5. Nel campo **Intervallo tentativi**, inserire il tempo di attesa del gateway prima di provare a inviare di nuovo il documento. Il valore predefinito è 300 secondi.
6. Nel campo **Numero di thread**, inserire il numero di documenti che devono 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 **Accodamento automatico**, selezionare **Sì** se si desidera che il gateway venga posizionato fuori linea (automaticamente), se un errore di recapito sta per verificarsi dato che il numero di tentativi è stato esaurito. Altrimenti, selezionare **No**. Il valore predefinito è **No**.

Quando si seleziona **Accodamento automatico**, tutti i documenti rimangono in coda fino a che il gateway viene posizionato in linea manualmente.

9. Nel campo **Timeout connessione**, inserire il numero di secondi in cui un socket rimane aperto senza traffico. Il valore predefinito è 120 secondi.
10. Nel campo **Utilizza nome file univoco**, lasciare la casella selezionata se si desidera che il documento disponga del nome di origine quando viene inviato a destinazione. Altrimenti, deselegzionarle tale casella di controllo; in questo caso WebSphere Partner Gateway assegnerà un nome al file.
11. Se si desidera configurare la procedura di preprocesso o postprocesso per il gateway, andare a "Configurazione dei gestori" a pagina 142. Altrimenti, fare clic su **Salva**.

---

## Configurazione di un gateway script FTP

Un gateway script FTP viene eseguito secondo la pianificazione impostata. Il funzionamento di un gateway script FTP è governato da uno script di comandi FTP.

### Creazione dello script FTP

Per utilizzare un gateway script FTP, viene creato un file che include tutti i comandi FTP necessari che possono essere accettati dal server FTP.

1. Creare uno script per i gateway, per indicare le azioni da 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 inviando tutti i file nella directory specificata sul server.

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

I segnaposti (ad esempio, %BCGSERVERIP%) vengono sostituiti quando il gateway viene inserito nel servizio dai valori immessi quando si crea una istanza specifica di un gateway script FTP, come mostrato nella seguente tabella:

*Tabella 17. Come i parametri dello script mappano alle voci del campo del gateway script FTP*

Parametro dello script	Voce del campo Gateway script FTP
%BCGSERVERIP%	IP server
%BCGUSERID%	ID utente
%BCGPASSWORD%	Password
%BCGOPTIONx%	Opzionex in <b>Attributi definiti dall'utente</b>

È possibile disporre di al massimo 10 opzioni definite dall'utente.

2. Salvare il file.

### Comandi script FTP

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

- ascii, binario, passivo

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 '?').
- open  
Questo comando fa riferimento a 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 del gateway dello script FTP deve essere:  
open %BCGSERVERIP% %BCGUSERID% %BCGPASSWORD%
- quit, bye  
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.

## Gateway script FTP

Se si utilizzano gateway script FTP, eseguire queste attività:

Per creare i gateway script FTP, attenersi alla seguente procedura.

1. Fare clic su **Gestione account > Profili > Partecipante comunità**.
2. Inserire il criterio di ricerca e fare clic su **Cerca**, o fare clic su **Cerca** senza inserire alcun criterio di ricerca per visualizzare un elenco di tutti i partecipanti.
3. Fare clic sull'icona **Visualizza i dettagli** per visualizzare il profilo del partecipante.
4. Fare clic su **Gateway**.
5. Fare clic su **Crea**.

## Dettagli del gateway

Dalla pagina Elenco gateway, eseguire questi passaggi:

1. Digitare un nome per identificare il gateway. Questo è un campo obbligatorio.

2. Facoltativamente, indicare lo stato del gateway. **Abilitato** è il valore predefinito. Un gateway che viene abilitato è pronto per inviare i documenti. Un gateway che viene disabilitato non può inviare i documenti.
3. Facoltativamente, indicare se il gateway è in linea o fuori linea. Quello predefinito è **In linea**.
4. Facoltativamente, inserire una descrizione del gateway.

## Configurazione del gateway

Nella sezione **Configurazione del gateway** della pagina, eseguire questi passaggi:

1. Selezionare **Script FTP** dall'elenco **Trasporto**.
2. Immettere l'indirizzo IP del server FTP a cui si inviano i documenti. Il valore immesso sostituisce %BCGSERVERIP% quando si esegue lo script FTP.
3. 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.
4. Se la destinazione è in modalità protetta, utilizzare il valore predefinito **Sì** per **Modalità FTPS**. Altrimenti, fare clic su **No**.
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 **Sfogli**a per navigare nel file.
  - c. Fare clic su **Carica file** per caricare il file di script nella casella di testo **File di script al momento caricato**.
  - d. Se il file di script è quello che si desidera utilizzare, fare clic su **Salva**.
  - e. Fare clic su **Chiudi finestra**.
6. Nel campo **Conteggio tentativi**, immettere il numero di volte in cui si desidera che il gateway tenti di inviare un documento prima di restituire un errore. Il valore predefinito è 3.
7. Nel campo **Intervallo tentativi**, inserire il tempo di attesa del gateway prima di provare a inviare di nuovo il documento. Il valore predefinito è 300 secondi.
8. Nel campo **Timeout connessione**, inserire il numero di secondi in cui un socket rimane aperto senza traffico. Il valore predefinito è 120 secondi.
9. Nel campo **Utente blocco**, specificare se il gateway richiederà un blocco, in modo che nessuna altra istanza di un gateway script FTP possa avere accesso alla stessa directory del server FTP nello stesso momento.

**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 128.

## Attributi definiti dall'utente

Se si desidera specificare attributi aggiuntivi, eseguire questi passaggi. Il valore immesso per l'opzione sostituisce %BCGOPTIONx% 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.

## Pianifica

Nella sezione Pianifica della pagina, eseguire questi passaggi:

1. 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 gateway (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 gateway.
    - 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 procedura di preprocesso o postprocesso per il gateway, andare a "Configurazione dei gestori". Altrimenti, fare clic su **Salva**.

---

## Configurazione dei gestori

Come descritto in Capitolo 1, "Introduzione", è possibile modificare i due punti di elaborazione per un gateway--Preprocesso e Postprocesso.

Non viene fornito alcun gestore per impostazione predefinita per il preprocesso e il postprocesso e, di conseguenza, nessun gestore viene elencato nell'**elenco Disponibili**. Se è stato caricato un gestore, è possibile selezionarlo e spostarlo nell'**elenco Configurati**.

Per applicare un gestore scritto dall'utente per questi punti di configurazione, caricare prima il gestore, come descritto in "Caricamento dei gestori definiti dall'utente" a pagina 32. (Selezionare **Gateway** invece di **Destinazione** per il passo 2 a pagina 32). Eseguire quindi questi passaggi:

1. Selezionare **preprocesso** o **postprocesso** dall'elenco **Gestori del punto di configurazione**.
2. Selezionare un gestore dall'**elenco Disponibili** e fare clic su **Aggiungi**.
3. Se si desidera modificare gli attributi del gestore, selezionarlo dall'**elenco Configurati** e fare clic su **Configura**. Viene visualizzato l'elenco di attributi da modificare. Apportare le modifiche necessarie e fare clic su **Imposta valori**.
4. Fare clic su **Salva**.

È possibile modificare ulteriormente l'**elenco Configurati** come segue:

- Rimuovere un gestore selezionandolo dall'**elenco Configurati** e facendo clic su **Rimuovi**. Il gestore viene spostato nell'**elenco Disponibili**.
- Riorganizzare l'ordine nel quale il gestore viene elaborato selezionando il gestore e facendo clic su **Sposta su** o **Sposta giù**.

---

## Configurazione di un gateway per il trasporto definito dall'utente

Se si desidera caricare un trasporto definito dall'utente, effettuare questi passaggi.

1. Fare clic su **Gestione account > Profili > Partecipante comunità**.
2. Fare clic su **Gateway**.
3. Fare clic su **Gestisci tipi di trasporti**.
4. Inserire il nome di un file XML che definisce il trasporto (o utilizzare **Sfoggia** per navigare nel file).
5. Utilizzare il valore predefinito **Sì** per **Salva nel database**. Selezionare **No** se si desidera controllare questo trasporto prima di metterlo in 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 possibile anche 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 dopo che è stato utilizzato per la creazione di un gateway.

8. Fare clic su **Crea**
9. Digitare un nome per identificare il gateway. Questo è un campo obbligatorio.
10. Facoltativamente, indicare lo stato del gateway. **Abilitato** è quello predefinito. Un gateway che viene abilitato è pronto per inviare i documenti. Un gateway che viene disabilitato non può inviare i documenti.
11. Facoltativamente, indicare se il gateway è in linea o fuori linea. Il valore predefinito è **In linea**.
12. Facoltativamente, inserire una descrizione del gateway.
13. Compilare i campi (che saranno univoci per ciascun trasporto definito dall'utente), quindi fare clic su **Salva**.

---

## Specifiche di un gateway predefinito

Dopo aver creato gateway per il Gestore comunità o il partecipante, selezionarne uno come gateway predefinito.

1. Fare clic su **Gestione account > Profili > Partecipante comunità**.
2. Inserire il criterio di ricerca e fare clic su **Cerca**, o fare clic su **Cerca** senza inserire alcun criterio di ricerca per visualizzare un elenco di tutti i partecipanti.
3. Fare clic sull'icona **Visualizza i dettagli** per visualizzare il profilo del partecipante.
4. Fare clic su **Gateway**.
5. Fare clic su **Visualizza gateway predefiniti**.

Viene visualizzato un elenco di gateway definiti per il partecipante.

6. Dall'elenco **Produzione**, selezionare il gateway che sarà quello predefinito per questo partecipante. Possono essere anche impostati gateway predefiniti per altri tipi di gateway, come ad esempio **Verifica**.
7. Fare clic su **Salva**.

---

## Capitolo 11. Creazione dei partecipanti e delle funzioni B2B

Per ciascun partecipante con cui si scambieranno i documenti, viene creato un profilo del partecipante. Si impostano, quindi, le funzioni B2B dei partecipanti (o i partecipanti possano eseguire questa procedura autonomamente).

In questo capitolo, vengono descritti i seguenti argomenti:

- “Creazione dei profili dei partecipanti”
- “Impostazione delle funzioni B2B” a pagina 146

---

### Creazione dei profili dei partecipanti

Per creare un partecipante, è necessario sapere, al minimo, le seguenti informazioni corrispondenti:

- L'indirizzo IP del partecipante
- L' ID aziendale che il partecipante utilizza. 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 essere un numero che il partecipante sceglie di utilizzare per identificare l'azienda

Per ciascun partecipante che si desidera aggiungere alla comunità hub, attenersi a questa procedura:

1. Fare clic su **Gestione account > Profili > Partecipante comunità**.
2. Fare clic su **Crea**.
3. Per **Nome accesso società**, immettere il nome che il partecipante utilizzerà nel campo Società, quando accede all'hub.
4. Per **Nome visualizzato partecipante**, immettere il nome della società o un altro nome descrittivo per il partecipante. Si tratta del nome che appare nell'elenco **Ricerca partecipante**.
5. Selezionare il tipo di partecipante. Poiché WebSphere Partner Gateway può disporre di un solo Gestore comunità e di un solo Operatore comunità, la scelta è limitata al **Partecipante comunità**.
6. Selezionare lo stato per il partecipante. Quando si crea un partecipante, si desidera utilizzare il valore predefinito di **Abilitato**.
7. Facoltativamente, inserire il tipo di società nel campo **Fornitore**.
8. Inserire facoltativamente il sito web del partecipante.
9. Fare clic su **Nuovo in ID aziendale**.
10. Specificare un tipo dall'elenco e inserire l'identificativo appropriato. WebSphere Partner Gateway utilizza il numero immesso qui per instradare il documento al e dal partecipante.

Osservare le seguenti indicazioni quando si digita l'identificativo:

  - 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 di un ID aziendale ad un partecipante. In alcuni casi, è necessario più di un ID aziendale. 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 Gestore comunità che i partecipanti coinvolti in questi tipi di flussi di documenti devono avere un ID DUNS e di Forma libera. L'ID in forma libera viene utilizzato per 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 in forma libera potrebbe essere specificato come ZZ-810810810.

11. Inserire facoltativamente un indirizzo IP per il partecipante effettuando questi passaggi:
  - a. In **Indirizzo IP**, fare clic su **Nuovo**.
  - b. Specificare il tipo di gateway.
  - c. Inserire un indirizzo IP del partecipante.
12. Fare clic su **Salva**.
13. Verrà rappresentato con una password che il partecipante utilizzerà per accedere sull'hub. Prendere nota della password. Verrà fornita all'utente Ammin partecipante.

Quando si crea un partecipante, si crea effettivamente l'utente Ammin per quel partecipante. Gli utenti ammin creano quindi i singoli utenti nelle organizzazioni o, come Ammin hub, è possibile creare gli utenti per i partecipanti.

Dopo aver creato un profilo per un partecipante, stabilire i gateway che l'hub utilizza per inviare i documenti al partecipante. Per la configurazione dei gateway dei partecipanti, fare riferimento alle seguenti sezioni:

- "Impostazione dei valori globali di trasporto" a pagina 128

**Nota:** Questi valori riguardano solo il gateway Script FTP.

- "Configurazione di un gateway HTTP" a pagina 129
- "Configurazione di un gateway HTTPS" a pagina 131
- "Configurazione di un gateway FTP" a pagina 132
- "Configurazione di un gateway SMTP" a pagina 133
- "Configurazione di un gateway JMS" a pagina 134
- "Configurazione di un gateway della directory del file" a pagina 136
- "Configurazione di un gateway FTPS" a pagina 138
- "Configurazione di un gateway script FTP" a pagina 139

---

## Impostazione delle funzioni B2B

Ciascun partecipante dispone di funzioni B2B che definiscono i tipi di documenti che il partecipante può inviare e ricevere.

Come Ammin hub, è possibile impostare le funzioni B2B dei partecipanti o i partecipanti possono effettuare questa attività da soli. In questo capitolo, è possibile vedere in che modo effettuare l'attività per i partecipanti.

Si utilizzano le funzioni B2B da associare alle funzioni B2B del partecipante con una definizione di flusso di documenti.

Attenersi alla seguente procedura per impostare le funzioni B2B di ogni partecipante.

1. Fare clic su **Gestione account > Profili > Partecipante comunità**.
2. Inserire il criterio di ricerca e fare clic su **Cerca**, o fare clic su **Cerca** senza inserire alcun criterio di ricerca per visualizzare un elenco di tutti i partecipanti.
3. Fare clic sull'icona **Visualizza i dettagli** per visualizzare il profilo del partecipante.
4. Fare clic su **Funzioni B2B**. Viene visualizzata la pagina Funzioni B2B. La parte destra della pagina illustra i pacchetti, i protocolli e i documenti supportati dal sistema come definizioni del flusso di documenti.
5. Fare clic sull'icona **Il ruolo non è attivo** nella colonna **Imposta origine** per i Pacchetti nella parte destra che contengono i documenti che i partecipanti invieranno al Gestore comunità.
6. Selezionare **Imposta origine** e **Imposta destinazione** se i partecipanti invieranno e riceveranno questi stessi documenti. La Console visualizza un controllo se è abilitata la definizione del flusso di documenti.

**Nota:** La selezione di Imposta origine è la stessa per tutte le azioni PIP in 2 modi, senza tenere conto del fatto che la richiesta ha origine da un partecipante e la conferma corrispondente dall'altro. Questo si applica a Imposta destinazione.

7. Fare clic sull'icona **Espandi** sul livello **Pacchetto** per espandere un singolo nodo al livello Definizione di flusso di documenti appropriato o selezionare un numero da **0 a 4** o **Tutti** per espandere tutte le Definizioni di flusso di documenti visualizzate nel livello selezionato.
8. Di nuovo, selezionare **Imposta origine**, **Imposta destinazione** o entrambi i ruoli per i livelli inferiori **Protocollo** e **Flusso documenti** per ciascuna definizione del flusso di documenti supportata dal sistema.  
Se è stata attivata una definizione a livello di **Flusso di documenti**, le definizioni **Azione** e **Attività** (se presenti) verranno attivate automaticamente.
9. Facoltativamente, fare clic su **Abilitato** nella colonna **Abilitato** per posizionare una Definizione di flusso di documenti fuori linea. (Quando si seleziona **Imposta origine** o **Imposta destinazione**, il record viene automaticamente abilitato). Fare clic su **Disabilitato** per metterlo in linea.  
Se un pacchetto viene disabilitato, vengono disabilitate tutte le definizioni del flusso di documenti di livello inferiore in uno stesso nodo, indipendentemente dal singolo stato in cui sono state precedentemente abilitate. Se una Definizione di flusso di documenti di livello inferiore viene disabilitata, tutte le definizioni di livello superiore nello stesso contesto rimangono abilitate. Quando una definizione di flusso di documenti viene disabilitata, tutte le connessioni preesistenti e gli attributi continuano a funzionare. La definizione di flusso di documenti disabilitata si vincola solo alla creazione di nuove connessioni.
10. Opzionalmente, fare clic sull'icona **Modifica**, se si desidera modificare uno degli attributi di un protocollo, pacchetto, flusso di documenti, 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**.



---

## Capitolo 12. Gestione delle connessioni

Dopo aver creato le funzioni B2B dei partecipanti, si stabiliscono le connessioni tra il Gestore comunità e i partecipanti. In questo capitolo, vengono descritti i seguenti argomenti:

- “Panoramica”
- “Attivazione delle connessioni del partecipante”
- “Specifica e modifica di attributi” a pagina 150

---

### Panoramica

Si configura una connessione tra partecipanti per ciascun tipo di documento che verrà scambiato. Si potrebbe, ad esempio, disporre di più connessioni dal Gestore comunità per lo stesso partecipante, perché l’impacchettamento, il protocollo, il flusso di documenti, l’azione o la mappa potrebbe essere differente.

Quando si attivano le connessioni, è possibile specificare gli attributi per il partecipante di origine e di destinazione. Gli attributi impostati sul livello della connessione hanno la precedenza sugli attributi impostati sul livello delle funzioni B2B (per un partecipante in particolare) o sul livello della definizione di flusso di documenti.

Per i documenti EDI, XML e ROD, si dispone di più connessioni per ciascuno scambio, se lo scambio coinvolge l’imbustamento e la trasformazione. Si possono definire connessioni per questi tipi di documenti selezionandole da un insieme di profili associati alla connessione. Fare riferimento a “Profili connessione” a pagina 104 per i dettagli.

---

### Attivazione delle connessioni del partecipante

Le connessioni del partecipante contengono le informazioni necessarie per lo scambio corretto di ogni flusso di documenti. Un documento non può essere instradato a meno che non esista una connessione tra il gestore comunità e uno dei suoi partecipanti.

Il sistema crea automaticamente le connessioni tra il Gestore comunità e i partecipanti in base alle funzioni B2B.

Si ricercano queste connessioni e si attivano.

Quando si seleziona Origine e Destinazione, osservare le seguenti indicazioni:

- L’Origine e la Destinazione devono essere uniche.
- Non scambiare un gateway di produzione con un gateway di prova quando si selezionano Origine e Destinazione; altrimenti, si verifica un errore.
- Sia l’Origine che la Destinazione devono essere gateway di verifica e di produzione.

Attenersi alla seguente procedura per effettuare la ricerca di base per le connessioni e quindi attivarle.

1. Fare clic su **Gestione account > Connessioni partecipante**. Viene visualizzata la pagina Gestisci connessioni.

2. In **Origine**, selezionare un'origine. Se, ad esempio, si configura uno scambio che proviene dal Gestore comunità, selezionare Gestore comunità.
3. In **Destinazione**, selezionare una destinazione. Se, ad esempio, si configura uno scambio che verrà ricevuto da un partecipante, selezionare quel partecipante.

**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. In questa pagina viene mostrato il pacchetto, il protocollo e il flusso di documenti 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, vedere "Specifica e modifica di attributi".

Se il PIP è un PIP di due azioni, attivare la connessione in entrambe le connessioni per supportare la seconda azione del PIP. Per fare ciò, 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

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.

Si supponga, ad esempio, che il Gestore comunità stia inviando un documento assemblato come Nessuno ad un partecipante. Il partecipante riceverà il documento assemblato come AS. Il Gestore comunità può disporre di più di un ID aziendale ad esso assegnato. 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 dall'elenco **Aggiorna** l'ID AS che si desidera inviare al partecipante.
- d. Fare clic su **Salva**.

**Nota:** Se, in precedenza, è stato specificato un ID AS (nella pagina Funzioni B2B, ad esempio), il valore immesso sostituirà quello precedente.

Un altro esempio di impostazione di un attributo è quello di immettere un valore per l'indirizzo MDN, quando si ricevono documenti assemblati come AS da un partecipante. L'indirizzo specifica dove viene consegnato MDN.

2. Fare clic su **Azioni**, se si desidera visualizzare o modificare un'azione o una mappa di trasformazione associata a questa connessione. Qualsiasi valore modificato qui sostituisce altri valori impostati per l'azione o la mappa.

3. Fare clic su **Gateway**, se si desidera visualizzare o modificare il gateway di origine e quello 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 sul livello della connessione hanno la precedenza sugli attributi impostati sul livello del protocollo o del flusso di documenti.



---

## Capitolo 13. Impostazione di sicurezza per gli scambi in arrivo e in uscita

Con WebSphere Partner Gateway, è possibile installare ed utilizzare molti tipi di certificati per le transazioni in entrata e in uscita. In questo capitolo, sono contenuti i seguenti argomenti:

- “Termini e concetti di protezione”
- “Creazione e installazione dei certificati SSL” a pagina 157
- “Creazione e installazione dei certificati di firma” a pagina 164
- “Creazione e installazione di certificati di codifica” a pagina 166
- “Configurazione di SSL in entrata per la Console e il Destinatario” a pagina 169
- “Panoramica certificati” a pagina 169

---

### Termini e concetti di protezione

In questa sezione, viene fornita una panoramica generale sui tipi di protezione, gli strumenti utilizzati per generare e caricare i certificati e i tipi di memorizzazioni di dati installati da WebSphere Partner Gateway.

### Meccanismi di protezione e protocolli utilizzati in WebSphere Partner Gateway

Questa sezione fornisce informazioni su SSL, le firme digitali e la codifica.

#### SSL

WebSphere Partner Gateway può utilizzare SSL per proteggere i documenti in entrata e in uscita. Un documento in entrata è l'unico che viene inviato all'hub. Un documento in uscita è l'unico che viene inviato dall'hub.

SSL è un protocollo generalmente utilizzato per la gestione della sicurezza in Internet. SSL fornisce connessioni protette consentendo alle due applicazioni collegate mediante la connessione di rete di autenticare ogni altra identificazione e per assicurare l'integrità e la riservatezza dei dati.

Una connessione SSL basata su HTTP è sempre iniziata dal client mediante un URL che inizia con `https://` invece di `http://`. Una connessione SSL comincia con un handshake. Durante questa fase, le applicazioni si scambiano certificati digitali, si accordano sugli algoritmi di codifica da utilizzare e generano chiavi di codifica utilizzate per il promemoria della sessione.

#### Note:

1. WebSphere Partner Gateway supporta gli algoritmi RC2 e TripleDES. Non supporta l'algoritmo RC5. Se si utilizza un algoritmo RC5 nel primo rilascio, passare ad uno di quelli supportati.
2. WebSphere Partner Gateway supporta anche gli algoritmi AES e DES. E' possibile impostare questi algoritmi nel file `bcg.properties` o con l'API `SecurityService`. Fare riferimento alla *Guida per l'amministratore* per informazioni sul file `bcg.properties`. Fare riferimento alla *Guida per il programmatore* per informazioni su `SecurityService`.

Il protocollo SSL fornisce le seguenti funzioni di sicurezza:

- L'autenticazione del server, il che significa che il server utilizza il certificato digitale per autenticarsi ai client
- L'autenticazione del client, una procedura facoltativa nella quale i client potrebbero richiedere di autenticarsi al server fornendo i propri certificati digitali

### **Firma digitale**

La firma digitale è il meccanismo per la garanzia del non-rifiuto. Non-rifiuto significa che un partecipante non può negare di aver originato e inviato un messaggio. Garantisce inoltre che un partecipante non può negare di aver ricevuto un messaggio.

Una firma digitale consente all'originator di firmare un messaggio in modo che l'originator viene verificato come la persona che ha effettivamente inviato il messaggio. Garantisce inoltre che il messaggio non è stato modificato da quando è stato firmato.

WebSphere Partner Gateway supporta formati di firma digitale PKCS#7 SignedData separati per protocolli aziendali.

### **Codifica**

WebSphere Partner Gateway utilizza un sistema di codifica noto come codifica di chiave pubblica per proteggere la comunicazione tra i partecipanti e l'hub. La codifica di chiave pubblica utilizza una coppia di chiavi matematicamente relazionate. Un documento codificato con la prima chiave deve essere decodificato con la seconda e un documento codificato con la seconda chiave deve essere decodificato con la prima.

Ogni partecipante è un sistema di chiave pubblico con una coppia di chiavi. Una delle chiavi viene conservata segretamente; questa è una chiave privata. L'altra chiave viene distribuita a chiunque la desideri; questa è una chiave pubblica. WebSphere Partner Gateway utilizza una chiave pubblica del partecipante per codificare un documento. La chiave privata viene utilizzata per decodificare un documento.

## **L'utilità iKeyman**

Come descritto nelle sezioni che seguono, si utilizza IBM Key Management Tool (iKeyman) per creare i database della chiave, coppie di chiavi pubbliche e private e richieste di certificato. È inoltre possibile utilizzare iKeyman per creare certificati autofirmati. L'utilità iKeyman si trova nella directory `/<ProductDir>/was/bin`, creata durante l'installazione di WebSphere Partner Gateway.

È inoltre possibile utilizzare iKeyman per generare una richiesta per un certificato all'Autorità di certificazione (CA).

## **Console comunità**

Si utilizza la Console comunità per installare tutti i certificati client, di firma e di codifica richiesti per la memoria di WebSphere Partner Gateway. È inoltre possibile utilizzare la Console comunità per installare i certificati Root e Intermedi CA (Autorità di certificazione).

**Nota:** Quando un certificato di un partecipante scade, è responsabilità del partecipante ottenere un nuovo certificato. La funzione Avviso della Console comunità include gli avvisi di scadenza del certificato per i certificati memorizzati in WebSphere Partner Gateway.

## Keystore e truststore

Quando si installa WebSphere Partner Gateway, vengono installati un keystore ed un truststore per il Destinatario e la Console.

- Un keystore è un file che contiene le chiavi pubbliche e private.
- Un truststore è un file di database delle chiavi che contiene le chiavi pubbliche per i certificati autofirmati e CA del partecipante. La chiave pubblica viene memorizzata come certificato del firmatario. Per il CA commerciale, viene aggiunto un CA root. Il file truststore può essere un file di database delle chiavi più pubblicamente accessibile che contiene tutti i certificati affidabili.

Per impostazione predefinita, i due file keystore e i due file truststore vengono creati nella directory `<ProductDir>/common/security/keystore`. I nomi sono:

- receiver.jks
- receiverTrust.jks
- console.jks
- consoleTrust.jks

### Modifica della password predefinita

La password predefinita per l'accesso a tutte e quattro le memorie è WebAS. WebSphere Application Server integrato viene configurato per utilizzare queste quattro memorie. E' possibile utilizzare l'utilità iKeyman per modificare la password. In alternativa, è possibile utilizzare il seguente comando UNIX per modificare la password del file key store:

```
/<ProductDir>/console/was/java/bin/keytool
-storepasswd -new $NEW_PASSWORD$ -keystore $KEYSTORE_LOCATION$
-storepass $CURRENT_PASSWORD$ -storetype JKS
```

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:

```
/<ProductDir>/bin
```

ed inviare il seguente comando:

```
./bcgwsadmin.sh -f /<ProductDir>/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 di un 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**.

## Catene di certificati

Una catena di certificati è costituita del certificato del partecipante e dei certificati utilizzati per autenticare il certificato del partecipante. Se, ad esempio, l'autorità di certificazione è stata utilizzata per creare il certificato del partecipante, quella autorità potrebbe essere stata certificata da un'altra autorità 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 l'aggancio dei trust e il certificato del partecipante (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'autorità di certificazione (CA), oppure può essere un certificato autofirmato generato dal partecipante.

## 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. 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 partecipante
- Firma del certificato dell'operatore hub
- Certificato del Client SSL dell'operatore hub

## Modifica dell'intensità della codifica

Si noti la seguente importante limitazione sull'utilizzo dei certificati di 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 limitazioni di codifica su algoritmi di chiavi simmetriche, come ad esempio DES3. Se è necessario un algoritmo di chiave simmetrica forte, la sostituzione del file di politica rimuove anche le limitazioni per le chiavi simmetriche.

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 non limitati dal link **File criteri IBM SDK** al seguente indirizzo web:  
<http://www.ibm.com/developerworks/java/jdk/security/142/>.
2. Decomprimere il file scaricato in una cartella temporanea
3. Copiare local\_policy.jar e US\_export\_policy.jar dalla cartella temporanea.
4. Passare alla cartella `<ProductDir>\was\java\jre\lib\security`.
5. Ridenominare i file local\_policy.jar e US\_export\_policy.jar esistenti come local\_policy.jar.bak e US\_export\_policy.jar.bak
6. Incollare i file jar copiati al passo 3 nella cartella `<ProductDir>\was\java\jre\lib\security`.
7. Riavviare il server.

Questi passi si applicano a tutte le istanze di WebSphere Application Server configurate.

---

## Creazione e installazione dei certificati 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 partecipanti hanno bisogno dei certificati SSL in entrata e in uscita.

### Handshake SSL

Una connessione SSL comincia con un handshake.

Quando un client (il partecipante del Gestore comunità) inizia uno scambio messaggi, vengono eseguiti questi passaggi:

1. Il client invia un messaggio di benvenuto al client in cui vengono elencate le funzioni di codifica del client (ordinate secondo l'ordine di preferenza del client), come ad esempio la versione di SSL, il pacchetto 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 (pacchetto 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 pacchetto di crittografia, o altrimenti l'handshake non riesce. Il server, in genere, sceglie il pacchetto 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 pacchetto 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, 7 e 9.

L'handshake SSL termina e i dati dell'applicazione codificati possono essere inviati.

## Certificati SSL in entrata

In questa sezione, viene descritto come configurare l'autenticazione del server e quella del client per le richieste di connessione in entrata da parte dei partecipanti.

### Autenticazione del server

WebSphere Application Server utilizza il certificato SSL quando riceve le richieste di connessione dai partecipanti mediante SSL. È il certificato che il Destinatario presenta per identificare l'hub nel partecipante. 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 per generare un certificato e una coppia di chiavi. Per ulteriori informazioni sull'utilizzo di iKeyman, fare riferimento alla documentazione disponibile dall'IBM.

Dopo aver generato il certificato e una coppia di chiavi, utilizzare il certificato per il traffico in entrata SSL per tutti i partecipanti. Se si dispone di più Destinatari e Console, copiare il keystore che ne risulta in ogni istanza. Se il certificato è autofirmato, fornire questo certificato ai partecipanti. Per ottenere questo certificato, utilizzare iKeyman per estrarre il certificato pubblico in un file.

**Utilizzo di un certificato autofirmato:** Se si utilizzano i certificati del server autofirmato, attenersi alla seguente procedura.

1. Avviare l'utilità ikeyman, che viene posizionata nella directory `/<ProductDir>/was/bin`. Se questa è la prima volta che si utilizza iKeyman, eliminare il certificato "fittizio" che si trova nel keystore.
2. Utilizzare iKeyman per generare un certificato autofirmato e una coppia di chiavi per il keystore di Destinatario e 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 JCEK.
4. Installare il file nel keystore di Destinatario e Console per il quale è stato creato.
5. Distribuire il certificato ai partecipanti. Il metodo preferito per la distribuzione è l'invio del certificato in un file compresso e protetto da password, via e-mail. I partecipanti devono chiamare e richiedere la password per il file compresso.

**Utilizzo di un certificato generato da un'Autorità di certificazione:** Se si utilizza un certificato firmato da un'autorità di certificazione, attenersi alla seguente procedura.

1. Avviare l'utilità ikeyman, che viene posizionata nella directory `/<ProductDir>/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 partecipanti.

## Autenticazione del client

Se si desidera autenticare i partecipanti che inviano documenti, eseguire i passaggi contenuti in questa sezione.

**Installazione del certificato del client:** Per l'autenticazione client, attenersi alla seguente procedura:

1. Ottenere il certificato del partecipante.
2. Installare il certificato o i certificati nel truststore mediante iKeyman.
3. Posizionare il CA o i CA correlati nel keystore corrispondente.

**Nota:** Quando si aggiungono più partecipanti alla comunità hub, è possibile utilizzare iKeyman per aggiungere i propri certificati al truststore. Se un partecipante lascia la comunità, è possibile utilizzare iKeyman per rimuovere i certificati del partecipante dal truststore.

**Impostazione dell'autenticazione del client:** 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: `/<ProductDir>/bin`

2. Per attivare l'autenticazione client, chiamare lo script come segue:

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

**Nota:** Per disattivare l'autenticazione client, chiamare lo script come segue:

```
./bcgwsadmin.sh -f /<ProductDir>/receiver/scripts/bcgClientAuth.jacl
-conntype NONE clear
```

E' necessario riavviare il server bcgreceiver per applicare le modifiche.

**Convalida del certificato del client:** 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 aziendali nei documenti in entrata. Per utilizzare questa funzione, creare il profilo del partecipante, importare il certificato client e contrassegnarlo come SSL.

1. Importare il certificato del client.
  - a. Fare clic su **Gestione account > Profili > Partecipante comunità**, e cercare il profilo del partecipante.
  - b. Fare clic su **Certificati**.
  - c. Fare clic su **Carica certificato**.
  - d. Selezionare **Client SSL** come tipo di certificato.
  - e. Immettere una descrizione del certificato (necessario).
  - f. Modificare lo stato in **Abilitato**.
  - g. Fare clic su **Sfoglia** e navigare nella directory nella quale è stato salvato il certificato.
  - h. Selezionare il certificato e fare clic su **Apri**.
  - i. Se si desidera selezionare un tipo di gateway diverso da **Production** (predefinito), selezionarlo dall'elenco.
  - j. Fare clic su **Carica** e fare clic su **Salva**.
2. Aggiornare il gateway del client.
  - a. Fare clic su **Gestione account > Profili > Partecipante comunità**, e cercare il profilo del partecipante.
  - b. Fare clic su **Gateway**.
  - c. Selezionare il gateway HTTPS creato in precedenza. Se non si è ancora creato il gateway HTTPS, vedere "Configurazione di un gateway HTTPS" a pagina 131.
  - d. Fare clic sull'icona **Modifica** per modificare il gateway.
  - e. Selezionare **Sì** per **Convalida certificato SSL client**.
  - f. Fare clic su **Salva**.

## Certificato SSL in uscita

Se la comunità non utilizza SSL, non è necessario un certificato SSL in entrata o in uscita.

### Autenticazione del server

Quando SSL viene utilizzato per inviare i documenti in uscita ai partecipanti, WebSphere Partner Gateway richiede un certificato sul lato server dai partecipanti. Lo stesso certificato CA può essere utilizzato per più partecipanti. Il certificato deve essere nel formato X.509 DER.

**Nota:** E' 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 key vuoto oppure aprire un key store 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 partecipante nel profilo dell'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. Fare clic su **Certificati**.
2. Fare clic su **Carica certificati**.
3. Selezionare **Root o Intermedio** come tipo di certificato.
4. Immettere una descrizione del certificato (necessario).
5. Modificare lo stato in **Abilitato**.
6. Fare clic su **Sfoggia** e navigare nella directory nella quale è stato salvato il certificato.
7. Selezionare il certificato e fare clic su **Apri**.
8. Fare clic su **Carica** e fare clic su **Salva**.

**Nota:** Non è necessario effettuare i passaggi precedenti se il certificato CA è già installato.

### **Autenticazione del client**

Se l'autenticazione client SSL è necessaria, il partecipante richiede allora 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 un certificato autofirmato, deve essere fornito al partecipante. Se è un certificato CA firmato, il certificato root CA deve essere fornito ai partecipanti in modo che è possibile aggiungerlo ai certificati affidabili.

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 dovesse scadere o se non fosse possibile altrimenti utilizzarlo.

**Utilizzo di un certificato autofirmato:** 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 partecipanti. Il metodo preferito per la distribuzione è l'invio del certificato in un file compresso che protetto da password, via e-mail. I partecipanti devono chiamare 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 **Gestione 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.

- 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 un tipo di gateway diverso da **Production** (predefinito), selezionarlo 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:** 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 un 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 partecipanti.

## Aggiunta di un CRL (Certificate Revocation List)

WebSphere Partner Gateway include una funzione CRL (Certificate Revocation List). Il CRL, emesso da un CA (Certificate Authority), identifica i partecipanti che hanno revocato i certificati prima della data di scadenza pianificata. Ai partecipanti 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.

I CRL vengono memorizzati alla seguente posizione:

`<shared_data_directory>/security/crl`. WebSphere Partner Gateway utilizza l'impostazione `bcg.CRLDir` nel file `bcg.properties` per identificare la posizione della directory CRL.

Creare un file .crl che contiene i certificati revocati e posizionarlo nella directory CRL.

Ad esempio, nel file bcg.properties, si utilizza la seguente impostazione:  
bcg.CRLDir=/<shared\_data\_directory>/security/crl

## Abilitazione dell'accesso ai punti di distribuzione CRL

CA conserva e aggiorna i CRL. In genere, questi CRL vengono memorizzati in un punto di distribuzione CRL. I CRL vengono utilizzati durante le verifiche di richiamo dei certificati per determinare se un determinato certificato viene richiamato.

Lo script bcgSetCRLDP.jacl può essere utilizzato per abilitare o disabilitare la verifica del punto di distribuzione CRL quando viene eseguita la verifica del richiamo. Se è necessario accedere ai punti di distribuzione CRL quando viene eseguita la verifica del richiamo di un certificato abilitare l'utilizzo dei punti di distribuzione CRL. Se i certificati installati contengono un'estensione DP CRL, è possibile abilitare l'uso dei punti di distribuzione CRL, in modo che sia possibile accedervi quando viene eseguita la verifica di richiamo. Se sono stati scaricati tutti i CRL richiesti nella directory in bcg.properties per property bcg.CRLDir, non è necessario abilitare l'utilizzo dei punti di distribuzione CRL. Se i CRL correnti non sono disponibili nella directory bcg.CRLDir, è necessario abilitare l'uso dei punti di distribuzione CRL.

Sono supportati i punti di distribuzione CRL accessibili via HTTP e LDAP. Inoltre, è possibile configurare i proxy per accedere ai punti di distribuzione CRL.

**Nota:** Per le installazioni Windows, utilizzare bcgwsadmin.bat invece di ./bcgwsadmin.sh nei comandi elencati in questa sezione.

Per abilitare l'utilizzo dei punti di distribuzione CRL, eseguire il seguente comando dalla directory <ProductDir>/bin:

```
./bcgwsadmin.sh -f <ProductDir>/scripts/bcgSetCRLDP.jacl install
<nodename> <serverName> CRLDP
```

dove:

<server\_root>

La directory root del server (ad esempio,  
/opt/ibm/receiver/was/profiles/bcgreceiver)

<serverName>

Può essere bcgdocmgr, bcgreceiver, o bcgconsole. E' necessario eseguire il comando dal <server\_root> corrispondente.

Per disabilitare l'utilizzo dei punti di distribuzione CRL, eseguire questo comando dalla directory <ProductDir>/bin:

```
./bcgwsadmin.sh -f <ProductDir>/scripts/bcgSetCRLDP.jacl uninstall
<nodename> <serverName> CRLDP
```

Per abilitare l'utilizzo dei punti di distribuzione CRL con un proxy, eseguire questo comando dalla directory <ProductDir>/bin:

```
./bcgwsadmin.sh -f <ProductDir>/scripts/bcgSetCRLDP.jacl install
<nodename> <serverName> CRLDP <proxyHost> <proxyPort>
```

Per specificare che non si desidera utilizzare un proxy, eseguire questo comando dalla directory `<ProductDir>/bin`:

