

*IBM WebSphere Business Integration Connect
Enterprise Edition and Advanced Edition*



Administrator Guide

Version 4.2.0

Note!

Before using this information and the product it supports, be sure to read the general information under "Notices and Trademarks" on page 137.

First Edition (September 2003)

This edition applies to Version 4, Release 2, Modification 0, of IBM® WebSphere® Business Integration Connect Advanced Edition (5724-E75) and Enterprise Edition (5724-E87), and to all subsequent releases and modifications until otherwise indicated in new editions.

IBM welcomes your comments. You can send to the following address:

*IBM Burlingame Laboratory
Information Development
577 Airport Blvd., Suite 800
Burlingame, CA 94010
U.S.A*

Include the title and order number of this book, and the page number or topic related to your comment.

When you send information to IBM, you grant IBM a nonexclusive right to use or distribute the information in anyway it believes appropriate without incurring any obligation to you.

© Copyright International Business Machines Corporation 2003. All rights reserved.

US Government Users Restricted Rights – Use, duplication or disclosure restricted by GSA ADP Schedule Contract with IBM Corp.

Table of Contents

Logging in to the Community Console 9

Starting Business Integration Connect	9
Logging in to the Community Console	9
Navigating through the Community Console	11
Community Console icons	12
Logging out of the Community Console	13
Stopping the Community Console	14
Stopping the Document Manager and Receiver	14

Hub Admin Activities 15

Branding the Community Console	15
Downloading sample images	16
Uploading a header background and company logo	18
Managing password policy	18
Viewing and editing password policy details	18
Configuring permissions	21
Viewing and editing permission details	21
Enabling or disabling permissions quickly	24
Configuring targets	25
Creating a new target	25
Viewing and editing target details	30
Enabling or disabling targets	33
Deleting targets	33
Configuring Document Flow Definitions and download packages	33
Understanding Document Flow Definitions	33
Creating Document Flow Definitions	35
Creating valid flow interactions	49
Searching for interactions	51
Configuring validation maps	52
Displaying the Manage Maps screen	52
Adding a validation map to a Document Flow Definition	54
Updating a validation map	55
Associating a map to a Document Flow Definition	55
Managing XML formats	57
Creating an XML format	57
Editing XML format values	60
Deleting an XML format	61

Enabling or disabling Actions	62
Managing event codes	63
Viewing and editing permission details	63
Saving event code names	65

Account Admin Activities 67

Managing Participant profiles	67
Creating Participants	67
Viewing and editing Participant profiles	72
Searching for Participants	75
Viewing your profile	76
Managing gateway configurations	79
Viewing and editing gateways	79
Viewing default gateways	82
Creating gateways	83
Deleting gateway configurations	84
Information required for gateway configuration	84
Creating an FTP account	85
Specifying an FTP server	85
Editing FTP details	87
Managing certificates	88
Viewing and editing digital certificates	88
Creating digital certificates	92
Disabling a digital certificate	94
Managing B2B capabilities	94
Types of Document Flow Definitions	95
Document Flow Definition attributes	95
Setting B2B capabilities	95
Changing B2B attribute values	97
Managing Participant connections	98
Connection components	99
Connection duplication	99
Searching for connections	101
Changing connection configurations	107
Managing Exclusion Lists	108
Adding Participants to the Exclusion List	108
Editing the Exclusion List	110

Using the Gateway Queue 111

Viewing the gateway list	111
Viewing queued documents	113
Removing documents from the queue	114
Viewing gateway details	114

Changing gateway status 114

Troubleshooting 115

Optimizing database query performance 115

Avoiding out-of-memory errors 115

Reprocessing events and business documents
that fail to log to the database 116

Poor performance and system events are
not working 117

Shutting down 117

Starting the system after a machine shutdown 118

 Starting DB2 118

 Starting WebSphere MQ 118

 Starting the Community Console,
Receiver, and Document Manager 118

Restarting the Document Manager after a crash 119

Administering Certificates 121

Certificate Overview 122

 Understanding terms and concepts 123

Creating and installing certificates 123

 Creating and installing inbound SSL
 certificates 123

Outbound SSL certificate 125

Inbound signature certificate 125

Outbound signature certificate 126

Inbound encryption certificate 126

Outbound encryption certificate 127

Configuring SSL for the Console and
Receiver 127

Notices and Trademarks 137

Notices 137

 Programming interface information.... 138

Trademarks and service marks 139

About this book

This document describes how IBM® WebSphere® Business Integration Connect can be configured and maintained to suit the requirements of the business-to-business (B2B) trading community.

Who should read this book

The parties involved with maintaining Business Integration Connect are the administrators. Business Integration Connect assumes two types of administrators:

- Hub Admin
- Operator Admin

The Hub Admin is the super-administrative user in the community. The Hub Admin is responsible for overall hub-community configuration and management, including Participant configuration and connection activation. The Operator Admin can access nearly all of the same features as the Hub Admin, except for the Hub Admin features. Only the Hub Admin can access the Hub Admin features.

The following table identifies the Console module activities available to Hub Admin and Operator Admin personnel. An “x” indicates that the individual has access to the module activity. When a Hub Admin or Operator Admin logs on to the Console, the Console only displays features that the Hub Admin or Operator Admin can access.

Modules and Activities	Hub Admin	Operator Admin
Hub Admin Activities (available to Hub Admin users only — see Chapter 2, page 15)		
Configuring Permissions	x	
Managing Password Policy	x	
Managing Event Codes	x	
Enabling or Disabling Actions	x	
Configuring Document Flow Definitions and Download Packages	x	
Configuring Validation Maps	x	
Configuring Targets	x	
Branding the Console	x	
Managing XML Formats	x	
Account Admin Activities (see Chapter 3, page 67)		
Managing Participant Profiles	x	x
Managing Gateway Configurations	x	x

Modules and Activities	Hub Admin	Operator Admin
Managing Users (see Note)	x	x
Managing Groups (see Note)	x	x
Managing Contacts (see Note)	x	x
Managing Addresses (see Note)	x	x
Managing Participant Connections	x	
Managing Exclusion Lists	x	
Managing Alerts (see Note)	x	x
Managing B2B Capabilities	x	x
Managing Certificates	x	x
Managing FTP	x	x
Viewers		
Event Viewer (see Note)	x	x
RosettaNet Viewer (see Note)	x	x
AS1/AS2 Viewer (see Note)	x	x
Document Viewer (see Note)	x	x
Gateway Queue (see Chapter 4, page 111)	x	
Tools (see Note)		
Document Analysis	x	x
Document Volume Report	x	x
Test Participant Connection	x	x
Community Participant Simulator Features (see Note)		
Initiate View Processes	x	x

NOTE: Some features can also be accessed by Community Participants and Community Managers. Though shared, Community Participants and Community Managers may not always see or have access to the same controls available to Hub Admin and Operator Admin personnel. For information about these shared features, see the WebSphere Business Integration Connect Community Console User Guide.

Conventions and terminology used in this book

This document used the following conventions:

bold	Indicates something you select in the User Interface.
blue text	Blue text, which is only visible when you view the manual online, indicates a cross-reference hyperlink. Click any blue text to jump to the object of the reference.

Terms

The following terms are unique to this product and document processing. Additional terms appear in this guide's Glossary.

Action: Also known as a business action. A message with content of a business nature such as a Purchase Order Request or a Request For Quote. The exchange of business actions and business signals comprise the message choreography necessary to complete a business activity specified by a given PIP.

Business action - see Action.

Business process: A predefined set of business transactions that represent the steps required to achieve a business objective.

Participant connection: A Participant connection defines the connection between two specific community members' environments by which one unique process is executed according to the associated action.

Community Console: The Community Console is a Web based tool used to configure Business Integration Connect and to manage the flow of your company's business documents to and from your Community Manager and Participants.

Document: A collection of information adhering to an organizational convention. In this context, there are multiple documents in a process.

Document protocol: A set of rules and instructions (protocol) used to format and transmit information across a computer network. Examples include RosettaNet, XML, flat file, and EDI.

Community Manager: The company that purchased and distributed Business Integration Connect to members in their hub-community. The Community Manager has one administrative user, the Manager Admin, who is responsible for the health and maintenance of the Community Manager's portion of the community. Community Console features excluded from the Community Manager's view relate to system configuration.

Community Operator: The individual responsible for the configuration and overall health and maintenance of the system, hub-wide (Hub Admin). The Hub Admin can access all features.

Packages: Identify document packaging formats used to transmit documents over the internet. For example, RNIF, AS1, and AS2.

Community Participant (Participant): The Participant sends business transactions to and receives business transactions from the Community Manager. Participants can access features that support their role in the community. Features excluded from the Participant's view relate to system configuration.

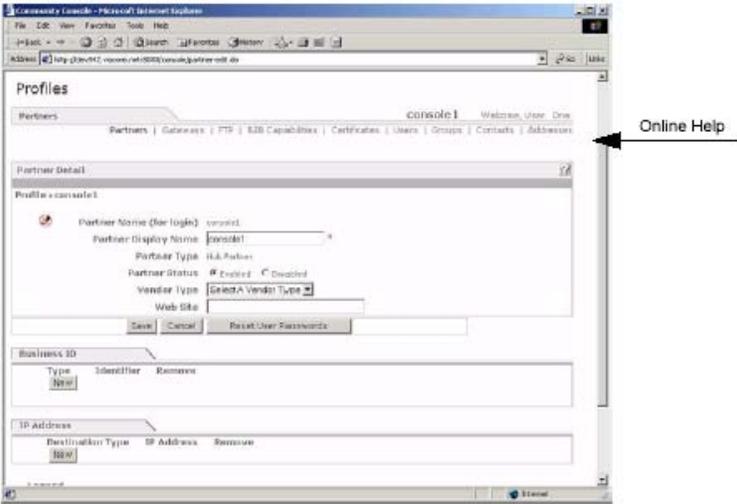
RosettaNet PIP (Partner Interface Process): A model that depicts the activities, decisions, and Partner Role Interactions that fulfill a business transaction between two partners in a given supply chain. (In Business Integration Connect, partners are called Participants.) Each Participant involved in the Partner Interface Process must fulfill the obligations specified in a PIP instance. If any one party fails to perform a service as specified in the PIP implementation guide, the business transaction is null and void.

Process: A process is a series of documents or messages executed between Community Managers and Participants. Taken as a whole, the documents make up a complete business process.

Getting help

Online Help

Click the **Help** link to access the online help.



The Community Console

Customer service

Software support

www.ibm.com/software/support

Passport Advantage®

www-3.ibm.com/software/howtobuy/passportadvantage/

Company web site

www.ibm.com/websphere/wbiconnect/

Chapter 1. Logging in to the Community Console

The administrator activities described in this guide are performed through the WebSphere Business Integration Connect Community Console. The Community Console is a Web-based facility that provides a secure Console access point. It features a friendly graphical user interface and convenient Web-based access capabilities.