```
./bcgwsadmin.sh -f <ProductDir>/scripts/bcgSetCRLDP.jac1
uninstall <nodename> <serverName> PROXY
```

Se si utilizza un'uscita utente Destinatario e se l'uscita utente utilizza l'API SecurityService, le impostazioni menzionate sono applicabili anche al server bcgreceiver. Per eseguire i comandi precedentemente menzionati per il Destinatario, sostituire bcgdocmgr con bcgreceiver.

---

## Creazione e installazione dei certificati di firma

In questa sezione vengono descritti i certificati di firma utilizzati per il non rifiuto e per la verifica dell'utente che firma. .

### Certificato di firma in entrata

Il Gestore documenti utilizza il certificato firmato del partecipante per verificare la firma del mittente quando si ricevono i documenti. I partecipanti inviano i certificati di firma autofirmati nel formato X.509 DER. Dopo la ricezione si installano i certificati del partecipante mediante la Console comunità nel rispettivo profilo del partecipante.

Per installare il certificato, attenersi alla seguente procedura.

1. Ricevere il certificato di firma del partecipante nel formato X.509 DER.
2. Installare il certificato mediante la Console comunità nel profilo del partecipante.
  - a. Fare clic su **Gestione account > Profili > Partecipante comunità**, e cercare il profilo del partecipante.
  - b. Fare clic su **Certificati**.
  - c. Fare clic su **Carica certificati**.
  - d. Selezionare **Firma digitale** come tipo di certificato.
  - e. Immettere una descrizione del certificato (necessario).
  - f. Modificare lo stato in **Abilitato**.
  - g. Fare clic su **Sfoggia** e navigare nella directory nella quale è stato salvato il certificato.
  - h. Selezionare il certificato e fare clic su **Apri**.
  - i. Fare clic su **Carica** e fare clic su **Salva**.
3. 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.
  - a. Utilizzare **Gestione account > Profili > 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 **Sfoggia** 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.

- 4. Abilitare la firma sul pacchetto (livello più elevato), partecipante o livello di connessione (livello inferiore). L'impostazione sostituisce le altre al livello di connessione. Il riepilogo di connessioni informa se un attributo necessario è mancante.

Ad esempio, per modificare gli attributi di una connessione del partecipante, fare clic su **Gestione account > Connessioni partecipante** e quindi selezionare i partecipanti. Fare clic su **Attributi** e quindi modificare l'attributo (ad esempio, **AS firmato**).

## Certificato di firma in uscita

Il Gestore documenti utilizza questo certificato quando invia i documenti firmati in uscita ai partecipanti. 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 dovesse scadere o se non fosse possibile altrimenti utilizzarlo.

### Utilizzo di un certificato autofirmato

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 partecipanti. Il metodo preferito per la distribuzione è l'invio del certificato in un file compresso e protetto da password, via e-mail. I partecipanti devono chiamare 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 coppia di chiavi private nella forma di un file PKCS12 mediante la funzione del certificato della Console comunità.
  - a. Utilizzare **Gestione 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**.

#### Note:

- 1) Il file PKCS12 che sta per essere caricato dovrebbe contenere solo una chiave privata e il certificato associato.
  - 2) Si può anche caricare il certificato e la chiave privata come certificato codificato DER e come chiave privata codificata PKCS#8.
- c. Selezionare **Firma digitale** come tipo di certificato.
  - d. Immettere una descrizione (necessaria).
  - e. Modificare lo stato in **Abilitato**.
  - f. Fare clic su **Sfoggia** e navigare nella directory nella quale è stato salvato il certificato.

- g. Selezionare il certificato e fare clic su **Apri**.
  - h. Immettere una password.
  - i. Se ci fossero due certificati di firma digitale, indicare quello principale e quello secondario selezionando **Principale** o **Secondario** dall'elenco **Utilizzo certificato**.
  - j. Fare clic su **Carica** e fare clic su **Salva**.
7. Ripetere il passo 6 a pagina 165 se il partecipante ha un secondo certificato di firma.

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**

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 partecipanti.

---

## **Creazione e installazione di certificati di codifica**

In questa sezione, vengono descritti i certificati di codifica.

### **Certificato di codifica in entrata**

Il certificato viene utilizzato dall'hub per decodificare i file codificati ricevuti dai partecipanti. 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.

Si noti la seguente importante limitazione sulla ricezione di messaggi AS2 codificati da parte dei partecipanti. Se un partecipante invia AS2 codificato ma utilizza il certificato non corretto, la decodifica non riesce. Tuttavia, non viene restituito alcun MDN al partecipante per indicare l'errore. Affinché il partecipante riceva i MDN in questa situazione, creare una connessione al partecipante con la seguente definizione di flusso di documenti:

- Pacchetto: **AS**
- Protocollo: **Binario**
- Flusso di documenti: **Binario**

### **Utilizzo di un certificato autofirmato**

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 partecipanti. Questi sono necessari per importare il file nel prodotto B2B per uso come certificato di codifica. Avvisarli di utilizzarlo quando desiderano inviare i file codificati al Gestore comunità. 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 in formato file PKCS12.
6. Installare il certificato autofirmato e la coppia di chiavi private nella forma di un file PKCS12 mediante la funzione del certificato della Console comunità.
  - a. Utilizzare **Gestione 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**.

**Note:**

- 1) Il file PKCS12 che sta per essere caricato dovrebbe contenere solo una chiave privata e il certificato associato.
  - 2) Si può anche caricare il certificato e la chiave privata come certificato codificato DER e come chiave privata codificata PKCS#8.
- c. Selezionare **Codifica** 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 una password.
  - i. Fare clic su **Carica** e fare clic su **Salva**.
7. Abilitare la codifica sul pacchetto (livello più elevato), partecipante o livello di connessione (livello inferiore). 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 partecipante, fare clic su **Ammin account > Connessioni partecipante** e quindi selezionare i partecipanti. Fare clic su **Attributi** e quindi modificare l'attributo (ad esempio, **AS codificato**).

### **Utilizzo di un certificato firmato da un'Autorità di certificazione**

Se si utilizza un certificato firmato da un'autorità di certificazione, 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 un 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 partecipanti.

## **Certificato di codifica in uscita**

Il certificato di codifica in uscita viene utilizzato quando l'hub invia i documenti ai partecipanti. WebSphere Partner Gateway codifica i documenti con le chiavi pubbliche dei partecipanti e i partecipanti decodificano i documenti con le proprie chiavi private.

Il partecipante può disporre di più di un certificato di codifica. Uno è quello principale, che è quello predefinito. L'altro è quello secondario, che viene utilizzato se il certificato principale dovesse scadere o se non fosse possibile altrimenti utilizzarlo.

1. Ottenere il certificato di codifica del partecipante. Il certificato deve essere nel formato X.509 DER. Si noti che WebSphere Partner Gateway supporta solo certificati X5.09.
2. Installare il certificato mediante la Console comunità nel profilo del partecipante.
  - a. Fare clic su **Gestione account > Profili > Partecipante comunità**, e cercare il profilo del partecipante.
  - b. Fare clic su **Certificati**.
  - c. Fare clic su **Carica certificato**.
  - d. Selezionare **Codifica** come tipo di certificato.
  - e. Immettere una descrizione del certificato (necessario).
  - f. Modificare lo stato in **Abilitato**.
  - g. Fare clic su **Sfogliare** e navigare nella directory nella quale è stato salvato il certificato.
  - h. Selezionare il certificato e fare clic su **Apri**.
  - i. Se ci fossero due certificati di codifica, indicare quello principale e quello secondario selezionando **Principale** o **Secondario** dall'elenco **Utilizzo certificato**.
  - j. Fare clic su **Carica** e fare clic su **Salva**.
3. Ripetere il passaggio 2 se il partecipante ha un secondo certificato di codifica.
4. 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.
  - a. Utilizzare **Gestione account > Profili > 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 **Sfogliare** 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 la precedente procedura se il certificato CA è già installato.

5. Abilitare la codifica sul pacchetto (livello più elevato), partecipante o livello di connessione (livello inferiore). L'impostazione sostituisce le altre al livello di connessione. Il riepilogo di connessioni informa se un attributo necessario è mancante.

Ad esempio, per modificare gli attributi di una connessione del partecipante, fare clic su **Gestione account > Connessioni partecipante** e quindi selezionare i partecipanti. 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 visualizzabile anche nel Visualizzatore eventi. Si noti che questi due eventi potrebbero essere separati da altri eventi. Per aprire il Visualizzatore eventi, fare clic su **Visualizzatori > Visualizzatore eventi**.

---

## Configurazione di SSL in entrata per la Console e il Destinatario

I keystore WebSphere Partner Gateway vengono preconfigurati in WebSphere Application Server. Questa sezione è valida solo se si stanno utilizzando keystore differenti.

Per configurare SSL per la Console e il Destinatario in WebSphere Partner Gateway, attenersi alla seguente procedura.

1. Ottenere le seguenti informazioni:
  - Nomi del percorso completo del file della chiave e del file truststore; ad esempio per il Destinatario:  
`<ProductDir>/common/security/keystore/receiver.jks`  
`<ProductDir>/common/security/keystore/receiverTrust.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, JCEK, 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 modificarla in `/<ProductDir>/bin` Il server non deve essere eseguito per modificare le password.
3. Inserire il seguente comando, sostituendo i valori che sono inclusi in `<>`. È necessario inserire tutti i valori.

```
./bcgwsadmin.sh -f /<ProductDir>/
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:** Ripetere queste procedure per la Console, sostituendo **console** con **destinatario** nel nome del percorso.

---

## Panoramica certificati

Tabella 18 a pagina 170 riepiloga il modo in cui vengono utilizzati i certificati in WebSphere Partner Gateway. Le posizioni dei certificati vengono illustrate in parentesi “( )”.

Tabella 18. Informazioni di riepilogo certificato

Metodo recapito messaggio (si veda la nota 1)	Certificato operatore hub	Otteni certificato e CA dal partecipante	CA (si veda nota 2)	Invia certificato al partecipante (si veda nota 3)	Commenti
SSL in entrata	Installare sull'SSL da parte del server di WebSphere Application. (Posizionare nel keystore di WebSphere Application Server.)	N/D	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 è autenticato CA.	
SSL in uscita	Se viene utilizzata l'autenticazione del client. (WebSphere Partner Gateway)	Il certificato da parte del server del partecipante o il certificato root CA se è autenticato CA.	WebSphere Partner Gateway	Il certificato dell'operatore dell'hub se autofirmato o la chiave pubblica se firmata da una terza persona.	
Codifica in entrata	Chiave privata (WebSphere Partner Gateway)	N/D	N/D	Certificato operatore hub	Per la codifica del messaggio
Firma in entrata	N/D	Certificato per la convalida utilizzato per la firma digitale. (WebSphere Partner Gateway)	WebSphere Partner Gateway	N/D	Per la verifica e il non rifiuto
Codifica in uscita	N/D	Utilizza il certificato ottenuto dal partecipante. (Il certificato è installato nel profilo del partecipante)	CA per il certificato client se non è autorifirmato	N/D	Per la codifica di messaggi in uscita
Firma in uscita	Chiave privata (WebSphere Partner Gateway)	N/D	N/D	Facoltativo, in base al partner, rilascia la chiave privata WebSphere Partner Gateway	
Certificato per la convalida DUNS	N/D	Carica il profilo partecipante	Carica lo stesso certificato (come quello che si trova nella colonna a sinistra) nel profilo operatore hub come certificato CA		Convalida il certificato per questo ID DUNS quando viene effettuata la verifica SSL

**Note:**

1. Un messaggio in entrata in WebSphere Partner Gateway da un partecipante. Un messaggio in uscita da WebSphere Partner Gateway verso un partecipante.
2. Se il certificato è stato emesso dal CA, il certificato CA emesso deve essere memorizzato. Ciò si applica ai certificati dell'operatore hub e ai certificati del partecipante.
3. Se è coinvolta una chiave privata, il certificato corrisponde alla chiave privata.



---

## Capitolo 14. Ultimazione della configurazione

Questo capitolo descrive le attività aggiuntive che è possibile effettuare per configurare l'hub. Sono inclusi i seguenti argomenti:

- “Abilitazione all'utilizzo degli API”
- “Specifica delle code utilizzate per gli eventi”
- “Specifica degli eventi notificabili” a pagina 174
- “Aggiornamento di un trasposto definito dall'utente” a pagina 175

---

### Abilitazione all'utilizzo degli API

WebSphere Partner Gateway fornisce una serie di API che possono essere utilizzati per accedere a determinate funzioni generalmente effettuate sulla Console comunità. Questi API vengono descritti nella *Guida del programmatore*.

Attenersi a questa procedura per abilitare l'utilizzo di API basati su XML in modo che i partecipanti 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 basati su XML**.
3. Selezionare la casella di controllo per abilitare l'utilizzo dell'API basato su XML.
4. Fare clic su **Salva**.

---

### Specifica delle code utilizzate per gli eventi

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. Se non si fornisce un valore in **Pacchetti URL provider** o nei campi **URL provider JMS**, si utilizzano i valori predefiniti che sono nella sezione Proprietà MQ del file `bcg.properties`. Questi valori predefiniti utilizzano i collegamenti JMS che sono stati generati al momento dell'installazione. Se si prendono i valori predefiniti, i collegamenti JMS utilizzano la porta 9999 sul MQ Server denominato durante l'installazione.

Per puntare a un diverso gruppo di collegamenti JMS, modificare i **Pacchetti URL del provider** per puntare a una directory che contiene un file di collegamento JMS preparato dall'utente. Modificare inoltre il nome **Factory della connessione di coda** e il **Nome coda** per corrispondere ai nomi scelti nei binding JMS. È preferibile fare ciò, se si desidera pubblicare gli eventi in una coda su un server MQ diverso da quello specificato durante l'installazione.

Per indicare dove è necessario recapitare gli eventi:

1. Dal menu principale, fare clic su **Gestione sistema > Elaborazione evento > Informazioni di recapito evento**.
2. Fare clic sull'icona **Modifica** accanto a **Abilita consegna evento**.

3. Selezionare la casella di controllo **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 sistema di file.
- Per **Pacchetti URL 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 la posizione del sistema di file predefinita 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**.

---

## Specifiche degli eventi notificabili

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 in Capitolo 5, "Definizione delle destinazioni" e in Capitolo 10, "Creazione gateway", a pagina 127, 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 gateway.

Il file XML che descrive il trasporto definito dall'utente include gli attributi per il trasporto. Questi attributi vengono visualizzati (nella sezione **Personalizza attributo di trasporto**) nella pagina di destinazione o del gateway, quando si specifica un trasporto definito dall'utente. Ad esempio, un trasporto definito dall'utente per un gateway potrebbe includere l'attributo GatewayRetryCount.

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 trasporti** per caricare il file. Eventuali modifiche agli attributi si riflettono nella pagina di destinazione o nel gateway.



---

## Appendice A. Esempi di base

In questa appendice vengono forniti esempi di configurazione dell'hub. Sono inclusi i seguenti argomenti:

- “Configurazione di base – Scambio di documenti EDI autorizzati”
- “Configurazione di base - Configurazione della protezione per documenti in entrata e in uscita” a pagina 183
- “Come estendere la configurazione di base” a pagina 188

Per gli esempi di scambio EDI che includono lo sbustamento, la trasformazione, l'imbustamento e la trasmissione del riconoscimento funzionale, viene fornita un'appendice separata. Vedere Appendice B, “Esempi EDI”, a pagina 193.

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 aziendali) in base alle esigenze dell'azienda.

---

### Configurazione di base – Scambio di documenti EDI autorizzati

In questo esempio, la configurazione hub è abbastanza semplice—due destinazioni vengono definite (una per i documenti che vanno nell'hub da un partecipante e uno per i documenti che entrano nell'hub dal sistema di backend del Gestore comunità). Gli scambi configurati in questo esempio utilizzano le definizioni del flusso di documenti fornite da WebSphere Partner Gateway; di conseguenza, è necessario solo creare le interazioni basate su questi flussi. Nessun XML personalizzato viene utilizzato in questo esempio.

In questo esempio viene mostrato uno scambio tra un'applicazione back-end del Gestore comunità ed un partecipante della comunità (Partner due).

#### Configurazione hub

La prima procedura nell'impostazione dell'hub è la creazione di due destinazioni.

- Una destinazione HTTP (denominata “DestinazioneHttp”) per ricevere documenti su HTTP (dal Partner due) che devono essere inviati al sistema di back-end del Gestore comunità
- Una Destinazione della directory di file (denominata “DestinazioneSistemafile”) per recuperare i documenti dal sistema di file (dal sistema back-end del Gestore comunità) che devono essere inviati a Partner due)

#### Definizione delle destinazioni

Per creare una destinazione per la ricezione di documenti su HTTP:

1. Fare clic su **Ammin hub > Configurazione hub > Destinazioni**.
2. Fare clic su **Crea destinazione**.
3. Per Nome destinazione, digitare: **HttpTarget**.
4. Dall'Elenco dei trasporti, selezionare **HTTP/S**.
5. Per il tipo di gateway, utilizzare quello predefinito di **Produzione**.
6. Per l'URI, digitare: **/bcgreceiver/submit**
7. Fare clic su **Salva**.

Successivamente, si crea una destinazione per effettuare il polling di una directory sul sistema di file. La creazione di una destinazione automaticamente crea una nuova directory sul sistema di file.

Per creare una destinazione del sistema di file:

1. Fare clic su **Ammin hub > Configurazione hub > Destinazioni**.
2. Fare clic su **Crea destinazione**.
3. Per il Nome destinazione, digitare: **FileSystemTarget**.
4. Dall'Elenco dei trasporti, selezionare **Directory file**.
5. Per il Tipo di gateway predefinito, utilizzare il predefinito di **Produzione**.
6. Per il Percorso root del documento, digitare: **\temp\FileSystemTarget**

**Nota:** Con questa operazione viene creata una directory FileSystemTarget all'interno della directory temporanea. Verificare che la directory temporanea esista nel file system.

7. Fare clic su **Salva**.

### **Definizione di flussi di documenti e interazioni**

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 si esegue lo sbustamento dello scambio EDI e non si verifica alcuna trasformazione. Per un esempio di apertura di uno scambio, di trasformazione delle transazioni e di invio di notifiche, consultare la sezione Appendice B, "Esempi EDI", a pagina 193.

In questa sezione, vengono descritti i seguenti scambi:

- Invio di un documento EDI-X12, con nessun impacchettamento, dal Gestore comunità al Partner due
- Invio di un documento EDI-X12, compresso in AS2, dal Partner due al Gestore comunità

A causa dell'impacchettamento e dei protocolli coinvolti, non è necessario creare una nuova definizione di flusso di documenti. I pacchetti, i protocolli e i flussi di documenti sono gli unici che vengono predefiniti nel sistema.

Tuttavia, non è necessario definire le interazioni in base ai flussi di documenti predefiniti.

Creare la prima interazione, in cui il formato di origine è un documento formattato ISA conforme allo standard EDI-X12 con nessun impacchettamento e la destinazione è un documento formattato ISA conforme allo standard EDI-X12 con impacchettamento AS.

1. Fare clic su **Ammin hub > Configurazione hub > Definizione di flusso di documenti**.
2. Fare clic su **Gestisci interazioni** e quindi su **Crea interazione**.
3. Dalla colonna **Origine**, espandere:
  - a. **Pacchetto: Nessuno**
  - b. **Protocollo: EDI-X12**
4. Fare clic su **Flusso di documenti: ISA**
5. Dalla colonna **Destinazione**, espandere:
  - a. **Pacchetto: AS**
  - b. **Protocollo: EDI-X12**

6. Fare clic su **Flusso di documenti: ISA**
7. Dall'elenco **Azione**, selezionare **Passaggio autorizzato**.
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 con nessun impacchettamento:

1. Fare clic su **Crea interazione**.
2. Dalla colonna **Origine**, espandere:
  - a. **Pacchetto:AS**
  - b. **Protocollo: EDI-X12**
3. Fare clic su **Flusso di documenti: ISA**
4. Dalla colonna **Destinazione**, espandere:
  - a. **Pacchetto: Nessuno**
  - b. **Protocollo: EDI-X12**
5. Fare clic su **Flusso di documenti:ISA**
6. Dall'elenco **Azione**, selezionare **Passaggio autorizzato**.
7. Fare clic su **Salva**.

## Creazione dei partecipanti e delle connessioni del partecipante

In questo esempio, un partecipante esterno viene creato, oltre al Gestore comunità. I gateway per i partecipanti includono i trasporti standard e nessun punto di configurazione viene definito per i gateway.

### Creazione dei partecipanti

Creare due nuovi partecipanti. Per definire il Gestore comunità:

1. Fare clic su **Ammin conto** dal menu principale. La pagina Ricerca partecipante è la vista predefinita.
2. Fare clic su **Crea**.
3. Per **Nome accesso società**, digitare: **Gestcom**.
4. Per **Nome visualizzato partecipante**, digitare: **Gest com**.
5. Per il **Tipo partecipante**, selezionare **Gestore comunità**.
6. Fare clic su **Nuovo in ID commerciale**.
7. Lasciare **Tipo** come **DUNS** e inserire un valore identificativo di **123456789**.

**Nota:** Qui e in tutto il manuale, i numeri DUNS sono solo esempi.

8. Fare clic su **Nuovo in ID commerciale**.
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 **Ammin conto > Profili > Partecipante comunità**.
2. Fare clic su **Crea**.
3. Per **Nome accesso società**, digitare: **partnerdue**
4. Per **Nome visualizzato partecipante**, digitare: **Partner due**
5. Per **Tipo partecipante**, selezionare **Partecipante comunità**.

6. Fare clic su **Nuovo in ID commerciale**.
7. Lasciare **Tipo** come **DUNS** e inserire **987654321** come Identificativo.
8. Fare clic su **Nuovo in ID commerciale**.
9. Selezionare **Forma libera** e inserire un valore Identificativo di **98-7654321**
10. Fare clic su **Salva**.

Adesso sono stati definiti sia il Gestore comunità che il Partner due nell'hub.

I passi successivi sono la configurazione dei gateway per il Gestore comunità e per il Partner due.

### Creazione dei gateway

Prima di creare un gateway della directory del file per il Gestore comunità, è necessario creare la struttura della directory utilizzata da questo gateway. Creare una nuova directory FileSystemGateway sull'unità root. Questa directory viene utilizzata dal Gestore comunità per memorizzare i file ricevuti dai partecipanti.

In questo caso, il gateway rappresenta il punto di entrata nel sistema di applicazione di back-end.

Per creare un gateway per il Gestore comunità:

1. Fare clic su **Ammin conto > Profili > Partecipante comunità**.
2. Fare clic su **Cerca**.
3. Selezionare **Gest com** facendo clic sull'icona **Visualizza i dettagli**.
4. Fare clic su **Gateway** dalla barra di navigazione orizzontale.
5. Fare clic su **Crea**.
6. Per **Nome gateway**, digitare: **FileSystemGateway**
7. Per **Trasporto**, selezionare **Directory file**.
8. Per **Indirizzo**, digitare: **file://C:\FileSystemGateway**
9. Fare clic su **Salva**.

Successivamente, impostare il gateway recentemente creato come gateway predefinito per il Gestore comunità.

1. Fare clic su **Elenco** per visualizzare tutti i gateway configurati per il Gestore comunità.
2. Fare clic su **Visualizza gateway predefiniti**.
3. Dall'elenco **Produzione**, selezionare **FileSystemGateway**.
4. Fare clic su **Salva**.

Creare un gateway per il Partner due

1. Fare clic su **Ammin conto > Profili > Partecipante comunità**.
2. Fare clic su **Cerca** e quindi selezionare **Partner due** facendo clic sull'icona **Visualizza i dettagli**.
3. Fare clic sui **Gateway** dalla barra di navigazione orizzontale.
4. Fare clic su **Crea**.
5. Per **Nome gateway**, digitare: **HttpGateway**
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**.

Si noti che questo esempio presume che il Partner due richieda un nome utente e una password per qualsiasi partecipante che acceda al sistema.

È nuovamente necessario definire un gateway predefinito per questo partecipante.

1. Fare clic su **Elenco** seguito da **Visualizza gateway predefiniti**.
2. Dall'elenco **Produzione**, selezionare **HttpGateway**.
3. Fare clic su **Salva**.

### **Impostazione delle capacità B2B**

Successivamente, definire le funzioni B2B per il Gestore comunità.

1. Dal menu principale, fare clic su **Gestione account > Profili > Partecipante comunità**.
2. Fare clic su **Cerca**.
3. Selezionare **Gest com** facendo clic sull'icona **Visualizza i dettagli**.
4. Fare clic su **Capacità B2B** dalla barra di navigazione orizzontale.
5. Imposta l'Origine e la Destinazione per il pacchetto: Nessuno, Protocollo: EDI-X12, e Flusso di documenti: ISA effettuando questi passaggi:
  - a. Fare clic sull'icona **Il ruolo non è attivo** sotto **Imposta origine per Pacchetto: Nessuno**
  - b. Fare clic sull'icona **Il ruolo non è attivo** sotto **Imposta destinazione per Pacchetto: Nessuno**
  - c. Fare clic sull'icona **Espandi** accanto a **Pacchetto: Nessuno**.
  - d. Fare clic sull'icona **Il ruolo non è attivo** per **Protocollo: EDI-X12 (TUTTI)** sia per l'origine che per la destinazione.
  - e. Fare clic sull'icona **Espandi** accanto a **Protocollo: EDI-X12 (TUTTI)**.
  - f. Fare clic sull'icona **Il ruolo non è attivo** per **Flusso di documenti: ISA** sia per l'origine che per la destinazione.

Quindi, impostare le capacità B2B per il Partner due.

1. Dal menu principale, fare clic su **Ammin conto > Profili > Partecipante comunità**.
2. Fare clic su **Cerca**.
3. Selezionare Partner due facendo clic sull'icona **Visualizza i dettagli**.
4. Fare clic su **Capacità B2B** dalla barra di navigazione orizzontale.
5. Selezionare Imposta origine e Imposta destinazione per il pacchetto: AS, Protocollo: EDI-X12 e Flusso di documenti: ISA effettuando questi passaggi:
  - a. Fare clic sull'icona **Il ruolo non è attivo** sotto **Imposta origine per Pacchetto: AS**
  - b. Fare clic sull'icona **Il ruolo non è attivo** sotto **Imposta destinazione per Pacchetto: AS**
  - c. Fare clic sull'icona **Espandi** accanto a **Pacchetto: AS**.
  - d. Fare clic sull'icona **Il ruolo non è attivo** per **Protocollo: EDI-X12 (TUTTI)** sia per l'origine che per la destinazione.
  - e. Fare clic sull'icona **Espandi** accanto a **Protocollo: EDI-X12 (TUTTI)**.
  - f. Fare clic sull'icona **Il ruolo non è attivo** per **Flusso di documenti: ISA** sia per l'origine che per la destinazione.

## Definizione delle connessioni del partecipante

Definire la connessione del partecipante per i documenti EDI con nessun impacchettamento che proviene dal Gestore comunità da consegnare al Partner due.

1. Fare clic su **Ammin conto > Connessioni partecipanti**.
2. Dall'elenco **Origine**, selezionare **Gest com**.
3. Dall'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) Pacchetto: **Nessuno (N/A)**
    - 2) Protocollo: **EDI-X12 (TUTTI)**
    - 3) Flusso di documenti: **ISA (TUTTI)**
  - b. **Destinazione**
    - 1) Pacchetto: **AS (N/A)**
    - 2) Protocollo: **EDI-X12 (TUTTI)**
    - 3) Flusso di documenti: **ISA (TUTTI)**

Successivamente, definire la connessione per i documenti EDI compresi nel pacchetto AS2 che provengono dal Partner due per essere consegnati al Gestore comunità, senza alcun 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 **Ammin conto > Connessioni partecipanti**.
2. Dall'elenco **Origine**, selezionare **Partner due**.
3. Dall'elenco **Destinazione**, selezionare **Gest com**.
4. Fare clic su **Cerca**.
5. Fare clic su **Attiva** per la connessione con i seguenti dettagli:
  - a. **Origine**
    - 1) Pacchetto: **AS (N/A)**
    - 2) Protocollo: **EDI-X12 (TUTTI)**
    - 3) Flusso di documenti: **ISA (TUTTI)**
  - b. **Destinazione**
    - 1) Pacchetto: **Nessuno (N/A)**
    - 2) Protocollo: **EDI-X12 (TUTTI)**
    - 3) Flusso di documenti: **ISA (TUTTI)**

In seguito, selezionare Attributi accanto alla casella **Pacchetto: AS (N/D)** per il Partner due.

1. Modifica il pacchetto: Attributi AS (N\D) spostandosi nella pagina e facendo clic sull'icona **Espandi** accanto a **Pacchetto: AS (N/D)**.
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 - Configurazione 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 Layers)
- Codifica
- Firme digitali

### Impostazione dell'autenticazione SSL per i documenti in entrata

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 `<ProductDir>/was/bin`.
2. Aprire il file di memorizzazione predefinito delle chiavi del Destinatario, receiver.jks. Dalla barra dei menu, selezionare **Apertura del file database della chiave**. In un'installazione predefinita, receiver.jks si trova nella directory: `<ProductDir>/common/security/keystore`
3. Quando richiesto, inserire la password predefinita per receiver.jks. Questa password è WebAS.
4. Presumendo che questa è la prima volta che è stato aperto receiver.jks, eliminare il certificato "fittizio".

La procedura 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'utility di 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 ricevuta 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, Partnerdue 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. Dal menu principale, fare clic su **Ammin conto > Profili > Partecipante comunità**.
2. Fare clic su **Cerca**.
3. Selezionare **Operatore hub** facendo clic sull'icona **Visualizza i 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 **Sfoggia** 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**.

Modificare il gateway del Partner due per utilizzare l'HTTP sicuro.

1. Fare clic su **Ammin conto > Profili > Partecipante comunità** dalla barra di navigazione orizzontale.
2. Fare clic su **Cerca** e quindi selezionare Partner due facendo clic sull'icona **Visualizza i dettagli**.
3. Fare clic sui **Gateway** dalla barra di navigazione orizzontale. Selezionare poi HTTPGateway facendo clic sull'icona **Visualizza i 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

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 **Ammin conto > Profili > Partecipante comunità** dalla barra di navigazione orizzontale.
2. Fare clic su **Cerca**.
3. Selezionare **Operatore hub** facendo clic sull'icona **Visualizza i 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 **Sfoggia** 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 il Tipo di gateway come **Produzione**.
12. Fare clic su **Carica** e quindi su **Salva**.

Questo completa la configurazione necessaria per consentire a un partecipante di inviare le transazioni codificate sull'HTTP sicuro nell'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 menzionato, la chiave pubblica viene utilizzata dall'hub quando si codificano le transazioni per essere inviate al partecipante. Per fare ciò, si carica il certificato di chiave pubblica nell'hub.

1. Dal menu principale, fare clic su **Ammin conto > Profili > Partecipante comunità** .
2. Fare clic su **Cerca**.
3. Selezionare Partner due facendo clic sull'icona **Visualizza i dettagli**.
4. Fare clic sui **Certificati** dalla barra di navigazione orizzontale.
5. Fare clic su **Carica certificato**.
6. Selezionare la casella di controllo accanto a **Codifica**.
7. Modificare la Descrizione per leggere **Codifica Partner due**.
8. Impostare lo stato in **Abilitato**.
9. Fare clic su **Sfoggia**.
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 il Tipo di gateway come **Produzione**
13. Fare clic su **Carica** e fare clic su **Salva**.

Il passaggio finale nella configurazione dell'hub per inviare i messaggi codificati sull'HTTP protetto mediante AS2 è quello di modificare la connessione del partecipante che esiste tra il Gestore comunità e il Partner due.

Per modificare la connessione del partecipante dalla Console comunità:

1. Fare clic su **Gestione account > Connessioni del partecipante** dalla barra di navigazione orizzontale.
2. Dall'elenco **Origine**, selezionare **Gest com**.
3. Dall'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 questo valore facendo clic sull'icona **Espandi** accanto a **Pacchetto: AS (N/D)**.

**Nota:** È necessario spostarsi nella pagina perché questa opzione si visualizzi.

7. Dall'elenco, aggiornare l'attributo **Codificato AS** su **Sì**, quindi fare clic su **Salva**.

## Impostazione della firma del documento

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 fornisce i passaggi necessari per configurare sia l'hub che un partecipante per l'utilizzo delle 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 **Ammin conto > Profili > Partecipante comunità** dalla barra di navigazione orizzontale.
2. Fare clic su **Cerca**.
3. Selezionare Partner due facendo clic sull'icona **Visualizza i dettagli**.
4. Scegliere **Certificati** dalla barra di navigazione orizzontale.
5. Fare clic su **Carica certificato**.
6. Selezionare la casella di spunta accanto alla **Firma digitale**.
7. Modificare Descrizione in **Firma CommMan**.
8. Impostare lo **Stato** in **Abilitato**.
9. Fare clic su **Sfoggia**.
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 partecipante utilizza il certificato pubblico per autenticare le transazioni firmate inviate all'hub.

L'hub utilizza la chiave privata per firmare digitalmente le transazioni in uscita inviate al partecipante. Si abilita prima la chiave privata per la firma digitale.

Per abilitare la chiave privata per la firma digitale:

1. Fare clic su **Ammin conto > Profili > Certificati** dalla barra di navigazione orizzontale.
2. Fare clic sull'icona **Visualizza i dettagli** accanto a **Operatore hub**.
3. Fare clic sull'icona **Visualizza i 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 controllo 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**.

Successivamente, si modificano gli attributi della connessione del partecipante esistente tra il Gestore comunità e il Partner due per sistemare l'AS2 firmato.

Per alterare gli attributi della connessione del partecipante:

1. Fare clic su **Gestione account > Connessioni del partecipante** dalla barra di navigazione orizzontale.
2. Selezionare **Gest com** dall'elenco **Origine**.

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 **Pacchetto: AS (N/D)**.
7. Selezionare **Sì** dall'elenco **Firmato AS**.
8. Fare clic su **Salva**.

Questo completa la configurazione necessaria per inviare una transazione AS2 firmata da WebSphere Partner Gateway al partecipante.

---

## Come estendere la configurazione di base

Questa sezione mostra in che modo modificare la configurazione di base descritta in questo appendice. Utilizzando gli stessi partner e l'impostazione descritta precedentemente (un Gestore comunità denominato Gest com, che utilizza un ID DUNS di 123456789 e un gateway della directory del file e un partecipante denominato Partnerdue con un ID DUNS di 987654321 e un gateway HTTP), questa sezione descrive in che modo aggiungere supporto per:

- Il trasporto FTP
- Documenti XML personalizzati
- File binari (con nessun pacchetto)

### Creazione di una destinazione FTP

La destinazione FTP riceve i file e li passa al Gestore documenti per l'elaborazione. Come descritto in "Configurazione del server FTP per la ricezione dei documenti" a pagina 17, prima di creare una destinazione FTP, è necessario avere un server FTP installato ed è necessario aver creato una directory FTP e configurato 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 **Ammin hub > Configurazione hub > Destinazioni**.
2. Fare clic su **Crea destinazione**.
3. Inserire le seguenti informazioni:
  - a. Nome destinazione: **Destinatario\_FTP**
  - 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 passaggi necessari per configurare l'hub in modo da ricevere documenti binari che il Partner due desidera inviare al Gestore comunità.

#### Creazione di un'interazione per i documenti binari

Per impostazione predefinita, WebSphere Partner Gateway fornisce quattro documenti binari che implicano interazioni. In caso contrario, tuttavia, viene fornita un'interazione per i documenti binari assemblati come Nessuno per un

partecipante con un documento assemblato come Nessuno. In questa sezione, si crea l'interazione necessaria per consentire ai documenti binari il passaggio autorizzato al sistema.

1. Fare clic su **Ammin hub > Configurazione hub > Definizione di flusso di documenti**.
2. Fare clic su **Gestisci interazioni**.
3. Fare clic su **Crea interazione**.
4. Da **Origine** selezionare: **Pacchetto: Nessun Protocollo: binario (1.0) Flusso di documenti: binario (1.0)**.
5. Da **Destinazione** selezionare: **Pacchetto: Nessun Protocollo: binario (1.0) Flusso di documenti: binario (1.0)**.
6. Dall'elenco **Azione**, selezionare **Passaggio autorizzato**.
7. Fare clic su **Salva**.

### **Aggiornamento delle funzioni B2B per il Gestore comunità**

In questa sezione, viene mostrato in che modo configurare il Gestore comunità in modo da essere in grado di accettare i documenti binari.

1. Fare clic su **Ammin conto > Profili > Partecipante comunità**.
2. Fare clic su **Cerca**.
3. Fare clic sull'icona **Visualizza i dettagli** accanto a **Gest com**.
4. Fare clic sulle **Capacità B2B**.
5. Fare clic sull'icona **Il ruolo non è attivo** sotto **Imposta Destinazione** per **Pacchetto: Nessuno** in modo da abilitarlo.
6. Fare clic sull'icona **Espandi** accanto a **Pacchetto: 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 **Flusso di documenti: Binari (1.0)** in **Imposta destinazione**.

### **Aggiornamento delle capacità B2B per Partner due**

Questa sezione mostra in che modo configurare Partner due per essere in grado di inviare i documenti binari.

1. Fare clic su **Ammin conto > Profili > Partecipante comunità**.
2. Fare clic su **Cerca**.
3. Fare clic sull'icona **Visualizza i dettagli** accanto a **Partner due**.
4. Fare clic sulle **Capacità B2B**.
5. Fare clic sull'icona **Il ruolo non è attivo** sotto **Imposta origine** per **Pacchetto: Nessuno** in modo da abilitarlo.
6. Fare clic sull'icona **Espandi** accanto a **Pacchetto: 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 **Flusso di documenti: Binario (1.0)** in **Imposta origine**.

### **Creazione di una nuova connessione del partecipante**

In questa sezione, viene mostrato in che modo configurare una nuova connessione di partecipante tra il Gestore comunità e il Partner due per i documenti binari.

1. Fare clic su **Ammin conto > Connessioni partecipante**.

2. Selezionare **Partner due** dall'elenco **Origine**.
3. Selezionare **Gest com** dall'elenco **Destinazione**.
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 "Documenti XML personalizzati" a pagina 78, 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 version="1.0" encoding="UTF-8"?>
 <!DOCTYPE Tester>
 <Tester>
 <From>987654321</From>
 <To>123456789</To>
 </Tester>
```

Il Gestore documenti utilizza RootTag per identificare il tipo di documento XML. Estrae i valori dai campi Da e A per identificare il Dal nome partecipante e Nel nome partecipante.

## Creazione del formato di definizione del protocollo CustomXML

La prima procedura prevede la creazione di un nuovo protocollo per l'XML personalizzato da scambiare.

1. Fare clic su **Ammin hub > Configurazione hub > Definizione di flusso di documenti**.
2. Fare clic su **Crea definizione di flusso di documenti**.
3. Selezionare **Protocollo** dall'elenco **Tipo di flusso di documenti**.
4. Inserire le seguenti informazioni:
  - a. Codice: **CustomXML**
  - b. Versione: **1.0**
  - c. Descrizione: **CustomXML**
5. Impostare il **Livello di documento** in **No**.
6. Impostare **Stato** in **Abilitato**.
7. Impostare **Visibilità: Operatore comunità** in **Sì**.
8. Impostare **Visibilità: Gestore comunità** in **Sì**.
9. Impostare **Visibilità: Partecipante comunità** in **Sì**.
10. Selezionare:
  - a. Pacchetto: **AS**
  - b. Pacchetto: **Nessuno**
  - c. Pacchetto: **Integrazione backend**.
11. Fare clic su **Salva**.

## Creazione di una definizione del documento Tester\_XML

La seconda procedura è la creazione di una definizione di flusso di documenti per il nuovo protocollo.

1. Fare clic su **Ammin hub > Configurazione hub > Definizione di flusso di documenti**.
2. Fare clic su **Crea definizione di flusso di documenti**.
3. Selezionare **Flusso di documenti** dall'elenco **Tipo di flusso di documenti**.

4. Inserire le seguenti informazioni:
  - a. Codice: **XML\_Tester**
  - b. Versione: **1.0**
  - c. Descrizione: **XML\_Tester**
5. Impostare **Livello documento** in **Si**.
6. Impostare **Stato** in **Abilitato**.
7. Impostare **Visibilità: Operatore comunità** in **Si**.
8. Impostare **Visibilità: Gestore comunità** in **Si**.
9. Impostare **Visibilità: Partecipante comunità** su **Si**.
10. Fare clic sull'icona **Espandi** accanto a **Pacchetto: AS** e selezionare **Protocollo: CustomXML**.
11. Fare clic sull'icona **Espandi** accanto a **Pacchetto: Nessuno** e selezionare **Protocollo: CustomXML**.
12. Fare clic sull'icona **Espandi** accanto a **Pacchetto: Integrazione backend** e selezionare **Protocollo: CustomXML**.
13. Fare clic su **Salva**.

### **Creazione del formato XML Tester\_XML**

In fine, si crea il formato XML associato al nuovo protocollo.

1. Fare clic su **Ammin hub > Configurazione hub >Formati XML**.
2. Fare clic su **Crea formato XML**.
3. Selezionare **CustomXML 1.0** dall'elenco **Formato instradamento**.
4. Selezionare **XML** dall'elenco **Tipo di file**.
5. Selezionare **Tag root** dall'elenco **Tipo di identificativo**, quindi digitare **Tester** come valore.
6. Selezionare **Percorso elemento** dall'elenco **ID aziendale di origine**, quindi digitare **/Tester/From** come valore.
7. Selezionare **Percorso elemento** dall'elenco **ID aziendale di origine**, quindi immettere **/Tester/To** come valore.
8. Selezionare **Costante** dall'elenco **Flusso di documenti di origine**, quindi digitare **XML\_Tester** come valore.
9. Selezionare **Costante** dall'elenco **Versione del flusso di documenti di origine**, quindi digitare **1.0** come valore.
10. Fare clic su **Salva**.

### **Creazione di un'interazione per i documenti XML XML\_Tester**

Non si dispone di alcun nuovo protocollo e flusso di documenti con il quale impostare un'interazione.

1. Fare clic su **Ammin hub > Configurazione hub > Definizione di flusso di documenti**.
2. Fare clic su **Gestisci interazioni**.
3. Fare clic su **Crea interazione**.
4. Da **Origine**, selezionare:
  - a. **Pacchetto: Nessuno**
  - b. **Protocollo: CustomXML (1.0)**
  - c. **Flusso di documenti: XML\_Tester (1.0)**
5. Da **Destinazione** selezionare:
  - a. **Pacchetto: Nessuno**

- b. Protocollo: **CustomXML (1.0)**
  - c. Flusso di documenti: **XML\_Tester (1.0)**.
6. Dall'elenco **Azione**, selezionare **Passaggio autorizzato**.
  7. Fare clic su **Salva**.

### **Aggiornamento delle funzioni B2B per il Gestore comunità**

Per abilitare lo scambio del documento XML personalizzato, è necessario aggiornare le capacità B2B dei partecipanti.

1. Fare clic su **Ammin conto > Profili > Partecipante comunità**.
2. Fare clic su **Cerca**.
3. Fare clic sull'icona **Visualizza i dettagli** accanto a **Gest com**.
4. Fare clic sulle **Capacità B2B**.
5. Fare clic sull'icona **Il ruolo non è attivo** sotto **Imposta Destinazione** per **Pacchetto: Nessuno** in modo da abilitarlo.
6. Fare clic sull'icona **Espandi** accanto a **Pacchetto: Nessuno**.
7. Fare clic sull'icona **Il ruolo non è attivo** per **Protocollo: CustomXML (1.0)** per **Imposta destinazione**.
8. Fare clic sull'icona **Espandi** accanto a **Protocollo: CustomXML (1.0)**.
9. Infine, fare clic sull'icona **Il ruolo non è attivo** per **Flusso di documenti: XML\_Tester (1.0)** per **Imposta destinazione**.

### **Aggiornamento delle capacità B2B per partnerdue**

Si aggiornano le capacità B2B di Partner due per abilitare lo scambio del nuovo formato XML personalizzato.

1. Fare clic su **Ammin conto > Profili > Partecipante comunità**.
2. Fare clic su **Cerca**.
3. Fare clic sull'icona **Visualizza i dettagli** accanto a **Partner due**.
4. Fare clic sulle **Capacità B2B**.
5. Fare clic sull'icona **Il ruolo non è attivo** sotto **Imposta origine** per **Pacchetto: Nessuno** in modo da abilitarlo.
6. Fare clic sull'icona **Espandi** accanto a **Pacchetto: Nessuno**.
7. Fare clic sull'icona **Il ruolo non è attivo** per **Protocollo: CustomXML (1.0)** per **Imposta origine**.
8. Fare clic sull'icona **Espandi** accanto a **Protocollo: CustomXML (1.0)**.
9. Infine, fare clic sull'icona **Il ruolo non è attivo** per **Flusso di documenti: XML\_Tester (1.0)** per **Imposta origine**.

### **Creazione di una nuova connessione del partecipante**

In fine, creare una nuova connessione del partecipante.

1. Fare clic su **Ammin conto > Connessioni partecipante**.
2. Selezionare **Partner due** dall'elenco **Origine**.
3. Selezionare **Gest com** dall'elenco **Destinazione**.
4. Fare clic su **Cerca**.
5. Individuare la connessione **Nessuno (N/D)**, **CustomXML (1.0)**, **XML\_Tester (1.0)** in **Nessuno (N/D)**, **CustomXML (1.0)**, **XML\_Tester (1.0)** e fare clic su **Attiva** per attivarla.

---

## Appendice B. Esempi EDI

In questa appendice, vengono forniti esempi di invio o ricezione di scambi EDI e trasformazione degli stessi nei e dai documenti ROD (dati orientati al record).

Gli esempi contenuti in questa appendice non sono correlati a quelli contenuti in Appendice A, "Esempi di base", a pagina 177. Nuove destinazioni, gateway e profili vengono creati per gli esempi di questa appendice.

**Nota:** Un esempio di interscambio EDI che viene trasmesso tramite l'hub (nessun sbustamento o trasformazione) viene incluso in Appendice A, "Esempi di base".

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 EDI in ROD"
- "Esempio EDI in XML" a pagina 206
- "Esempio da XML a EDI" a pagina 212
- "Esempio ROD in EDI" a pagina 219

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 aziendali) in base alle esigenze dell'azienda.

---

### Esempio EDI in ROD

In questa sezione, viene fornito un esempio di invio di una transazione EDI (in una busta) all'hub, in cui viene trasformata in un documento ROD ed inviata al Gestore comunità.

#### Sbustamento e trasformazione di un interscambio EDI

In questo esempio, si presume che l'esperto delle mappature di Data Interchange Services abbia creato una mappa di trasformazione che utilizza una transazione EDI 850 standard (definita con il dizionario X12V5R1, corrispondente alla versione 5010 di X12) e la trasforma in un documento ROD (Record Oriented Document) che verrà elaborato dall'applicazione di back-end del Gestore comunità. 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 trasformazione 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 trasformazione

In questa sezione, vengono descritti i passaggi per importare una mappa di trasformazione che utilizzerà l'input EDI e lo trasformerà nel formato ROD. Nel

processo di importazione della mappa di trasformazione, si importa anche la definizione del documento associato alla mappa.

Prima che sia possibile importare la mappa di trasformazione, lo specialista della mappatura Data Interchange Services deve inviarla all'utente. Questo insieme di passaggi tiene conto che il file S\_DT\_EDT\_TO\_ROD.eif si trovi sul sistema.

1. Aprire la finestra dei comandi.
2. Immettere il seguente comando o script:

- In un sistema UNIX:

```
<ProductDir>/bin/bcgDISImport.sh <database_user_ID>
<password> S_DT_EDT_TO_ROD.eif
```

- In un sistema Windows:

```
<ProductDir>\bin\bcbDISImport.bat <database_user_ID>
<password> S_DT_EDT_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 della mappa di trasformazione e delle definizioni di flusso di documenti

Per verificare se le mappe di trasformazione e le definizioni di flusso di documenti importate sono disponibili nella Console comunità, eseguire questi passaggi:

1. Fare clic su **Ammin hub > Configurazione hub > Mappe > Mappe di trasformazione**.

Viene visualizzata la mappa S\_DT\_EDT\_TO\_ROD.

2. Fare clic sull'icona **Visualizza i dettagli** accanto alla mappa.

Si visualizzano le definizioni del flusso di documenti cui la mappa è associata:

Tabella 19. Definizione di flusso di documenti associata alla mappa

Origine	Destinazione
Pacchetto: N/D	Pacchetto: Nessuno
Protocollo: X12V5R1 (TUTTI)	Protocollo: DEMO850CL_DICTIONARY (TUTTI)
Flusso di documenti: 850 (TUTTI)	Flusso di documenti: DEMO850CLSUW (TUTTI)

La mappa S\_DT\_EDT\_TO\_ROD è stata definita per utilizzare una transazione X12 850 (conforme allo standard X12V5R1) e la trasforma in un protocollo (DEMO850CL\_DICTIONARY) e in un flusso di documenti (DEMO850CLSUW) personalizzati.

## Configurazione della destinazione

In questa sezione, si crea una destinazione della directory del sistema di file per l'hub:

1. Fare clic su **Ammin hub > Configurazione hub > Destinazioni**, quindi fare clic su **Crea destinazione**.
2. Per Nome destinazione, digitare: **EDIFileTarget**
3. Dall'Elenco dei trasporti, selezionare **Directory file**.
4. Per Percorso root, digitare: **/Data/Manager/editarget**
5. Fare clic su **Salva**.

Il partecipante della comunità invia lo scambio EDI a questa destinazione.

## Creazione delle interazioni

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 **Ammin hub > Configurazione hub > Definizione di flusso di documenti**.
2. Fare clic su **Gestisci interazioni**, quindi su **Crea interazione**.
3. In **Origine**, espandere **Pacchetto: Nessuno** e **Protocollo: EDI-X12**, quindi selezionare **Flusso di documenti: ISA**.
4. In **Destinazione**, espandere **Pacchetto: N/D** e **Protocollo: EDI-X12**, quindi selezionare **Flusso di documenti: ISA**.
5. Dall'elenco Azione, selezionare **File sbustamento**.

**Nota:** Non si verifica alcuna trasformazione in questa interazione. Lo scambio EDI viene sbustato e risulta in una singola transazione (850). Di conseguenza, non è necessaria una mappa di trasformazione 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 trasformato.

1. Fare clic su **Ammin hub > Configurazione hub > Definizione di flusso di documenti**.
2. Fare clic su **Gestisci interazioni**, quindi fare clic su **Crea interazione**.
3. In **Origine**, espandere **Pacchetto: N/D** e **Protocollo: X12V5R1**, quindi selezionare **Flusso di documenti: 850**.
4. In **Destinazione**, espandere **Pacchetto: nessuno** e **Protocollo: DEMO850CL\_DICTIONARY** e selezionare **Flusso di documenti: DEMO850CLSUW**.
5. Dall'elenco delle mappe di trasformazione, selezionare **S\_DT\_EDI\_TO\_ROD**.
6. Dall'elenco Azione, selezionare **Convalida EDI e conversione EDI**.
7. Fare clic su **Salva**.

Questa interazione rappresenta la trasformazione di una transazione EDI X12 850 standard in un formato differente e, di conseguenza, è necessario selezionare una mappa di trasformazione.

## Creazione di partecipanti

Per questo esempio, si hanno due partecipanti: Gestore comunità (Gestore) e partecipante (TP1).

Creare il profilo Gestore comunità:

1. Fare clic su **Gestione account > Profili > Partecipante comunità**, quindi fare clic su **Crea**.
2. Per Nome accesso società, digitare: **Gestcom**
3. Per Nome visualizzato partecipante, digitare: **Gestore**
4. Per Tipo partecipante, selezionare **Gestore comunità**.
5. Fare clic su **Nuovo** per l'ID aziendale e immettere 0000000000 come ID in forma libera.

**Nota:** Assicurarsi di selezionare Forma libera e non DUNS.

6. Fare di nuovo clic su **Nuovo** per l'ID aziendale e immettere 01-000000000 come ID in forma libera.
7. Fare clic su **Salva**.

Creare il secondo partecipante:

1. Fare clic su **Ammin conto > Profili > Partecipante comunità**, quindi fare clic su **Crea**.
2. Per Nome accesso società, digitare: **TP1**
3. Per Nome visualizzato partecipante, digitare, **TP1**
4. Per Tipo partecipante, selezionare **Partecipante comunità**.
5. Fare clic su **Nuovo** per l'ID aziendale e immettere 000000001 come ID in forma libera.

**Nota:** Assicurarsi di selezionare Forma libera e non DUNS.

6. Fare di nuovo clic su **Nuovo** per l'ID aziendale e immettere 01-000000001 come ID in forma libera.
7. Fare clic su **Salva**.

### Creazione dei gateway

Creare i gateway della directory del file per entrambi i partecipanti in questo esempio. In primo luogo, creare un gateway per il Gestore:

1. Fare clic su **Gestione account > Profili > Partecipante comunità**, quindi fare clic su **Cerca**.
2. Fare clic sull'icona **Visualizza i dettagli** accanto al profilo Gestore.
3. Fare clic su **Gateway**, quindi su **Crea**.
4. Immettere i seguenti valori per il gateway. Ricordare che la directory di file (l'intero percorso) deve già esistere sul sistema di file.
  - a. Per Nome, digitare **ManagerFileGateway**.
  - b. Dall'Elenco dei trasporti, selezionare **Directory file**.
  - c. Per Indirizzo, digitare: **file:///Data Manager/filegateway**
  - d. Fare clic su **Salva**.
5. Fare clic su **Elenco** per visualizzare tutti i gateway configurati per il Gestore comunità.
6. Fare clic su **Visualizza gateway predefiniti**.
7. Dall'elenco **Produzione**, selezionare il gateway creato al passo 4.
8. Fare clic su **Salva**.

In seguito, creare un gateway per il partecipante.

1. Fare clic su **Gestione account > Profili > Partecipante comunità**, quindi fare clic su **Cerca**.
2. Selezionare l'altro partecipante creato per questo esempio facendo clic sull'icona **Visualizza i dettagli** accanto a **TP1**.
3. Fare clic su **Gateway**, quindi su **Crea**.
4. Immettere i seguenti valori per il gateway. Ricordare che la directory di file (l'intero percorso) deve già esistere.
  - a. Per Nome, digitare **TP1FileGateway**.
  - b. Dall'elenco dei trasporti, selezionare **Directory file**.
  - c. Per Indirizzo, digitare: **file:///Data/TP1/filegateway**
  - d. Fare clic su **Salva**.

5. Fare clic su **Elenco** per visualizzare tutti i gateway configurati per il partecipante.
6. Fare clic su **Visualizza gateway predefiniti**.
7. Dall'elenco **Produzione**, selezionare il gateway creato al passo 4 a pagina 196.
8. Fare clic su **Salva**.

### **Impostazione delle funzioni B2B**

Abilitare le funzioni B2B dei due partecipanti in questo scambio. In questo esempio, lo scambio EDI nasce con il partecipante della comunità (TP1) e verrà consegnato al Gestore comunità.

1. Fare clic su **Gestione account > Profili > Partecipante comunità**, quindi fare clic su **Cerca**.
2. Fare clic sull'icona **Visualizza i dettagli** per il partecipante di origine per questo esempio (TP1).
3. Fare clic su **Funzioni B2B**.
4. Abilitare i due gruppi di funzioni per il partecipante di origine.
  - a. In primo luogo, abilitare la definizione di flusso di documenti che rappresenta la busta EDI:
    - 1) Fare clic sull'icona **Il ruolo non è attivo** sotto **Imposta origine** per **Pacchetto: Nessuno** in modo da abilitarlo.
    - 2) Espandere **Pacchetto: Nessuno**.
    - 3) Fare clic sull'icona **Il ruolo non è attivo** sotto **Imposta origine** per **Protocollo EDI-X12 (TUTTI)**.
    - 4) Espandere **Protocollo: EDI-X12 (TUTTI)**
    - 5) Fare clic sull'icona **Il ruolo non è attivo** sotto **Imposta origine** per **Flusso di documenti: ISA (TUTTI)**.
  - b. In seguito, abilitare la definizione del flusso di documenti che rappresenta la transazione 850:
    - 1) Fare clic sull'icona **Il ruolo non è attivo** in **Imposta origine** per **Pacchetto: N/D** per abilitarlo.
    - 2) Espandere **Pacchetto: N/D**.
    - 3) Fare clic sull'icona **Il ruolo non è attivo** sotto **Imposta origine** per **Protocollo: X12V5R1 (TUTTI)**.
    - 4) Espandere **Protocollo: X12V5R1 (TUTTI)**.
    - 5) Fare clic sull'icona **Il ruolo non è attivo** sotto **Imposta origine** per **Flusso di documenti: 850**.
5. Fare clic su **Gestione account > Profili > Partecipante comunità**, quindi fare clic su **Cerca**.
6. Fare clic sull'icona **Visualizza i dettagli** per il partecipante di destinazione per questo esempio (Gestore).
7. Fare clic su **Funzioni B2B**.
8. Abilitare i due gruppi di funzioni per il partecipante di destinazione.
  - a. In primo luogo, abilitare la definizione del flusso di documenti che rappresentano la busta:
    - 1) Fare clic sull'icona **Il ruolo non è attivo** in **Imposta destinazione** per **Pacchetto: N/D** per abilitarlo.
    - 2) Espandere **Pacchetto: N/D**.
    - 3) Fare clic sull'icona **Il ruolo non è attivo** sotto **Imposta destinazione** per **Protocollo: EDI-X12 (TUTTI)**.

- 4) Espandere **Protocollo: EDI-X12 (TUTTI)**.
  - 5) Fare clic sull'icona **Il ruolo non è attivo** sotto **Imposta destinazione per Flusso di documenti: ISA (TUTTI)**.
- b. In seguito, abilitare la definizione del flusso di documenti che rappresenta il documento trasformato:
- 1) Fare clic sull'icona **Il ruolo non è attivo** sotto **Imposta Destinazione per Pacchetto: Nessuno** in modo da abilitarlo.
  - 2) Espandere **Pacchetto: Nessuno**.
  - 3) Fare clic sull'icona **Il ruolo non è attivo** sotto **Imposta destinazione per Protocollo: DEMO850CL\_DICTIONARY (TUTTI)**.
  - 4) Espandere **Protocollo: DEMO850CL\_DICTIONARY (TUTTI)**.
  - 5) Fare clic su **Il ruolo non è attivo** sotto **Imposta destinazione per Flusso di documenti: DEMO850CLSUW(TUTTI)**.

### Attivazione delle connessioni

Per attivare le connessioni:

1. Fare clic su **Gestione account > Connessioni partecipanti**.
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 20. Connessione busta*

Origine	Destinazione
Pacchetto: Nessuno (N/D) Protocollo: EDI-X12 (TUTTI) Flusso di documenti: ISA (TUTTI)	Pacchetto: N/D (N/D) Protocollo: EDI-X12 (TUTTI) Flusso di documenti: ISA(TUTTI)

6. Fare clic su **Attiva** per la connessione che rappresenta la transazione 850 per il documento trasformato:

*Tabella 21. Connessione transazione EDI al documento ROD*

Origine	Destinazione
Pacchetto: N/D (N/D) Protocollo: X12V5R1 Flusso di documenti: 850 (TUTTI)	Pacchetto: Nessuno (N/D) Protocollo: DEMO850CL_DICTIONARY (TUTTI) Flusso di documenti: DEMO850CLSUW (TUTTI)

### Aggiunta di attributi

Impostare l'attributo che consente i documenti con ID duplicati:

1. Fare clic su **Ammin hub > Configurazione hub > Definizione di flusso di documenti**.
2. Fare clic su **Espandi** accanto a **Pacchetto: Nessuno**.
3. Fare clic sull'icona **Modifica valori dell'attributo** accanto a **Protocollo: EDI-X12**.
4. Scorrere tutta la sezione della pagina Attributi del contesto del flusso di documenti. Alla riga **Consenti documenti con ID duplicati**, selezionare **Sì** dall'elenco.
5. Fare clic su **Salva**.

A questo punto, se TP1 ha inviato uno scambio EDI che contiene una transazione 850 al Gestore comunità, lo scambio EDI dovrebbe essere sbustato e dovrebbe dare

come risultato una transazione 850. La transazione 850 dovrebbe essere, quindi, trasformata nel tipo di documento DEMO850CLS UW e il documento trasformato dovrebbe essere inviato al gateway del Gestore comunità.

## Aggiunta di un TA1 ad uno 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

Per associare la mappa con una definizione di flusso di documenti, eseguire i passi riportati:

1. Fare clic su **Ammin hub > Configurazione hub > Mappe > Mappe FA EDI**.  
Viene visualizzata la mappa &WDI\_TA1\_ACK.
2. Fare clic sull'icona **Visualizza i dettagli** accanto alla mappa.  
Si visualizzano le informazioni sulla mappa nonché una cartella per ciascun tipo di pacchetto disponibile sul sistema.
3. Creare l'associazione alla definizione di flusso di documenti eseguendo questi passaggi:
  - a. Selezionare la casella di controllo accanto a **Pacchetto: Nessuno**, quindi espandere la cartella.
  - b. Selezionare la casella di controllo accanto a **Protocollo: EDI-X12 (TUTTI)**, quindi espandere la cartella.
  - c. Selezionare la casella di controllo accanto a **Flusso di documenti: ISA (TUTTI)**.
  - d. Fare clic su **Salva**.

E' stata creata un'associazione tra la mappa &WDI\_TA1\_ACK1 e la definizione del flusso di documenti per la busta.

### Creazione interazioni

Creare un'interazione che rappresenti la transazione TA1.

1. Fare clic su **Ammin hub > Configurazione hub > Definizione di flusso di documenti**.
2. Fare clic su **Gestisci interazioni** e quindi su **Crea interazione**.
3. In **Origine**, espandere **Pacchetto: N/D** e **Protocollo: &X44TA1** e selezionare **Flusso di documenti: TA1**.
4. In **Destinazione**, espandere **Pacchetto: N/D** e **Protocollo: &X44TA1** e selezionare **Flusso di documenti: TA1**.
5. Dall'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 **Ammin hub > Configurazione hub > Definizione di flusso di documenti**.

2. Fare clic su **Gestisci interazioni**, quindi su **Crea interazione**.
3. In **Origine**, espandere **Pacchetto: N/D** e **Protocollo: EDI-X12**, quindi selezionare **Flusso di documenti: ISA**.
4. In **Destinazione**, espandere **Pacchetto: Nessuno** e **Protocollo: EDI-X12**, quindi selezionare **Flusso di documenti: ISA**.
5. Dall'elenco **Azione**, selezionare **Pass Through**.
6. Fare clic su **Salva**.

### **Abilitazione delle funzioni B2B**

In seguito, si aggiungono le interazioni appena create alle funzioni B2B dei partecipanti.

1. Fare clic su **Gestione account > Profili > Partecipante comunità**, quindi fare clic su **Cerca**.
2. Fare clic sull'icona **Visualizza i dettagli** per il partecipante di origine per questo esempio (**Gestore**).

**Nota:** Ricordare che TA1 fluisce dal partecipante che riceve il documento ROD al partecipante che lo invia. In questo esempio, il Gestore è l'origine del TA1 e il partecipante TP1 è la destinazione.

3. Fare clic su **Funzioni B2B**.
4. Abilitare i due gruppi di funzioni per il partecipante di origine.
  - a. In primo luogo, abilitare la funzionalità per TA1.
    - 1) Fare clic sull'icona **Il ruolo non è attivo** in **Imposta origine** per **Pacchetto: N/D** per abilitarlo.
    - 2) Espandere **Pacchetto: N/D**.
    - 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** sotto **Imposta origine** per **Flusso di documenti: TA1 (TUTTI)**.
  - b. In seguito, abilitare la funzionalità per la busta:
    - 1) Fare clic sull'icona **Il ruolo non è attivo** in **Imposta origine** per **Pacchetto: N/D** per abilitarlo.
    - 2) Espandere **Pacchetto: N/D**.
    - 3) Fare clic sull'icona **Il ruolo non è attivo** sotto **Imposta origine** per **Protocollo: EDI-X12**.
    - 4) Espandere **Protocollo: EDI-X12 (TUTTI)**.
    - 5) Fare clic sull'icona **Il ruolo non è attivo** sotto **Imposta origine** per **Flusso di documenti: ISA (TUTTI)**.
5. Fare clic su **Gestione account > Profili > Partecipante comunità**, quindi fare clic su **Cerca**.
6. Fare clic sull'icona **Visualizza i dettagli** per il partecipante di destinazione per questo esempio (**TP1**).
7. Fare clic su **Funzioni B2B**.
8. Abilitare i due gruppi di funzioni per il partecipante di destinazione.
  - a. In primo luogo, abilitare la definizione di flusso di documenti che rappresenta il TA1:
    - 1) Fare clic sull'icona **Il ruolo non è attivo** in **Imposta destinazione** per **Pacchetto: N/D** per abilitarlo.

- 2) Espandere **Pacchetto: N/D**.
  - 3) Fare clic sull'icona **Il ruolo non è attivo** sotto **Imposta destinazione per Protocollo: &X44TA1 (TUTTI)**.
  - 4) Espandere **Protocollo: &X44TA1 (TUTTI)**.
  - 5) Fare clic sull'icona **Il ruolo non è attivo** sotto **Imposta destinazione per Flusso di documenti: TA1 (TUTTI)**.
- b. In seguito, abilitare la definizione di flusso di documenti che rappresenta la busta EDI:
- 1) Fare clic sull'icona **Il ruolo non è attivo** sotto **Imposta Destinazione per Pacchetto: Nessuno** in modo da abilitarlo.
  - 2) Espandere **Pacchetto: Nessuno**.
  - 3) Fare clic sull'icona **Il ruolo non è attivo** sotto **Imposta destinazione per Protocollo: EDI-X12 (TUTTI)**.
  - 4) Espandere **Protocollo: EDI-X12 (TUTTI)**.
  - 5) Fare clic sull'icona **Il ruolo non è attivo** sotto **Imposta destinazione per Flusso di documenti: ISA (TUTTI)**.

### Creazione del profilo busta

Si crea il profilo per la busta che contiene un TA1:

1. Fare clic su **Ammin hub > Configurazione hub > EDI > Profilo busta**.
2. Fare clic su **Crea**.
3. Digitare il nome del profilo: **EnvProf1**.
4. Dall'elenco degli standard EDI, selezionare **X12**.
5. Il pulsante **Generale** è selezionato per impostazione predefinita. Immettere i seguenti valori per gli attributi generali della 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 partecipante

Per attivare le connessioni:

1. Fare clic su **Gestione account > Connessioni partecipanti**.
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 22. Connessione TA1

Origine	Destinazione
Pacchetto: N/D (N/D) Protocollo: &X44TA1 (TUTTI) Flusso di documenti: TA1(TUTTI)	Pacchetto: N/D (N/D) Protocollo: &X44TA1 (TUTTI) Flusso di documenti: TA1(TUTTI)

6. Attivare la connessione che rappresenta la busta:

Tabella 23. Connessione busta

Origine	Destinazione
Pacchetto: N/D (N/D) Protocollo: EDI-X12 (TUTTI) Flusso di documenti: ISA (TUTTI)	Pacchetto: Nessuno (N/D) Protocollo: EDI-X12 (TUTTI) Flusso di documenti: ISA (TUTTI)

## Configurazione degli attributi

Per specificare gli attributi per il profilo busta:

1. Fare clic su **Gestione account > Profili > Partecipante comunità**, quindi fare clic su **Cerca**.
2. Selezionare **TP1** dall'elenco.
3. Fare clic su **Funzioni B2B**.
4. Fare clic su **Espandi** accanto a **Pacchetto: Nessuno**.
5. Fare clic sull'icona **Modifica** accanto a **Protocollo: EDI-X12 (TUTTI)**.
6. Nella riga **Consenti una richiesta TA1**, selezionare **Sì**.
7. Fare clic su **Salva**.
8. Fare clic di nuovo su **Funzioni B2B**.
9. Fare clic sull'icona **Espandi** accanto a **Pacchetto: N/D**.
10. Fare clic su **Modifica** accanto a **Protocollo: &X44TA1 (TUTTI)**.
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 EDI in ROD" a pagina 193. Il riconoscimento funzionale fornisce una conferma al mittente che la transazione è stata ricevuta.

**Nota:** Questo esempio è simile a "Aggiunta di un TA1 ad uno scambio" a pagina 199. Tuttavia, non è direttamente correlato a quell'esempio. Invece, viene creato sulle attività eseguite in "Esempio EDI in ROD" a pagina 193.

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 il rilascio del messaggio. Ad esempio, la versione 2 del rilascio 4 del messaggio di riconoscimento funzionale 997 viene denominata \$DT\_997V2R4. Per un elenco delle mappe fornito con WebSphere Partner Gateway, consultare la sezione “Riconoscimenti funzionali” a pagina 120.

### Creazione delle associazioni

Per associare la mappa con una definizione di flusso di documenti, eseguire i passi riportati:

1. Fare clic su **Ammin hub > Configurazione hub > Mappe > Mappe FA EDI**. Viene visualizzata la mappa &DT\_FA997V2R4.
2. Fare clic sull'icona **Visualizza i dettagli** accanto alla mappa. Si visualizzano le informazioni sulla mappa nonché una cartella per ciascun tipo di pacchetto disponibile sul sistema.
3. Creare l'associazione alla definizione di flusso di documenti eseguendo questi passaggi:
  - a. Selezionare la casella di controllo accanto a **Pacchetto: N/D** ed espandere la cartella.
  - b. Selezionare la casella di controllo accanto a **Protocollo: X12V5R1**, quindi espandere la cartella.
  - c. Selezionare la casella di controllo accanto a **Flusso di documenti: 850**.
  - d. Fare clic su **Salva**.

Questa mappa di notifica funzionale 997 è stata associata al protocollo X12.

### Creazione interazioni

Creazione di un'interazione che rappresenta la notifica 997.

1. Fare clic su **Ammin hub > Configurazione hub > Definizione di flusso di documenti**.
2. Fare clic su **Gestisci interazioni** e quindi su **Crea interazione**.
3. In **Origine**, espandere **Pacchetto: N/D** e **Protocollo: &DT99724**, quindi selezionare **Flusso di documenti: 997**.
4. In **Destinazione**, espandere **Pacchetto: N/A** e **Protocollo: &DT99724**, quindi selezionare **Flusso di documenti: 997**.
5. Dall'elenco Azione, selezionare **Pass Through**.
6. Fare clic su **Salva**.

Creare un'interazione che rappresenta la busta.

1. Fare clic su **Ammin hub > Configurazione hub > Definizione di flusso di documenti**.
2. Fare clic su **Gestisci interazioni**, quindi su **Crea interazione**.
3. Espandere **Pacchetto: N/D** e **Protocollo: EDI-X12** e selezionare **Flusso di documenti: ISA**.
4. Espandere **Pacchetto: Nessuno** e **Protocollo: EDI-X12** e selezionare **Flusso di documenti: ISA**.
5. Dall'elenco Azione, selezionare **Pass Through**.
6. Fare clic su **Salva**.

## Abilitazione delle funzioni B2B

In seguito, si aggiungono le interazioni appena create alle funzioni B2B dei partecipanti.

1. Fare clic su **Gestione account > Profili > Partecipante comunità**, quindi fare clic su **Cerca**.
2. Fare clic sull'icona **Visualizza i dettagli** per il partecipante di origine per questo esempio (**Gestore**).

**Nota:** Ricordare che il riconoscimento funzionale fluisce dal partecipante che riceve il documento ROD al partecipante che lo invia. In questo esempio, il Gestore è l'origine del riconoscimento funzionale e il partecipante TP1 è la destinazione.

3. Fare clic su **Funzioni B2B**.
4. Abilitare i due gruppi di funzioni per il partecipante di origine.
  - a. In primo luogo, abilitare le funzioni di FA.
    - 1) Fare clic sull'icona **Il ruolo non è attivo in Imposta origine per Pacchetto: N/D** per abilitarlo.
    - 2) Espandere **Pacchetto: N/D**.
    - 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 sotto Imposta origine per Flusso di documenti: 997 (TUTTI)**.
  - b. In seguito, abilitare la funzionalità per la busta:
    - 1) Fare clic sull'icona **Il ruolo non è attivo in Imposta origine per Pacchetto: N/D** per abilitarlo.
    - 2) Espandere **Pacchetto: N/D**.
    - 3) Fare clic sull'icona **Il ruolo non è attivo sotto Imposta origine per Protocollo: EDI-X12**.
    - 4) Espandere **Protocollo: EDI-X12 (TUTTI)**.
    - 5) Fare clic sull'icona **Il ruolo non è attivo sotto Imposta origine per Flusso di documenti: ISA (TUTTI)**.
5. Fare clic su **Gestione account > Profili > Partecipante comunità**, quindi fare clic su **Cerca**.
6. Fare clic sull'icona **Visualizza i dettagli** per il partecipante di destinazione per questo esempio (**TP1**).
7. Fare clic su **Funzioni B2B**.
8. Abilitare i due gruppi di funzioni per il partecipante di destinazione.
  - a. In primo luogo, abilitare la definizione di flusso di documenti che rappresenta il 997:
    - 1) Fare clic sull'icona **Il ruolo non è attivo in Imposta destinazione per Pacchetto: N/D** per abilitarlo.
    - 2) Espandere **Pacchetto: N/D**.
    - 3) Fare clic sull'icona **Il ruolo non è attivo sotto Imposta destinazione per Protocollo: &DT99724 (TUTTI)**.
    - 4) Espandere **Protocollo: &DT99724 (TUTTI)**.
    - 5) Fare clic sull'icona **Il ruolo non è attivo sotto Imposta destinazione per Flusso di documenti: 997 (TUTTI)**.

- b. In seguito, abilitare la definizione di flusso di documenti che rappresenta la busta EDI:
- 1) Fare clic sull'icona **Il ruolo non è attivo** sotto **Imposta Destinazione per Pacchetto: Nessuno** in modo da abilitarlo.
  - 2) Espandere **Pacchetto: Nessuno**.
  - 3) Fare clic sull'icona **Il ruolo non è attivo** sotto **Imposta destinazione per Protocollo: EDI-X12 (TUTTI)**.
  - 4) Espandere **Protocollo: EDI-X12 (TUTTI)**.
  - 5) Fare clic sull'icona **Il ruolo non è attivo** sotto **Imposta destinazione per Flusso di documenti: ISA(TUTTI)**.

### Creazione del profilo busta

Si crea, in seguito, il profilo per la busta che contiene il 997: Un riconoscimento funzionale, come una transazione, deve essere imbustato prima che possa essere inviato.

1. Fare clic su **Ammin hub > Configurazione hub > EDI > Profilo busta**.
2. Fare clic su **Crea**.
3. Digitare il nome del profilo: **EnvProf1**.
4. Dall'elenco degli standard EDI, selezionare **X12**.
5. Il pulsante **Generale** è selezionato per impostazione predefinita. Immettere i seguenti valori per gli attributi generali della 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 partecipante

Per attivare le connessioni:

1. Fare clic su **Gestione account > Connessioni partecipanti**.
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 24. Connessione riconoscimento funzionale

Origine	Destinazione
Pacchetto: N/D (N/D) Protocollo: &DT99724 (TUTTI) Flusso di documenti: 997 (TUTTI)	Pacchetto: N/D (N/D) Protocollo: &DT99724 (TUTTI) Flusso di documenti: 997 (TUTTI)

- Fare clic su **Attiva** per la connessione che rappresenta la busta EDI inviata di nuovo a chi ha originato lo scambio:

Tabella 25. Connessione busta

Origine	Destinazione
Pacchetto: N/D (N/D) Protocollo: EDI-X12 (TUTTI) Flusso di documenti: ISA (TUTTI)	Pacchetto: Nessuno (N/D) Protocollo: EDI-X12 (TUTTI) Flusso di documenti: ISA (TUTTI)

## Configurazione di attributi

In primo luogo, si specifica la mappa FA da utilizzare:

- Fare clic su **Gestione account > Profili > Partecipante comunità**, quindi fare clic su **Cerca**.
- Selezionare **TP1** dall'elenco.
- Fare clic su **Funzioni B2B**.
- Fare clic sull'icona **Espandi** accanto a **Pacchetto: N/D**.
- Fare clic sull'icona **Modifica** accanto a **Protocollo: X12V5R1 (TUTTI)**.
- Nella riga Mappa FA, selezionare **&DT\_FA997V2R4**.
- Fare clic di nuovo su **Funzioni B2B**.
- Fare clic sull'icona **Espandi** accanto a **Pacchetto: N/D**.
- Fare clic su **Modifica** accanto a **Protocollo: &DT99724 (TUTTI)**.
- Specificare i seguenti attributi:
  - Nella riga Profilo busta, selezionare **EnvProf1** dall'elenco.
  - Nella riga Qualificatore scambio, selezionare **01**.
  - Nella riga Identificativo scambio, selezionare **000000001**.
  - Nella riga Indicatore utilizzo scambio, selezionare **T**.
- Fare clic su **Salva**.

In questa serie di attività, è stato aggiunto il riconoscimento funzionale EDI-X12 997 allo scambio, cosicché quando il Gestore comunità riceve il documento, lo invia di nuovo al mittente (TP1). Il 997 viene inviato in una busta conforme al profilo busta EnvProf1.

## Esempio EDI in XML

In questa sezione viene fornito un esempio di invio di una transazione EDI (all'interno di una busta) all'hub, in cui viene trasformata in un documento XML e inviata al Gestore comunità.

In questo esempio, si presume che lo specialista della mappatura Data Interchange Services abbia creato una mappa di trasformazione che utilizza una transazione EDI 879 standard (definita con il dizionario X12V5R1, corrispondente alla versione 5010 di X12) e la trasforma in un documento XML che verrà elaborato dall'applicazione back-end del Gestore comunità. 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 trasformazione 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 importarla in WebSphere Partner Gateway. In questa appendice, si presume il secondo scenario.

## Importazione della mappa di trasformazione

In questa sezione, vengono descritti i passaggi per importare una mappa di trasformazione che utilizzerà l'input EDI e lo trasformerà nel formato XML. Nel processo di importazione della mappa di trasformazione, si importa anche la definizione del documento associato alla mappa.