Topics covered in this chapter include:

- “Starting Business Integration Connect” on page 9
- “Logging in to the Community Console” on page 9
- “Navigating through the Community Console” on page 11
- “Community Console icons” on page 12
- “Logging out of the Community Console” on page 13
- “Stopping the Community Console” on page 14
- “Stopping the Document Manager and Receiver” on page 14

Starting Business Integration Connect

To start Business Integration Connect, run the following script needs for all components.

```
INSTALLATION_DIRECTORY/bin/startServer.sh server1
```

NOTE: When running this command, a warning message appears. This can be safely ignored.

Logging in to the Community Console

The following procedure describes how to log in to the Community Console. The Community Console requires one To log in, you need one of the following Web browsers:

- Microsoft® Internet Explorer versions 5.5 or higher
- Netscape Navigator versions 6.x or higher

Be sure to install the latest available Service Pack and updates for your browser.

For optimum viewing, use a screen resolution of 1024 x 768 DPI.

1. Enter the following URL in the location field of any Web browser:

```
http://<hostname>.<domain>:8080/console
```

Where <hostname> and <domain> are the name and location of the computer hosting the Community Console component.

The Community Console login screen is displayed.

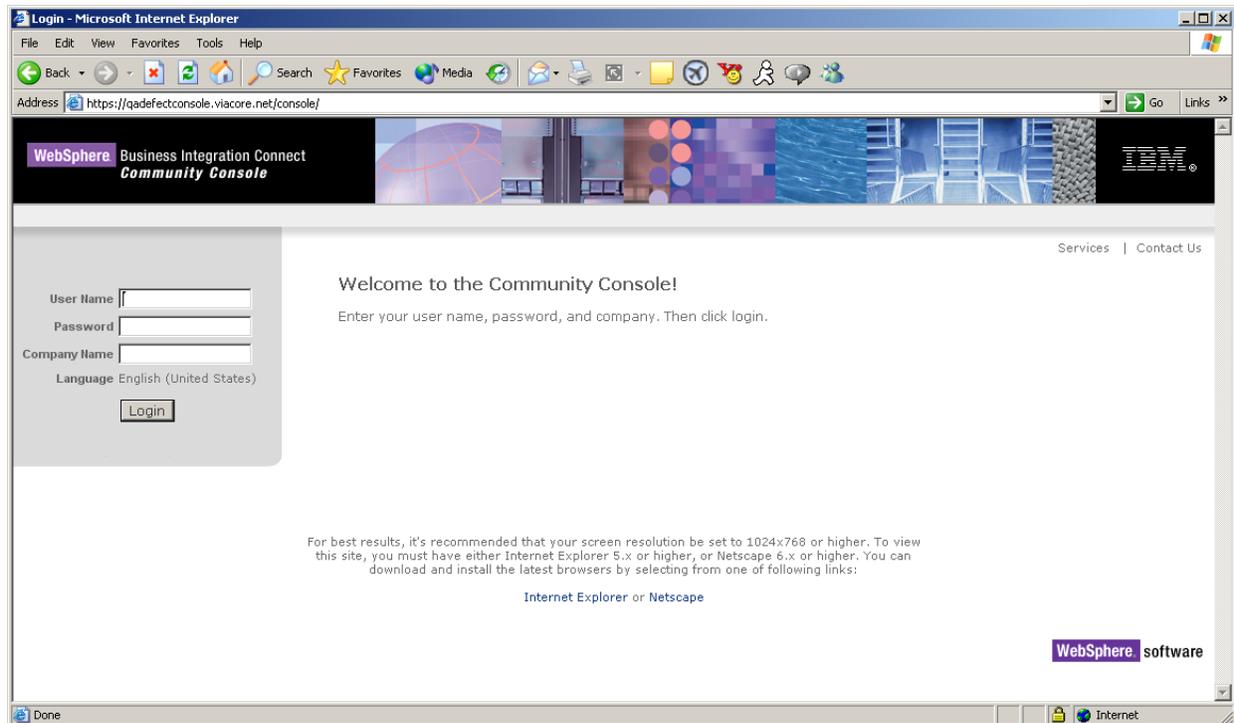


Figure 1-1. Community Console Login Screen

2. Next to **User Name**, enter the appropriate user name.
 - For the Hub Admin, the default user name is **hubadmin**
 - For the Operator Admin, the default user name is **Admin**
3. Next to **Password**, enter the password for your company. The default password is **Pa55word**
4. Next to **Company Name**, enter the Admin login name. The default Admin login name for both the Hub Admin and Operator Admin user is **Operator**
5. Click **Login**.
6. The first time you log in, the system prompts you to create a new password. Enter a new password, then enter it again in the **Verify** text box.
7. Click **Save**. The system displays the Console's initial entry screen.

Navigating through the Community Console

The Community Console user interface consists of a main menu, a horizontal navigation bar, and tabs (see [Figure 1-2](#)). You click the names that appear on these entities to navigate through the Community Console interface.

When you click a menu in the main menu:

- The horizontal navigation bar shows the names of the screens associated with the menu you selected.
- The main area shows a screen associated with the menu and horizontal navigation bar item selected.
- A set of tabs might appear in the main area. Each tab corresponds to a different screen associated with the item selected in the main menu and horizontal navigation bar.

If you click **Account Admin** in the main menu and **Profiles** in the horizontal navigation bar, the screen in [Figure 1-2](#) is displayed.

The following two links appear at the top-right corner of each screen:

- **Logout** allows you to log out from the current WebSphere Business Integration Connect session. The application continues to run in the background. To log in again, use the procedure under [“Logging in to the Community Console”](#) on page 9.
- **Help** allows you to access the online help for WebSphere Business Integration Connect.

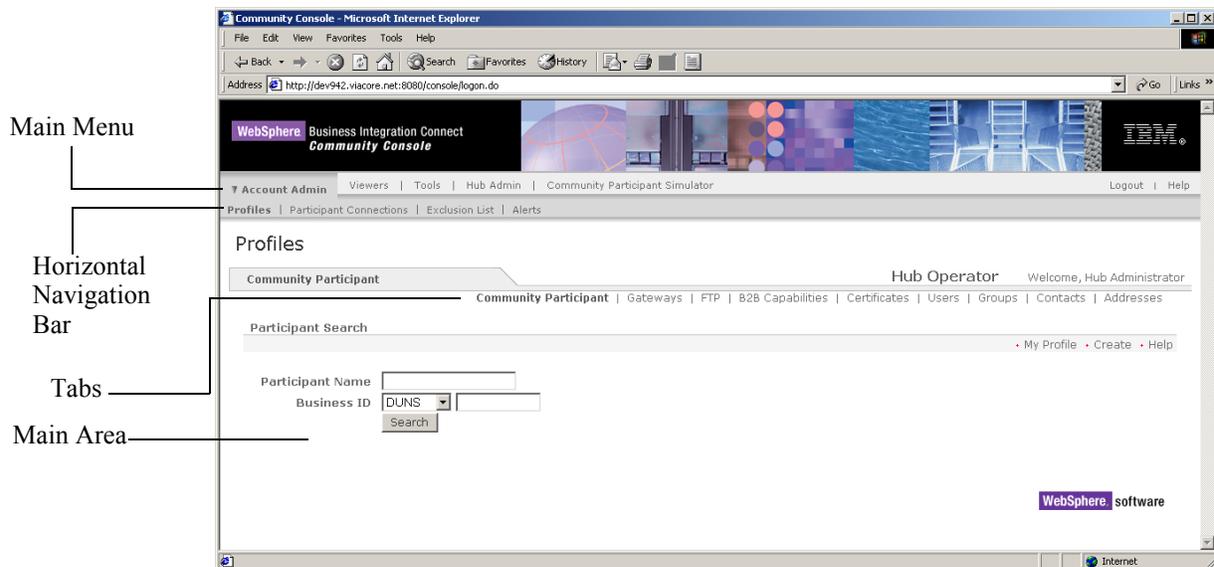


Figure 1-2. User Interface Controls

Community Console icons

For your convenience, the Community Console screens use icons on various screens. Some of these icons can be clicked to perform a task, while other icons indicate information. [Table 1-1](#) lists the icons used throughout the Community Console screens.

Table 1-1. Community Console Icons

Icon	Description
Clickable icons	
	Click to view detailed information.
	Click to modify a selected item.
	Click to delete one or more selected items or to activate the associated inactive item.
	Click to display a raw document.
	Click to continue.
	Click to pause.
	Click to export a report.
	Click to print a document or report.
	Click to view greater details.
	Click to close the detailed view.
	Click to view the groups to which a user belongs.
	Click to view users in a group.
	Click to export information from the system.
	Click to deactivate the associated active item.
	Click to edit a Document Flow Definition.
	Click to view Document Flow Definition attribute setup.
	Click to upload a new map.
	Click to download a map.

Table 1-1. Community Console Icons (continued)

Icon	Description
	Click to edit attribute values.
	Click to edit RosettaNet attribute values.
	Click to view a previously sent original document when there is a duplicate document event.
	Click to hide search criteria.
	Click to view permissions.
	Roll is not active; click to create role.
	Click to view the Help system.
Icons that show information	
	Indicates that the field requires input from the user.
	Indicates that a Trade Participant Agreement (TPA) has been entered.
	Indicates that a Participant or gateway is disabled.
	Indicates that a document contains an attachment.
	Indicates that document currently in progress.
	Indicates that document processing was successful.
	Indicates that document processing failed.
	Indicates that a hierarchical tree is in the “collapsed” view.
	Indicates that a hierarchical tree is in the “expanded” view.

Logging out of the Community Console

When you finish using the Business Integration Connect Community Console, use the following procedure to log out.

1. Click **Logout** at the top-right side of any Console screen (see [Figure 1-1 on page 10](#)). The system logs you out and returns you to the Console Login screen.

Stopping the Community Console

To stop the Community Console, run the following script.

```
INSTALLATION_DIRECTORY/bin/stopServer.sh server1
```

NOTE: When running this command, a warning message appears. This can be safely ignored.

Stopping the Document Manager and Receiver

To stop the Document Manager and Receiver, run the following script.

```
INSTALLATION_DIRECTORY/bin/shutdown_bcg.sh
```

NOTE: When running this command, a warning message appears. This can be safely ignored.