Prima che sia possibile importare la mappa di trasformazione, 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:

```
<ProductDir>/bin/bcgDISImport.sh <database_user_ID>
<password> S_DT_EDI_TO_XML.eif
```

- In un sistema Windows:

```
<ProductDir>\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 della mappa di trasformazione e delle definizioni di flusso di documenti

Per verificare le mappe di trasformazione e le definizioni di flusso di documenti importate sono disponibili nella Console comunità, eseguire questi passaggi:

1. Fare clic su **Ammin hub > Configurazione hub > Mappe > Mappe di trasformazione**.

Viene visualizzata la mappa S\_DT\_EDI\_TO\_XML.

2. Fare clic sull'icona **Visualizza i dettagli** accanto alla mappa.

Si visualizzano le definizioni del flusso di documenti cui la mappa è associata:

Tabella 26. Definizione di flusso di documenti associata alla mappa

Origine	Destinazione
Pacchetto: N/D Protocollo: X12V5R1 Flusso di documenti: 879 (TUTTI)	Pacchetto: Nessuno Protocollo: FVT-XML-TEST (TUTTI) Flusso di documenti: WWRE_ITEMCREATIONINTERNAL (TUTTI)

La mappa S\_DT\_EDI\_TO\_XML è stata definita per utilizzare una transazione X12 879 (conforme allo standard X12V5R1) e la trasforma in un protocollo personalizzato.

## Configurazione della destinazione

In questa sezione, si crea una destinazione della directory del sistema di file per l'hub:

1. Fare clic su **Ammin hub > Configurazione hub > Destinazioni**, quindi fare clic su **Crea destinazione**.
2. Per Nome destinazione, digitare: **EDIFileTarget**
3. Dall'Elenco dei trasporti, selezionare **Directory file**.
4. Per Percorso root, digitare: **/Data/Manager/editarget**
5. Fare clic su **Salva**.

Il partecipante della comunità invia lo scambio EDI a questa destinazione.

## Creazione delle interazioni

Si creano due interazioni, una per la busta EDI e l'altra per la transazione nella busta EDI.

Creare un'interazione che rappresenti la busta EDI.

1. Fare clic su **Ammin hub > Configurazione hub > Definizione di flusso di documenti**.
2. Fare clic su **Gestisci interazioni** e quindi su **Crea interazione**.
3. Espandere **Pacchetto: Nessuno** e **Protocollo: EDI-X12** e selezionare **Flusso di documenti: ISA**.
4. Espandere **Pacchetto: N/D** e **Protocollo: EDI-X12** e selezionare **Flusso di documenti: ISA**.
5. Dall'elenco Azione, selezionare **File sbustamento**.

**Nota:** Non si verifica alcuna trasformazione in questa interazione. Lo scambio EDI viene sbustato e risulta in una singola transazione (879). Di conseguenza, non è necessaria una mappa di trasformazione per questa transazione.

6. Fare clic su **Salva**.

Creare un'interazione che abbia un'origine che rappresenti la transazione 879 ed una destinazione che rappresenti il documento trasformato.

1. Fare clic su **Ammin hub > Configurazione hub > Definizione di flusso di documenti**.
2. Fare clic su **Gestisci interazioni**, quindi su **Crea interazione**.
3. Espandere **Pacchetto: N/D** e **Protocollo: X12V5R1**, quindi selezionare **Flusso di documenti: 879**.
4. Espandere **Pacchetto: Nessuno** e **Protocollo: FVT-XML-TEST**, quindi selezionare **Flusso di documenti: WWRE\_ITEMCREATIONINTERNAL**.
5. Dall'elenco delle mappe di trasformazione, selezionare **S\_DT\_EDI\_TO\_XML**.
6. Dall'elenco Azione, selezionare **Convalida EDI e conversione EDI**.
7. Fare clic su **Salva**.

Questa interazione rappresenta la trasformazione di una transazione EDI X12 879 standard in un formato differente e, di conseguenza, è necessario selezionare una mappa di trasformazione.

## Creazione di partecipanti

Per questo esempio, si hanno due partecipanti: Gestore comunità (Gestore) e partecipante (TP1).

Creare il profilo Gestore comunità:

1. Fare clic su **Gestione account > Profili > Partecipante comunità**, quindi fare clic su **Crea**.
2. Per Nome accesso società, digitare: **Gestcom**
3. Per Nome visualizzato partecipante, digitare: **Gestore**
4. Per Tipo partecipante, selezionare **Gestore comunità**.
5. Fare clic su **Nuovo** per l'ID aziendale e immettere 000000000 come ID in forma libera.

**Nota:** Assicurarsi di selezionare Forma libera e non DUNS.

6. Fare di nuovo clic su **Nuovo** per l'ID aziendale, quindi immettere 01-000000000 come ID in forma libera.
7. Fare clic su **Salva**.

Creare il secondo partecipante:

1. Fare clic su **Ammin conto > Profili > Partecipante comunità**, quindi fare clic su **Crea**.
2. Per Nome accesso società, digitare: **TP1**
3. Per Nome visualizzato partecipante, digitare, **TP1**
4. Per Tipo partecipante, selezionare **Partecipante comunità**.
5. Fare clic su **Nuovo** per l'ID aziendale e immettere 000000001 come ID in forma libera.

**Nota:** Assicurarsi di selezionare Forma libera e non DUNS.

6. Fare di nuovo clic su **Nuovo** per l'ID aziendale e immettere 01-000000001 come ID in forma libera.
7. Fare clic su **Salva**.

## Creazione dei gateway

Creare i gateway della directory del file per entrambi i partecipanti in questo esempio. In primo luogo, creare un gateway per il Gestore:

1. Fare clic su **Gestione account > Profili > Partecipante comunità**, quindi fare clic su **Cerca**.
2. Fare clic sull'icona **Visualizza i dettagli** accanto al profilo Gestore.
3. Fare clic su **Gateway**, quindi su **Crea**.
4. Immettere i seguenti valori per il gateway. Ricordare che la directory di file (l'intero percorso) deve già esistere sul sistema di file.
  - a. Per Nome, digitare **ManagerFileGateway**.
  - b. Dall'elenco dei trasporti, selezionare **Directory file**.
  - c. Per Indirizzo, digitare: **file:///Data Manager/filegateway**
  - d. Fare clic su **Salva**.
5. Fare clic su **Elenco** per visualizzare tutti i gateway configurati per il Gestore comunità.
6. Fare clic su **Visualizza gateway predefiniti**.
7. Dall'elenco **Produzione**, selezionare il gateway creato al passo 4.
8. Fare clic su **Salva**.

In seguito, creare un gateway per il partecipante.

1. Fare clic su **Gestione account > Profili > Partecipante comunità**, quindi fare clic su **Cerca**.

2. Selezionare l'altro partecipante creato per questo esempio facendo clic sull'icona **Visualizza i dettagli** accanto a **TP1**.
3. Fare clic su **Gateway**, quindi su **Crea**.
4. Immettere i seguenti valori per il gateway. Ricordare che la directory di file (l'intero percorso) deve già esistere.
  - a. Per Nome, digitare **TP1FileGateway**.
  - b. Dall'elenco dei trasporti, selezionare **Directory file**.
  - c. Per Indirizzo, digitare: **file:///Data/TP1/filegateway**
  - d. Fare clic su **Salva**.
5. Fare clic su **Elenco** per visualizzare tutti i gateway configurati per il partecipante.
6. Fare clic su **Visualizza gateway predefiniti**.
7. Dall'elenco **Produzione**, selezionare il gateway creato al passo 4.
8. Fare clic su **Salva**.

## Impostazione delle funzioni B2B

Abilitare le funzioni B2B dei due partecipanti in questo scambio. In questo esempio, lo scambio EDI nasce con il partecipante della comunità (TP1) e verrà consegnato al Gestore comunità.

1. Fare clic su **Gestione account > Profili > Partecipante comunità**, quindi fare clic su **Cerca**.
2. Fare clic sull'icona **Visualizza i dettagli** per il partecipante di origine per questo esempio (**TP1**).
3. Fare clic su **Funzioni B2B**.
4. Abilitare i due gruppi di funzioni per il partecipante di origine.
  - a. In primo luogo, abilitare la definizione di flusso di documenti che rappresenta la busta EDI:
    - 1) Fare clic sull'icona **Il ruolo non è attivo** sotto **Imposta origine per Pacchetto: Nessuno** in modo da abilitarlo.
    - 2) Espandere **Pacchetto: Nessuno**.
    - 3) Fare clic sull'icona **Il ruolo non è attivo** sotto **Imposta origine per Protocollo EDI-X12 (TUTTI)**.
    - 4) Espandere **Protocollo: EDI-X12 (TUTTI)**
    - 5) Fare clic sull'icona **Il ruolo non è attivo** sotto **Imposta origine per Flusso di documenti: ISA (TUTTI)**.
  - b. In seguito, abilitare la definizione del flusso di documenti che rappresenta la transazione:
    - 1) Fare clic sull'icona **Il ruolo non è attivo** in **Imposta origine per Pacchetto: N/D** per abilitarlo.
    - 2) Espandere **Pacchetto: N/D**.
    - 3) Fare clic sull'icona **Il ruolo non è attivo** sotto **Imposta origine per Protocollo: X12V5R1 (TUTTI)**.
    - 4) Espandere **Protocollo: X12V5R1 (TUTTI)**.
    - 5) Fare clic sull'icona **Il ruolo non è attivo** sotto **Imposta origine per Flusso di documenti: 879**.
5. Fare clic su **Gestione account > Profili > Partecipante comunità**, quindi fare clic su **Cerca**.

6. Fare clic sull'icona **Visualizza i dettagli** per il partecipante di destinazione per questo esempio (**Gestore**).
7. Fare clic su **Funzioni B2B**.
8. Abilitare i due gruppi di funzioni per il partecipante di destinazione.
  - a. In primo luogo, abilitare la definizione di flusso di documenti:
    - 1) Fare clic sull'icona **Il ruolo non è attivo in Imposta destinazione per Pacchetto: N/D** per abilitarlo.
    - 2) Espandere **Pacchetto: N/D**.
    - 3) Fare clic sull'icona **Il ruolo non è attivo** sotto **Imposta destinazione per Protocollo: EDI-X12 (TUTTI)**.
    - 4) Espandere **Protocollo: EDI-X12 (TUTTI)**.
    - 5) Fare clic sull'icona **Il ruolo non è attivo** sotto **Imposta destinazione per Flusso di documenti: ISA (TUTTI)**.
  - b. In seguito, abilitare la definizione del flusso di documenti che rappresenta il documento trasformato:
    - 1) Fare clic sull'icona **Il ruolo non è attivo** sotto **Imposta Destinazione per Pacchetto: Nessuno** in modo da abilitarlo.
    - 2) Espandere **Pacchetto: Nessuno**.
    - 3) Fare clic sull'icona **Il ruolo non è attivo** sotto **Imposta destinazione per Protocollo: FVT-XML-TEST (TUTTI)**.
    - 4) Espandere **Protocollo: FVT-XML-TEST (TUTTI)**.
    - 5) Fare clic sull'icona **Il ruolo non è attivo** sotto **Imposta destinazione per Flusso di documenti: WWRE\_ITEMCREATIONINTERNAL(TUTTI)**.

## Attivazione delle connessioni

Per attivare le connessioni:

1. Fare clic su **Gestione account > Connessioni partecipanti**.
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 27. Connessione busta*

Origine	Destinazione
Pacchetto: Nessuno (N/D)	Pacchetto: N/D (N/D)
Protocollo: EDI-X12 (TUTTI)	Protocollo: EDI-X12 (TUTTI)
Flusso di documenti: ISA (TUTTI)	Flusso di documenti: ISA (TUTTI)

6. Fare clic su **Attiva** per la connessione che rappresenta la transazione 879 per il documento trasformato:

*Tabella 28. Transazione EDI per la connessione del documento XML*

Origine	Destinazione
Pacchetto: N/D (N/D)	Pacchetto: Nessuno (N/D)
Protocollo: X12V5R1 (TUTTI)	Protocollo: FVT-XML-TEST (TUTTI)
Flusso di documenti: 879 (TUTTI)	Flusso di documenti: WWRE_ITEMCREATIONINTERNAL (TUTTI)

A questo punto, se TP1 ha inviato uno scambio EDI che contiene una transazione 879 al Gestore comunità, lo scambio EDI dovrebbe essere sbustato e dovrebbe dare

come risultato una transazione 879. La transazione 879 dovrebbe essere, quindi, trasformata e il documento trasformato dovrebbe essere inviato al gateway del Gestore comunità.

---

## Esempio da XML a EDI

In questa sezione, viene fornito un esempio del Gestore comunità che invia un documento XML all'hub, dove viene trasformato in una transazione EDI, imbustato in uno scambio EDI ed inviato ad un partecipante.

In questo esempio, si presume che lo specialista della mappatura Data Interchange Services abbia creato una mappa di trasformazione che utilizza un documento XML e lo trasforma in una transazione EDI 850 standard (definita con il dizionario MX12V3R1) che verrà elaborata dal partecipante. 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 trasformazione 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 trasformazione

In questa sezione, vengono descritti i passaggi per importare una mappa di trasformazione che utilizzerà l'input XML e la si trasformerà in una transazione EDI. Nel processo di importazione della mappa di trasformazione, si importa anche la definizione del documento associato alla mappa.

Prima che sia possibile importare la mappa di trasformazione, 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:

```
<ProductDir>/bin/bcgDISImport.sh <database_user_ID>
<password> S_DT_XML_TO_EDI.eif
```

- In un sistema Windows:

```
<ProductDir>\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 della mappa di trasformazione e delle definizioni di flusso di documenti

Per verificare se le mappe di trasformazione e le definizioni di flusso di documenti importate sono disponibili nella Console comunità, eseguire questi passaggi:

1. Fare clic su **Ammin hub > Configurazione hub > Mappe > Mappe di trasformazione**.

Viene visualizzata la mappa S\_DT\_XML\_TO\_EDI.

2. Fare clic sull'icona **Visualizza i dettagli** accanto alla mappa.

Si visualizzano le definizioni del flusso di documenti cui la mappa è associata:

Tabella 29. Definizioni di flusso di documenti associate alla mappa

Origine	Destinazione
Pacchetto: Nessuno Protocollo: FVT-XML-TEST (TUTTI) Flusso di documenti: ICGCPO (TUTTI)	Pacchetto: N/D Protocollo: MX12V3R1 (TUTTI) Flusso di documenti: 850 (TUTTI)

La mappa S\_DT\_XML\_TO\_EDI è stata definita per utilizzare un documento XML e trasformarlo in transazione EDI.

## Configurazione della destinazione

In questa sezione, si crea una destinazione della directory del sistema di file per l'hub:

1. Fare clic su **Ammin hub > Configurazione hub > Destinazioni**, quindi fare clic su **Crea destinazione**.
2. Per Nome destinazione, digitare: **XMLFileTarget**
3. Dall'Elenco dei trasporti, selezionare **Directory file**.
4. Per Percorso root, digitare: **/Data/Manager/xmltarget**
5. Dall'elenco Punto di configurazione, selezionare **Preprocesso**.
6. Selezionare **com.ibm.bcg.edi.receiver.preprocesshandler.XMLSplitterHandler** dall'elenco Disponibili e fare clic su **Aggiungi** per spostarlo nell'elenco Configurati.
7. Fare clic su **Salva**.

Il Gestore comunità invia il documento XML a questa destinazione.

## Creazione delle interazioni

Creare due interazioni - una per la trasformazione 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 trasformata.

1. Fare clic su **Ammin hub > Configurazione hub > Definizione di flusso di documenti**.
2. Fare clic su **Gestisci interazioni** e quindi su **Crea interazione**.
3. Espandere **Pacchetto: Nessuno** e **Protocollo: FVT-XML-TEST**, quindi selezionare **Flusso di documenti: ICGCPO**.
4. Espandere **Pacchetto: N/D** e **Protocollo: MX12V3R1**, quindi selezionare **Flusso di documenti: 850**.
5. Dall'elenco delle mappe di trasformazione, selezionare **S\_DT\_XML\_TO\_EDI**.
6. Dall'elenco Azione, selezionare **Convalida EDI e conversione XML**.
7. Fare clic su **Salva**.

Questa interazione rappresenta la trasformazione di un documento XML in transazione EDI e, di conseguenza, è necessario selezionare una mappa di trasformazione.

Creare un'interazione che rappresenta la busta EDI.

1. Fare clic su **Ammin hub > Configurazione hub > Definizione di flusso di documenti**.
2. Fare clic su **Gestisci interazioni**, quindi su **Crea interazione**.
3. Espandere **Pacchetto: N/D** e **Protocollo: EDI-X12** e selezionare **Flusso di documenti: ISA**.
4. Espandere **Pacchetto: Nessuno** e **Protocollo: EDI-X12**, quindi selezionare **Flusso di documenti: ISA**.
5. Dall'elenco Azione, selezionare **Pass Through**.

**Nota:** Non si verifica alcuna trasformazione in questa interazione.

6. Fare clic su **Salva**.

## Creazione di partecipanti

Per questo esempio, si hanno due partecipanti: Gestore comunità (Gestore) e partecipante (TP1).

Creare il profilo Gestore comunità:

1. Fare clic su **Gestione account > Profili > Partecipante comunità**, quindi fare clic su **Crea**.
2. Per Nome accesso società, digitare: **Gestcom**
3. Per Nome visualizzato partecipante, immettere: **Manager**.
4. Per Tipo partecipante, selezionare **Gestore comunità**.
5. Fare clic su **Nuovo** per l'ID aziendale e immettere 000000000 come ID in forma libera.

**Nota:** Assicurarsi di selezionare Forma libera e non DUNS.

6. Fare di nuovo clic su **Nuovo** per l'ID aziendale, quindi immettere 01-000000000 come ID in forma libera.
7. Fare clic su **Salva**.

Creare il secondo partecipante:

1. Fare clic su **Ammin conto > Profili > Partecipante comunità**, quindi fare clic su **Crea**.
2. Per Nome accesso società, digitare: **TP1**
3. Per Nome visualizzato partecipante, digitare, **TP1**
4. Per Tipo partecipante, selezionare **Partecipante**.
5. Fare clic su **Nuovo** per l'ID aziendale e immettere 000000001 come ID in forma libera.

**Nota:** Assicurarsi di selezionare Forma libera e non DUNS.

6. Fare di nuovo clic su **Nuovo** per l'ID aziendale, quindi immettere 01-000000001 come ID in forma libera.
7. Fare clic su **Salva**.

## Creazione dei gateway

Creare i gateway della directory del file per entrambi i partecipanti in questo esempio. In primo luogo, creare un gateway per il Gestore:

1. Fare clic su **Gestione account > Profili > Partecipante comunità**, quindi fare clic su **Cerca**.
2. Fare clic sull'icona **Visualizza i dettagli** accanto al profilo Gestore.

3. Fare clic su **Gateway**, quindi su **Crea**.
4. Immettere i seguenti valori per il gateway. Ricordare che la directory di file (l'intero percorso) deve già esistere sul sistema di file.
  - a. Per Nome, digitare **ManagerFileGateway**.
  - b. Dall'Elenco dei trasporti, selezionare **Directory file**.
  - c. Per Indirizzo, digitare: **file:///Data Manager/filegateway**
  - d. Fare clic su **Salva**.
5. Fare clic su **Elenco** per visualizzare tutti i gateway configurati per il Gestore comunità.
6. Fare clic su **Visualizza gateway predefiniti**.
7. Dall'elenco **Produzione**, selezionare il gateway creato al passo 4.
8. Fare clic su **Salva**.

In seguito, creare un gateway per il partecipante.

1. Fare clic su **Gestione account > Profili > Partecipante comunità**, quindi fare clic su **Cerca**.
2. Selezionare l'altro partecipante creato per questo esempio facendo clic sull'icona **Visualizza i dettagli** accanto a **TP1**.
3. Fare clic su **Gateway**, quindi su **Crea**.
4. Immettere i seguenti valori per il gateway. Ricordare che la directory di file (l'intero percorso) deve già esistere.
  - a. Per Nome, digitare **TP1FileGateway**.
  - b. Dall'elenco dei trasporti, selezionare **Directory file**.
  - c. Per Indirizzo, digitare: **file:///Data/TP1/filegateway**
  - d. Fare clic su **Salva**.
5. Fare clic su **Elenco** per visualizzare tutti i gateway configurati per il partecipante.
6. Fare clic su **Visualizza gateway predefiniti**.
7. Dall'elenco **Produzione**, selezionare il gateway creato al passo 4.
8. Fare clic su **Salva**.

## Impostazione delle funzioni B2B

Abilitare le funzioni B2B dei due partecipanti in questo scambio. In questo esempio, il documento XML dal Gestore della comunità e verrà consegnato al partecipante.

1. Fare clic su **Gestione account > Profili > Partecipante comunità**, quindi fare clic su **Cerca**.
2. Fare clic sull'icona **Visualizza i dettagli** per il partecipante di origine per questo esempio (**Gestcom**).
3. Fare clic su **Funzioni B2B**.
4. Abilitare tre gruppi di funzioni per il partecipante di origine.
  - a. Abilitare la definizione del flusso di documenti che rappresenta il documento XML:
    - 1) Fare clic sull'icona **Il ruolo non è attivo** sotto **Imposta origine** per **Pacchetto: Nessuno** in modo da abilitarlo.
    - 2) Espandere **Pacchetto: Nessuno**.
    - 3) Fare clic sull'icona **Il ruolo non è attivo** in **Imposta origine** per **Protocollo: FVT-XML-TEST (TUTTI)**.

- 4) Espandere **Protocollo: FVT-XML-TEST (TUTTI)**.
  - 5) Fare clic sull'icona **Il ruolo non è attivo** sotto **Imposta origine** per **Flusso di documenti: ICGCPO (TUTTI)**.
- b. In seguito, abilitare la definizione del flusso di documenti che rappresenta il documento trasformato:
- 1) Fare clic sull'icona **Il ruolo non è attivo** in **Imposta origine** per **Pacchetto: N/D** per abilitarlo.
  - 2) Espandere **Pacchetto: N/D**.
  - 3) Fare clic sull'icona **Il ruolo non è attivo** sotto **Imposta origine** per **Protocollo: MX12V3R1 (TUTTI)**.
  - 4) Espandere **Protocollo: MX12V3R1 (TUTTI)**.
  - 5) Fare clic sull'icona **Il ruolo non è attivo** sotto **Imposta origine** per **Flusso di documenti: 850**.
- c. Quindi, abilitare la definizione di flusso di documenti che rappresenta la busta EDI:
- 1) Fare clic sull'icona **Il ruolo non è attivo** in **Imposta origine** per **Pacchetto: N/D** per abilitarlo.
  - 2) Espandere **Pacchetto: N/D**.
  - 3) Fare clic sull'icona **Il ruolo non è attivo** sotto **Imposta origine** per **Protocollo EDI-X12 (TUTTI)**.
  - 4) Espandere **Protocollo: EDI-X12 (TUTTI)**
  - 5) Fare clic sull'icona **Il ruolo non è attivo** sotto **Imposta origine** per **Flusso di documenti: ISA (TUTTI)**.
5. Fare clic su **Gestione account > Profili > Partecipante comunità**, quindi fare clic su **Cerca**.
6. Fare clic sull'icona **Visualizza i dettagli** per il partecipante di destinazione per questo esempio (**TP1**).
7. Fare clic su **Funzioni B2B**.
8. Abilitare i due gruppi di funzioni per il partecipante di destinazione.
- a. In seguito, abilitare la definizione del flusso di documenti che rappresenta la transazione EDI 850:
- 1) Fare clic sull'icona **Il ruolo non è attivo** in **Imposta destinazione** per **Pacchetto: N/D** per abilitarlo.
  - 2) Espandere **Pacchetto: N/D**.
  - 3) Fare clic sull'icona **Il ruolo non è attivo** sotto **Imposta destinazione** per **Protocollo: MX12V3R1 (TUTTI)**.
  - 4) Espandere **Protocollo: MX12V3R1 (TUTTI)**.
  - 5) Fare clic sull'icona **Il ruolo non è attivo** sotto **Imposta destinazione** per **Flusso di documenti: 850 (TUTTI)**.
- b. In seguito, abilitare la definizione di flusso di documenti:
- 1) Fare clic sull'icona **Il ruolo non è attivo** sotto **Imposta Destinazione** per **Pacchetto: Nessuno** in modo da abilitarlo.
  - 2) Espandere **Pacchetto: Nessuno**.
  - 3) Fare clic sull'icona **Il ruolo non è attivo** sotto **Imposta destinazione** per **Protocollo: EDI-X12 (TUTTI)**.
  - 4) Espandere **Protocollo: EDI-X12 (TUTTI)**.
  - 5) Fare clic sull'icona **Il ruolo non è attivo** sotto **Imposta destinazione** per **Flusso di documenti: ISA(TUTTI)**.

## Creazione del profilo busta

Si crea, in seguito, il profilo per la busta che contiene la transazione 850 trasformata:

1. Fare clic su **Ammin hub > Configurazione hub > EDI > Profilo busta**.
2. Fare clic su **Crea**.
3. Digitare il nome del profilo: **EnvProf1**.
4. Dall'elenco degli standard EDI, selezionare **X12**.
5. Il pulsante **Generale** è selezionato per impostazione predefinita. Immettere i seguenti valori per gli attributi generali della 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

In questa sezione, si crea il formato XML personalizzato.

1. Fare clic su **Ammin 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 aziendale di origine, selezionare **Costante** e digitare **000000000**.
7. Per ID aziendale di destinazione, selezionare **Costante** e digitare **000000001**.
8. Per Flusso di documenti di origine, selezionare **Costante** e digitare **ICGCPO**.
9. Per Versione del flusso di documenti di origine, selezionare **Costante** e digitare **TUTTI**.
10. Fare clic su **Salva**.

## Attivazione delle connessioni

Attivare le connessioni del partecipante:

1. Fare clic su **Gestione account > Connessioni partecipanti**.
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 30. Connessione documento XML in transazione EDI

Origine	Destinazione
Pacchetto: Nessuno (N/D) Protocollo: FVT-XML-TEST (TUTTI) Flusso di documenti: ICGCPO (TUTTI)	Pacchetto: N/D (N/D) Protocollo: MX12V3R1 (TUTTI) Flusso di documenti: 850 (TUTTI)

6. Fare clic su **Attiva** per la connessione che rappresenta la busta EDI:

Tabella 31. Connessione busta EDI

Origine	Destinazione
Pacchetto: N/D (N/D) Protocollo: EDI-X12 (TUTTI) Flusso di documenti: ISA (TUTTI)	Pacchetto: Nessuno (N/D) Protocollo: EDI-X12 (TUTTI) Flusso di documenti: ISA (TUTTI)

## Configurazione di attributi

Configurare gli attributi delle funzioni B2B del partecipante di destinazione (TP1) e il partecipante di origine (Gestore):

1. Fare clic su **Gestione account > Profili > Partecipante comunità**, quindi fare clic su **Cerca**.
2. Fare clic sull'icona **Visualizza i dettagli** accanto a **TPI** per selezionarla.
3. Fare clic su **Funzioni B2B**.
4. Fare clic sull'icona **Espandi** accanto a **Pacchetto: N/D**.
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 **Gestione account > Profili > Partecipante comunità**, quindi fare clic su **Cerca**.
9. Fare clic sull'icona **Visualizza i dettagli** accanto a **Gestore** per selezionarla.
10. Fare clic su **Funzioni B2B**.
11. Fare clic sull'icona **Espandi** accanto a **Pacchetto: N/D**.
12. Fare clic sull'icona **Modifica** accanto a **Protocollo: MX12V3R1 (TUTTI)**.
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**.

A questo punto, se il partecipante di origine (il Gestore comunità invia un documento XML al partecipante, verrebbe convertito (nell'hub) in una transazione EDI, imbustato e inviato al gateway del partecipante.

---

## Esempio ROD in EDI

In questa sezione, viene fornito un esempio del Gestore comunità che invia un documento ROD all'hub, dove viene trasformato in una transazione EDI, imbustato in uno scambio EDI ed inviato ad un partecipante.

In questo esempio, si presume che lo specialista della mappatura Data Interchange Services abbia creato una mappa di trasformazione che utilizza un documento ROD e lo trasforma in una transazione EDI 850 standard (definita con il dizionario X12V5R1, corrispondente alla versione 5010 di X12) che verrà elaborata dal partecipante. 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 trasformazione 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 importarla in WebSphere Partner Gateway. In questa appendice, si presume il secondo scenario.

### Importazione della mappa di trasformazione

In questa sezione, vengono descritti i passaggi per importare una mappa di trasformazione che utilizzerà l'input ROD e lo trasformerà in una transazione X12. Nel processo di importazione della mappa di trasformazione, si importa anche la definizione del documento associato alla mappa.

Prima che sia possibile importare la mappa di trasformazione, 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:

```
<ProductDir>/bin/bcgDISImport.sh <database_user_ID>
<password> S_DT_ROD_TO_EDI.eif
```

- In un sistema Windows:

```
<ProductDir>\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 della mappa di trasformazione e delle definizioni di flusso di documenti

Per verificare le mappe di trasformazione e le definizioni di flusso di documenti importate sono disponibili nella Console comunità, eseguire questi passaggi:

1. Fare clic su **Ammin hub > Configurazione hub > Mappe > Mappe di trasformazione**.

Viene visualizzata la mappa The S\_DT\_ROD\_TO\_EDI.

2. Fare clic sull'icona **Visualizza i dettagli** accanto alla mappa.

Si visualizzano le definizioni del flusso di documenti cui la mappa è associata:

Tabella 32. Definizioni di flusso di documenti associate alla mappa

Origine	Destinazione
Pacchetto: Nessuno Protocollo: ROD-TO-EDI_DICT (TUTTI) Flusso di documenti: DTROD-TO-EDL_ROD (TUTTI)	Pacchetto: N/D Protocollo: X12V5R1(TUTTI) Flusso di documenti: 850 (TUTTI)

La mappa S\_DT\_ROD\_TO\_EDI è stata definita per utilizzare un documento ROD associato al dizionario ROD-TO-EDI\_DICT e trasformarlo in una transazione X12 850 conforme allo standard X12V5R1.

## Configurazione della destinazione

In questa sezione, si crea una destinazione della directory del sistema di file per l'hub:

1. Fare clic su **Ammin hub > Configurazione hub > Destinazioni**, quindi fare clic su **Crea destinazione**.
2. Per Nome destinazione, digitare: **RODFileTarget**
3. Dall'Elenco dei trasporti, selezionare **Directory file**.
4. Per Percorso root, digitare: **/Data/Manager/rodtarget**
5. Dall'elenco Punto di configurazione, selezionare **Preprocesso**.
6. Selezionare **com.ibm.bcg.edi.receiver.preprocesshandler.RODSplitterHandler** dall'elenco Disponibili e fare clic su **Aggiungi** per spostarlo nell'elenco Configurati.
7. Selezionare **com.ibm.bcg.edi.receiver.preprocesshandler.RODSplitterHandler** dall'elenco Configurati e fare clic su **Configura**.
8. Aggiungere i valori mostrati nella tabella:

Tabella 33. Attributi Gestore splitter ROD

Campo	Valore
Da nome impacchettamento	Nessuno
Da versione impacchettamento	N/D
Da nome protocollo	ROD-TO-EDI_DICT
Da versione protocollo	TUTTI
Da codice processo	DTROD-TO-EDI_ROD
Da versione processo	TUTTI
METADIZIONARIO	ROD-TO-EDI_DICT
METADOCUMENTO	DTROD-TO-EDI_ROD
METASINTASSI	rod
CODIFICA	ascii
BCG_BATCHDOCS	ON

9. Fare clic su **Imposta valori**.
10. Fare clic su **Salva**.

Il Gestore comunità invia il documento ROD a questa destinazione.

## Creazione delle interazioni

Si creano due interazioni, una per la busta EDI che verrà inviata dall'hub e l'altra per la trasformazione 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 **Ammin hub > Configurazione hub > Definizione di flusso di documenti**.
2. Fare clic su **Gestisci interazioni** e quindi su **Crea interazione**.
3. Espandere **Pacchetto: Nessuno** e **Protocollo: ROD-TO-EDI\_DICT**, quindi selezionare **DTROD-TO-EDI\_ROD**.
4. Espandere **Pacchetto: N/D** e **Protocollo: X12V5R1**, quindi selezionare **Flusso di documenti: 850**.
5. Dall'elenco delle mappe di trasformazione, selezionare **S\_DT\_ROD\_TO\_EDI**.
6. Dall'elenco Azione, selezionare **Convalida EDI e conversione EDI**.
7. Fare clic su **Salva**.

Questa interazione rappresenta la trasformazione di un documento ROD in transazione X12 standard e, di conseguenza, è necessario selezionare una mappa di trasformazione.

Creare un'interazione che rappresenti la busta EDI.

1. Fare clic su **Ammin hub > Configurazione hub > Definizione di flusso di documenti**.
2. Fare clic su **Gestisci interazioni**, quindi su **Crea interazione**.
3. Espandere **Pacchetto: N/D** e **Protocollo: EDI-X12** e selezionare **Flusso di documenti: ISA**.
4. Espandere **Pacchetto: Nessuno** e **Protocollo: EDI-X12**, quindi selezionare **Flusso di documenti: ISA**.
5. Dall'elenco Azione, selezionare **Pass Through**.

**Nota:** Non si verifica alcuna trasformazione in questa interazione. Questa interazione è valida per lo scambio EDI.

6. Fare clic su **Salva**.

## Creazione di partecipanti

Per questo esempio, si hanno due partecipanti: Gestore comunità (Gestore) e partecipante (TP1).

Creare il profilo Gestore comunità:

1. Fare clic su **Gestione account > Profili > Partecipante comunità**, quindi fare clic su **Crea**.
2. Per Nome accesso società, digitare: **Gestcom**
3. Per Nome visualizzato partecipante, digitare: **Gestore**
4. Per Tipo partecipante, selezionare **Gestore comunità**.
5. Fare clic su **Nuovo** per l'ID aziendale e immettere 0000000000 come ID in forma libera.

**Nota:** Assicurarsi di selezionare Forma libera e non DUNS.

6. Fare di nuovo clic su **Nuovo** per l'ID aziendale e immettere 01-000000000 come ID in forma libera.
7. Fare clic su **Salva**.

Creare il secondo partecipante:

1. Fare clic su **Ammin conto > Profili > Partecipante comunità**, quindi fare clic su **Crea**.
2. Per Nome accesso società, digitare: **TP1**
3. Per Nome visualizzato partecipante, digitare, **TP1**
4. Per Tipo partecipante, selezionare **Partecipante comunità**.
5. Fare clic su **Nuovo** per l'ID aziendale e immettere 000000001 come ID in forma libera.

**Nota:** Assicurarsi di selezionare Forma libera e non DUNS.

6. Fare di nuovo clic su **Nuovo** per l'ID aziendale e immettere 01-000000001 come ID in forma libera.
7. Fare clic su **Salva**.

## Creazione dei gateway

Creare i gateway della directory del file per entrambi i partecipanti in questo esempio. In primo luogo, creare un gateway per il Gestore:

1. Fare clic su **Gestione account > Profili > Partecipante comunità**, quindi fare clic su **Cerca**.
2. Fare clic sull'icona **Visualizza i dettagli** accanto al profilo Gestore.
3. Fare clic su **Gateway**, quindi su **Crea**.
4. Immettere i seguenti valori per il gateway. Ricordare che la directory di file (l'intero percorso) deve già esistere sul sistema di file.
  - a. Per Nome, digitare **ManagerFileGateway**.
  - b. Dall'elenco dei trasporti, selezionare **Directory file**.
  - c. Per Indirizzo, digitare: **file:///Data Manager/filegateway**
  - d. Fare clic su **Salva**.
5. Fare clic su **Elenco** per visualizzare tutti i gateway configurati per il Gestore comunità.
6. Fare clic su **Visualizza gateway predefiniti**.
7. Dall'elenco **Produzione**, selezionare il gateway creato al passo 4
8. Fare clic su **Salva**.

In seguito, creare un gateway per il partecipante.

1. Fare clic su **Gestione account > Profili > Partecipante comunità**, quindi fare clic su **Cerca**.
2. Selezionare l'altro partecipante creato per questo esempio facendo clic sull'icona **Visualizza i dettagli** accanto a **TP1**.
3. Fare clic su **Gateway**, quindi su **Crea**.
4. Immettere i seguenti valori per il gateway. Ricordare che la directory di file (l'intero percorso) deve già esistere.
  - a. Per Nome, digitare **TP1FileGateway**.
  - b. Dall'elenco dei trasporti, selezionare **Directory file**.
  - c. Per Indirizzo, digitare: **file:///Data/TP1/filegateway**

- d. Fare clic su **Salva**.
5. Fare clic su **Elenco** per visualizzare tutti i gateway configurati per il partecipante.
6. Fare clic su **Visualizza gateway predefiniti**.
7. Dall'elenco **Produzione**, selezionare il gateway creato al passo 4 a pagina 222.
8. Fare clic su **Salva**.

## Impostazione delle funzioni B2B

Abilitare le funzioni B2B dei due partecipanti in questo scambio. In questo esempio, il documento ROD dal Gestore della comunità e verrà consegnato al partecipante (TP1)

1. Fare clic su **Gestione account > Profili > Partecipante comunità**, quindi fare clic su **Cerca**.
2. Fare clic sull'icona **Visualizza i dettagli** per il partecipante di origine per questo esempio (**Gestore**).
3. Fare clic su **Funzioni B2B**.
4. Abilitare i due gruppi di funzioni per il partecipante di origine.
  - a. In primo luogo, abilitare la definizione del flusso di documenti che rappresenta il documento ROD:
    - 1) Fare clic sull'icona **Il ruolo non è attivo** sotto **Imposta origine** per **Pacchetto: Nessuno** in modo da abilitarlo.
    - 2) Espandere **Pacchetto: Nessuno**.
    - 3) Fare clic sull'icona **Il ruolo non è attivo** in **Imposta origine** per **Protocollo: ROD-TO-EDI\_DICT (TUTTI)**.
    - 4) Espandere **Protocollo: ROD-TO-EDI\_DICT (TUTTI)**.
    - 5) Fare clic sull'icona **Il ruolo non è attivo** in **Imposta origine** per **Flusso di documenti: DTROD-TO-EDI\_ROD (TUTTI)**.
  - b. In seguito, abilitare la definizione di flusso di documenti che rappresenta la busta EDI:
    - 1) Fare clic sull'icona **Il ruolo non è attivo** in **Imposta origine** per **Pacchetto: N/D** per abilitarlo.
    - 2) Espandere **Pacchetto: N/D**.
    - 3) Fare clic sull'icona **Il ruolo non è attivo** sotto **Imposta origine** per **Protocollo EDI-X12 (TUTTI)**.
    - 4) Espandere **Protocollo: EDI-X12 (TUTTI)**
    - 5) Fare clic sull'icona **Il ruolo non è attivo** sotto **Imposta origine** per **Flusso di documenti: ISA (TUTTI)**.
5. Fare clic su **Gestione account > Profili > Partecipante comunità**, quindi fare clic su **Cerca**.
6. Fare clic sull'icona **Visualizza i dettagli** per il partecipante di destinazione per questo esempio (**TP1**).
7. Fare clic su **Funzioni B2B**.
8. Abilitare i due gruppi di funzioni per il partecipante di destinazione.
  - a. In seguito, abilitare la definizione del flusso di documenti che rappresenta la transazione EDI 850:
    - 1) Fare clic sull'icona **Il ruolo non è attivo** in **Imposta destinazione** per **Pacchetto: N/D** per abilitarlo.
    - 2) Espandere **Pacchetto: N/D**.

- 3) Fare clic sull'icona **Il ruolo non è attivo** sotto **Imposta destinazione** per **Protocollo: X12V5R1 (TUTTI)**.
  - 4) Espandere **Protocollo: X12V5R1 (TUTTI)**.
  - 5) Fare clic sull'icona **Il ruolo non è attivo** sotto **Imposta destinazione** per **Flusso di documenti: 850 (TUTTI)**.
- b. In seguito, abilitare la definizione del flusso di documenti che rappresenta la busta:
- 1) Fare clic sull'icona **Il ruolo non è attivo** sotto **Imposta Destinazione** per **Pacchetto: Nessuno** in modo da abilitarlo.
  - 2) Espandere **Pacchetto: Nessuno**.
  - 3) Fare clic sull'icona **Il ruolo non è attivo** sotto **Imposta destinazione** per **Protocollo: EDI-X12 (TUTTI)** .
  - 4) Espandere **Protocollo: EDI-X12 (TUTTI)**.
  - 5) Fare clic sull'icona **Il ruolo non è attivo** sotto **Imposta destinazione** per **Flusso di documenti: ISA (TUTTI)**.

## Creazione del profilo busta

Si crea, in seguito, il profilo per la busta che contiene la transazione 850 trasformata:

1. Fare clic su **Ammin hub > Configurazione hub > EDI > Profilo busta**.
2. Fare clic su **Crea**.
3. Digitare il nome del profilo: **EnvProf1**.
4. Dall'elenco degli standard EDI, selezionare **X12**.
5. Il pulsante **Generale** è selezionato per impostazione predefinita. Immettere i seguenti valori per gli attributi generali della 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

Per attivare le connessioni:

1. Fare clic su **Gestione account > Connessioni partecipanti**.
2. Selezionare **Gestore** dall'elenco Origine.
3. Selezionare **TP1** dall'elenco Destinazione.
4. Fare clic su **Cerca**.

- Fare clic su **Attiva** per la connessione che rappresenta il documento ROD alla transazione EDI:

Tabella 34. Connessione ROD a EDI

Origine	Destinazione
Pacchetto: N/D (N/D) Protocollo: ROD-TO-EDI_DICT (TUTTI) Flusso di documenti: DTROD-TO-EDI_ROD (TUTTI)	Pacchetto: Nessuno (N/D) Protocollo: X12V5R1(TUTTI) Flusso di documenti: 850

- Fare clic su **Attiva** per la connessione che rappresenta la busta:

Tabella 35. Connessione busta

Origine	Destinazione
Pacchetto: Nessuno (N/D) Protocollo: EDI-X12 (TUTTI) Flusso di documenti: ISA (TUTTI)	Pacchetto: N/D (N/D) Protocollo: EDI-X12 (TUTTI) Flusso di documenti: ISA(TUTTI)

## Configurazione di attributi

Per specificare gli attributi per il profilo busta:

- Fare clic su **Gestione account > Profili > Partecipante comunità**, quindi fare clic su **Cerca**.
- Selezionare **TP1** dall'elenco.
- Fare clic su **Funzioni B2B**.
- Fare clic sull'icona **Espandi** accanto a **Pacchetto: N/D**.
- Fare clic sull'icona **Modifica** accanto a **Protocollo: X12V5R1**.
- Specificare i seguenti attributi:
  - Nella riga Profilo busta, selezionare **EnvProf1** dall'elenco.
  - Nella riga Qualificatore scambio, selezionare **01**.
  - Nella riga Identificativo scambio, selezionare **000000001**.
  - Nella riga Indicatore utilizzo scambio, selezionare **T**.
- Fare clic su **Salva**.

A questo punto, se il Gestore comunità ha inviato un documento ROD all'hub, il documento dovrebbe essere trasformato in una transazione 850, che dovrebbe essere imbustata ed inviata al gateway del partecipante.



---

## Appendice C. Informazioni su RosettaNet aggiuntive

In questa appendice, vengono fornite informazioni aggiuntive sul supporto RosettaNet. Sono inclusi i seguenti argomenti:

- “Disattivazione dei PIP”
- “Come fornire la notifica dell’errore”
- “Creazione di pacchetti di flusso di documenti PIP” a pagina 229
- “Contenuti del pacchetto del flusso di documenti PIP” a pagina 241

---

### Disattivazione dei PIP

Dopo il caricamento di un pacchetto 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 partecipanti, eseguire questi passaggi:

1. Fare clic su **Ammin hub > Configurazione hub > Definizione di flusso di documenti**.
2. Espandere l’albero delle Definizioni del flusso di documenti per rilevare la Definizione del flusso di documenti del PIP che si desidera disabilitare.
3. Nella colonna Stato del pacchetto, fare clic su **Abilitato**. La colonna Stato ora visualizza **Disabilitato** e WebSphere Partner Gateway non può utilizzare la definizione di flusso di documenti per il PIP.

Per disattivare una comunicazione PIP con un partecipante specifico, disattivare la connessione del partecipante definito per il PIP.

---

### Come fornire la notifica dell’errore

In questa sezione vengono descritte le notifiche di errore.

#### PIP 0A1

Se si verifica un errore durante l’elaborazione di un messaggio PIP, WebSphere Partner Gateway utilizza PIP 0A1 come meccanismo di trasmissione dell’errore al sistema del partecipante o 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 e invia un messaggio RosettaNet ad un partecipante. WebSphere Partner Gateway attende la risposta al messaggio di RosettaNet fino a quando il tempo di attesa raggiunge il limite di timeout. Una volta che questo si verifica, WebSphere Partner Gateway crea un PIP 0A1 e lo invia al partecipante. Il PIP 0A1 identifica la condizione di eccezione in modo che il partecipante possa quindi compensare l’errore del PIP 3A4.

Per fornire la notifica di errore, caricare un pacchetto 0A1 e creare una connessione PIP al partecipante che utilizza questo pacchetto.

## 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 <ProductDir>/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 degli attributi di RosettaNet

Per il supporto RosettaNet, una definizione di flusso di documenti ha un gruppo specifico 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 pacchetti 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 di flusso di documenti di un'azione, eseguire questi passaggi:

1. Fare clic su **Ammin hub > Configurazione hub > Definizione del flusso di documenti**.
2. Fare clic sulle icone **Espandi** per espandere singolarmente un nodo al livello di definizione di flusso di documenti appropriato o selezionare **Tutti** per espandere l'intero l'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 36. 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 partecipante o sistema di back-end che invia il messaggio
Al servizio	Contiene il nome del servizio del componente di rete del partecipante o sistema di back-end che riceve il messaggio
Dal ruolo	Contiene il nome del ruolo del partecipante o del sistema di back-end che invia il messaggio
Al ruolo	Contiene il nome del ruolo del partecipante o del sistema di backend che riceve il messaggio

Tabella 36. Attributi RosettaNet (Continua)

Attributo RosettaNet	Descrizione
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 degli attributi e dei valori sostituisce gli attributi ereditati e modifica la funzionalità della definizione di flusso di documenti.
6. Fare clic su **Salva**.

---

## Creazione di pacchetti di flusso di documenti PIP

Poiché RosettaNet aggiunge PIP di volta in volta, potrebbe essere necessario creare i pacchetti PIP per supportare questi nuovi PIP o per supportare gli aggiornamenti nei PIP. Eccetto quando indicato, le procedure in questa sezione descrivono in che modo creare il pacchetto del flusso di documenti PIP per PIP 5C4 V01.03.00. WebSphere Partner Gateway fornisce un pacchetto del flusso di documenti PIP per il PIP 5C4 V01.02.00. Le procedure, quindi, documentano come eseguire l'aggiornamento. Tuttavia, la creazione di un pacchetto del flusso di documenti PIP è simile e le procedure identificano quelle aggiuntive.

Prima di iniziare, scaricare le specifiche PIP da [www.rosettanet.org](http://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 commerciali per PIP.
- Note di rilascio 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 aggiornamento di un pacchetto del flusso di documenti PIP comporta le seguenti procedure:

- Creazione dei file XSD
- Creazione del file XML
- Creazione dei pacchetti

## Creazione di file XSD

Un pacchetto del flusso di documenti PIP contiene i file dello schema XML che definiscono i formati del messaggio e i valori accettabili 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 "Convalida" a pagina 239.

Per creare i file XSD per il pacchetto del flusso di documenti PIP, procedere come segue:

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, digitare il nome del nuovo file XSD. Nel caso dell'esempio, è preferibile digitare 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 secondari 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 secondari con le seguenti cardinalità:

- 1 contactName
- 1 EmailAddress
- 0..1 facsimileNumber
- 1 telephoneNumber

Nel file XSD, tuttavia, ogni elemento secondario 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 pacchetto del flusso di documenti PIP di un'altra versione del pacchetto e si desidera riutilizzare una definizione dall'altra versione, procedere come segue per ciascuna di queste definizioni:

- a. Eliminare la definizione dell'elemento. Ad esempio, eliminare l'elemento di Contact Information.
- b. Aprire il pacchetto del flusso di documenti PIP della versione da sostituire. 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_EmailAddress_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 che si crea per il pacchetto del flusso di documenti 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 un pacchetto del flusso di documenti PIP o si aggiorna un pacchetto del flusso di documenti PIP, ma la definizione necessaria non è presente nell'altra versione, procedere come segue per ogni istanza dell'elemento trovato nelle istruzioni:

- a. Eliminare la definizione dell'elemento. Ad esempio, eliminare l'elemento delle informazioni di contatto.

- 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` 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 pacchetto del flusso di documenti PIP in base ad un'altra versione del pacchetto e si desidera utilizzare un insieme di valori di enumerazione dell'altra versione, procedere come segue per ciascun insieme:

- a. Eliminare la definizione per l'elemento. Ad esempio, eliminare l'elemento GlobalRegistrationComplexityLevelCode:
- b. Aprire il pacchetto del flusso di documenti PIP della versione da sostituire. 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 che si crea per il pacchetto del flusso di documenti 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 un pacchetto del flusso di documenti PIP o si aggiorna un pacchetto del flusso di documenti PIP, ma le definizioni del valore di enumerazione necessarie non sono presenti nell'altra versione, eseguire questi passaggi per ogni 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 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 commerciali fondamentali:

Se si aggiorna il pacchetto del flusso di documenti PIP su un'altra versione del pacchetto e si desidera utilizzare una definizione dell'entità dei dati dall'altra versione, procedere come segue per ciascun insieme:

- a. Eliminare la definizione per l'elemento di entità dei dati. Ad esempio, eliminare l'elemento Data e ora.
- b. Aprire il pacchetto del flusso di documenti PIP della versione da sostituire. 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 che si crea per il pacchetto del flusso di documenti 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 un pacchetto del flusso di documenti PIP o si aggiorna un pacchetto del flusso di documenti PIP, ma la definizione dell'entità dei dati necessaria non è presente nell'altra versione, procedere come segue per ogni elemento di entità dei 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 a pagina 236 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 del file XML

Dopo la creazione dei file XSD per il pacchetto del flusso di documenti PIP, si è pronti per creare il file XML per il pacchetto RNIF e il file XML per il pacchetto di Integrazione di backend. Ad esempio, questi pacchetti 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 pacchetto RNIF:

1. Estrarre il file XML da un file del pacchetto del flusso di documenti RNIF PIP. Se si sta effettuando l'aggiornamento, estrarre il file dalla versione precedente del pacchetto (ad esempio BCG\_Package\_RNIFV02.00\_5C4V01.02.zip). Se si sta creando un nuovo pacchetto, estrarre il file da un pacchetto del flusso di documenti PIP che è simile a quello che si sta creando. Ad esempio, se si sta creando un pacchetto per supportare un PIP di due azioni, copiare il file XML da un altro pacchetto 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 informazioni sul PIP. Ad esempio, la seguente tabella elenca le informazioni 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 37. 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

Tabella 37. Informazioni di aggiornamento 5C4 PIP (Continua)

Informazioni da modificare	Valore vecchio	Valore nuovo
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 Notifica	Pip5C4RegistrationStatus Notifica
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 38. Le informazioni di aggiornamento 5C4 PIP dalla specifica PIP

Informazioni da aggiornare	Descrizione	Valore nel pacchetto 5C4
Nome attività	Specificato nella Tabella 3-2	Stato di registrazione di distribuzione
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 pacchetto. Se si sta effettuando un aggiornamento, confrontare le specifiche per le versioni poiché questi valori potrebbero non dover essere aggiornati.

**Nota:** Se si desidera creare il pacchetto Integrazione Backend, saltare questo passaggio ed andare al passaggio 6 a pagina 238.

Tabella 39. Aggiornamenti dell'attributo 5C4 PIP

Informazioni da aggiornare	Descrizione	Valore nel pacchetto 5C4	Percorso dell'elemento nel file XML
NonRepudiation Required	Specificato nella Tabella 3-3	N	ns1:Package ns1:Protocol ns1:Process ns1:Attribute (il relativo ATTRIBUTEKEY è NonRepudiationRequired) ns1:AttributeValue AttributePickListItem ATTRVALUEKEY
NonRepudiationOf Receipt	Specificato nella Tabella 3-3	N	ns1:Package ns1:Protocol ns1:Process ns1:Attribute (il relativo ATTRIBUTEKEY è NonRepudiationOfReceipt) ns1:AttributeValue AttributePickListItem ATTRVALUEKEY
DigitalSignature Required	Specificato nella Tabella 5-1	Y	ns1:Package ns1:Protocol ns1:Process ns1:Attribute (il relativo ATTRIBUTEKEY è DigitalSignatureRequired) ns1:AttributeValue AttributePickListItem ATTRVALUEKEY
TimeToAcknowledge	Specificato nella Tabella 3-3	2 (120 min)	ns1:Package ns1:Protocol ns1:Process ns1:Attribute (il relativo ATTRIBUTEKEY è TimeToAcknowledge) ns1:AttributeValue ATTRVALUE
TimeToPerform	Specificato nella Tabella 3-3	2 (120 min)	ns1:Package ns1:Protocol ns1:Process ns1:Attribute (il relativo ATTRIBUTEKEY è TimeToPerform) ns1:AttributeValue ATTRVALUE
RetryCount	Specificato nella Tabella 3-3	3	ns1:Package ns1:Protocol ns1:Process ns1:Attribute (il relativo ATTRIBUTEKEY è 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 pacchetto di Integrazione Backend, ripetere i passaggi compresi tra 1 e 6, tranne che le seguenti differenze:

- Nel passaggio 1 a pagina 236, estrarre il file XML dal pacchetto di Integrazione Backend (ad esempio, BCG\_Package\_RNSC1.0\_RNIFV02.00\_5C4V01.02.zip).
- Non eseguire il passaggio 5 a pagina 237.

Dopo aver creato l'XML e i file XSD, si è pronti per creare i pacchetti del flusso di documentazione PIP.

## Creazione del pacchetto

Per creare il pacchetto RNIF, eseguire questi passaggi:

1. Creare una directory GuidelineMaps e copiare i file XSD del pacchetto in questa directory.
2. Creare una directory Packages e copiare il file XML RNIF in questa directory.
3. Andare alla directory principale e creare un pacchetto del flusso di documenti PIP (file ZIP) che contiene la directory GuidelineMaps and Packages. È necessario conservare la struttura della directory nel file ZIP.

Per creare il pacchetto 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 pacchetto PIP, è possibile caricarlo mediante la procedura descritta in "RNIF e pacchetti di flusso dei documenti PIP" a pagina 61.

---

## 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. In ogni pacchetto del flusso di documenti 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. Se, tuttavia, si eseguono, vedere "Creazione di pacchetti di flusso di documenti PIP" a pagina 229 per informazioni sui passaggi necessari per aggiornare i file XSD per convalidare i messaggi e in che modo creare un pacchetto del flusso di documenti 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="E" />
 <xsd:enumeration value="Update" />
 </xsd:restriction>
</xsd:simpleType>
```