Chapter 2. Hub Admin Activities

This chapter describes the tasks that a Hub Admin user can perform. These tasks are:

- [“Branding the Community Console,”](#) below
- [“Managing password policy”](#) on page 18
- [“Configuring permissions”](#) on page 21
- [“Configuring targets”](#) on page 25
- [“Configuring Document Flow Definitions and download packages”](#) on page 33
- [“Configuring validation maps”](#) on page 52
- [“Managing XML formats”](#) on page 57
- [“Enabling or disabling Actions”](#) on page 62
- [“Managing event codes”](#) on page 63

Branding the Community Console

You can customize the look and feel of the Community Console by changing the branding images. Branding of the Community Console consists of importing two images: header background and company logo.

- The header background spans across the top of the Community Console.
- The company logo is displayed at the top right of the Community Console.

The images must be .JPG format files and must conform to the following size restrictions:

Table 2-1. Header Background and Company Logo Size Restrictions

Specification	Header Background	Company Logo
Height	80 pixels	80 pixels
Width	1100 pixels minimum (including the company logo image)	200 pixels maximum
Size	32k maximum	32k maximum



Figure 2-1. Image Specifications

Downloading sample images

To download a sample header background image and company logo, use the following procedure.

1. Click **Hub Admin** on the main menu and **Console Branding** on the horizontal navigation bar. The Console displays the Console Branding screen (see [Figure 2-2 on page 17](#)).

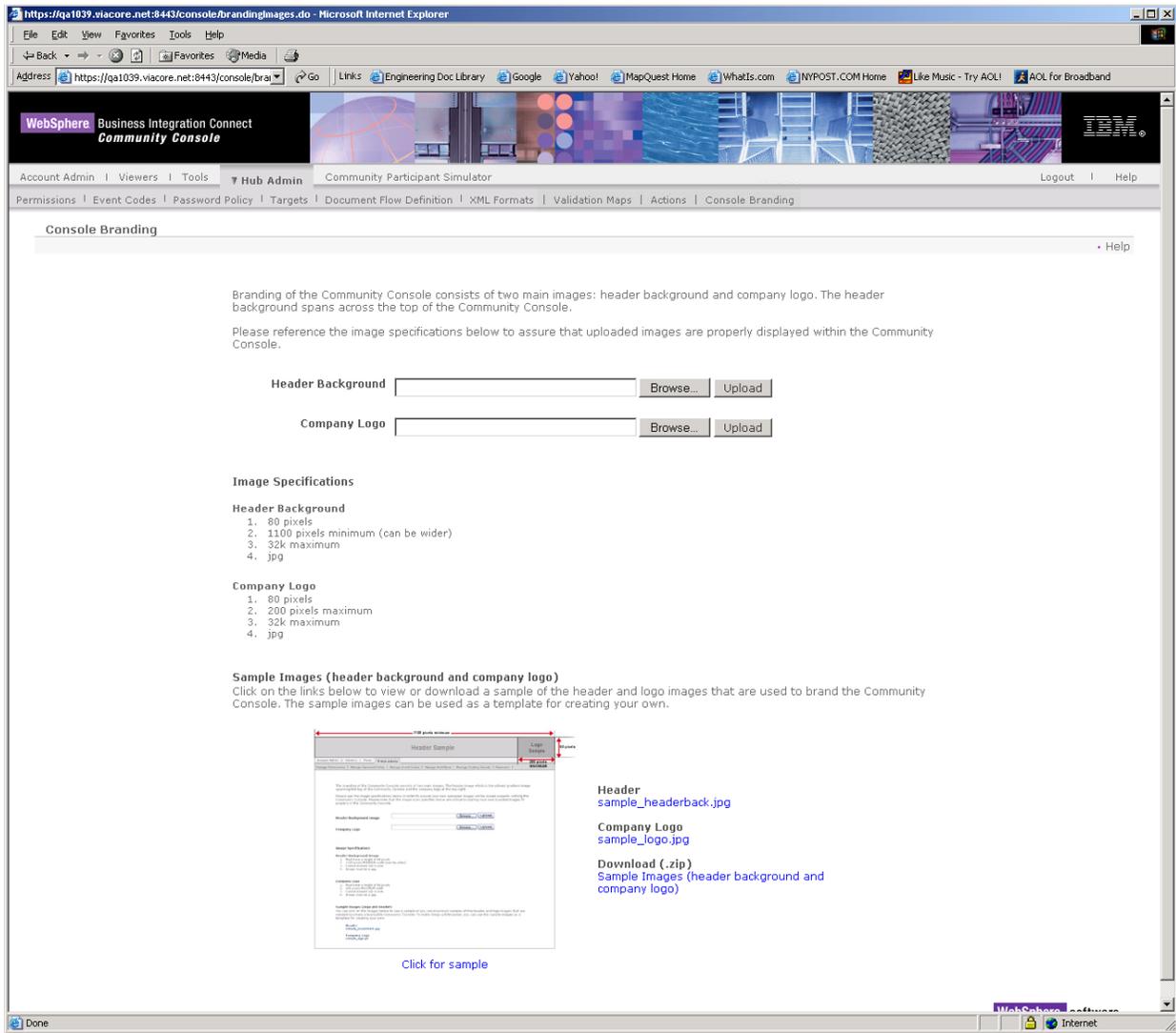


Figure 2-2. Console Branding Screen

2. Scroll down to the **Sample Images** portion of the screen.
3. To view a sample header background image, click the **sample_headerback.jpg** link.
4. To view a sample company logo, click the **sample_logo.jpg** link.
5. To view a sample image, click the **Click for Sample** link or the graphic above it.
6. To download sample images (header background and company logo) in a zip file, click the **Sample Images (header background and company logo)** link.

Uploading a header background and company logo

To upload a header background and company logo, use the following procedure.

1. Click **Hub Admin** on the main menu and **Console Branding** on the horizontal navigation bar. The Console displays the Console Branding screen (see [Figure 2-2 on page 17](#)).
2. In the **Header Background Image** field, type the path and name of the image file you want to use for the header background or browse and select the file.
3. Next to **Company Logo**, type the path and name of the logo file you want to use for the company logo or browse and select the file.
4. Click **Upload**.

NOTE: Replacing the header background and company logo require that the Community Console be restarted for the changes to take effect. See your system administrator to restart the Community Console.

Managing password policy

The Password Policy screen lets you set up the password policy for the Hub community. Using this screen, you can implement a strong password policy that includes limiting a password's life span. The Password Policy screen also allows you to use special characters in the password to prevent susceptibility to dictionary attack. It also lets you prevent the use of passwords that resemble those previously used or passwords that are similar to a user's login or full name.

Viewing and editing password policy details

The following procedure describes how to view password policy details. As part of this procedure, you can change the maximum length, expire time, uniqueness, special character, and name variation checking parameters.

1. Click **Hub Admin** on the main menu and **Password Policy** on the horizontal navigation bar. The Console displays the Password Policy screen (see [Figure 2-3 on page 19](#)).

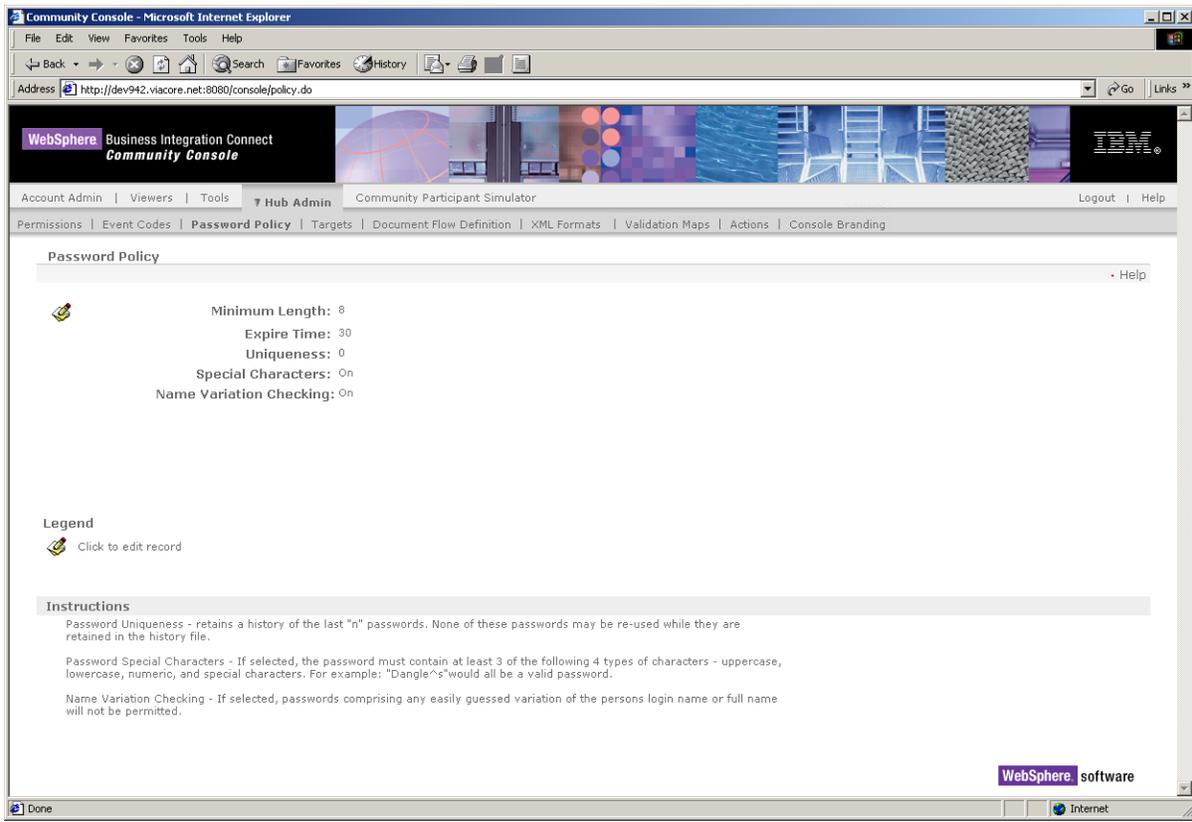


Figure 2-3. Password Policy Screen

2. Click the  icon. The Console displays the Password Policy Details screen (see [Figure 2-4](#) on page 20).