Tutti gli elementi dl tipo \_local\_GlobalDesignRegistrationNotificationCode in un messaggio devono avere solo "Initial" o "Update" per i propri valori.

---

## Contenuti del pacchetto del flusso di documenti PIP

Nelle sezioni successive, vengono mostrati i pacchetti del flusso di documenti PIP forniti da WebSphere Partner Gateway per ciascun PIP. In ogni pacchetto c'è un file XML contenuto in una directory Packages e diversi file XSD contenuti nella directory GuidelineMaps, che sono comuni a tutti i pacchetti del flusso di documenti PIP per il PIP.

### 0A1 Notification of Failure V1.0

Nella seguente sezione, viene descritto il contenuto del pacchetto PIP 0A1 Notification of Failure V1.0.

#### Contenuto del file del pacchetto

Nella seguente tabella vengono mostrati i file ZIP e i file XML corrispondenti per il PIP 0A1 Notification of Failure V1.0. Le mappe della direttiva comune a tutte le versioni vengono mostrate nella sezione successiva.

Tabella 40. File ZIP e XML del PIP 0A1 Notification of Failure 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 Notification of Failure 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 Notification of Failure V02.00

Nella seguente sezione, viene descritto il contenuto del pacchetto PIP 0A1 Notification of Failure V02.00.

#### Contenuto del file del pacchetto

Nella seguente tabella vengono mostrati i file ZIP e i file XML corrispondenti per il PIP 0A1 Notification of Failure V02.00. Le mappe della direttiva comune a tutte le versioni vengono mostrate nella sezione successiva.

Tabella 41. File ZIP e XML del PIP 0A1 Notification of Failure 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 Notification of Failure 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 Distribute New Product Information

Nella seguente sezione, viene descritto il contenuto del pacchetto PIP 2A1 Distribute New Product Information.

### Contenuto del file del pacchetto

Nella seguente tabella vengono mostrati i file ZIP e i file XML corrispondenti per il PIP 2A1 Distribute New Product Information. Le mappe della direttiva comune a tutte le versioni vengono mostrate nella sezione successiva.

Tabella 42. File ZIP e XML di 2A1 Distribute New Product Information

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 Distribute New Product Information:

- BCG\_2A1ProductCatalogInformationNotification\_V02.00.xsd
- BCG\_BusinessDescription\_Types.xsd
- BCG\_BusinessDescription\_Types\_V422.xsd
- BCG\_BusinessDescription\_Types\_V43.xsd
- BCG\_BusinessTaxIdentifier\_Types.xsd
- BCG\_common.xsd
- BCG\_common\_V422.xsd
- BCG\_common\_V43.xsd
- BCG\_ContactInformation\_Types.xsd
- BCG\_ContactInformation\_Types\_V422.xsd
- BCG\_ContactInformation\_Types\_V43.xsd
- BCG\_GlobalCountryCode.xsd
- BCG\_GlobalCurrencyCode.xsd
- BCG\_GlobalDocumentReferenceTypeCode.xsd
- BCG\_GlobalIntervalCode.xsd
- BCG\_GlobalLeadTimeClassificationCode\_V43.xsd
- BCG\_GlobalMonetaryAmountTypeCode.xsd
- BCG\_GlobalPackageTypeCode\_V422.xsd
- BCG\_GlobalPartnerClassificationCode\_V43.xsd
- BCG\_GlobalPartnerRoleClassificationCode\_V422.xsd

- BCG\_GlobalPriceTypeCode\_V43.xsd
- BCG\_GlobalProductAssociationCode\_V43.xsd
- BCG\_GlobalProductLifeCycleStatusCode.xsd
- BCG\_GlobalProductProcurementTypeCode\_V43.xsd
- BCG\_GlobalProductTypeCode\_V43.xsd
- BCG\_GlobalProductUnitofMeasureCode\_V43.xsd
- BCG\_GlobalProprietaryProductIdentificationTypeCode\_V43.xsd
- BCG\_GlobalStandardClassificationSchemeCode\_V43.xsd
- BCG\_GlobalWarrantyTypeCode\_V43.xsd
- BCG\_InvoiceChargeTypeCode\_V422.xsd
- BCG\_NationalExportControlClassificationCode.xsd
- BCG\_PartnerDescription\_Types\_V43.xsd
- BCG\_PhysicalAddress\_Types.xsd
- BCG\_PhysicalAddress\_Types\_V422.xsd
- BCG\_string\_len\_0.xsd
- BCG\_xml.xsd

## 2A12 Distribute Product Master

Nella seguente sezione, viene descritto il contenuto del pacchetto PIP 2A12 Distribute Product Master.

### Contenuto del file del pacchetto

Nella seguente tabella vengono mostrati i file ZIP e i file XML corrispondenti al PIP 2A12 Distribute Product Master. Le mappe della direttiva comune a tutte le versioni vengono mostrate nella sezione successiva.

Tabella 43. File ZIP e XML di 2A12 Distribute Product Master

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
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 Distribute Product Master:

- BCG\_2A12ProductMasterNotification\_V01.03.xsd
- BCG\_BusinessDescription\_Types.xsd
- BCG\_BusinessTaxIdentifier\_Types.xsd
- BCG\_common.xsd
- BCG\_ContactInformation\_Types.xsd
- BCG\_GlobalAssemblyLevelCode.xsd
- BCG\_GlobalCountryCode.xsd
- BCG\_GlobalIntervalCode.xsd
- BCG\_GlobalLeadTimeClassificationCode.xsd
- BCG\_GlobalPartnerClassificationCode.xsd
- BCG\_GlobalPartnerRoleClassificationCode.xsd

- BCG\_GlobalProductLifeCycleStatusCode.xsd
- BCG\_GlobalProductProcurementTypeCode.xsd
- BCG\_GlobalProductUnitOfMeasureCode.xsd
- BCG\_PartnerDescription\_Types.xsd
- BCG\_PhysicalAddress\_Types.xsd
- BCG\_string\_len\_0.xsd
- BCG\_xml.xsd

## 3A1 Request Quote

Nella seguente sezione viene descritto il contenuto del pacchetto PIP 3A1 Request Quote.

### Contenuto del file del pacchetto

Nella seguente tabella vengono mostrati i file ZIP e i file XML corrispondenti per il PIP 3A1 Request Quote. Le mappe della direttiva comune a tutte le versioni vengono mostrate nella sezione successiva.

Tabella 44. File ZIP e XML di 3A1 Request Quote

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 Request Quote:

- BCG\_3A1QuoteConfirmation\_V02.00.xsd
- BCG\_3A1QuoteRequest\_V02.00.xsd
- BCG\_BusinessDescription\_Types.xsd
- BCG\_BusinessTaxIdentifier\_Types.xsd
- BCG\_common.xsd
- BCG\_ContactInformation\_Types.xsd
- BCG\_GlobalCountryCode.xsd
- BCG\_GlobalCurrencyCode.xsd
- BCG\_GlobalGovernmentPriorityRatingCode.xsd
- BCG\_GlobalMonetaryAmountTypeCode.xsd
- BCG\_GlobalPartnerClassificationCode.xsd
- BCG\_GlobalPartnerRoleClassificationCode.xsd
- BCG\_GlobalProductSubstitutionReasonCode.xsd
- BCG\_GlobalProductTermsCode.xsd
- BCG\_GlobalProductUnitOfMeasureCode.xsd
- BCG\_GlobalQuoteLineItemStatusCode.xsd
- BCG\_GlobalQuoteTypeCode.xsd
- BCG\_GlobalStockIndicatorCode.xsd
- BCG\_GlobalTaxExemptionCode.xsd
- BCG\_PartnerDescription\_Types.xsd

- BCG\_PhysicalAddress\_Types.xsd
- BCG\_string\_len\_0.xsd
- BCG\_xml.xsd

## 3A2 Request Price and Availability

Nella seguente sezione viene descritto il contenuto del pacchetto PIP 3A2 Request Price and Availability.

### Contenuto del file del pacchetto

Nella seguente tabella vengono mostrati i file ZIP e i file XML corrispondenti per il PIP 3A2 Request Price And Availability. Le mappe della direttiva comune a tutte le versioni vengono mostrate nella sezione successiva.

Tabella 45. File ZIP e XML di 3A2 Request Price And Availability

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 Request Price And Availability:

- BCG\_3A2PriceAndAvailabilityRequest\_R02.01.xsd
- BCG\_3A2PriceAndAvailabilityResponse\_R02.01.xsd
- BCG\_BusinessDescription\_Types.xsd
- BCG\_BusinessTaxIdentifier\_Types.xsd
- BCG\_common.xsd
- BCG\_ContactInformation\_Types.xsd
- BCG\_GlobalCountryCode.xsd
- BCG\_GlobalCurrencyCode.xsd
- BCG\_GlobalCustomerAuthorizationCode.xsd
- BCG\_GlobalPartnerClassificationCode.xsd
- BCG\_GlobalPricingTypeCode.xsd
- BCG\_GlobalProductAvailabilityCode.xsd
- BCG\_GlobalProductStatusCode.xsd
- BCG\_GlobalProductSubstitutionReasonCode.xsd
- BCG\_GlobalProductUnitOfMeasureCode.xsd
- BCG\_PartnerDescription\_Types.xsd
- BCG\_PhysicalAddress\_Types.xsd
- BCG\_string\_len\_0.xsd
- BCG\_xml.xsd

## 3A4 Request Purchase Order V02.00

Nella seguente sezione viene descritto il contenuto del pacchetto PIP 3A4 Request Purchase Order V02.00.

## Contenuto del file del pacchetto

Nella seguente tabella vengono mostrati i file ZIP e i file XML corrispondenti per il PIP 3A4 Request Purchase Order. Le mappe della direttiva comune a tutte le versioni vengono mostrate nella sezione successiva.

Tabella 46. File ZIP e XML di 3A4 Request Purchase Order

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 Request Purchase Order:

- BCG\_3A4PurchaseOrderConfirmation\_V02.00.xsd
- BCG\_3A4PurchaseOrderRequest\_V02.00.xsd
- BCG\_BusinessDescription\_Types.xsd
- BCG\_BusinessDescription\_Types\_V422.xsd
- BCG\_BusinessTaxIdentifier\_Types.xsd
- BCG\_common.xsd
- BCG\_common\_V422.xsd
- BCG\_ContactInformation\_Types.xsd
- BCG\_GlobalAccountClassificationCode.xsd
- BCG\_GlobalConfirmationTypeCode.xsd
- BCG\_GlobalCountryCode.xsd
- BCG\_GlobalCreditCardClassificationCode.xsd
- BCG\_GlobalCurrencyCode.xsd
- BCG\_GlobalDocumentReferenceTypeCode.xsd
- BCG\_GlobalDocumentReferenceTypeCode\_V422.xsd
- BCG\_GlobalFinanceTermsCode.xsd
- BCG\_GlobalGovernmentPriorityRatingCode.xsd
- BCG\_GlobalMonetaryAmountTypeCode.xsd
- BCG\_GlobalPartnerClassificationCode.xsd
- BCG\_GlobalPartnerRoleClassificationCode\_V422.xsd
- BCG\_GlobalPaymentConditionCode.xsd
- BCG\_GlobalPriceUnitOfMeasureCode.xsd
- BCG\_GlobalProductSubstitutionReasonCode.xsd
- BCG\_GlobalProductUnitOfMeasureCode.xsd
- BCG\_GlobalPurchaseOrderAcknowledgmentReasonCode.xsd
- BCG\_GlobalPurchaseOrderFillPriorityCode.xsd
- BCG\_GlobalPurchaseOrderStatusCode.xsd
- BCG\_GlobalPurchaseOrderTypeCode.xsd
- BCG\_GlobalShipmentTermsCode.xsd
- BCG\_GlobalShipmentTermsCode\_V422.xsd
- BCG\_GlobalShippingServiceLevelCode.xsd

- BCG\_GlobalSpecialFulfillmentRequestCode.xsd
- BCG\_GlobalSpecialHandlingCode\_V422.xsd
- BCG\_GlobalTaxExemptionCode.xsd
- BCG\_GlobalTaxExemptionCode\_V422.xsd
- BCG\_InvoiceChargeTypeCode.xsd
- BCG\_PartnerDescription\_Types.xsd
- BCG\_PhysicalAddress\_Types.xsd
- BCG\_PhysicalAddress\_Types\_V422.xsd
- BCG\_string\_len\_0.xsd
- BCG\_xml.xsd

## 3A4 Request Purchase Order V02.02

Nella seguente sezione viene descritto il contenuto del pacchetto PIP 3A4 Request Purchase Order V02.02.

### Contenuto del file del pacchetto

Nella seguente tabella vengono mostrati i file ZIP e i file XML corrispondenti per il PIP 3A4 Request Purchase Order. Le mappe della direttiva comune a tutte le versioni vengono mostrate nella sezione successiva.

Tabella 47. File ZIP e XML di 3A4 Request Purchase Order

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 Request Purchase Order:

- BCG\_3A4PurchaseOrderConfirmation\_V02.02.xsd
- BCG\_3A4PurchaseOrderRequest\_V02.02.xsd
- BCG\_BusinessDescription\_Types.xsd
- BCG\_BusinessTaxIdentifier\_Types.xsd
- BCG\_common.xsd
- BCG\_ContactInformation\_Types.xsd
- BCG\_GlobalAccountClassificationCode.xsd
- BCG\_GlobalConfirmationTypeCode.xsd
- BCG\_GlobalCountryCode.xsd
- BCG\_GlobalCreditCardClassificationCode.xsd
- BCG\_GlobalCurrencyCode.xsd
- BCG\_GlobalDocumentReferenceTypeCode.xsd
- BCG\_GlobalFinanceTermsCode.xsd
- BCG\_GlobalGovernmentPriorityRatingCode.xsd
- BCG\_GlobalMonetaryAmountTypeCode.xsd
- BCG\_GlobalPartnerClassificationCode.xsd
- BCG\_GlobalPartnerRoleClassificationCode.xsd

- BCG\_GlobalPaymentConditionCode.xsd
- BCG\_GlobalPriceUnitOfMeasureCode.xsd
- BCG\_GlobalProductSubstitutionReasonCode.xsd
- BCG\_GlobalProductUnitOfMeasureCode.xsd
- BCG\_GlobalPurchaseOrderAcknowledgmentReasonCode.xsd
- BCG\_GlobalPurchaseOrderFillPriorityCode.xsd
- BCG\_GlobalPurchaseOrderStatusCode.xsd
- BCG\_GlobalPurchaseOrderTypeCode.xsd
- BCG\_GlobalShipmentTermsCode.xsd
- BCG\_GlobalShippingServiceLevelCode.xsd
- BCG\_GlobalSpecialFulfillmentRequestCode.xsd
- BCG\_GlobalSpecialHandlingCode.xsd
- BCG\_GlobalTaxExemptionCode.xsd
- BCG\_InvoiceChargeTypeCode.xsd
- BCG\_PartnerDescription\_Types.xsd
- BCG\_PhysicalAddress\_Types.xsd
- BCG\_string\_len\_0.xsd
- BCG\_xml.xsd

### 3A5 Query Order Status

Nella seguente sezione, viene descritto il contenuto del pacchetto PIP 3A5 Query Order Status.

#### Contenuto del file del pacchetto

Nella seguente tabella vengono mostrati i file ZIP e i file XML corrispondenti per il PIP 3A5 QueryOrder Status. Le mappe della direttiva comune a tutte le versioni vengono mostrate nella sezione successiva.

Tabella 48. File ZIP e XML di 3A5 Query Order Status

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 Order Status:

- BCG\_3A5PurchaseOrderStatusQuery\_R02.00.xsd
- BCG\_3A5PurchaseOrderStatusResponse\_R02.00.xsd
- BCG\_BusinessDescription\_Types.xsd
- BCG\_BusinessTaxIdentifier\_Types.xsd
- BCG\_common.xsd
- BCG\_ContactInformation\_Types.xsd
- BCG\_GlobalAccountClassificationCode.xsd
- BCG\_GlobalCountryCode.xsd
- BCG\_GlobalCreditCardClassificationCode.xsd

- BCG\_GlobalCurrencyCode.xsd
- BCG\_GlobalCustomerTypeCode.xsd
- BCG\_GlobalDocumentReferenceTypeCode.xsd
- BCG\_GlobalFinanceTermsCode.xsd
- BCG\_GlobalFreeOnBoardCode.xsd
- BCG\_GlobalGovernmentPriorityRatingCode.xsd
- BCG\_GlobalLineItemStatusCode.xsd
- BCG\_GlobalOrderQuantityTypeCode.xsd
- BCG\_GlobalPartnerClassificationCode.xsd
- BCG\_GlobalPartnerRoleClassificationCode.xsd
- BCG\_GlobalProductSubstitutionReasonCode.xsd
- BCG\_GlobalProductUnitOfMeasureCode.xsd
- BCG\_GlobalPurchaseOrderAcknowledgmentReasonCode.xsd
- BCG\_GlobalPurchaseOrderFillPriority
- BCG\_GlobalPurchaseOrderStatusCode.xsd
- BCG\_GlobalPurchaseOrderTypeCode.xsd
- BCG\_GlobalShipmentTermsCode.xsd
- BCG\_GlobalShippingServiceLevelCode.xsd
- BCG\_GlobalSpecialFulfillmentRequestCode.xsd
- BCG\_GlobalSpecialHandlingCode.xsd
- BCG\_GlobalTaxExemptionCode.xsd
- BCG\_GlobalTransportEventCode.xsd
- BCG\_PartnerDescription\_Types.xsd
- BCG\_PhysicalAddress\_Types.xsd
- BCG\_string\_len\_0.xsd
- BCG\_xml.xsd

### 3A6 Distribute Order Status

Nella seguente sezione viene descritto il contenuto del pacchetto PIP 3A6 Distribute Order Status.

#### Contenuto del file del pacchetto

Nella seguente tabella vengono mostrati i file ZIP e i file XML corrispondenti per il PIP 3A6 Distribute Order Status. Le mappe della direttiva comune a tutte le versioni vengono mostrate nella sezione successiva.

Tabella 49. File ZIP e XML di 3A6 Distribute Order Status

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 Distribute Order Status:

- BCG\_3A6PurchaseOrderStatusNotification\_V02.02.xsd

- BCG\_BusinessDescription\_Types.xsd
- BCG\_BusinessTaxIdentifier\_Types.xsd
- BCG\_common.xsd
- BCG\_ContactInformation\_Types.xsd
- BCG\_GlobalAccountClassificationCode.xsd
- BCG\_GlobalCountryCode.xsd
- BCG\_GlobalCreditCardClassificationCode.xsd
- BCG\_GlobalCurrencyCode.xsd
- BCG\_GlobalDocumentReferenceTypeCode.xsd
- BCG\_GlobalFinanceTermsCode.xsd
- BCG\_GlobalGovernmentPriorityRatingCode.xsd
- BCG\_GlobalLineItemStatusCode.xsd
- BCG\_GlobalMonetaryAmountTypeCode.xsd
- BCG\_GlobalNotificationReasonCode.xsd
- BCG\_GlobalOrderQuantityTypeCode.xsd
- BCG\_GlobalPartnerClassificationCode.xsd
- BCG\_GlobalPartnerRoleClassificationCode.xsd
- BCG\_GlobalPaymentConditionCode.xsd
- BCG\_GlobalPriceUnitOfMeasureCode.xsd
- BCG\_GlobalProductSubstitutionReasonCode.xsd
- BCG\_GlobalProductUnitOfMeasureCode.xsd
- BCG\_GlobalPurchaseOrderAcknowledgmentReasonCode.xsd
- BCG\_GlobalPurchaseOrderFillPriorityCode.xsd
- BCG\_GlobalPurchaseOrderStatusCode.xsd
- BCG\_GlobalPurchaseOrderTypeCode.xsd
- BCG\_GlobalShipmentTermsCode.xsd
- BCG\_GlobalShippingServiceLevelCode.xsd
- BCG\_GlobalSpecialFulfillmentRequestCode.xsd
- BCG\_GlobalSpecialHandlingCode.xsd
- BCG\_GlobalTaxExemptionCode.xsd
- BCG\_GlobalTrackingReferenceTypeCode.xsd
- BCG\_InvoiceChargeTypeCode.xsd
- BCG\_PartnerDescription\_Types.xsd
- BCG\_PhysicalAddress\_Types.xsd
- BCG\_string\_len\_0.xsd
- BCG\_xml.xsd

### 3A7 Notify of Purchase Order Update

Nella seguente sezione viene descritto il contenuto del pacchetto PIP 3A7 Notify of Purchase Order Update.

#### Contenuto del file del pacchetto

Nella seguente tabella vengono mostrati i file ZIP e i file XML corrispondenti per il PIP 3A7 Notify of Purchase Order Update. Le mappe della direttiva comune a tutte le versioni vengono mostrate nella sezione successiva.

Tabella 50. File ZIP e XML di 3A7 Notify of Purchase Order Update

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 Notify of Purchase Order Update:

- BCG\_3A7PurchaseOrderUpdateNotification\_V02.02.xsd
- BCG\_BusinessDescription\_Types.xsd
- BCG\_BusinessTaxIdentifier\_Types.xsd
- BCG\_common.xsd
- BCG\_ContactInformation\_Types.xsd
- BCG\_GlobalAccountClassificationCode.xsd
- BCG\_GlobalActionCode.xsd
- BCG\_GlobalConfirmationTypeCode.xsd
- BCG\_GlobalCountryCode.xsd
- BCG\_GlobalCreditCardClassificationCode.xsd
- BCG\_GlobalCurrencyCode.xsd
- BCG\_GlobalDocumentReferenceTypeCode.xsd
- BCG\_GlobalFinanceTermsCode.xsd
- BCG\_GlobalGovernmentPriorityRatingCode.xsd
- BCG\_GlobalMonetaryAmountTypeCode.xsd
- BCG\_GlobalPartnerClassificationCode.xsd
- BCG\_GlobalPartnerRoleClassificationCode.xsd
- BCG\_GlobalPaymentConditionCode.xsd
- BCG\_GlobalPriceUnitOfMeasureCode.xsd
- BCG\_GlobalProductSubstitutionReasonCode.xsd
- BCG\_GlobalProductUnitOfMeasureCode.xsd
- BCG\_GlobalPurchaseOrderAcknowledgmentReasonCode.xsd
- BCG\_GlobalPurchaseOrderFillPriorityCode.xsd
- BCG\_GlobalPurchaseOrderStatusCode.xsd
- BCG\_GlobalPurchaseOrderTypeCode.xsd
- BCG\_GlobalShipmentTermsCode.xsd
- BCG\_GlobalShippingServiceLevelCode.xsd
- BCG\_GlobalSpecialFulfillmentRequestCode.xsd
- BCG\_GlobalSpecialHandlingCode.xsd
- BCG\_GlobalTaxExemptionCode.xsd
- BCG\_InvoiceChargeTypeCode.xsd
- BCG\_PartnerDescription\_Types.xsd
- BCG\_PhysicalAddress\_Types.xsd
- BCG\_string\_len\_0.xsd
- BCG\_xml.xsd

## 3A8 Request Purchase Order Change V01.02

Nella seguente sezione viene descritto il contenuto del pacchetto PIP 3A8 Request Purchase Order Change V01.02.

### Contenuto del file del pacchetto

Nella seguente tabella vengono mostrati i file ZIP e i file XML corrispondenti per il PIP 3A8 Request Purchase Order Change. Le mappe della direttiva comune a tutte le versioni vengono mostrate nella sezione successiva.

Tabella 51. File ZIP e XML di 3A8 Request Purchase Order Change

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 Request Purchase Order Change:

- BCG\_3A8PurchaseOrderChangeConfirmation\_V01.02.xsd
- BCG\_3A8PurchaseOrderChangeRequest\_V01.02.xsd
- BCG\_BusinessDescription\_Types.xsd
- BCG\_BusinessTaxIdentifier\_Types.xsd
- BCG\_common.xsd
- BCG\_ContactInformation\_Types.xsd
- BCG\_GlobalAccountClassificationCode.xsd
- BCG\_GlobalActionCode.xsd
- BCG\_GlobalConfirmationTypeCode.xsd
- BCG\_GlobalCountryCode.xsd
- BCG\_GlobalCreditCardClassificationCode.xsd
- BCG\_GlobalCurrencyCode.xsd
- BCG\_GlobalDocumentReferenceTypeCode.xsd
- BCG\_GlobalFinanceTermsCode.xsd
- BCG\_GlobalGovernmentPriorityRatingCode.xsd
- BCG\_GlobalMonetaryAmountTypeCode.xsd
- BCG\_GlobalPartnerClassificationCode.xsd
- BCG\_GlobalPartnerRoleClassificationCode.xsd
- BCG\_GlobalPaymentConditionCode.xsd
- BCG\_GlobalPriceUnitOfMeasureCode.xsd
- BCG\_GlobalProductSubstitutionReasonCode.xsd
- BCG\_GlobalProductUnitOfMeasureCode.xsd
- BCG\_GlobalPurchaseOrderAcknowledgmentReasonCode.xsd
- BCG\_GlobalPurchaseOrderFillPriorityCode.xsd
- BCG\_GlobalPurchaseOrderStatusCode.xsd
- BCG\_GlobalPurchaseOrderTypeCode.xsd
- BCG\_GlobalShipmentTermsCode.xsd

- BCG\_GlobalShippingServiceLevelCode.xsd
- BCG\_GlobalSpecialFulfillmentRequestCode.xsd
- BCG\_GlobalSpecialHandlingCode.xsd
- BCG\_GlobalTaxExemptionCode.xsd
- BCG\_InvoiceChargeTypeCode.xsd
- BCG\_PartnerDescription\_Types.xsd
- BCG\_PhysicalAddress\_Types.xsd
- BCG\_string\_len\_0.xsd
- BCG\_xml.xsd

### 3A8 Request Purchase Order Change V01.03

Nella seguente sezione, viene descritto il contenuto del pacchetto PIP 3A8 Request Purchase Order Change V01.03.

#### Contenuto del file del pacchetto

Nella seguente tabella vengono mostrati i file ZIP e i file XML corrispondenti per il PIP 3A8 Request Purchase Order Change. Le mappe della direttiva comune a tutte le versioni vengono mostrate nella sezione successiva.

Tabella 52. File ZIP e XML di 3A8 Request Purchase Order Change

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 Request Purchase Order Change:

- BCG\_3A8PurchaseOrderChangeConfirmation\_V01.03.xsd
- BCG\_3A8PurchaseOrderChangeRequest\_V01.03.xsd
- BCG\_BusinessDescription\_Types.xsd
- BCG\_BusinessDescription\_Types\_V43.xsd
- BCG\_BusinessTaxIdentifier\_Types.xsd
- BCG\_common.xsd
- BCG\_common\_V422.xsd
- BCG\_common\_V43.xsd
- BCG\_ContactInformation\_Types.xsd
- BCG\_GlobalAccountClassificationCode.xsd
- BCG\_GlobalActionCode.xsd
- BCG\_GlobalConfirmationTypeCode.xsd
- BCG\_GlobalCountryCode.xsd
- BCG\_GlobalCreditCardClassificationCode.xsd
- BCG\_GlobalCurrencyCode.xsd
- BCG\_GlobalDocumentReferenceTypeCode.xsd
- BCG\_GlobalFinanceTermsCode.xsd
- BCG\_GlobalFreeOnBoardCode\_V422.xsd

- BCG\_GlobalGovernmentPriorityRatingCode.xsd
- BCG\_GlobalMonetaryAmountTypeCode.xsd
- BCG\_GlobalPartnerClassificationCode\_V43.xsd
- BCG\_GlobalPartnerRoleClassificationCode\_V43.xsd
- BCG\_GlobalPaymentConditionCode.xsd
- BCG\_GlobalProductSubstitutionReasonCode.xsd
- BCG\_GlobalProductUnitOfMeasureCode\_V43.xsd
- BCG\_GlobalPurchaseOrderAcknowledgmentReasonCode.xsd
- BCG\_GlobalPurchaseOrderFillPriorityCode.xsd
- BCG\_GlobalPurchaseOrderStatusCode.xsd
- BCG\_GlobalPurchaseOrderTypeCode.xsd
- BCG\_GlobalShipmentTermsCode.xsd
- BCG\_GlobalShippingServiceLevelCode.xsd
- BCG\_GlobalSpecialFulfillmentRequestCode.xsd
- BCG\_GlobalSpecialHandlingCode\_V43.xsd
- BCG\_GlobalTaxExemptionCode.xsd
- BCG\_GlobalTransportEventCode.xsd
- BCG\_InvoiceChargeTypeCode\_V422.xsd
- BCG\_PartnerDescription\_Types.xsd
- BCG\_PartnerDescription\_Types\_V43.xsd
- BCG\_PhysicalAddress\_Types.xsd
- BCG\_string\_len\_0.xsd
- BCG\_xml.xsd

### 3A9 Request Purchase Order Cancellation

Nella seguente sezione, viene descritto il contenuto del pacchetto PIP 3A9 Request Purchase Order Cancellation.

#### Contenuto del file del pacchetto

Nella seguente tabella vengono mostrati i file ZIP e i file XML corrispondenti per il PIP 3A9 Request Purchase Order Cancellation. Le mappe della direttiva comune a tutte le versioni vengono mostrate nella sezione successiva.

Tabella 53. File ZIP e XML di 3A9 Request Purchase Order Cancellation

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 Request Purchase Order Cancellation:

- BCG\_3A9PurchaseOrderCancellationConfirmation\_V01.01.xsd
- BCG\_3A9PurchaseOrderCancellationRequest\_V01.01.xsd
- BCG\_BusinessDescription\_Types.xsd
- BCG\_BusinessTaxIdentifier\_Types.xsd

- BCG\_common.xsd
- BCG\_ContactInformation\_Types.xsd
- BCG\_GlobalCountryCode.xsd
- BCG\_GlobalPartnerClassificationCode.xsd
- BCG\_GlobalPurchaseOrderCancellationCode.xsd
- BCG\_GlobalPurchaseOrderCancellationResponseCode.xsd
- BCG\_PartnerDescription\_Types.xsd
- BCG\_PhysicalAddress\_Types.xsd
- BCG\_string\_len\_0.xsd
- BCG\_xml.xsd

## 3B2 Notify of Advance Shipment

Nella seguente sezione, viene descritto il contenuto del pacchetto PIP 3B2 Notify of Advance Shipment.

### Contenuto del file del pacchetto

Nella seguente tabella vengono mostrati i file ZIP e i file XML corrispondenti per il PIP 3B2 Notify of Advance Shipment. Le mappe della direttiva comune a tutte le versioni vengono mostrate nella sezione successiva.

Tabella 54. File ZIP e XML di 3B2 Notify of Advance Shipment

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 Notify of Advance Shipment:

- BCG\_3B2AdvanceShipmentNotification\_V01.01.xsd
- BCG\_BusinessDescription\_Types.xsd
- BCG\_BusinessTaxIdentifier\_Types.xsd
- BCG\_common.xsd
- BCG\_ContactInformation\_Types.xsd
- BCG\_GlobalCountryCode.xsd
- BCG\_GlobalDocumentReferenceTypeCode.xsd
- BCG\_GlobalIncotermsCode.xsd
- BCG\_GlobalLotQuantityClassificationCode.xsd
- BCG\_GlobalPackageTypeCode.xsd
- BCG\_GlobalPartnerClassificationCode.xsd
- BCG\_GlobalPhysicalUnitOfMeasureCode.xsd
- BCG\_GlobalProductUnitOfMeasureCode.xsd
- BCG\_GlobalShipDateCode.xsd
- BCG\_GlobalShipmentChangeDispositionCode.xsd
- BCG\_GlobalShipmentModeCode.xsd
- BCG\_GlobalShippingServiceLevelCode.xsd

- BCG\_GlobalTrackingReferenceTypeCode.xsd
- BCG\_NationalExportControlClassificationCode.xsd
- BCG\_PartnerDescription\_Types.xsd
- BCG\_PhysicalAddress\_Types.xsd
- BCG\_string\_len\_0.xsd
- BCG\_xml.xsd

## 3B3 Distribute Shipment Status

Nella seguente sezione, viene descritto il contenuto del pacchetto PIP 3B3 Distribute Shipment Status.

### Contenuto del file del pacchetto

Nella seguente tabella vengono mostrati i file ZIP e i file XML corrispondenti per il PIP 3B3 Distribute Shipment Status. Le mappe della direttiva comune a tutte le versioni vengono mostrate nella sezione successiva.

Tabella 55. File ZIP e XML di 3B3 Distribute Shipment Status

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 Distribute Shipment Status:

- 3B3 Distribute Shipment Status\_R01.00.xsd
- BCG\_BusinessDescription\_Types.xsd
- BCG\_BusinessDescription\_Types\_V422.xsd
- BCG\_BusinessDescription\_Types\_V43.xsd
- BCG\_BusinessTaxIdentifier\_Types.xsd
- BCG\_common\_V422.xsd
- BCG\_common\_V43.xsd
- BCG\_ContactInformation\_Types.xsd
- BCG\_ContactInformation\_Types\_V422.xsd
- BCG\_ContactInformation\_Types\_V43.xsd
- BCG\_GlobalCountryCode.xsd
- BCG\_GlobalDocumentReferenceTypeCode\_V43.xsd
- BCG\_GlobalPartnerClassificationCode\_V43.xsd
- BCG\_GlobalShipmentDispositionCode.xsd
- BCG\_GlobalShipmentModeCode.xsd
- BCG\_GlobalShipmentStatusCode\_V43.xsd
- BCG\_GlobalShipmentStatusReportingLevelCode\_V43.xsd
- BCG\_GlobalTrackingReferenceTypeCode.xsd
- BCG\_PartnerDescription\_Types\_V43.xsd
- BCG\_PhysicalAddress\_Types.xsd
- BCG\_PhysicalAddress\_Types\_V422.xsd

- BCG\_PhysicalAddress\_Types\_V423.xsd
- BCG\_string\_len\_0.xsd
- BCG\_xml.xsd

## 3B11 Notify of Shipping Order

Nella seguente sezione, viene descritto il contenuto del pacchetto PIP 3B11 Notify of Shipping Order.

### Contenuto del file del pacchetto

Nella seguente tabella vengono mostrati i file ZIP e i file XML corrispondenti per il PIP 3B11 Notify of Shipping Order. Le mappe della direttiva comune a tutte le versioni vengono mostrate nella sezione successiva.

Tabella 56. File ZIP e XML di 3B11 Notify of Shipping Order

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 Notify of Shipping Order:

- 3B11 ShippingOrderNotification\_R01.00A.xsd
- BCG\_BusinessDescription\_Types.xsd
- BCG\_BusinessDescription\_Types\_V422.xsd
- BCG\_BusinessTaxIdentifier\_Types.xsd
- BCG\_common.xsd
- BCG\_ContactInformation\_Types.xsd
- BCG\_ContactInformation\_Types\_V422.xsd
- BCG\_GlobalCountryCode.xsd
- BCG\_GlobalCurrencyCode.xsd
- BCG\_GlobalDocumentReferenceTypeCode\_V422.xsd
- BCG\_GlobalFreightPaymentTermsCode\_V422.xsd
- BCG\_GlobalIncotermsCode.xsd
- BCG\_GlobalOrderAdminCode\_V422.xsd
- BCG\_GlobalPartnerClassificationCode.xsd
- BCG\_GlobalPartnerRoleClassificationCode.xsd
- BCG\_GlobalProductUnitOfMeasureCode.xsd
- BCG\_GlobalShipDateCode.xsd
- BCG\_GlobalShipmentModeCode.xsd
- BCG\_GlobalShippingServiceLevelCode.xsd
- BCG\_GlobalSpecialHandlingCode.xsd
- BCG\_GlobalWarrantyTypeCode\_V43.xsd
- BCG\_PartnerDescription\_Types.xsd
- BCG\_PartnerDescription\_Types\_V422.xsd
- BCG\_PhysicalAddress\_Types.xsd

- BCG\_string\_len\_0.xsd
- BCG\_xml.xsd

## 3B12 Request Shipping Order

Nella seguente sezione, viene descritto il contenuto del pacchetto PIP 3B12 Request Shipping Order.

### Contenuto del file del pacchetto

Nella seguente tabella vengono mostrati i file ZIP e i file XML corrispondenti per il PIP 3B12 Request Shipping Order. Le mappe della direttiva comune a tutte le versioni vengono mostrate nella sezione successiva.

Tabella 57. File ZIP e XML di 3B12 Request Shipping Order

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 Request Shipping Order:

- BCG\_3B12ShippingOrderConfirmation\_V01.01.xsd
- BCG\_3B12ShippingOrderRequest\_V01.01.xsd
- BCG\_BusinessTaxIdentifier\_Types.xsd
- BCG\_common.xsd
- BCG\_common\_V422.xsd
- BCG\_ContactInformation\_Types.xsd
- BCG\_ContactInformation\_Types\_V422.xsd
- BCG\_GlobalCountryCode.xsd
- BCG\_GlobalCurrencyCode.xsd
- BCG\_GlobalDocumentReferenceTypeCode.xsd
- BCG\_GlobalIncotermsCode.xsd
- BCG\_GlobalPackageTypeCode.xsd
- BCG\_GlobalPartnerClassificationCode.xsd
- BCG\_GlobalPartnerRoleClassificationCode.xsd
- BCG\_GlobalPhysicalUnitOfMeasureCode.xsd
- BCG\_GlobalProductUnitOfMeasureCode.xsd
- BCG\_GlobalShipDateCode.xsd
- BCG\_GlobalShippingServiceLevelCode.xsd
- BCG\_GlobalSpecialHandlingCode.xsd
- BCG\_PartnerDescription\_Types.xsd
- BCG\_PartnerDescription\_Types\_V422.xsd
- BCG\_PhysicalAddress\_Types.xsd
- BCG\_string\_len\_0.xsd
- BCG\_xml.xsd

## 3B13 Notify of Shipping Order Confirmation

Nella seguente sezione, viene descritto il contenuto del pacchetto PIP 3B13 Notify of Shipping Order Confirmation.

### Contenuto del file del pacchetto

Nella seguente tabella vengono mostrati i file ZIP e i file XML corrispondenti per il PIP 3B13 Notify of Shipping Order Confirmation. Le mappe della direttiva comune a tutte le versioni vengono mostrate nella sezione successiva.

Tabella 58. File ZIP e XML di 3B13 Notify of Shipping Order Confirmation

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 Notify of Shipping Order Confirmation:

- BCG\_3B13ShippingOrderConfirmationNotification\_V01.01.xsd
- BCG\_BusinessDescription\_Types.xsd
- BCG\_BusinessTaxIdentifier\_Types.xsd
- BCG\_common.xsd
- BCG\_common\_V422.xsd
- BCG\_ContactInformation\_Types.xsd
- BCG\_GlobalCountryCode.xsd
- BCG\_GlobalCurrencyCode.xsd
- BCG\_GlobalDocumentReferenceTypeCode.xsd
- BCG\_GlobalPartnerClassificationCode.xsd
- BCG\_GlobalPartnerRoleClassificationCode.xsd
- BCG\_GlobalPhysicalUnitOfMeasureCode.xsd
- BCG\_GlobalProductUnitOfMeasureCode.xsd
- BCG\_GlobalShipDateCode.xsd
- BCG\_GlobalShippingServiceLevelCode.xsd
- BCG\_GlobalSpecialHandlingCode.xsd
- BCG\_GlobalTrackingReferenceTypeCode.xsd
- BCG\_PartnerDescription\_Types.xsd
- BCG\_PhysicalAddress\_Types.xsd
- BCG\_string\_len\_0.xsd
- BCG\_xml.xsd

## 3B14 Request Shipping Order Cancellation

Nella seguente sezione, viene descritto il contenuto del pacchetto PIP 3B14 Request Shipping Order Cancellation.

## Contenuto del file del pacchetto

Nella seguente tabella vengono mostrati i file ZIP e i file XML corrispondenti per il PIP 3B14 Request Shipping Order Cancellation. Le mappe della direttiva comune a tutte le versioni vengono mostrate nella sezione successiva.

Tabella 59. File ZIP e XML di 3B14 Request Shipping Order Cancellation

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 Request Shipping Order Cancellation:

- 3B14\_ShippingOrderCancellationConfirmation\_V01.00.xsd
- 3B14\_ShippingOrderCancellationRequest\_V01.00.xsd
- BCG\_common.xsd
- BCG\_common\_V422.xsd
- BCG\_ContactInformation\_Types.xsd
- BCG\_GlobalDocumentReferenceTypeCode.xsd
- BCG\_GlobalOrderAdminCode\_V22.xsd
- BCG\_GlobalPartnerRoleClassificationCode.xsd
- BCG\_GlobalPartnerRoleClassificationCode\_V43.xsd
- BCG\_GlobalShippingOrderCancellationStatusReasonCode\_V43.xsd
- BCG\_PartnerDescription\_Types.xsd
- BCG\_PartnerDescription\_Types\_V43.xsd
- BCG\_string\_len\_0.xsd
- BCG\_xml.xsd

## 3B18 Notify of Shipping Documentation

Nella seguente sezione, viene descritto il contenuto del pacchetto PIP 3B18 Notify of Shipping Documentation.

### Contenuto del file del pacchetto

Nella seguente tabella vengono mostrati i file ZIP e i file XML corrispondenti per il PIP 3B18 Notify of Shipping Documentation. Le mappe della direttiva comune a tutte le versioni vengono mostrate nella sezione successiva.

Tabella 60. File ZIP e XML di 3B18 Notify of Shipping Documentation

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 Notify of Shipping Documentation:

- BCG\_3B18ShippingDocumentationNotification\_V01.00.xsd
- BCG\_BusinessDescription\_Types.xsd
- BCG\_BusinessDescription\_Types\_V422.xsd
- BCG\_common\_V422.xsd
- BCG\_ContactInformation\_Types.xsd
- BCG\_GlobalCountryCode.xsd
- BCG\_GlobalCurrencyCode.xsd
- BCG\_GlobalDocumentReferenceTypeCode.xsd
- BCG\_GlobalFreeOnBoardCode\_V422.xsd
- BCG\_GlobalFreightPaymentTermsCode\_V422.xsd
- BCG\_GlobalIncotermsCode.xsd
- BCG\_GlobalMonetaryAmountTypeCode.xsd
- BCG\_GlobalOrderAdminCode\_V422.xsd
- BCG\_GlobalPackageTypeCode\_V422.xsd
- BCG\_GlobalPartnerClassificationCode\_V422.xsd
- BCG\_GlobalPartnerRoleClassificationCode\_V422.xsd
- BCG\_GlobalPaymentTermsCode.xsd
- BCG\_GlobalPhysicalUnitOfMeasureCode\_V422.xsd
- BCG\_GlobalPortIdentifierAuthorityCode\_V422.xsd
- BCG\_GlobalPortTypeCode\_V422.xsd
- BCG\_GlobalProductUnitOfMeasureCode.xsd
- BCG\_GlobalShipDateCode.xsd
- BCG\_GlobalShipmentModeCode.xsd
- BCG\_GlobalShippingDocumentCode\_V422.xsd
- BCG\_GlobalShippingServiceLevelCode.xsd
- BCG\_GlobalSpecialHandlingCode\_V422.xsd
- BCG\_GlobalTrackingReferenceTypeCode.xsd
- BCG\_InvoiceChargeTypeCode\_V422.xsd
- BCG\_NationalExportControlClassificationCode.xsd
- BCG\_PhysicalAddress\_Types.xsd
- BCG\_string\_len\_0.xsd
- BCG\_xml.xsd

## 3C1 Return Product

Nella seguente sezione, viene descritto il contenuto del pacchetto PIP 3C1 Return Product.

### Contenuto del file del pacchetto

Nella seguente tabella vengono mostrati i file ZIP e i file XML corrispondenti per il PIP 3C1 Return Product. Le mappe della direttiva comune a tutte le versioni vengono mostrate nella sezione successiva.

Tabella 61. File ZIP e XML di 3C1 Return Product

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 Return Product:

- BCG\_3C1ReturnProductConfirmation\_V01.00.xsd
- BCG\_3C1ReturnProductRequest\_V01.00.xsd
- BCG\_BusinessDescription\_Types.xsd
- BCG\_BusinessDescription\_Types\_V43.xsd
- BCG\_common.xsd
- BCG\_common\_V42.xsd
- BCG\_common\_V43.xsd
- BCG\_ContactInformation\_Types.xsd
- BCG\_GlobalCurrencyCode.xsd
- BCG\_GlobalDocumentReferenceTypeCode.xsd
- BCG\_GlobalFailureTypeCode\_V43.xsd
- BCG\_GlobalPartnerClassificationCode\_V43.xsd
- BCG\_GlobalPartnerRoleClassificationCode\_V43.xsd
- BCG\_GlobalProductUnitOfMeasureCode\_V43.xsd
- BCG\_GlobalShippingServiceLevelCode.xsd
- BCG\_PartnerDescription\_Types.xsd
- BCG\_PartnerDescription\_Types\_V43.xsd
- BCG\_PhysicalAddress\_Types.xsd
- BCG\_string\_len\_0.xsd
- BCG\_xml.xsd

## 3C3 Notify of Invoice

Nella seguente sezione, viene descritto il contenuto del pacchetto PIP 3C3 Notify of Invoice.

### Contenuto del file del pacchetto

Nella seguente tabella vengono mostrati i file ZIP e i file XML corrispondenti per il PIP 3C3 Notify of Invoice. Le mappe della direttiva comune a tutte le versioni vengono mostrate nella sezione successiva.

Tabella 62. File ZIP e XML di 3C3 Notify of Invoice

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 Notify of Invoice:

- BCG\_3C3InvoiceNotification\_V01.01.xsd
- BCG\_BusinessDescription\_Types.xsd
- BCG\_BusinessTaxIdentifier\_Types.xsd
- BCG\_common.xsd
- BCG\_ContactInformation\_Types.xsd
- BCG\_GlobalCountryCode.xsd
- BCG\_GlobalCurrencyCode.xsd
- BCG\_GlobalDocumentTypeCode.xsd
- BCG\_GlobalMonetaryAmountTypeCode.xsd
- BCG\_GlobalPartnerClassificationCode.xsd
- BCG\_GlobalPartnerRoleClassificationCode.xsd
- BCG\_GlobalPaymentTermsCode.xsd
- BCG\_GlobalProductUnitOfMeasureCode.xsd
- BCG\_GlobalSaleTypeCode.xsd
- BCG\_GlobalShipmentTermsCode.xsd
- BCG\_GlobalShippingServiceLevelCode.xsd
- BCG\_GlobalSpecialHandlingCode.xsd
- BCG\_InvoiceChargeTypeCode.xsd
- BCG\_NationalExportControlClassificationCode.xsd
- BCG\_PartnerDescription\_Types.xsd
- BCG\_PhysicalAddress\_Types.xsd
- BCG\_string\_len\_0.xsd
- BCG\_xml.xsd

## 3C4 Notify of Invoice Reject

Nella seguente sezione, viene descritto il contenuto del pacchetto PIP 3C4 Notify of Invoice Reject.

### Contenuto del file del pacchetto

Nella seguente tabella vengono mostrati i file ZIP e i file XML corrispondenti per il PIP 3C4 Notify of Invoice Reject. Le mappe della direttiva comune a tutte le versioni vengono mostrate nella sezione successiva.

Tabella 63. File ZIP e XML di 3C4 Notify of Invoice Reject

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 Notify of Invoice Reject:

- BCG\_3C4InvoiceRejectNotification\_V01.00.xsd

- BCG\_BusinessDescription\_Types.xsd
- BCG\_BusinessTaxIdentifier\_Types.xsd
- BCG\_common.xsd
- BCG\_ContactInformation\_Types.xsd
- BCG\_GlobalCountryCode.xsd
- BCG\_GlobalInvoiceRejectionCode.xsd
- BCG\_GlobalMonetaryAmountTypeCode.xsd
- BCG\_GlobalPartnerClassificationCode.xsd
- BCG\_PartnerDescription\_Types.xsd
- BCG\_PhysicalAddress\_Types.xsd
- BCG\_string\_len\_0.xsd
- BCG\_xml.xsd

### 3C6 Notify of Remittance Advice

Nella seguente sezione, viene descritto il contenuto del pacchetto PIP 3C6 Notify of Remittance Advice.

#### Contenuto del file del pacchetto

Nella seguente tabella vengono mostrati i file ZIP e i file XML corrispondenti per il PIP 3C6 Notify of Remittance Advice. Le mappe della direttiva comune a tutte le versioni vengono mostrate nella sezione successiva.

Tabella 64. File ZIP e XML di 3C6 Notify of Remittance Advice

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
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 Notify of Remittance Advice:

- BCG\_3C6RemittanceAdviceNotification\_V01.00.xsd
- BCG\_BusinessDescription\_Types.xsd
- BCG\_BusinessTaxIdentifier\_Types.xsd
- BCG\_common.xsd
- BCG\_ContactInformation\_Types.xsd
- BCG\_GlobalCountryCode.xsd
- BCG\_GlobalCurrencyCode.xsd
- BCG\_GlobalDocumentTypeCode.xsd
- BCG\_GlobalFinancialAdjustmentReasonCode.xsd
- BCG\_GlobalInvoiceRejectionCode.xsd
- BCG\_GlobalMonetaryAmountTypeCode.xsd
- BCG\_GlobalPartnerClassificationCode.xsd
- BCG\_GlobalPaymentMethodCode.xsd
- BCG\_PartnerDescription\_Types.xsd
- BCG\_PhysicalAddress\_Types.xsd

- BCG\_string\_len\_0.xsd
- BCG\_xml.xsd

## 3C7 Notify of Self-Billing Invoice

Nella seguente sezione, viene descritto il contenuto del pacchetto PIP 3C7 Notify of Self-Billing Invoice.

### Contenuto del file del pacchetto

Nella seguente tabella vengono mostrati i file ZIP e i file XML corrispondenti per il PIP 3C7 Notify of Self-Billing Invoice. Le mappe della direttiva comune a tutte le versioni vengono mostrate nella sezione successiva.

Tabella 65. File ZIP e XML di 3C7 Notify of Self-Billing Invoice

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 Notify of Self-Billing Invoice:

- BCG\_3C7SelfBillingInvoiceNotification\_V01.00.xsd
- BCG\_BusinessDescription\_Types.xsd
- BCG\_BusinessDescription\_Types\_V422.xsd
- BCG\_BusinessTaxIdentifier\_Types.xsd
- BCG\_common.xsd
- BCG\_common\_V422.xsd
- BCG\_ContactInformation\_Types.xsd
- BCG\_GlobalCountryCode.xsd
- BCG\_GlobalCurrencyCode.xsd
- BCG\_GlobalDocumentReferenceTypeCode.xsd
- BCG\_GlobalDocumentTypeCode.xsd
- BCG\_GlobalDocumentTypeCode\_V422.xsd
- BCG\_GlobalMonetaryAmountTypeCode.xsd
- BCG\_GlobalPartnerClassificationCode.xsd
- BCG\_GlobalPartnerRoleClassificationCode.xsd
- BCG\_GlobalPaymentTermsCode.xsd
- BCG\_GlobalProductUnitOfMeasureCode.xsd
- BCG\_GlobalSaleTypeCode.xsd
- BCG\_GlobalShipmentTermsCode.xsd
- BCG\_GlobalShippingServiceLevelCode.xsd
- BCG\_InvoiceChargeTypeCode.xsd
- BCG\_NationalExportControlClassificationCode.xsd
- BCG\_PartnerDescription\_Types.xsd
- BCG\_PhysicalAddress\_Types.xsd
- BCG\_string\_len\_0.xsd

- BCG\_xml.xsd

## 3D8 Distribute Work in Process

Nella seguente sezione, viene descritto il contenuto del pacchetto PIP 3D8 Distribute Work in Process.

### Contenuto del file del pacchetto

Nella seguente tabella vengono mostrati i file ZIP e i file XML corrispondenti per il PIP 3D8 Distribute Work in Process. Le mappe della direttiva comune a tutte le versioni vengono mostrate nella sezione successiva.

Tabella 66. File ZIP e XML di 3D8 Distribute Work in Process

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 Distribute Work in Process:

- BCG\_3D8WorkInProgressNotification\_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\_GlobalWorkInProgressLocationCode.xsd
- BCG\_GlobalWorkInProgressPartTypeCode.xsd
- BCG\_PartnerDescription\_Types.xsd
- BCG\_PhysicalAddress\_Types.xsd
- BCG\_string\_len\_0.xsd
- BCG\_xml.xsd

## 4A1 Notify of Strategic Forecast

Nella seguente sezione, viene descritto il contenuto del pacchetto PIP 4A1 Notify of Strategic Forecast.

## Contenuto del file del pacchetto

Nella seguente tabella vengono mostrati i file ZIP e i file XML corrispondenti per il PIP 4A1 Notify of Strategic Forecast. Le mappe della direttiva comune a tutte le versioni vengono mostrate nella sezione successiva.

Tabella 67. File ZIP E XML di 4A1 Notify of Strategic Forecast

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 Notify of Strategic Forecast:

- BCG\_4A1StrategicForecastNotification\_V02.00.xsd
- BCG\_BusinessDescription\_Types.xsd
- BCG\_BusinessTaxIdentifier\_Types.xsd
- BCG\_common.xsd
- BCG\_ContactInformation\_Types.xsd
- BCG\_GlobalCountryCode.xsd
- BCG\_GlobalCurrencyCode.xsd
- BCG\_GlobalForecastEventCode.xsd
- BCG\_GlobalForecastIntervalCode.xsd
- BCG\_GlobalForecastTypeCode.xsd
- BCG\_GlobalPartnerClassificationCode.xsd
- BCG\_GlobalPartnerReferenceTypeCode.xsd
- BCG\_GlobalProductUnitOfMeasureCode.xsd
- BCG\_PartnerDescription\_Types.xsd
- BCG\_PhysicalAddress\_Types.xsd
- BCG\_StrategicForecastQuantityTypeCode.xsd
- BCG\_string\_len\_0.xsd
- BCG\_xml.xsd

## 4A3 Notify of Threshold Release Forecast

Nella seguente sezione, viene descritto il contenuto del pacchetto PIP 4A3 Notify of Threshold Release Forecast.

### Contenuto del file del pacchetto

Nella seguente tabella vengono mostrati i file ZIP e i file XML corrispondenti per il PIP 4A3 Notify of Threshold Release Forecast. Le mappe della direttiva comune a tutte le versioni vengono mostrate nella sezione successiva.

Tabella 68. File ZIP e XML di 4A3 Notify of Threshold Release Forecast

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

Tabella 68. File ZIP e XML di 4A3 Notify of Threshold Release Forecast (Continua)

Nome file ZIP	Nome file 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 Notify of Threshold Release Forecast:

- BCG\_4A3ThresholdReleaseForecastNotification\_V02.00.xsd
- BCG\_BusinessDescription\_Types.xsd
- BCG\_BusinessTaxIdentifier\_Types.xsd
- BCG\_common.xsd
- BCG\_ContactInformation\_Types.xsd
- BCG\_GlobalCountryCode.xsd
- BCG\_GlobalCurrencyCode.xsd
- BCG\_GlobalForecastEventCode.xsd
- BCG\_GlobalForecastIntervalCode.xsd
- BCG\_GlobalForecastInventoryTypeCode.xsd
- BCG\_GlobalForecastReferenceTypeCode.xsd
- BCG\_GlobalPartnerClassificationCode.xsd
- BCG\_GlobalPartnerReferenceTypeCode.xsd
- BCG\_GlobalProductUnitOfMeasureCode.xsd
- BCG\_OrderForecastQuantityTypeCode.xsd
- BCG\_PartnerDescription\_Types.xsd
- BCG\_PhysicalAddress\_Types.xsd
- BCG\_string\_len\_0.xsd
- BCG\_xml.xsd

## 4A4 Notify of Planning Release Forecast

Nella seguente sezione, viene descritto il contenuto del pacchetto PIP 4A4 Notify of Planning Release Forecast.

### Contenuto del file del pacchetto

Nella seguente tabella vengono mostrati i file ZIP e i file XML corrispondenti per il PIP 4A4 Notify of Planning Release Forecast. PIP. Le mappe della direttiva comune a tutte le versioni vengono mostrate nella sezione successiva.

Tabella 69. File ZIP e XML di 4A4 Notify of Planning Release Forecast

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 Notify of Planning Release Forecast:

- BCG\_4A4PlanningReleaseForecastNotification\_R02.00A.xsd

- BCG\_BusinessDescription\_Types.xsd
- BCG\_BusinessTaxIdentifier\_Types.xsd
- BCG\_common.xsd
- BCG\_ContactInformation\_Types.xsd
- BCG\_GlobalCountryCode.xsd
- BCG\_GlobalCurrencyCode.xsd
- BCG\_GlobalForecastInventoryTypeCode.xsd
- BCG\_GlobalForecastQuantityTypeCode\_V422.xsd
- BCG\_GlobalForecastReferenceTypeCode.xsd
- BCG\_GlobalIntervalCode.xsd
- BCG\_GlobalPartnerClassificationCode.xsd
- BCG\_GlobalPartnerReferenceTypeCode.xsd
- BCG\_GlobalProductUnitOfMeasureCode.xsd
- BCG\_GlobalTransportEventCode.xsd
- BCG\_PartnerDescription\_Types.xsd
- BCG\_PhysicalAddress\_Types.xsd
- BCG\_PhysicalAddress\_Types\_V422.xsd
- BCG\_string\_len\_0.xsd
- BCG\_xml.xsd

## 4A5 Notify of Forecast Reply

Nella seguente sezione, viene descritto il contenuto del pacchetto PIP 4A5 Notify of Forecast Reply.

### Contenuto del file del pacchetto

Nella seguente tabella vengono mostrati i file ZIP e i file XML corrispondenti per il PIP 4A5 Notify of Forecast Reply. Le mappe della direttiva comune a tutte le versioni vengono mostrate nella sezione successiva.

Tabella 70. File ZIP e XML di 4A5 Notify of Forecast Reply

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 Notify of Forecast Reply:

- BCG\_4A5ForecastReplyNotification\_V02.00.xsd
- BCG\_BusinessDescription\_Types.xsd
- BCG\_BusinessTaxIdentifier\_Types.xsd
- BCG\_common.xsd
- BCG\_ContactInformation\_Types.xsd
- BCG\_ForecastReplyQuantityTypeCode.xsd
- BCG\_GlobalCountryCode.xsd
- BCG\_GlobalCurrencyCode.xsd

- BCG\_GlobalForecastEventCode.xsd
- BCG\_GlobalForecastIntervalCode.xsd
- BCG\_GlobalForecastInventoryTypeCode.xsd
- BCG\_GlobalForecastReferenceTypeCode.xsd
- BCG\_GlobalForecastResponseCode.xsd
- BCG\_GlobalForecastRevisionReasonCode.xsd
- BCG\_GlobalPartnerClassificationCode.xsd
- BCG\_GlobalPartnerReferenceTypeCode.xsd
- BCG\_GlobalProductUnitOfMeasureCode.xsd
- BCG\_PartnerDescription\_Types.xsd
- BCG\_PhysicalAddress\_Types.xsd
- BCG\_string\_len\_0.xsd
- BCG\_xml.xsd

## 4B2 Notify of Shipment Receipt

Nella seguente sezione, viene descritto il contenuto del pacchetto PIP 4B2 Notify of Shipment Receipt.

### Contenuto del file del pacchetto

Nella seguente tabella vengono mostrati i file ZIP e i file XML corrispondenti per il PIP 4B2 Notify of Shipment Receipt. Le mappe della direttiva comune a tutte le versioni vengono mostrate nella sezione successiva.

Tabella 71. File ZIP e XML di 4B2 Notify of Shipment Receipt

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 Notify of Shipment Receipt:

- BCG\_4B2ShipmentReceiptNotification\_V01.00.xsd
- BCG\_BusinessDescription\_Types.xsd
- BCG\_BusinessTaxIdentifier\_Types.xsd
- BCG\_common.xsd
- BCG\_ContactInformation\_Types.xsd
- BCG\_GlobalCountryCode.xsd
- BCG\_GlobalDocumentReferenceTypeCode.xsd
- BCG\_GlobalLotDiscrepancyReasonCode.xsd
- BCG\_GlobalPartnerClassificationCode.xsd
- BCG\_GlobalPartnerRoleClassificationCode.xsd
- BCG\_GlobalProductUnitOfMeasureCode.xsd
- BCG\_GlobalReceivingDiscrepancyCode.xsd
- BCG\_GlobalReceivingDiscrepancyReasonCode.xsd
- BCG\_GlobalSpecialFulfillmentRequestCode.xsd

- BCG\_GlobalSpecialHandlingCode.xsd
- BCG\_GlobalTrackingReferenceTypeCode.xsd
- BCG\_PartnerDescription\_Types.xsd
- BCG\_PhysicalAddress\_Types.xsd
- BCG\_string\_len\_0.xsd
- BCG\_xml.xsd

## 4B3 Notify of Consumption

Nella seguente sezione, viene descritto il contenuto del pacchetto PIP 4B3 Notify of Consumption.

### Contenuto del file del pacchetto

Nella seguente tabella vengono mostrati i file ZIP e i file XML corrispondenti per il PIP 4B3 Notify of Consumption. Le mappe della direttiva comune a tutte le versioni vengono mostrate nella sezione successiva.

Tabella 72. File ZIP e XML di 4B3 Notify of Consumption

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 Notify of Consumption:

- BCG\_4B3ConsumptionNotification\_V01.00.xsd
- BCG\_BusinessDescription\_Types.xsd
- BCG\_BusinessDescription\_Types\_V422.xsd
- BCG\_BusinessDescription\_Types\_V43.xsd
- BCG\_BusinessTaxIdentifier\_Types.xsd
- BCG\_common.xsd
- BCG\_common\_V43.xsd
- BCG\_ContactInformation\_Types.xsd
- BCG\_ContactInformation\_Types\_V422.xsd
- BCG\_ContactInformation\_Types\_V43.xsd
- BCG\_GlobalCountryCode.xsd
- BCG\_GlobalCurrencyCode.xsd
- BCG\_GlobalDocumentReferenceTypeCode\_V43.xsd
- BCG\_GlobalInventoryCode\_V43.xsd
- BCG\_GlobalPartnerClassificationCode\_V422.xsd
- BCG\_GlobalPartnerClassificationCode\_V43.xsd
- BCG\_GlobalProductUnitOfMeasureCode.xsd
- BCG\_PartnerDescription\_Types\_V43.xsd
- BCG\_PhysicalAddress\_Types.xsd
- BCG\_string\_len\_0.xsd
- BCG\_xml.xsd

## 4C1 Distribute Inventory Report V02.01

Nella seguente sezione, viene descritto il contenuto del pacchetto PIP 4C1 Distribute Inventory Report V02.01.

### Contenuto del file del pacchetto

Nella seguente tabella vengono mostrati i file ZIP e i file XML corrispondenti per il PIP 4C1 Distribute Inventory Report. Le mappe della direttiva comune a tutte le versioni vengono mostrate nella sezione successiva.

Tabella 73. File ZIP e XML di 4C1 Distribute Inventory Report

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 Distribute Inventory Report:

- BCG\_4C1InventoryReportNotification\_V02.01.xsd
- BCG\_BusinessDescription\_Types.xsd
- BCG\_BusinessTaxIdentifier\_Types.xsd
- BCG\_common.xsd
- BCG\_common\_V422.xsd
- BCG\_ContactInformation\_Types.xsd
- BCG\_ContactInformation\_Types\_V422.xsd
- BCG\_GlobalCountryCode.xsd
- BCG\_GlobalDocumentReferenceTypeCode.xsd
- BCG\_GlobalInventoryCode.xsd
- BCG\_GlobalPartnerClassificationCode.xsd
- BCG\_GlobalPartnerRoleClassificationCode.xsd
- BCG\_GlobalProductUnitOfMeasureCode.xsd
- BCG\_PhysicalAddress\_Types.xsd
- BCG\_PhysicalAddress\_Types\_V422.xsd
- BCG\_string\_len\_0.xsd
- BCG\_xml.xsd

## 4C1 Distribute Inventory Report V02.03

Nella seguente sezione, viene descritto il contenuto del pacchetto PIP 4C1 Distribute Inventory Report V02.03.

### Contenuto del file del pacchetto

Nella seguente tabella vengono mostrati i file ZIP e i file XML corrispondenti per il PIP 4C1 Distribute Inventory Report. Le mappe della direttiva comune a tutte le versioni vengono mostrate nella sezione successiva.

Tabella 74. File ZIP e XML di 4C1 Distribute Inventory Report

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 Distribute Inventory Report:

- BCG\_4C1InventoryReportNotification\_V02.03.xsd
- BCG\_BusinessDescription\_Types.xsd
- BCG\_BusinessTaxIdentifier\_Types.xsd
- BCG\_common.xsd
- BCG\_ContactInformation\_Types.xsd
- BCG\_GlobalCountryCode.xsd
- BCG\_GlobalDocumentReferenceTypeCode.xsd
- BCG\_GlobalInventoryCode.xsd
- BCG\_GlobalPartnerClassificationCode.xsd
- BCG\_GlobalPartnerRoleClassificationCode.xsd
- BCG\_GlobalProductUnitOfMeasureCode.xsd
- BCG\_PhysicalAddress\_Types.xsd
- BCG\_string\_len\_0.xsd
- BCG\_xml.xsd

## 5C1 Distribute Product List

Nella seguente sezione, viene descritto il contenuto del pacchetto PIP 5C1 Distribute Product List.

### Contenuto del file del pacchetto

Nella seguente tabella vengono mostrati i file ZIP e i file XML corrispondenti per il PIP 5C1 Distribute Product List. Le mappe della direttiva comune a tutte le versioni vengono mostrate nella sezione successiva.

Tabella 75. File ZIP e XML di 5C1 Distribute Product List

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 Distribute Product List:

- BCG\_5C1ProductListNotification\_V01.00.xsd
- BCG\_BusinessDescription\_Types.xsd
- BCG\_BusinessTaxIdentifier\_Types.xsd

- BCG\_common.xsd
- BCG\_ContactInformation\_Types.xsd
- BCG\_GlobalCountryCode.xsd
- BCG\_GlobalCurrencyCode.xsd
- BCG\_GlobalPartnerClassificationCode.xsd
- BCG\_GlobalPartnerRoleClassificationCode.xsd
- BCG\_GlobalPriceTypeCode.xsd
- BCG\_PartnerDescription\_Types.xsd
- BCG\_PhysicalAddress\_Types.xsd
- BCG\_string\_len\_0.xsd
- BCG\_xml.xsd

## 5C2 Request Design Registration

Nella seguente sezione, viene descritto il contenuto del pacchetto PIP 5C2 Request Design Registration.

### Contenuto del file del pacchetto

Nella seguente tabella vengono mostrati i file ZIP e i file XML corrispondenti per il PIP 5C2 Request Design Registration. Le mappe della direttiva comune a tutte le versioni vengono mostrate nella sezione successiva.

Tabella 76. File ZIP e XML di 5C2 Request Design Registration

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 Request Design Registration:

- BCG\_5C2DesignRegistrationConfirmation\_V01.00.xsd
- BCG\_5C2DesignRegistrationRequest\_V01.00.xsd
- BCG\_BusinessDescription\_Types.xsd
- BCG\_common.xsd
- BCG\_common\_V422.xsd
- BCG\_common\_V43.xsd
- BCG\_ContactInformation\_Types.xsd
- BCG\_DesignWinStatusReasonCode\_V43.xsd
- BCG\_GlobalAttachmentDescriptionCode\_V422.xsd
- BCG\_GlobalCountryCode.xsd
- BCG\_GlobalCurrencyCode.xsd
- BCG\_GlobalDocumentReferenceTypeCode.xsd
- BCG\_GlobalMimeTypeQualifierCode\_V43.xsd
- BCG\_GlobalMonetaryAmountTypeCode.xsd
- BCG\_GlobalPartnerClassificationCode\_V43.xsd
- BCG\_GlobalPartnerRoleClassificationCode\_V43.xsd

- BCG\_GlobalPriceTypeCode\_V43.xsd
- BCG\_GlobalRegistrationComplexityLevelCode.xsd
- BCG\_GlobalRegistrationInvolvementLevelCode.xsd
- BCG\_InvoiceChargeTypeCode\_V422.xsd
- BCG\_PartnerDescription\_Types.xsd
- BCG\_PartnerDescription\_Types\_V43.xsd
- BCG\_PhysicalAddress\_Types.xsd
- BCG\_string\_len\_0.xsd
- BCG\_xml.xsd

## 5C4 Distribute Registration Status

Nella seguente sezione, viene descritto il contenuto del pacchetto PIP 5C4 Distribute Registration Status.

### Contenuto del file del pacchetto

Nella seguente tabella vengono mostrati i file ZIP e i file XML corrispondenti per il PIP 5C4 Distribute Registration Status. Le mappe della direttiva comune a tutte le versioni vengono mostrate nella sezione successiva.

Tabella 77. File ZIP e XML di 5C4 Distribute Registration Status

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 Distribute Registration Status:

- BCG\_5C4RegistrationStatusNotification\_V01.02.xsd
- BCG\_BusinessDescription\_Types.xsd
- BCG\_BusinessTaxIdentifier\_Types.xsd
- BCG\_common.xsd
- BCG\_ContactInformation\_Types.xsd
- BCG\_GlobalCountryCode.xsd
- BCG\_GlobalPartnerClassificationCode.xsd
- BCG\_GlobalPartnerRoleClassificationCode.xsd
- BCG\_GlobalRegistrationComplexityLevelCode.xsd
- BCG\_GlobalRegistrationInvolvementLevelCode.xsd
- BCG\_PartnerDescription\_Types.xsd
- BCG\_PhysicalAddress\_Types.xsd
- BCG\_string\_len\_0.xsd
- BCG\_xml.xsd

## 5D1 Request Ship From Stock And Debit Authorization

Nella seguente sezione, viene descritto il contenuto del pacchetto PIP 5D1 Request Ship From Stock And Debit Authorization.

## Contenuto del file del pacchetto

Nella seguente tabella vengono mostrati i file ZIP e i file XML corrispondenti per il PIP 5D1 Request Ship From Stock And Debit Authorization. Le mappe della direttiva comune a tutte le versioni vengono mostrate nella sezione successiva.