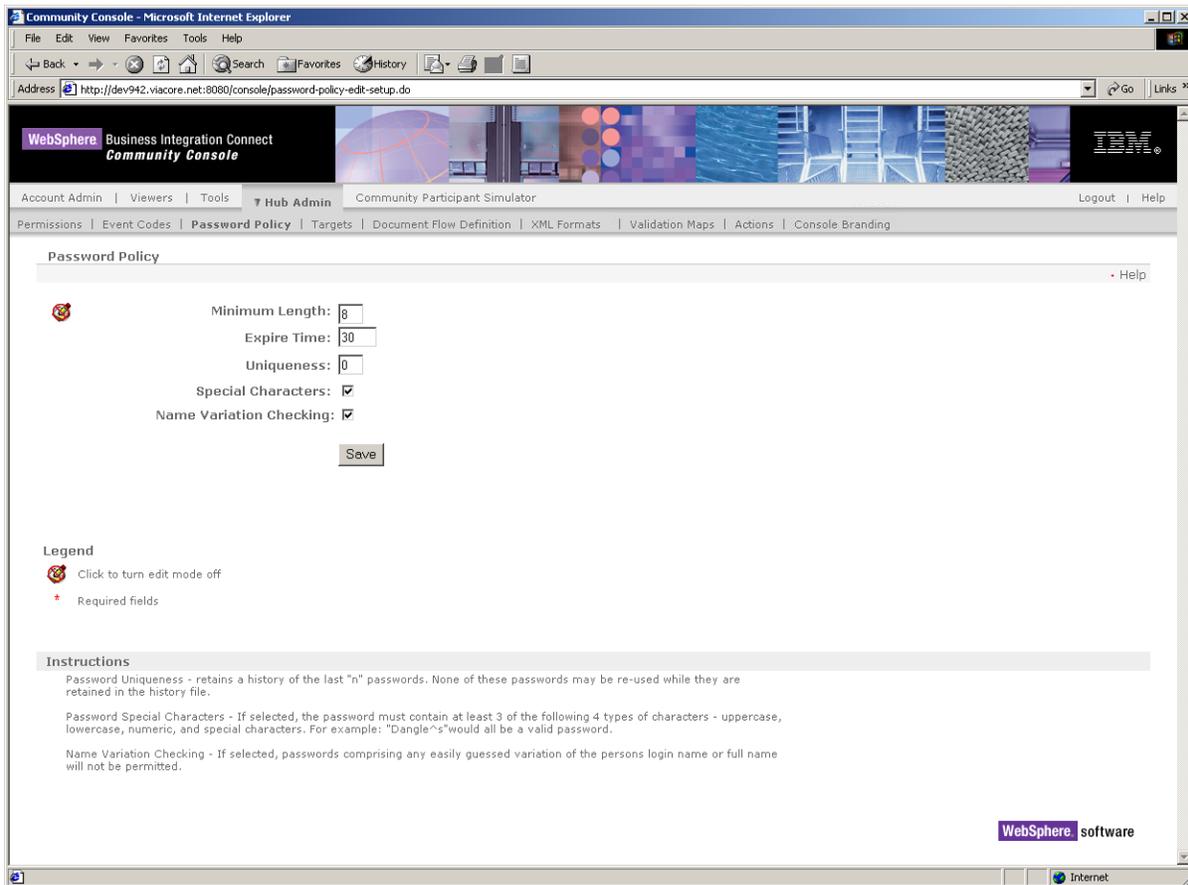


Figure 2-4. Password Policy Details Screen

3. Complete the following parameters in the screen:

Table 2-2. Password Policy Details

Parameter	Description
Minimum Length	Minimum number of characters used for the password.
Expire Time	Number of days until the password expires.
Uniqueness	Retains a numeric history of previously used passwords. An old password cannot be reused if it exists in the history file.
Special Characters	When checked, passwords must contain at least three of the following types of special characters: <ul style="list-style-type: none"> • Upper-case characters • Lower-case characters • Numeric characters • Special characters
Name Variation Checking	When checked, prevents the use of passwords that comprise an easily guessed variation of the user's login or full name.

4. Click **Save**.

Configuring permissions

Permissions represent privileges required for accessing various Console modules. The Community Console provides the Permission List screen to display the following information for each module:

- The name of the module
- The description of the permission
- The status (Enabled or Disabled) of each permission

From the Permission List screen, you can set whether users must have permission to use a module and change the description of the permission descriptions. You cannot, however, define new permissions.

Viewing and editing permission details

The following procedure describes how to view details for a permission. As part of this procedure, you can edit the permission description that is displayed on the Permission List screen and enable or disable the permission.

1. Click **Hub Admin** on the main menu and **Permissions** on the horizontal navigation bar. The Console displays the Permission List screen (see [Figure 2-5 on page 22](#)).