Tabella 78. File ZIP e XML di 5D1 Request Ship from Stock and Debit Authorization

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 pacchetto PIP 5D1 Request Ship From Stock And Debit Authorization:

- BCG\_5D1ShipFromStockAndDebitAuthorizationConfirmation\_V01.00.xsd
- BCG\_5D1ShipFromStockAndDebitAuthorizationRequest\_V01.00.xsd
- BCG\_BusinessDescription\_Types.xsd
- BCG\_BusinessTaxIdentifier\_Types.xsd
- BCG\_common.xsd
- BCG\_ContactInformation\_Types.xsd
- BCG\_GlobalCountryCode.xsd
- BCG\_GlobalCurrencyCode.xsd
- BCG\_GlobalDocumentReferenceTypeCode.xsd
- BCG\_GlobalPartnerClassificationCode.xsd
- BCG\_GlobalPartnerRoleClassificationCode.xsd
- BCG\_GlobalPriceTypeCode.xsd
- BCG\_GlobalProductUnitOfMeasureCode.xsd
- BCG\_GlobalShipFromStockAndDebitAuthorizationRejectionCode.xsd
- BCG\_PartnerDescription\_Types.xsd
- BCG\_PhysicalAddress\_Types.xsd
- BCG\_string\_len\_0.xsd
- BCG\_xml.xsd

## 6C1 Query Service Entitlement

Nella seguente sezione, viene descritto il contenuto del pacchetto PIP 6C1 Query Service Entitlement.

### Contenuto del file del pacchetto

Nella seguente tabella vengono mostrati i file ZIP e i file XML corrispondenti per il PIP 6C1 Query Service Entitlement. Le mappe della direttiva comune a tutte le versioni vengono mostrate nella sezione successiva.

Tabella 79. File ZIP e XML di 6C1 Query Service Entitlement

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

Tabella 79. File ZIP e XML di 6C1 Query Service Entitlement (Continua)

Nome file ZIP	Nome file 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 Service Entitlement:

- BCG\_6C1ServiceEntitlementQuery\_V01.00.xsd
- BCG\_6C1ServiceEntitlementStatusResponse\_V01.00.xsd
- BCG\_common\_V43.xsd
- BCG\_ContactInformation\_Types.xsd
- BCG\_ContactInformation\_Types\_V43.xsd
- BCG\_GlobalCurrencyCode.xsd
- BCG\_GlobalNotificationCode\_V43.xsd
- BCG\_GlobalPartnerClassificationCode\_V43.xsd
- BCG\_GlobalPaymentTypeCode\_V43.xsd
- BCG\_GlobalServiceDeliveryMethodCode\_V43.xsd
- BCG\_GlobalShippingServiceLevelCode.xsd
- BCG\_GlobalWarrantyMethodCode\_V43.xsd
- BCG\_GlobalWarrantyProgramCode\_V43.xsd
- BCG\_GlobalWarrantyTypeCode\_V43.xsd
- BCG\_PartnerDescription\_Types\_V43.xsd
- BCG\_string\_len\_0.xsd
- BCG\_xml.xsd

## 6C2 Request Warranty Claim

Nella seguente sezione, viene descritto il contenuto del pacchetto PIP 6C2 Request Warranty Claim.

### Contenuto del file del pacchetto

Nella seguente tabella vengono mostrati i file ZIP e i file XML corrispondenti per il PIP 6C2 Request Warranty Claim. Le mappe della direttiva comune a tutte le versioni vengono mostrate nella sezione successiva.

Tabella 80. File ZIP e XML di 6C2 Request Warranty Claim

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 Request Warranty Claim:

- BCG\_6C2WarrantyClaimConfirmation\_V01.00.xsd
- BCG\_6CWarrantyClaimRequest\_V01.00.xsd
- BCG\_common.xsd

- BCG\_ContactInformation\_Types.xsd
- BCG\_GlobalCurrencyCode.xsd
- BCG\_GlobalDocumentReferenceTypeCode.xsd
- BCG\_GlobalFailureTypeCode\_V43.xsd
- BCG\_GlobalOperatingSystemCode\_V43.xsd
- BCG\_GlobalPartnerClassificationCode\_V43.xsd
- BCG\_GlobalPartnerRoleClassificationCode\_V43.xsd
- BCG\_GlobalPaymentTypeCode\_V43.xsd
- BCG\_GlobalServiceDeliveryMethodCode\_V43.xsd
- BCG\_GlobalWarrantyTypeCode\_V43.xsd
- BCG\_PartnerDescription\_Types\_V43.xsd
- BCG\_string\_len\_0.xsd
- BCG\_xml.xsd

## 7B1 Distribute Work in Process

Nella seguente sezione, viene descritto il contenuto del pacchetto PIP 7B1 Distribute Work in Process.

### Contenuto del file del pacchetto

Nella seguente tabella vengono mostrati i file ZIP e i file XML corrispondenti per il PIP 7B1 Distribute Work in Process. Le mappe della direttiva comune a tutte le versioni vengono mostrate nella sezione successiva.

Tabella 81. File ZIP e XML di 7B1 Distribute Work in Process

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 Distribute Work in Process:

- BCG\_7B1WorkInProgressNotification\_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\_GlobalWorkInProgressLocationCode.xsd
- BCG\_GlobalWorkInProgressPartTypeCode.xsd
- BCG\_GlobalWorkInProgressQuantityChangeCode.xsd
- BCG\_GlobalWorkInProgressTypeCode.xsd
- BCG\_PartnerDescription\_Types.xsd
- BCG\_PhysicalAddress\_Types.xsd
- BCG\_string\_len\_0.xsd
- BCG\_xml.xsd

## 7B5 Notify Of Manufacturing Work Order

Nella seguente sezione, viene descritto il contenuto del pacchetto PIP 7B5 Notify Of Manufacturing Work Order.

### Contenuto del file del pacchetto

Nella seguente tabella vengono mostrati i file ZIP e i file XML corrispondenti per il PIP 7B5 Notify Of Manufacturing Work Order. Le mappe della direttiva comune a tutte le versioni vengono mostrate nella sezione successiva.

Tabella 82. File ZIP e XML di 7B5 Notify of Manufacturing Work Order

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 Notify Of Manufacturing Work Order:

- 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\_GlobalWorkInProgressLocationCode.xsd
- BCG\_PartnerDescription\_Types.xsd
- BCG\_PhysicalAddress\_Types.xsd
- BCG\_string\_len\_0.xsd
- BCG\_xml.xsd

## 7B6 Notify Of Manufacturing Work Order Reply

Nella seguente sezione, viene descritto il contenuto del pacchetto PIP 7B6 Notify Of Manufacturing Work Order Reply.

### Contenuto del file del pacchetto

Nella seguente tabella vengono mostrati i file ZIP e i file XML corrispondenti per il PIP 7B6 Notify Of Manufacturing Work Order Reply. Le mappe della direttiva comune a tutte le versioni vengono mostrate nella sezione successiva.

Tabella 83. File ZIP e XML di 7B6 Notify of Manufacturing Work Order Reply

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 Notify Of Manufacturing Work Order Reply:

- 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

---

## Appendice D. Attributi

Questa appendice descrive gli attributi che è possibile impostare dalla Console comunità. Tali attributi sono riportati di seguito:

- “Attributi EDI”
- “Attributi AS” a pagina 293
- “Attributi RosettaNet” a pagina 296
- “Attributo integrazione di backend” a pagina 298

---

### Attributi EDI

Questa sezione contiene una descrizione degli attributi EDI che è possibile utilizzare durante l'impostazione degli scambi EDI. Alcuni di questi attributi vengono definiti in precedenza nella stringa di controllo che rappresenta la mappa di trasformazione associata al documento EDI. I valori impostati nella stringa di controllo (sul client Data Interchange Services) sostituiscono quelli immessi sulla Console comunità.

#### attributi profilo busta

È possibile impostare vari attributi per un profilo della busta EDI. Gli attributi disponibili dipendono al tipo EDI. In generale, gli attributi corrispondono ad uno standard EDI ed i valori consentiti dipendono dal profilo della busta EDI standard che rappresentano.

Nessuno degli attributi richiede un valore. Per alcuni di essi, viene utilizzato un valore predefinito, se non viene immesso alcun valore. Nelle tabelle contenute in questa sezione vengono elencati gli attributi con i valori predefiniti associati.

**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 valori predefiniti.

**Attributi generali:** In Tabella 84 sono elencati gli attributi generali per i quali vengono forniti valori predefiniti.

Tabella 84. Attributi generali

Nome campo	Necessario?	Descrizione	Predefinito
INTCTLEN (Lunghezza numero di controllo scambio)	No	Definisce una lunghezza specifica per il numero di controllo dello scambio. Se si immette un valore, deve essere un intero.  In caso contrario, viene utilizzata la lunghezza predefinita.	9

Tabella 84. Attributi generali (Continua)

Nome campo	Necessario?	Descrizione	Predefinito
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.	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 in base a ID transazione)	No	Si 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 scambio:** Non viene richiesto alcun attributo X12 e gli attributi non hanno valori predefiniti.

**Attributi gruppo:** In Tabella 85 vengono elencati gli attributi del gruppo per i quali vengono forniti valori predefiniti.

Tabella 85. Attributi gruppo

Nome campo	Necessario?	Descrizione	Predefinito
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 UCS

In questa sezione, viene descritto se i valori predefiniti vengono applicati ad uno scambio, gruppo e transazione UCS.

**Attributi generali:** In Tabella 86 a pagina 283 sono elencati gli attributi generali per i quali vengono forniti valori predefiniti.

Tabella 86. Attributi generali

Nome campo	Necessario?	Descrizione	Predefinito
INTCTLLEN (Lunghezza numero di controllo scambio)	No	Definisce una lunghezza specifica per il numero di controllo dello 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 del 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 in base a ID transazione)	No	Si 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 scambio:** Non viene richiesto alcun attributo dello scambio. Gli attributi non hanno valori predefiniti.

**Attributi gruppo:** In Tabella 87 vengono elencati gli attributi del gruppo per i quali vengono forniti valori predefiniti.

Tabella 87. Attributi gruppo

Nome campo	Necessario?	Descrizione	Predefinito
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 88 sono elencati gli attributi generali per i quali vengono forniti valori predefiniti.

Tabella 88. Attributi generali

Nome campo	Necessario?	Descrizione	Predefinito
INTCTLLEN (Lunghezza numero di controllo scambio)	No	Definisce una lunghezza specifica per il numero di controllo dello 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).  Si indica che è necessario creare i gruppi funzionali (segmenti UNG/UNE) per EDIFACT DATA.  No indica il contrario.	No
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 in base a ID transazione)	No	Si 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 scambio:** Non viene richiesto alcun attributo dello scambio. Gli attributi non hanno valori predefiniti.

**Attributi gruppo:** In Tabella 89 vengono elencati gli attributi del gruppo per i quali vengono forniti valori predefiniti.

Tabella 89. Attributi gruppo

Nome campo	Necessario?	Descrizione	Predefinito
UNG01 (ID gruppo funzionale)	No	Identificativo del gruppo.	Il valore predefinito deriva dall'instestazione 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 90 sono elencati gli attributi del messaggio per i quali vengono forniti valori predefiniti.

Tabella 90. Attributi messaggio

Nome campo	Necessario?	Descrizione	Predefinito
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 (Rilascio messaggio)	No	Rilascio del messaggio.	Per valore standard
UNH0204 (Agenzia controllo)	No	Codice che identifica un'agenzia di controllo.	UN

## Attributi definizione flusso di documenti e connessione

In questa sezione, vengono elencati gli attributi della definizione del flusso di documenti per una busta. Alcuni di questi attributi possono essere impostati solo a livello di protocollo o connessione, come indicato.

### Attributi separatore e delimitatore

In questa sezione, vengono elencati i caratteri utilizzati come delimitatori o separatori in uno scambio EDI. In Tabella 91 viene mostrato l'attributo come appare sulla Console comunità, il termine corrispondente in X12 e EDIFACT (ISO 9735 Versione 4, Rilascio 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 91.

**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 91. Attributi profilo busta

Attributo	Termine X12	Termine EDIFACT	Descrizione
delimitatore segmento	terminazione segmento	terminazione segmento	<p>Si tratta di un carattere singolo, che appare sull'ultimo carattere di un segmento. Il carattere può essere un valore esadecimale.</p> <p>Il valore predefinito si basa sul tipo EDI.</p> <p><b>X12</b> ~ (tilde)</p> <p><b>EDIFACT</b> ' (apici)</p> <p><b>UCS</b> ~ (tilde)</p>

Tabella 91. Attributi profilo busta (Continua)

Attributo	Termine X12	Termine EDIFACT	Descrizione
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. <b>X12</b> * (asterisco) <b>EDIFACT</b> + (segno più) <b>UCS</b> * (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. <b>X12</b> \ (barra inversa) <b>EDIFACT</b> : (due punti) <b>UCS</b> \ (barra inversa)
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. <b>EDIFACT</b> ? (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. <b>X12</b> ^ (accento circonflesso) <b>EDIFACT</b> * (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 91 a pagina 285 vengono utilizzati in uno scambio.

Un messaggio EDI consiste di una serie di segmenti secondo un ordine particolare. Un 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 il delimitatore del segmento.

### Attributi EDI aggiuntivi

In questa sezione, vengono elencati gli attributi EDI che è possibile impostare sul livello della definizione di flusso di documenti o a livello di connessione.

Tabella 92. Attributi EDI aggiuntivi

Attributo	Necessario	Descrizione	Limitazioni	Predefinito
Output segmento	No	Utilizzato nella trasformazione 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

Tabella 92. Attributi EDI aggiuntivi (Continua)

Attributo	Necessario	Descrizione	Limitazioni	Predefinito
Consenti documenti con ID documento duplicati	No	<p>Si indica che gli ID del documento duplicato (numeri di controllo dello scambio) sono consentiti.</p> <p>No indica che i numeri di controllo dello scambio duplicato devono essere considerati come un errore.</p>	Limitato al protocollo o alla connessione	No
Livello max errore su trasformazione	No	<p>Indica il numero massimo di errori che possono verificarsi durante una trasformazione prima che questa non riesca.</p> <p>I valori validi sono 0, 1 o 2.</p> <p>Se la mappa di trasformazione 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 trasformazione non riesce.</p>	Limitato al protocollo o alla connessione	0
Mappa FA	No	<p>Fornisce la mappa da utilizzare per la conversione del valore FA generico interno in quello specifico.</p> <p><b>Nota:</b> Selezionare questo attributo da un elenco di mappe identificato come mappe FA (tipo di mappa "K").</p>	Limitato al protocollo o alla connessione	
Profilo busta	Sì	Nome del profilo della busta EDI da utilizzare per l'imbustamento. Tutti i profili della busta definiti sono disponibili dall'elenco.		
Attivo XMLNS	No	<p>Elaborazione dello spazio dei nomi per il documento XML di input. Questo attributo viene utilizzato dalla procedura di trasformazione XML.</p> <p>I valori validi sono Sì o No.</p>		Schema: Sì DTD: No
Livello max errore di convalida	No	<p>Livello massimo accettabile dell'errore di convalida (gravità dell'errore da accettare prima di considerare la transazione "non riuscita").</p> <p>I valori validi sono 0, 1 o 2.</p> <p><b>0</b> Consenti solo convalida senza errori</p> <p><b>1</b> Non riesce per documenti che presentano solo errori di convalida degli elementi semplici</p> <p><b>2</b> Non riesce per documenti che presentano solo errori di convalida su elementi o segmenti</p>		0

Tabella 92. Attributi EDI aggiuntivi (Continua)

Attributo	Necessario	Descrizione	Limitazioni	Predefinito
Livello di convalida	No	<p>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 quell'attributo è impostato su Sì.</p> <p>I valori validi sono 0, 1 o 2.</p> <p><b>0</b> 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.</p> <p><b>1</b> Esegue il livello 0 di convalida, più la convalida dei valori dell'elemento rispetto agli elenchi di codici specificati per l'elemento dati.</p> <p><b>2</b> Esegue il livello 1 di convalida, più la convalida che il valore dell'elemento è corretto per il tipo di dati dell'elemento.</p>		0
Tabella di convalida set di caratteri	No	<p>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.</p> <p>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. Quest'area contiene anche gli elenchi codici utilizzati per altri scopi, come ad esempio la convalida di certi elementi EDI.</p>		CHARSET
Tabella di convalida alfanumerica	No	<p>Indica la tabella da utilizzare per la convalida alfanumerica. Questa tabella viene utilizzata solo quando l'attributo del livello di convalida è 2.</p> <p>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. Quest'area contiene anche gli elenchi codici utilizzati per altri scopi, come ad esempio la convalida di certi elementi EDI.</p>		ALPHANUM

Tabella 92. Attributi EDI aggiuntivi (Continua)

Attributo	Necessario	Descrizione	Limitazioni	Predefinito
Attributo Genera info livello gruppo nel riconoscimento funzionale	No	Questo attributo si applica a EDI-X12. I valori validi sono Sì o No.  <b>Sì</b> Genera info livello gruppo nel riconoscimento funzionale.  <b>No</b> 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
Convalida dettagliata del segmento	No	Questo attributo si applica alle seguenti intestazioni ed elementi di coda del segmento: <ul style="list-style-type: none"> <li>• X12 <ul style="list-style-type: none"> <li>- ISA, IEA</li> <li>- GS, GE</li> <li>- ST, SE</li> </ul> </li> <li>• EDIFACT <ul style="list-style-type: none"> <li>- UNA</li> <li>- UNB, UNZ</li> <li>- UNG, UNE</li> <li>- UNH, UNT</li> </ul> </li> <li>• UNTUCS <ul style="list-style-type: none"> <li>- BG, EG</li> <li>- GS, GE</li> <li>- ST, SE</li> </ul> </li> </ul> I valori validi sono Sì o No.  <b>Sì</b> Esegue la convalida dettagliata del segmento della busta. La profondità del controllo viene effettuata dall'attributo Livello di convalida.  <b>No</b> 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

Tabella 92. Attributi EDI aggiuntivi (Continua)

Attributo	Necessario	Descrizione	Limitazioni	Predefinito
Eliminazione errore	No	Questo attributo viene utilizzato nell'elaborazione polimorfica.  Nel caso di un batch che risulta dallo sbustamento, 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'Envelope 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 interscambio	No	Il codice utilizzato per identificare il formato dell'identificativo del mittente o del destinatario dell'interscambio.		
Identificativo interscambio	No	Identifica il mittente o il destinatario specifico del documento. Il tipo di dati immessi viene determinata dall'attributo del qualificatore di interscambio.		
Indicatore utilizzo scambio	No	Indica se i documenti di origine convertiti sono classificati come documenti di Produzione, Test 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 interscambio	No	Indica l'indirizzo cui il destinatario deve recapitare le risposte.		
Indirizzo instradamento interscambio	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.		

## Proprietà del client Data Interchange Services

In questa sezione, vengono elencate le proprietà che possono essere impostate come parte della mappa di trasformazione nel client Data Interchange Services e negli attributi di WebSphere Partner Gateway corrispondenti.

Tabella 93. Proprietà della mappa ed attributi corrispondenti

Proprietà del client Data Interchange Services	Sostituisce l'attributo WebSphere Partner Gateway
AckReq	Richiesta conferma di ricezione
Alphanumeric	Tabella di convalida alfanumerica
Charset	Tabella di convalida set di caratteri
CtlNumFlag	Numero di controllo per ID transazione
EdiDecNot (Notazione decimale)	Notazione decimale
EdiDeDlm (Separatore elemento dati)	Delimitatore elementi dati
EdiDeSep (Repeating data element separator)	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 interscambio
SegOutput	Output segmento
ValLevel	Livello di convalida
ValErrLevel	Livello max errore di convalida
ValMap	Mappa di convalida

In Tabella 94 vengono elencate le proprietà aggiuntive del client Data Interchange Services e gli attributi WebSphere Partner Gateway associati.

Tabella 94. 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 interscambio
IchgSndrQL	Qualificatore mittente scambio
IchgSndrId	ID mittente interscambio
IchgRcvrQL	Qualificatore destinatario interscambio
IchgRcvrId	ID destinatario interscambio
IchgDate	Data interscambio
IchgTime	Ora interscambio
IchgPswd	Password interscambio
IchgUsgInd	Indicatore utilizzo scambio
IchgAppRef	Riferimento applicazione interscambio
IchgVerRel	Versione e rilascio interscambio

Tabella 94. Proprietà del client Data Interchange Services ed attributi associati (Continua)

Proprietà del client Data Interchange Services	Sostituisce l'attributo WebSphere Partner Gateway
IchgGrpCnt	Numero dei gruppi nell'interscambio
IchgCtlTotal	Controllo totale dal segmento di coda dell'interscambio
IchgTrxCnt	Numero di documenti nell'interscambio
GrpCtlNum	Numero di controllo gruppo
GrpFuncGrpId	ID gruppo funzionale
GrpAppSndrId	ID mittente applicazione gruppo
GrpAppRcvrId	ID destinatario applicazione gruppo
GrpDate	Data gruppo
GrpTime	Ora gruppo
GrpPswd	Password gruppo
GrpVer Versione gruppo.	Versione gruppo
GrpRel Rilascio gruppo.	Rilascio gruppo
GrpTrxCnt	Numero di documenti nel gruppo
TrxCtlNum	Numero di controllo transazione
TrxCode	Codice transazione
TrxVer	Versione transazione
TrxRel	Rilascio transazione
TrxSegCnt	Numero di segmenti EDI nel documento

## Attributi AS

La sezione descrive gli attributi AS.

Tabella 95. Attributi AS

Attributo	Necessario	Descrizione	Limitazioni	Predefinito
Ora di notifica	No	L'intervallo di tempo di attesa per una notifica MDN prima di reinviare la richiesta di origine. Questo attributo funziona insieme al Conteggio tentativi. Le unità sono espresse in minuti.	Limitato al pacchetto o alla connessione	30
Conteggio tentativi	No	Il numero di volte per inviare una richiesta se non viene ricevuto un MDN. Questo attributo funziona insieme a Ora di notifica.  Ad esempio, se questo attributo viene impostato su 3, la richiesta può essere inviata potenzialmente quattro volte (la prima volta più tre tentativi).	Limitato al pacchetto o alla connessione	3
Compresso AS	No	Comprime i dati. Questo attributo funziona insieme all'attributo Compresso AS prima della firma.	Limitato al pacchetto o alla connessione	No

Tabella 95. Attributi AS (Continua)

Attributo	Necessario	Descrizione	Limitazioni	Predefinito
Compresso 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 venga firmato. Questo attributo funziona insieme all'attributo Compresso AS.	Limitato al pacchetto o alla connessione	Sì
Codificato AS	No	Indica se deve essere eseguita la codifica. <b>Nota:</b> Non è uguale alla codifica SSL.  Per la parte TO dello scambio (quando si inviano documenti a un partner) specifica se codificare il documento o meno.  Per la parte FROM dello scambio (quando si ricevono documenti da un partner), se l'attributo è impostato su Sì, deve essere codificata una richiesta AS inviata dal partner. Se l'attributo è impostato su No, il documento proveniente dal partner può essere codificato o decodificato.  I valori validi sono Sì o No. <b>Sì</b> La codifica è richiesta. <b>No</b> La codifica non è richiesta.	Limitato al pacchetto o alla connessione	No
AS MDN richiesto	No	Specifica se è richiesta una risposta MDN. Se è impostato su Sì, questo attributo consente la compilazione dell'intestazione "Disposizione-notifica trasporto a" con il valore dell'attributo dell'indirizzo e-mail AS MDN.  I valori validi sono Sì e No. <b>Sì</b> Richiedi un MDN. <b>No</b> Non richiedere un MDN.	Limitato al pacchetto o alla connessione	Sì
Indirizzo e-mail AS MDN	Sì se l'attributo "AS MDN asincrono" è Sì e si utilizza AS1.	Specifica l'indirizzo e-mail per il partner da utilizzare per l'invio di MDN asincroni. Questo attributo è utilizzato insieme all'attributo AS MDN richiesto. Il valore dell'attributo Indirizzo e-mail AS MDN viene utilizzato nel campo "Disposizione-notifica a".  Solo per AS1, questo attributo funziona insieme all'attributo asincrono AS MDN nel formato mailto:xxx@company.com.	Limitato al pacchetto o alla connessione	
URL HTTP MDN AS	Sì se l'attributo "AS MDN asincrono" è Sì e si utilizza AS2.	Questo attributo si applica ad AS2 e viene utilizzato per specificare l'URL cui un partner dovrebbe inviare un MDN asincrono. Questo attributo funziona insieme all'attributo AS MDN asincrono.	Limitato al pacchetto o alla connessione	

Tabella 95. Attributi AS (Continua)

Attributo	Necessario	Descrizione	Limitazioni	Predefinito
AS MDN asincrono	No	<p>Specifica se deve essere restituito un MDN in modo sincronico o asincrono. Il valore di questo attributo condiziona l'utilizzo degli attributi URL HTTP MDN AS o Indirizzo e-mail MDN AS.</p> <p>I valori validi sono Sì e No.</p> <p><b>Sì</b> Asincrono <b>No</b> Sincronico</p> <p>Se questo attributo è impostato su Sì, il campo "opzione ricevimento- recapito" viene compilato in base all'attributo URL HTTP MDN AS (per AS2) o l'attributo Indirizzo e-mail MDN AS (per AS1).</p>	Limitato al pacchetto o alla connessione	Sì
Firmato AS MDN	No	<p>Indica se alla richiesta deve essere restituito un MSN firmato. Questo attributo funziona insieme a AS MDN richiesto.</p> <p>Se il valore è impostato su Sì, viene compilato il campo "Opzioni disposizione-notifica: firmato-ricevuta-protocollo".</p> <p>I valori validi sono Sì e No.</p> <p><b>Sì</b> Richiesto MDN firmato <b>No</b> MDN firmato non richiesto</p> <p>Se l'attributo è impostato su Sì, l'MDN inviato dal partner deve essere firmato.</p> <p>Se questo attributo è impostato su No, l'MDN può essere firmato o meno.</p>	Limitato al pacchetto o alla connessione	No
Algoritmo raccolta messaggio AS	No	<p>L'algoritmo di raccolta messaggio da utilizzare durante la firma. Questo attributo viene utilizzato insieme agli attributi AS firmato e AS MDN firmato.</p> <p>Per gli MDN firmati, questo valore viene utilizzato per compilare l'intestazione "Opzioni disposizione-notifica: firmato-ricevimento-micalg".</p>	Limitato al pacchetto o alla connessione	sha1

Tabella 95. Attributi AS (Continua)

Attributo	Necessario	Descrizione	Limitazioni	Predefinito
Firmato AS	No	<p>Specifica se firmare il documento.</p> <p>Per la parte TO dello scambio (quando si inviano documenti a un partner) specifica se firmare il documento o meno.</p> <p>Per la parte FROM dello scambio (quando si ricevono documenti da un partner), se l'attributo è impostato su Sì, deve essere firmata una richiesta AS inviata dal partner. Se l'attributo è impostato su No, il documento proveniente dal partner può essere firmato o meno.</p> <p><b>Sì</b> Firma documento</p> <p><b>No</b> Il documento firmato non è richiesto</p>	Limitato al pacchetto o alla connessione	No
ID aziendale AS	No	<p>L'ID aziendale AS da utilizzare nell'intestazione "AS2-A". Se un valore non viene fornito, WebSphere Partner Gateway utilizza l'ID aziendale del destinatario utilizzato nel documento di origine.</p> <p><b>Nota:</b> L'intestazione "AS2-Da" viene impostata dal documento di origine che passa in WebSphere Partner Gateway e che viene inviato come AS.</p>	Limitato al pacchetto o alla connessione	

## Attributi RosettaNet

In questa sezione vengono descritti gli attributi RosettaNet.

Tabella 96. Attributi RosettaNet

Attributo	Necessario	Descrizione	Limitazioni	Predefinito
Ora di notifica	Sì	<p>L'intervallo di tempo di attesa per una notifica di ricevimento prima di reinviare la richiesta di origine. Questo attributo funziona insieme al Conteggio tentativi. Le unità sono espresse in minuti.</p> <p>Il valore predefinito è desunto dal documento di specifica PIP RosettaNet.</p>	Limitato al pacchetto o alla connessione	120
Ora di esecuzione	Sì	L'intervallo di tempo di attesa per una risposta ad un'azione di richiesta prima di inviare un messaggio di notifica di errore.	Limitato al pacchetto o alla connessione	

Tabella 96. Attributi RosettaNet (Continua)

Attributo	Necessario	Descrizione	Limitazioni	Predefinito
Conteggio tentativi	Sì	<p>Il numero di volte per inviare una richiesta se non viene ricevuta una notifica di ricevimento. Questo attributo funziona insieme a Ora di notifica.</p> <p>Ad esempio, con un impostazione di 3, la richiesta può essere inviata potenzialmente 4 volte (la prima volta più altri tre tentativi).</p> <p>Il valore predefinito è desunto dal documento di specifica PIP RosettaNet.</p>	Limitato al pacchetto o alla connessione	3
Firma digitale richiesta	No	<p>Indica se il messaggio PIP richiede una firma digitale.</p> <p>Il valore predefinito è desunto dal documento di specifica PIP RosettaNet.</p>	Limitato al pacchetto o alla connessione	Sì
Richiesta non rifiuto	No	<p>Indica se memorizzare il documento di origine nella memoria di non rifiuto.</p> <p>Il valore predefinito è desunto dal documento di specifica PIP RosettaNet.</p>	Limitato al pacchetto o alla connessione	Sì
Richiesta di non rifiuto della ricevuta	No	<p>Indica se memorizzare il documento di notifica della ricevuta nella memorizzazione di non rifiuto.</p> <p>Il valore predefinito è desunto dal documento di specifica PIP RosettaNet.</p>	Limitato al pacchetto o alla connessione	Sì
Sync supportata		<p>Indica se PIP supporta la comunicazione sincrona.</p> <p>Il valore predefinito è fornito in base alla specifica PIP.</p>	<p>Limitato al pacchetto o alla connessione.</p> <p>Questo attributo è disponibile solo per RNIF 2.0.</p>	
Ric sinc richiesto		<p>Indica se PIP richiede una notifica di ricevimento sincrona.</p> <p>Il valore predefinito è fornito in base alla specifica PIP.</p>	<p>Limitato al pacchetto o alla connessione.</p> <p>Questo attributo è disponibile solo per RNIF 2.0.</p>	
Global Supply Chain Code	Richiesto per RNIF 1.1	<p>Il codice che identifica la catena di fornitura per la funzione del partecipante.</p> <p>I valori possibili sono:</p> <ul style="list-style-type: none"> <li>• Componenti elettronici</li> <li>• Information Technology</li> <li>• Tecnologia semiconduttore</li> </ul>	Limitato al pacchetto o alla connessione	

Tabella 96. Attributi RosettaNet (Continua)

Attributo	Necessario	Descrizione	Limitazioni	Predefinito
Codifica		<p>Questo attributo indica se eseguire la codifica.  <b>Nota:</b> Non è uguale alla codifica SSL.</p> <p>Per la parte TO dello scambio (quando si inviano documenti a un partner) specifica se codificare il documento o meno.</p> <p>Per la parte FROM dello scambio (quando si ricevono documenti da un partner), se l'attributo è impostato su Sì, deve essere codificata una richiesta RNIF inviata dal partner. Se l'attributo è impostato su No, il documento proveniente dal partner può essere codificato o decodificato.</p> <p>I valori possibili sono:</p> <p><b>Nessuno</b>                      La codifica non è richiesta.</p> <p><b>Payload</b>                      Codifica solo in contenuto del servizio RosettaNet.</p> <p><b>Payload e Container</b>                      Codifica il contenuto del servizio RosettaNet insieme all'intestazione del servizio.</p>	<p>Limitato al pacchetto o alla connessione.</p> <p>Questo attributo è disponibile solo per RNIF 2.0.</p>	Nessuno

## Attributo integrazione di backend

La sezione descrive l'attributo associato all'impacchettamento di integrazione di backend.

Tabella 97. Attributo Integrazione backend

Attributo	Descrizione	Predefinito
Flag busta	<p>Questo attributo indica se avviluppare il documento in una busta XML.</p> <p>I valori validi sono Sì e No.</p>	No

---

## Appendice E. Informazioni particolari

E' possibile che negli altri paesi IBM non offra i prodotti, le funzioni o i servizi illustrati in questo documento. Consultare il rappresentante IBM locale per informazioni sui prodotti e sui servizi disponibili nel proprio paese. Ogni riferimento relativo a prodotti, programmi o servizi IBM non implica che solo quei prodotti, programmi o servizi IBM possano essere utilizzati. Al loro posto può essere usato qualsiasi prodotto, programma o servizio funzionalmente equivalente che non comporti violazione dei diritti di proprietà intellettuale o di altri diritti di IBM. È responsabilità dell'utente valutare e verificare la possibilità di utilizzare altri programmi e/o prodotti, fatta eccezione per quelli espressamente indicati dall'IBM.

IBM può avere brevetti o domande di brevetto in corso relativi a quanto trattato nel presente documento. La fornitura di questa pubblicazione non implica la concessione di alcuna licenza su essi. Chi desiderasse inviare domande relative a tali licenze può rivolgersi, per iscritto, a:

IBM Director of Licensing  
IBM Corporation  
North Castle Drive  
Armonk, NY 10504-1785  
U.S.A.

Il seguente paragrafo non è valido per il Regno Unito o per tutti i paesi le cui leggi nazionali siano in contrasto con le disposizioni in esso contenute:

INTERNATIONAL BUSINESS MACHINES CORPORATION FORNISCE QUESTA PUBBLICAZIONE "NELLO STATO IN CUI SI TROVA SENZA" ALCUNA GARANZIA, ESPLICITA O IMPLICITA, IVI INCLUSE EVENTUALI GARANZIE DI COMMERCIALIZZABILITA', NON VIOLAZIONE DEI DIRITTI ALTRUI ED IDONEITA' AD 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 sono soggette a modifiche periodiche che saranno incorporate nelle nuove edizioni della pubblicazione. L'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 di IBM contenuti in questo documento sono forniti solo a titolo informativo e non implicano in alcun modo l'approvazione da parte di IBM. I materiali disponibili sui siti Web non fanno parte di questo prodotto e l'utilizzo di questi è a discrezione dell'utente.

L'IBM può utilizzare o divulgare le informazioni ricevute dagli utenti secondo le modalità ritenute appropriate, senza alcun obbligo nei loro confronti.

I possessori di licenza di questo programma che desiderano informazioni sul programma stesso a scopo di consentire: (i) lo scambio di informazioni tra programmi creati indipendentemente e altri programmi (incluso questo) e (ii) l'uso reciproco delle informazioni scambiate, si rivolgano a:

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

Queste informazioni possono essere rese disponibili, secondo condizioni contrattuali appropriate, compreso, in alcuni casi, il pagamento di un addebito.

Il programma su licenza descritto in questo manuale e tutto il materiale su licenza ad esso relativo sono forniti dall'IBM nel rispetto delle condizioni previste dalla licenza d'uso.

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 misure potrebbero essere state ricavate mediante estrapolazione. I risultati possono quindi 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. L'IBM non ha necessariamente verificato tali prodotti e non può garantirne l'accuratezza delle prestazioni. Eventuali commenti relativi alle prestazioni dei prodotti non IBM devono essere indirizzati ai fornitori di tali prodotti.

Queste informazioni possono contenere esempi di dati e report utilizzati quotidianamente nelle operazioni aziendali. Per meglio illustrarli, tali esempi possono contenere nomi di persone, società, marchi e prodotti. Tutti i nomi contenuti nel manuale sono fittizi e ogni riferimento a nomi ed indirizzi reali è puramente casuale.

Tutte le dichiarazioni riguardanti la futura direzione o le intenzioni dell'IBM sono soggette a sostituzione o al ritiro senza preavviso e rappresentano scopi e obiettivi della IBM stessa.

#### LICENZA DI COPYRIGHT

Queste informazioni possono contenere esempi di programmi applicativi in linguaggio sorgente, che illustrano tecniche di programmazione su varie piattaforme operative. È possibile copiare, modificare e distribuire questi esempi di programmi sotto qualsiasi forma senza alcun pagamento alla 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. La IBM, quindi, non può garantire o assicurare l'affidabilità, l'utilità o il funzionamento di questi programmi di esempio.

WebSphere Partner Gateway contiene il codice denominato ICU4J che viene concesso su licenza dall'IBM in base ai termini dell'International Program License Agreement, soggetto ai termini dei Componenti esclusi. Tuttavia, all'IBM viene richiesto di fornire all'utente le seguenti informazioni come avviso:

## COPYRIGHT E AVVISO DI PERMESSO

Copyright (c) 1995-2003 International Business Machines Corporation e altri

Tutti i diritti riservati.

L'autorizzazione viene quindi concessa, gratuitamente, a qualsiasi persona che ottiene una copia di questo software e i file di documentazione associati (il "Software"), per operare con il Software senza restrizioni, comprese la limitazione dei diritti all'uso, alla riproduzione, alla modifica, alla fusione, alla divulgazione, alla distribuzione, e/o vendita di copie del Software e per permettere alle persone a cui viene fornito il Software di fare ciò, a condizione che l'avviso di copyright in alto e quelli di autorizzazione presenti in tutte le copie del Software e gli avvisi di copyright in alto e questa autorizzazione viene visualizzata nella documentazione di supporto.

IL SOFTWARE VIENE FORNITO "COSÌ COM'È", SENZA GARANZIA DI ALCUN TIPO, ESPRESSA O IMPLICITA, COMPRESA MA NON LIMITATA ALLE GARANZIE DI COMMERCIALIZZABILITÀ, ADATTABILITÀ PER UN PARTICOLARE SCOPO E NON VIOLAZIONE DEI DIRITTI ALTRUI. IN NESSUN CASO I TITOLARI DEL COPYRIGHT INCLUSI IN QUESTO AVVISO SARANNO RESPONSABILI DI EVENTUALI RECLAMI O DI EVENTUALI DANNI SPECIALI O CONSEGUENZIALI O DI DANNI A TERZI CHE PRODUCONO UNA PERDITA IRREPARABILE, DEI DATI DI PROFITTO, SE IN UN'AZIONE DI CONTRATTO, NEGLIGENZA O ALTRE AZIONI TORTUOSE NASCONO DA O IN CONCOMITANZA DALL'USO O DALLE PRESTAZIONI DI QUESTO SOFTWARE.

Tranne quelle contenute in questo avviso, il nome del titolare del copyright non verrà utilizzato in annunci pubblicitari o altri tipi di promozione alla vendita, utilizzo o altri trattamenti in questo Software senza una precedente autorizzazione scritta del titolare del copyright.

---

## 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 di uso generale consentono di scrivere il software di applicazione che ottiene 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.

**Avvertenza:** Non utilizzare le informazioni di diagnosi, modifica e ottimizzazione come un'interfaccia di programmazione perché è soggetta a modifiche.

---

## Marchi commerciali e marchi di servizio

I seguenti termini sono marchi della International Business Machines Corporation negli Stati Uniti, in altri paesi, o in entrambi:

i5/OS  
IBM  
il logo IBM  
AIX  
CICS

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

Microsoft, Windows, Windows NT e il logo Windows sono marchi della Microsoft Corporation.

MMX, Pentium, e ProShare sono marchi della Intel Corporation negli Stati, e/o in altri paesi.

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 della 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 e Advanced Editions dispongono di software sviluppati dal progetto Eclipse ([www.eclipse.org](http://www.eclipse.org)).



WebSphere Partner Gateway Enterprise e Advanced Editions, versione 6.0.

# Indice analitico

## Caratteri speciali

&Mappa DT99724 120  
&Mappa DT99735 120  
&Mappa DT99933 120  
&Mappa DTCTL 120  
&Mappa DTCTL21 120  
&Mappa WDIEVAL 121  
&Mappa X44TA1 121

## Numerico

0A1 Notification of Failure  
    V02.02 PIP 241  
    V1.0 PIP 241  
3A4 Request Purchase Order  
    V02.00 PIP 245  
    V02.02 PIP 247  
3A8 Request Purchase Order Change  
    V01.02 PIP 252  
    V01.03 PIP 253  
3B14 Request Shipping Order  
    Cancellation 259  
4C1 Distribute Inventory Report  
    V02.01 PIP 272  
    V02.03 PIP 272

## A

accesso alla Console comunità 26  
Agenzia di controllo 103, 285  
Agenzia gruppo 103  
Agenzia gruppo GS07 103  
aggancio trust 156  
API, abilitazione 173  
API basati su XML, abilitazione 173  
Associazione assegnata 103  
Associazione assegnata UNG0703 103  
attributi  
    busta EDIFACT 283  
    busta UCS 282  
    busta X12 281  
    connessione partecipante 57, 89  
    definizione di flusso di documenti 55, 87  
    delimitatore 285  
    EDI, elenco di 281  
    flusso documento EDI 113  
    funzioni B2B 56, 88  
    gestore splitter 44  
    livello di protocollo EDI 113  
    precedenza 149  
    profilo busta 100, 281  
    profilo connessione 104  
    separatore 285  
    trasporto globale 33  
Attributi AS  
    Algoritmo raccolta messaggio AS 295  
    AS MDN asincrono 295  
    AS MDN richiesto 294  
    Codificato AS 167, 168, 294

Attributi AS (*Continua*)  
    Compresso AS 293  
    Compresso AS prima della firma 294  
    Conteggio tentativi 293  
    Firmato AS 165, 296  
    Firmato AS MDN 295  
    ID aziendale AS 125, 150, 296  
    Indirizzo e-mail AS MDN 294  
    Ora di notifica 293  
attributi busta 100  
Attributi busta EDIFACT 283  
Attributi buste EDI 102  
    Agenzia gruppo GS07 103  
    Associazione assegnata UNG0703 103  
    Codice associazione assegnato UNH0205 103  
    CRPCTLLEN Lunghezza del numero di controllo del gruppo 283  
    CTLNUMFLAG Numeri di controllo per ID transazione 282, 283, 284  
    delimitatore 285  
    Destinatario applicazione GS03 103  
    EDIFACTGRP Crea gruppi per EDI 284  
    GRPCTLLEN Lunghezza del numero di controllo del gruppo 284  
    Gruppo funzionale GS01 102, 282, 283  
    ID accordo comunicazioni UNB10 102  
    ID comunicazioni BG01 102  
    ID destinatario applicazione UNG0301 103  
    ID mittente applicazione UNG0201 103  
    ID sintassi UNB0101 102  
    ID versione interscambio ISA12 101  
    Indicatore di prova UNB11 (indicatore utilizzo) 102  
    Informazioni autorizzazione ISA02 101  
    Informazioni sulla sicurezza ISA04 101  
    INTCTLLEN Lunghezza del numero di controllo dell'interscambio 281, 283, 284  
    Lunghezza del numero di controllo del gruppo 101, 282  
    Lunghezza del numero di controllo della transazione 101  
    Lunghezza del numero di controllo dello scambio 101  
    MAXDOCS Numero max di transazioni 282, 283, 284  
    Mittente applicazione GS02 102  
    Numeri di controllo per ID transazione 101  
    Numero max di transazioni 101  
    Password applicazione UNG08 103  
    Password comunicazioni BG02 102

Attributi buste EDI (*Continua*)  
    Priorità UNB08 102  
    Qualificatore ID destinatario applicazione UNG0302 103  
    Qualificatore ID mittente applicazione UNG0202 103  
    Qualificatore informazioni autorizzazione ISA01 101  
    Qualificatore informazioni di sicurezza ISA03 101  
    Qualificatore riferimento/password destinatari UNB0602 102  
    Richiesta di notifica ISA14 102  
    Richiesta di notifica UNB09 102  
    Riferimento accesso comune UNH03 104  
    Riferimento applicazione UNB07 102  
    Riferimento/password destinatari UNB0601 102  
    Rilascio messaggio UNG0703 103  
    separatore 286  
    Standard di interscambio ISA11 101  
    TRXCTLLEN Lunghezza numero di controllo della transazione 282, 283, 284  
    UNG01 Gruppo funzionale 103, 284  
    UNG06 Agenzia di controllo 103  
    UNG0701 Versione messaggio 103  
    UNH0201 Tipo messaggio 103, 285  
    UNH0202 Versione messaggio 103, 285  
    UNH0203 Rilascio messaggio 103, 285  
    UNH0204 Agenzia di controllo 103, 285  
    Versione gruppo GS08 103, 282, 283  
    Versione sintassi UNB0102 102  
attributi delimitatore 285  
Attributi di gruppo, profilo busta 102  
attributi di trasporto globale destinazione 33  
Attributi EDI  
    Anno controllo secolo 290  
    Attivo XMLNS 288  
    Attributo Genera info livello gruppo nel riconoscimento funzionale 290  
    Consenti elementi duplicati 288  
    Convalida dettagliata di segmenti 290  
    Eliminazione errore 291  
    Identificativo destinatario applicazione gruppo 291  
    Identificativo interscambio 291  
    Identificativo mittente applicazione gruppo 291  
    Indicatore utilizzo scambio 291  
    Indirizzo instradamento interscambio 291  
    Instradamento inverso interscambio 291  
    Livello di convalida 289

- Attributi EDI (*Continua*)
  - Livello max errore di convalida 288
  - Livello max errore su trasformazione 288
  - Mappa FA 288
  - Output segmento 287
  - Password applicazione gruppo 291
  - Qualificatore destinatario applicazione di gruppo 291
  - Qualificatore interscambio 291
  - Qualificatore mittente applicazione di gruppo 291
  - Qualificatore profilo connessione 1 105, 291
  - sostituzione TA1 290
  - Tabella di convalida alfanumerica 289
  - Tabella di convalida set di caratteri 289
- Attributi generali, profilo busta 101
- attributi globali di trasporto gateway 128
- Attributi GS 102
- Attributi RosettaNet
  - Codifica 65, 298
  - Conteggio tentativi 297
  - Firma digitale richiesta 297
  - Global Supply Chain Code 65, 297
  - modifica 228
  - Ora di esecuzione 296
  - Ora di notifica 296
  - Ric sinc richiesto 65, 297
  - Richiesta di non rifiuto della ricevuta 297
  - Richiesta non rifiuto 297
  - Sinc supportata 65
  - Sync supportata 297
- attributi separatore 285
- Attributi transazione, profilo busta 103
- Attributo algoritmo raccolta messaggio AS 295
- Attributo Anno controllo secolo 290
- Attributo AS MDN richiesto 294
- Attributo asincrono AS MDN 295
- Attributo Attivo XMLNS 288
- attributo BCG\_BATCHDOCS 45, 92, 98
- attributo carattere elemento dati ripetitivo 287
- attributo carattere rilascio 286, 287
- Attributo codificato AS 167, 168, 294
- Attributo compresso AS 293
- Attributo Compresso AS prima della firma 294
- Attributo Consenti elementi duplicati 288
- Attributo conteggio tentativi 293, 297
- Attributo Convalida dettagliata di segmenti 290
- attributo delimitatore elementi dati 286, 287
- attributo delimitatore elemento secondario 286
- attributo delimitatore segmento 287
- Attributo destinatario applicazione di gruppo 291
- Attributo di codifica 298
- Attributo Eliminazione errore 291

- Attributo firmato AS 165, 296
- Attributo firmato AS MDN 295
- Attributo flag busta 298
- Attributo Genera info livello gruppo nel riconoscimento funzionale 290
- Attributo Global Supply Chain Code 297
- Attributo ID azienda AS 125, 150, 296
- Attributo identificativo destinatario dell'applicazione di gruppo 291
- Attributo identificativo interscambio 291
- Attributo identificativo mittente applicazione di gruppo 291
- Attributo indirizzo e-mail AS MDN 294
- Attributo instradamento inverso interscambio 291
- Attributo Livello di convalida 289
- Attributo Livello max errore di convalida 288
- Attributo Livello max errore su trasformazione 288
- Attributo Mappa FA 288
- attributo maxOccurs 239
- Attributo metadizionario 45
- Attributo metadocumento 45
- Attributo metasintassi 45
- attributo minOccurs 239
- Attributo mittente applicazione di gruppo 291
- attributo notazione decimale 286
- Attributo Output segmento 287
- Attributo password applicazione di gruppo 291
- Attributo qualificatore interscambio 291
- Attributo Qualificatore profilo connessione 1 105, 291
- Attributo richiesta di non rifiuto della ricevuta 297
- Attributo richiesta firma digitale 297
- Attributo richiesta non rifiuto 297
- attributo separatore elemento dati ripetitivo 286
- Attributo Sostituzione TA1 290
- Attributo Sync Ack richiesto 297
- Attributo Sync supportato 297
- Attributo Tabella di convalida alfanumerica 289
- Attributo Tabella di convalida set di caratteri 289
- Attributo URL AS MDN Http 294
- autenticazione del client
  - configurazione 159
  - SSL in entrata 159
  - SSL in uscita 161
- autenticazione del server
  - SSL in entrata 158
  - SSL in uscita 160
- autorizzazioni
  - descrizione 30
  - modifica autorizzazioni predefinite 30
- azioni
  - copia 53
  - creazione 52
  - descrizione 13
  - gestori 51

## B

- banner, aggiunta 27
- blocchi
  - Envelope 98, 99
  - trasporto di script FTP 33, 128
- bundle di risorsa 28
- buste X12, attributi 281

## C

- CA (autorità di certificazione) root 156
- Campo durata max coda 99
- Campo Qualifier1 105
- Campo tempo max blocco 99
- carattere rilascio 286
- cardinalità 239
- catene, certificato 156
- catene di certificati 156
- certificati
  - autofirmato 156
  - destinazione 156
  - elenco 169
  - firma 164, 165
  - formato, conversione 161
  - intermedio 156
  - principale 156
  - revocato 162
  - scaduto, sostituzione 155
  - secondario 156
- certificati di codifica, limiti sulla lunghezza 156
- certificati di destinazione 156
- certificati di firma
  - in entrata 164
  - in uscita 165
- Certificati di firma in entrata 164
- Certificati firma in uscita 165
- certificati intermedi 156
- certificati principali
  - certificato di firma digitale 165
  - codifica in uscita 168
  - descrizione 156
  - SSL in uscita 161
- certificati revocati 162
- certificati secondari
  - certificato di firma digitale 165
  - codifica in uscita 168
  - descrizione 156
  - SSL in uscita 161
- Certificati SSL
  - autenticazione client, in uscita 161
  - autenticazione del client, in entrata 159
  - autenticazione del server, in entrata 158
  - autenticazione del server, in uscita 160
  - in entrata 158
  - certificato autofirmato 156
  - Certificato revocato o messaggio scaduto 169
  - certificato scaduto, sostituzione 155
  - chiave privata 154
  - chiave pubblica 154
  - chiavi
    - privata 154

- chiavi (*Continua*)
  - pubblica 154
- client Data Interchange Services
  - descrizione 24, 110
  - proprietà 292
  - specialista della mappa 24
- Client Data Interchange Services
  - specialista della mappa 85
- code
  - evento 173
  - JMS, creazione 21
- code di eventi, specifica 173
- Codice associazione assegnata 103
- Codice associazione assegnato UNH0205 103
- Codifica
  - abilitazione 167, 168
  - descrizione 154
- Codifica degli attributi 44
- comandi, FTP 40, 139
- comandi ascii 40, 139
- comandi FTP
  - ascii 40, 139
  - binario 40, 139
  - bye 41, 140
  - cd 40, 140
  - delete 40, 140
  - get 40
  - getdel 40
  - mget 40
  - mgetdel 41
  - mkdir 41, 140
  - mput 140
  - open 41, 140
  - passivo 40, 139
  - quit 41, 140
  - quote 41, 140
  - rename 41
  - rmdir 41, 140
  - site 41, 140
- comando binario 40, 139
- comando bye 41, 140
- comando cd 40, 140
- comando delete 40, 140
- comando get 40
- comando getdel 40
- comando mget 40
- comando mgetdel 41
- comando mkdir 41, 140
- comando mput 140
- comando open 41, 140
- comando passivo 40, 139
- comando quit 41, 140
- comando quote 41, 140
- comando rename 41
- comando rmdir 41, 140
- comando site 41, 140
- Compressione del protocollo
  - gestori 51
  - passo, descrizione 13
- concatenamento, mappa 85
- concatenamento mappa 85
- configurazione JMS, definizione 22
- connessioni, partecipante
  - attivazione 149
  - attributi 57, 89
  - descrizione 56, 89

- connessioni partecipante
  - attivazione 149
  - attributi 57, 89
  - descrizione 56, 89
- Console comunità
  - accesso alla 26
  - avvio 25
  - banner 27
  - intestazione sfondo 27
  - logo, aggiunta 27
  - marchio 27
- contenuto del pacchetto PIP
  - 0A1 Notification of Failure 241
  - 0A1 Notification of Failure V02.00 241
  - 2A1 Distribute New Product Information 242
  - 2A12 Distribute Product Master 243
  - 3A1 Request Quote 244
  - 3A2 Request Price and Availability 245
  - 3A4 Request Purchase Order V02.00 245
  - 3A4 Request Purchase Order V02.02 247
  - 3A5 Query Order Status 248
  - 3A6 Distribute Order Status 249
  - 3A7 Notify of Purchase Order Update 250
  - 3A8 Request Purchase Order Change V01.02 252
  - 3A8 Request Purchase Order Change V01.03 253
  - 3A9 Request Purchase Order Cancellation 254
  - 3B11 Notify of Shipping Order 257
  - 3B12 Request Shipping Order 258
  - 3B13 Notify of Shipping Order Confirmation 259
  - 3B14 Request Shipping Order Cancellation 259
  - 3B18 Notify of Shipping Documentation 260
  - 3B2 Notify of Advance Shipment 255
  - 3B3 Distribute Shipment Status 256
  - 3C1 Return Product 261
  - 3C3 Notify of Invoice 262
  - 3C4 Notify of Invoice Reject 263
  - 3C6 Notify of Remittance Advice 264
  - 3C7 Notify of Self-Billing Invoice 265
  - 3D8 Distribute Work in Process 266
  - 4A1 Notify of Strategic Forecast 266
  - 4A3 Notify of Threshold Release Forecast 267
  - 4A4 Notify of Planning Release Forecast 268
  - 4A5 Notify of Forecast Reply 269
  - 4B2 Notify of Shipment Receipt 270
  - 4B3 Notify of Consumption 271
  - 4C1 Distribute Inventory Report V02.01 272
  - 4C1 Distribute Inventory Report V02.03 272
  - 5C1 Distribute Product List 273
  - 5C2 Distribute Product List 274
  - 5C4 Distribute Registration Status 275

- contenuto del pacchetto PIP (*Continua*)
  - 5D1 Request Ship From Stock and Debit Authorization 275
  - 6C1 Query Service Entitlement 276
  - 6C2 Request Warranty Claim 277
  - 7B1 Distribute Work in Process 278
  - 7B5 Notify Of Manufacturing Work Order 279
  - 7B6 Notify Of Manufacturing Work Order Reply 280
- contesto JMS, definizione 22
- Crea gruppi per EDI 284
- CRL (certificate revocation list)
  - aggiunta 162
  - punti di distribuzione 163
- CRL (Certificate Revocation List)
  - aggiunta 162
  - punti di distribuzione 163
- CTLNUMFLAG (Numeri di controllo in base a ID transazione) 282, 283, 284

## D

- Da attributo codice processo 45
- Da attributo nome impacchettamento 45
- Da attributo nome protocollo 45
- Da attributo versione
  - impacchettamento 45
- Da attributo versione processo 45
- Da attributo versione protocollo 45
- Data Interchange Services
  - mappe, importazione 111
- Decompressione del protocollo
  - gestori 51
  - passo, descrizione 12
- definizione di flussi di documenti
  - descrizione 55
  - panoramica 3
- definizione documenti, Data Interchange Services 111
- definizione protocollo XML, personalizzato 78
- definizioni del flusso di documenti RNIF 61
- definizioni del protocollo XML 78
- definizioni di flussi di documenti
  - attributi 55, 87
  - come assicurarsi della disponibilità 55, 87
  - descrizione 87
  - mappe di convalida, associazione 81
  - servizi Web 69
  - tipi 58
- delimitatore segmento 285
- descrizione SSL 153
- descrizione SSL (Security Sockets Layer) 153
- destinatario
  - descrizione 7
- Destinatario
  - avvio 25
  - descrizione 31
- Destinatario applicazione 103
- Destinatario applicazione GS03 103
- destinazioni
  - attributi di trasporto globale 33
  - descrizione 8, 31

- destinazioni (*Continua*)
  - FTP 34
  - gestore splitter 44
  - HTTP 33
  - JMS 37
  - punti di configurazione 9, 44
  - punto di configurazione
    - Postprocesso 48
  - punto di configurazione
    - Preprocesso 44
  - punto di configurazione
    - SyncCheck 44
  - script FTP 39
  - sistema di file 38
  - SMTP 36
- destinazioni del sistema di file 38
- destinazioni FTP 34
- destinazioni HTTP
  - gestori SyncCheck 47
  - impostazione 33
- destinazioni JMS
  - gestori SyncCheck 47
  - impostazione 37
- destinazioni POP3 36
- destinazioni script FTP 39
- destinazioni SMTP 36
- directory
  - Binary 19
  - Documents 19
  - JMS 21
  - Production 18
  - server FTP 18
  - Test 18
- directory Binary 19
- directory Documents 19
- directory JMS, creazione 21
- directory Production 18
- directory Test 18
- direttive del messaggio XML di
  - RosettaNet 229
- Distribute Inventory Report
  - V02.01 PIP 272
  - V02.03 PIP 272
- documenti binari 58
- documenti cXML
  - definizioni di flussi di documenti 77
  - DTD 74
  - elemento root 74
  - esempio 74
  - intestazioni tipo contenuto 76
  - tipo messaggio 75
  - tipo richiesta 75
  - tipo risposta 75
- documenti raw, visualizzazione 81, 122
- documenti ROD
  - descrizione 86
  - elaborazione di 97
- documenti ROD (record-oriented data) 86
- documenti XML
  - descrizione 86
  - elaborazione di 97
- DTD
  - conversione in schema XML 230
  - documenti cXML 74
- durata coda, Enveloper 99

## E

- EDI
  - attributi, elenco di 281
  - elementi dati 83
    - panoramica 83
    - scambi 83
    - segmenti 83
    - transazioni 83
  - EDI con flusso autorizzato
    - esempio 177
    - impostazione 59
  - EDIFACTGRP (Crea gruppi per EDI) 284
  - elementi dati
    - componente 287
    - composto 286
    - descrizione 83
    - semplice 286
  - elementi dati componente 287
  - elementi di tipo
    - common\_LineNumber\_R 240
  - elemento dati composto 286, 287
  - elemento dati semplice 286
  - elemento del tipo DayofMonth 240
  - elemento del tipo
    - GlobalLocationIdentifier 240
  - enumerazione 240
  - Enveloper
    - blocco 98
    - descrizione 98
    - durata accodamento 99
    - modalità batch 99
    - pianificazione basata sull'intervallo 99
    - tempo blocco massimo 99
    - valori predefiniti, modifica 98
  - esempi
    - EDI autorizzati 177
    - EDI in ROD 193
    - EDI in XML 206
    - protezione 183
    - riconoscimenti funzionali 202
    - Riconoscimento TA1 199
    - ROD in EDI 219
    - XML in EDI 212
  - eventi, notificabile 174
  - eventi notificabili 174

## F

- FA (riconoscimento funzionale)
  - descrizione 120
  - esempio 202
- file BCG.Properties
  - aggiornamento delle informazioni sul contatto PIP 0A1 228
  - bcg.CRLDir 162
- file binari
  - convenzione di denominazione 19
  - elaborazione 19
- file criteri di protezione, JRE 156
- File criteri di protezione legislazione JRE 156
- file JMSAdmin.config 21
- file WSDL
  - importazione 70

- file WSDL (*Continua*)
  - privati 70
  - pubblici 70
  - requisiti archivio ZIP 70
  - schemi XML 71
- file WSDL privati 70
- file WSDL pubblici 70
- file XML
  - creazione di pacchetti di Integrazione Backend 236
  - creazione di pacchetti RNIF 236
  - elaborazione 20
- Firma digitale
  - abilitazione 165
  - descrizione 154
- flussi di documenti
  - descrizione 6
  - personalizzato 79
- flussi di lavoro
  - fisso in uscita 13
  - gestori definiti dall'utente 50
  - in entrata fisso 11
- flussi di lavoro fissi in entrata
  - descrizione 11
  - gestori 50
  - gestori definiti dall'utente 50
- flussi di lavoro fissi in uscita
  - descrizione 13
  - gestori 51
  - gestori definiti dall'utente 50
- flusso documenti ROD in EDI
  - descrizione 91
  - impostazione 117
- flusso documenti XML in EDI
  - descrizione 91
  - impostazione 117
- flusso EDI in EDI
  - descrizione 89
  - impostazione 112
- flusso EDI in ROD
  - descrizione 90
  - esempio 193
  - impostazione 114
- flusso EDI in XML
  - esempio 206
  - impostazione 114
- Flusso EDI in XML
  - descrizione 90
- flusso ROD in EDI
  - esempio 219
  - impostazione 116
- Flusso ROD in EDI
  - descrizione 91
- flusso ROD in ROD
  - descrizione 93
  - impostazione 119
- flusso ROD in XML
  - descrizione 92
  - impostazione 118
- flusso XML in EDI
  - descrizione 91
  - esempio 212
- Flusso XML in EDI
  - impostazione 116
- flusso XML in ROD
  - descrizione 92
  - impostazione 118

- flusso XML in XML
  - descrizione 93
  - impostazione 119
- foglio di stile, modifica 28
- formati XML
  - creazione 78
  - descrizione 78
- Formati XML
  - creazione 80
- formato, mappe di convalida 240
- funzioni B2B
  - attributi 56, 88
  - descrizione 56, 88
  - Gestore comunità 124
  - partecipanti 146

## G

- gateway
  - descrizione 14
  - directory di file 17, 136
  - FTP 132, 133
  - FTPS 138
  - HTTP 130
  - HTTPS 131
  - JMS 134, 135
  - predefinito 143
  - punti di configurazione 14
  - punto di configurazione
    - Postprocesso 15, 142
    - punto di configurazione
      - Preprocesso 15, 142
    - script FTP 140
    - Script FTP 139
    - SMTP 133, 134
    - trasporti definiti dall'utente 143
    - trasporti supportati 127
  - gateway directory di file 17
  - gateway FTP 133
  - gateway JMS 135
  - gateway predefinito, impostazione 143
  - gateway SMTP 134
  - gestore AS2 SyncCheck 47
  - Gestore comunità
    - descrizione 2, 123
    - funzioni B2B 124
    - profilo 123
  - gestore cXML SyncCheck 47
  - gestore del flusso di documenti
    - generici 47
  - Gestore documenti
    - avvio 26
    - descrizione 10
  - gestore RNIF SyncCheck 47
  - gestore SOAP SyncCheck 47
  - gestore splitter EDI 46
  - gestore splitter ROD 46, 86
  - gestore splitter XML 46
  - gestori
    - caricamento 32, 49
    - Compressione del protocollo 51
    - Decompressione del protocollo 51
    - definiti dall'utente 49, 50
    - descrizione 9
    - Protocollo che elabora 51
  - gestori definiti dall'utente
    - aggiornamento 50

- gestori definiti dall'utente (*Continua*)
  - caricamento 32, 49
  - flusso di lavoro 50
- gestori splitter
  - attributi 44
  - descrizione 86
  - elenco 46
- GRPCTLLEN (Lunghezza numero di controllo gruppo) 282, 283, 284
- gruppi, EDI
  - descrizione 84
  - segmenti dell'elemento di coda 84
  - segmenti di intestazione 84
- Gruppo funzionale GS01 102, 282, 283

## H

- handshake, SSL 157
- handshake SSL 157

## I

- IBM Key Management Tool (ikeyman)
  - descrizione 154
  - posizione 154
- ID accordo comunicazioni 102
- ID accordo comunicazioni UNB10 102
- ID aziendale 124, 145, 146
- ID comunicazioni 102
- ID comunicazioni BG01 102
- ID destinatario applicazione 103
- ID destinatario applicazione
  - UNG0301 103
- ID gruppo funzionale 102, 103, 282, 284
- ID mittente applicazione 103
- ID mittente applicazione UNG0201 103
- ID rilascio messaggio 103
- ID sintassi 102
- ID sintassi UNB0101 102
- ID standard di interscambio ISA11 101
- ID standard di scambio 101
- ID versione di scambio 101
- ID versione interscambio ISA12 101
- impacchettamento
  - AS 4
  - concetto N/D 5
  - descrizione 3
  - integrazione backend 4
  - Nessuno 4
  - RNIF 4
- impacchettamento AS 4
- Impacchettamento integrazione backend
  - creazione 239
  - descrizione 4
- impacchettamento RNIF 4
- Indicatore di prova 102
- Indicatore di prova (indicatore
  - utilizzo) 102
- Indicatore di prova ISA15 102
- Indicatore di prova UNB11 (indicatore
  - utilizzo) 102
- Indicatore utilizzo interscambio 291
- Indirizzo instradamento
  - interscambio 291
- Informazioni autorizzazione ISA02 101
- Informazioni di autorizzazione 101

- informazioni di contatto, PIP 0A1 228
- Informazioni sulla sicurezza 101
- Informazioni sulla sicurezza ISA04 101
- INTCTLLEN (Lunghezza numero di controllo scambio) 281, 283, 284
- interazioni
  - descrizione 56, 88
  - documenti cXML 78
  - documenti RosettaNet 66
  - servizi Web 73
- interscambi di sbustamento 94
- interscambi EDI
  - elaborazione di 94
  - struttura 83, 84
- intestazioni tipo contenuto, cXML 76
- IP 0A1 227

## J

- JMS, modifica della configurazione
  - predefinita 21

## K

- keystore
  - descrizione 155
  - password predefinita 155
  - utilizzo di valori non predefiniti 169

## L

- logo, aggiunta di società 27
- logo società, aggiunta 27
- Lunghezza del numero di controllo del gruppo 101, 282, 283, 284
- Lunghezza del numero di controllo della transazione 101, 282, 283, 284
- Lunghezza del numero di controllo dello scambio 101, 281, 283, 284

## M

- mappe
  - convalida 80, 81, 86
  - importazione 110
  - riconoscimento funzionale 85
  - trasformazione 85
- mappe di convalida
  - aggiunta 80
  - definizione di flusso di documenti,
    - associazione 81
  - descrizione 80
  - EDI standard 86
  - formato 240
  - importazione 110
  - RosettaNet 239
- mappe di notifica funzionale
  - descrizione 85
  - fornito dal sistema 120
  - importazione 110
- mappe di trasformazione
  - descrizione 85
  - importazione 110
  - proprietà 292

mappe FA (notifica funzionale)  
 descrizione 85  
 fornito dal sistema 120  
 marchio della Console comunità 27  
 maschere, numero di controllo 107  
 max certificato di codifica 2048 byte 156  
 MAXDOCS (Numero max  
 transazioni) 282, 283, 284  
 messaggi RNSC 61  
 messaggi RosettaNet  
 notifica evento 61  
 versioni supportate 61  
 messaggi RosettaNet Service Content 61  
 messaggio Non sono stati trovati  
 attributi 229  
 Mittente applicazione 102  
 Mittente applicazione GS02 102  
 modalità batch 98, 99

## N

nessun impacchettamento 4  
 nome segmento 83, 287  
 Non è stato trovato alcun certificato di  
 codifica valido 169  
 non rifiuto 154  
 notazione decimale 286  
 note di rilascio PIP 229  
 notifica errore, elaborazione PIP 227  
 Notifica richiesta 102  
 Notification of Failure  
 V02.00 PIP 241  
 V1.0 PIP 241  
 numeri di controllo  
 descrizione 106  
 inizializzazione 109  
 maschere 107  
 visualizzazione 110  
 Numeri di controllo per ID  
 transazione 101, 282, 283, 284  
 Numero max di transazioni 101, 282,  
 283, 284

## O

Opzione Convalida certificato SSL  
 client 160  
 Ora di esecuzione attributo 296  
 Ora di notifica attributo 293, 296

## P

pacchetti del flusso di documenti,  
 PIP 63  
 pacchetti PIP  
 aggiornamento 229  
 creazione 229  
 pacchetti RNIF  
 creazione 239  
 ubicazione 61  
 pagina Elenco gestori 48  
 partecipanti  
 creazione 145  
 funzioni B2B 146  
 password  
 key store predefinito 155

password (*Continua*)  
 predefinito 26  
 trust store predefinito 155  
 Password applicazione 103  
 Password applicazione UNG08 103  
 Password comunicazioni 102  
 Password comunicazioni BG02 102  
 pianificazione  
 destinazione SMTP (POP3) 36  
 destinazioni script FTP 43  
 Enveloper 99  
 pianificazione basata sul calendario  
 destinazione SMTP (POP3) 36  
 destinazioni script FTP 43  
 Enveloper 99  
 pianificazione basata sull'intervallo  
 destinazione SMTP (POP3) 36  
 destinazioni script FTP 43  
 Enveloper 99  
 PIP  
 0A1 227  
 caricamento dei pacchetti 64  
 contenuto del pacchetto del flusso di  
 documenti 241  
 descrizione 61  
 disattivazione 227  
 elaborazione messaggi 61  
 elenco di PIP supportati 62  
 file schema XML, creazione  
 schemi 230  
 file XSD, creazione 230  
 notifica errore 227  
 pacchetti di flusso di documenti 63  
 PIP (Partner Interface Process) 61  
 PIP 2A1 Distribute New Product 242  
 PIP 2A12 Distribute Product Master 243  
 PIP 3A1 Request Quote 244  
 PIP 3A2 Request Price and  
 Availability 245  
 PIP 3A5 Query Order Status 248  
 PIP 3A6 Distribute Order Status 249  
 PIP 3A7 Notify of Purchase Order 250  
 PIP 3A9 Request Purchase Order  
 Cancellation 254  
 PIP 3B11 Notify of Shipping Order 257  
 PIP 3B12 Request Shipping Order 258  
 PIP 3B13 Notify of Shipping Order  
 Confirmation 259  
 PIP 3B18 Notify of Shipping  
 Documentation 260  
 PIP 3B2 Notify of Advance  
 Shipment 255  
 PIP 3B3 Distribute Shipment Status 256  
 PIP 3C1 Return Product 261  
 PIP 3C3 Notify of Invoice 262  
 PIP 3C4 Notify of Invoice Reject 263  
 PIP 3C6 Notify of Remittance  
 Advice 264  
 PIP 3C7 Notify of Self-Billing  
 Invoice 265  
 PIP 3D8 Distribute Work in Process 266  
 PIP 4A1 Notify of Strategic Forecast 266  
 PIP 4A3 Notify of Threshold Release  
 Forecast 267  
 PIP 4A4 Notify of Planning Release  
 Forecast 268  
 PIP 4A5 Notify of Forecast Reply 269

PIP 4B2 Notify of Shipment Receipt 270  
 PIP 4B3 Notify of Consumption 271  
 PIP 5C1 Distribute Product List 273  
 PIP 5C2 Request Design  
 Registration 274  
 PIP 5C4 Distribute Registration  
 Status 275  
 PIP 5D1 Request Ship From Stock and  
 Debit Authorization 275  
 PIP 6C1 Query Service Entitlement 276  
 PIP 6C2 Request Warranty Claim 277  
 PIP 7B1 Distribute Work in Process 278  
 PIP 7B5 Notify of Manufacturing Work  
 Order 279  
 PIP 7B6 Notify of Manufacturing Work  
 Order Reply 280  
 PIP Distribute New Product  
 Information 242  
 PIP Distribute Order Status 249  
 PIP Distribute Product List 273, 274  
 PIP Distribute Product Master 243  
 PIP Distribute Registration Status 275  
 PIP Distribute Shipment Status 256  
 PIP Distribute Work in Process 266, 278  
 PIP Notify of Advance Shipment 255  
 PIP Notify of Consumption 271  
 PIP Notify of Forecast Reply 269  
 PIP Notify of Invoice 262  
 PIP Notify of Invoice Reject 263  
 PIP Notify Of Manufacturing Work  
 Order 279  
 PIP Notify Of Manufacturing Work Order  
 Reply 280  
 PIP Notify of Planning Release  
 Forecast 268  
 PIP Notify of Purchase Order  
 Update 250  
 PIP Notify of Remittance Advice 264  
 PIP Notify of Self-Billing Invoice 265  
 PIP Notify of Shipment Receipt 270  
 PIP Notify of Shipping  
 Documentation 260  
 PIP Notify of Shipping Order 257  
 PIP Notify of Shipping Order  
 Confirmation 259  
 PIP Notify of Strategic Forecast 266  
 PIP Notify of Threshold Release  
 Forecast 267  
 PIP Query Order Status 248  
 PIP Query Service Entitlement 276  
 PIP Request Purchase Order  
 Cancellation 254  
 PIP Request Quote 244  
 PIP Request Ship From Stock and Debit  
 Authorization 275  
 PIP Request Shipping Order 258  
 PIP Request Shipping Order  
 Cancellation 259  
 PIP Request Warranty Claim 277  
 PIP Return Product 261  
 più certificati 156  
 più documenti in un file 86  
 politica di password, impostazione 29  
 Priorità 102  
 Priorità UNB08 102  
 profili  
 busta 99

- profili (*Continua*)
  - connessione 104
  - Gestore comunità 123
  - partecipante 145
- profili busta
  - attributi 100, 281
  - Attributi generali 101
  - Attributi Gruppo 102
  - attributi Interchange 101
  - attributi Transazione 103
  - creazione 100
  - descrizione 99
- profili connessione
  - attributi 104
  - descrizione 104
  - impostazione 106
  - per transazioni 104
  - scambi 105
- proprietà
  - client Data Interchange Services 292
  - mappa di trasformazione 292
- proprietà bcg\_CRLDir 162
- protezione
  - considerazioni sul server FTPS 20
  - elenco certificati 169
  - esempio 183
  - panoramica 153
  - tipi supportati 153
- protocolli
  - binario 5
  - cXML 6
  - EDI-Consent 5
  - EDI-EDIFACT 5
  - EDI-X12 5
  - elenco 5
  - RNSC 6
  - RosettaNet 6
  - servizio Web 6
  - XML personalizzato 78
  - XMLEvent 6
- protocolli aziendali 5
- protocollo binario 5
- Protocollo che elabora
  - gestori 51
  - passo, descrizione 12
- protocollo cXML 6
- protocollo EDI-Consent 5
- protocollo EDI-EDIFACT1 5
- protocollo EDI-X12 5
- protocollo RNSC 6
- protocollo RosettaNet 6
- protocollo servizio Web 6
- protocollo XMLEvent 6, 68
- punti di configurazione
  - destinazione 9, 44
  - gateway 14, 142
  - Postprocesso 10, 48, 142
  - Preprocesso 10, 44, 142
  - scambi sincroni 44
  - SyncCheck 10, 47
- punti di configurazione, destinazione
  - modifica 48
  - panoramica 9
  - Postprocesso 10, 48
  - Preprocesso 10, 44
  - SyncCheck 10, 47

- punti di configurazione, gateway
  - modifica 142
  - Postprocesso 15, 142
  - Preprocesso 15, 142
- punto di configurazione Postprocesso
  - destinazione 10, 48
  - gateway 15, 142
  - tipi di gestore 48
- punto di configurazione Preprocesso
  - destinazione 10, 44
  - gateway 15, 142
- punto di configurazione SyncCheck
  - descrizione 10
  - destinazione HTTP/S 47
  - destinazione JMS 47
  - elenco di gestori 47
  - ordine di gestori 48
  - quando richiesto 44

## Q

- Qualificatore ID destinatario
  - applicazione 103
- Qualificatore ID destinatario applicazione
  - UNG0302 103
- Qualificatore ID mittente
  - applicazione 103
- Qualificatore ID mittente applicazione
  - UNG0202 103
- Qualificatore informazioni autorizzazione
  - ISA01 101
- Qualificatore informazioni di autorizzazione 101
- Qualificatore informazioni di sicurezza 101
- Qualificatore informazioni di sicurezza
  - ISA03 101
- Qualificatore riferimento/password
  - destinatari 102
- Qualificatore riferimento/password
  - destinatari UNB0602 102

## R

- Request Purchase Order
  - V02.00 PIP 245
  - V02.02 PIP 247
- Request Purchase Order Change
  - V01.02 PIP 252
  - V01.03 PIP 253
- requisiti archivio ZIP per file WSDL 70
- Richiesta conferma di ricezione 102
- Richiesta di notifica ISA14 102
- Richiesta di notifica UNB09 102
- riconoscimenti funzionali
  - descrizione 120
  - esempio 202
- Riconoscimenti TA1
  - descrizione 121
  - esempio 199
- Riferimento accesso comune 104
- Riferimento accesso comune
  - UNH03 104
- Riferimento applicazione 102
- Riferimento applicazione UNB07 102
- Riferimento/password destinatari 102

- Riferimento/password destinatari
  - UNB0601 102
- Rilascio messaggio 103, 285
- RNIF, descrizione di 61
- RosettaNet
  - descrizione 60
  - sito Web 61
- RosettaNet Implementation
  - Framework 61
- runtime Java, aggiunta 22

## S

- scambi
  - elaborazione di 94
  - profili connessione 105
  - struttura 83
- scambi sincroni, requisiti del punto di configurazione 44
- schema del messaggio XML di
  - RosettaNet 229
- schemi
  - file WSDL 71
  - pacchetti PIP 230
- schemi XML
  - conversione dal file DTD 230
  - file WDSL 71
  - pacchetti PIP 230
- script bcgChgPassword.jacl 155
- script bcgClientAuth.jacl
  - configurazione dell'autenticazione di un client 159
  - reimpostazione dopo l'utilizzo di bcgssl.jacl 169
- script bcgssl.jacl 169
- script FTP
  - comandi consentiti in 40, 139
  - descrizione 23
  - destinazioni 40
  - gateway 139
- segmenti, EDI 83
- segmenti di controllo 84
- segmenti di servizio 84
- segmento, descrizione 286
- segmento dell'elemento di coda 84
- segmento di intestazione 84
- separatore elemento componente 286
- separatore elemento dati 286, 287
- separatore elemento dati
  - componente 286
- separatore ripetitivo 286
- separatori 86
- server FTP
  - configurazione 20
  - directory Binary 19
  - directory Documents 19
  - struttura directory 18
- server FTPS, considerazioni di protezione 20
- servizi Web
  - definizioni di flussi di documenti 69
  - limitazioni 73
  - partecipanti, identificazione 69
  - standard supportati 73
- servlet bcgreceiver 33
- sfondo intestazione, aggiunta 27
- sistema di guida, avvio 26

- specialista della mappa 24, 85
- specifica N/D 5
- SSL in entrata
  - autenticazione del client 159
  - autenticazione del server 158
  - configurazione di keystore non predefiniti 169
- SSL in uscita
  - autenticazione del client 161
  - autenticazione del server 160
- standard AS1 4
- standard AS2 4
- struttura di interscambio EDI-X12 84

## T

- tag segmento 83, 287
- terminazione segmento 285, 287
- tipi di gestore 49
- Tipo di busta 282, 283, 284
- Tipo di busta ENVTYPE 282, 283, 284
- Tipo messaggio 103, 285
- transazioni, EDI
  - descrizione 83, 84
  - profili connessione 104
  - segmenti dell'elemento di coda 84
  - segmenti di intestazione 84
- trasporti
  - gateway, fornito dal sistema 127
  - panoramica 2
- trasporti, definiti dall'utente
  - aggiornamento 175
  - destinazione 43
  - eliminazione 43, 143
  - gateway 143
- trasporti definiti dall'utente
  - aggiornamento 175
  - destinazione 43
  - eliminazione 43, 143
  - gateway 143
- trust store
  - descrizione 155
  - password predefinita 155
- TRXCTLLEN (Lunghezza numero di controllo transazione) 282, 283, 284

## U

- UCS
  - attributi busta 282
  - descrizione 83
- UN/EDIFACT 83
- UNG01 Gruppo funzionale 103, 284
- UNG06 Agenzia di controllo 103
- UNG0701 Versione messaggio 103
- UNG0702 Rilascio messaggio 103
- UNH0201 Tipo messaggio 103, 285
- UNH0202 Versione messaggio 103, 285
- UNH0203 Rilascio messaggio 103, 285
- UNH0204 Agenzia di controllo 103, 285
- Utente admin Hub xi, 26
- utente Ammin
  - creazione di 30
  - Gestore comunità 124
  - partecipante 146
- utilità bcgDISImport 111

- Utilità ikeyman
  - descrizione 154
  - posizione 154
- Utilizzare il campo Modalità Batch 99

## V

- Versione gruppo 103, 282, 283
- Versione gruppo GS08 103, 282, 283
- Versione messaggio 103, 285
- Versione sintassi 102
- Versione sintassi UNB0102 102
- Visualizzatore di documenti 81, 122
- Visualizzatore di eventi 169

## W

- WebSphere MQ
  - avvio 25
  - modifica implementazione JMS 21

## X

- X12
  - descrizione 83
  - struttura di interscambio 84





Stampato in Italia