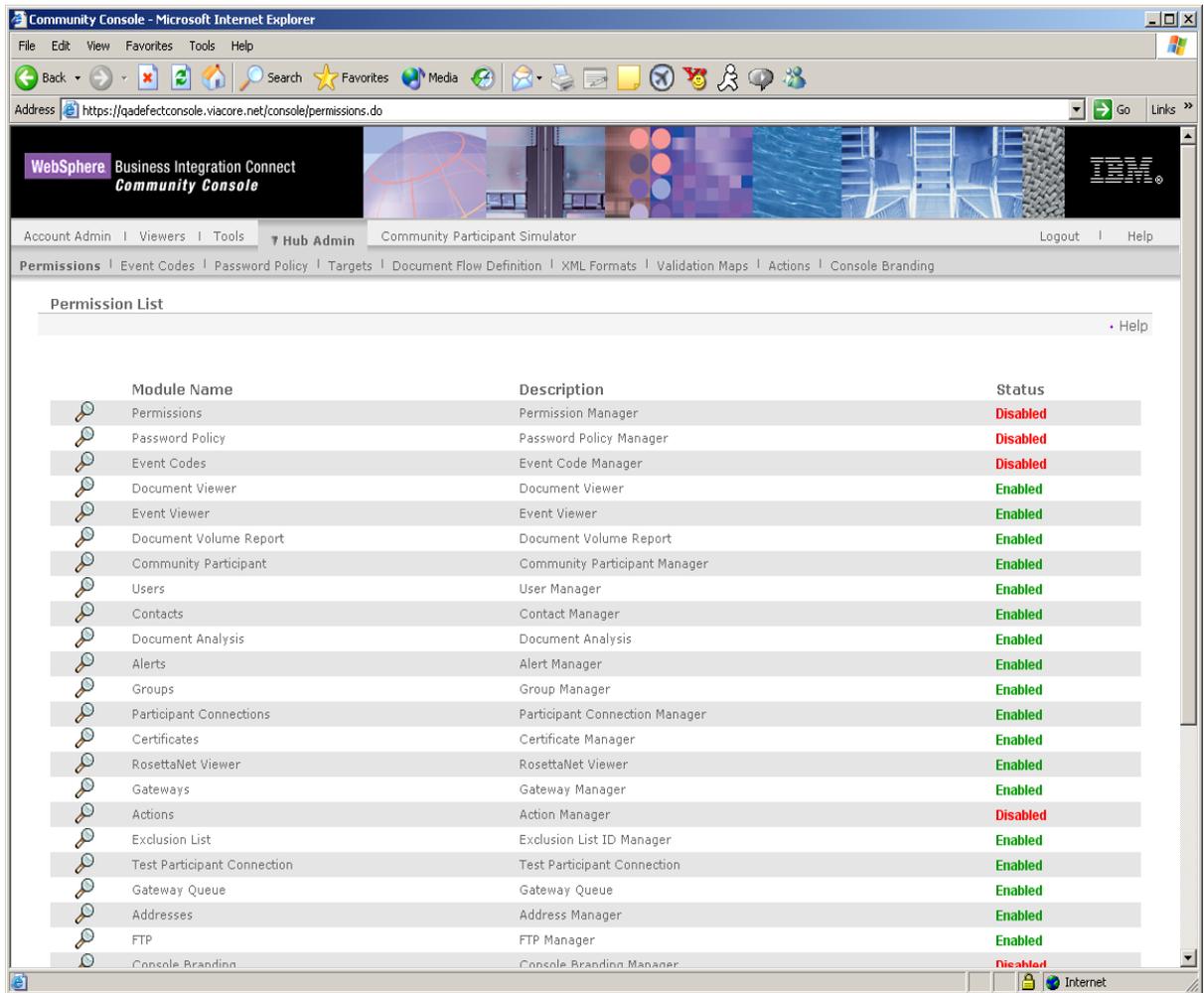


Figure 2-5. Permission List Screen

2. Click the  icon next to the permission whose details you want to view. The Console displays the Permission Detail screen (see [Figure 2-6 on page 23](#)).

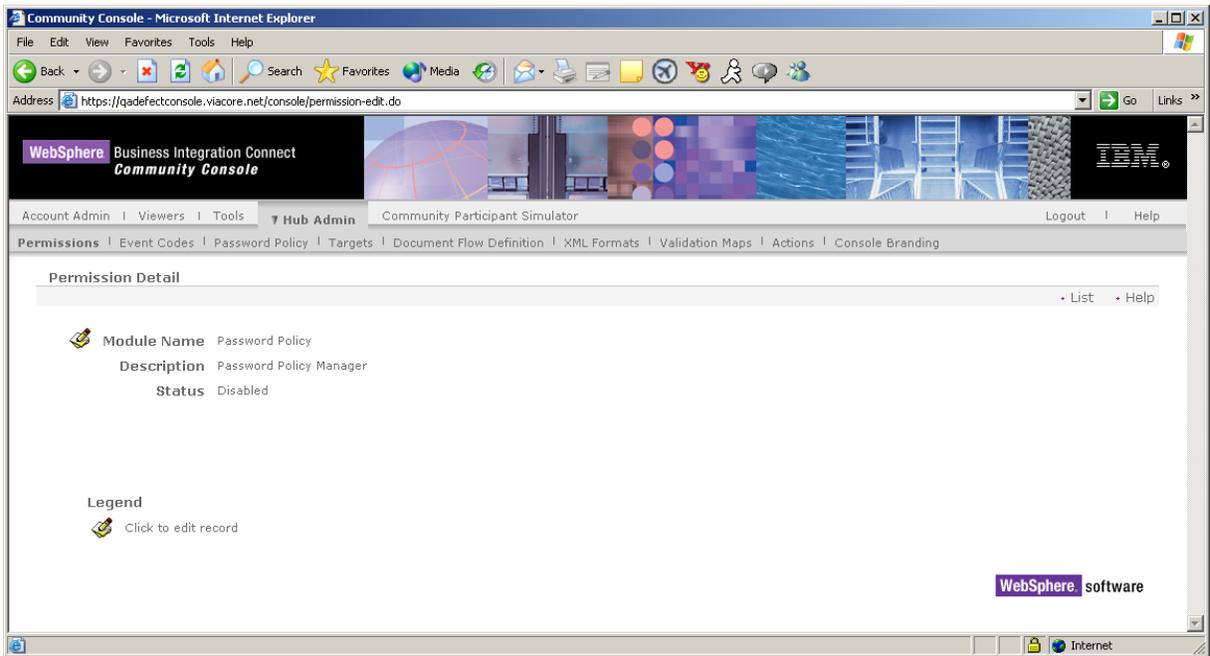


Figure 2-6. Permission Detail Screen

3. To edit the description of the permission you are viewing, click the  icon. The Console displays the Permission Detail screen (see [Figure 2-7](#)).

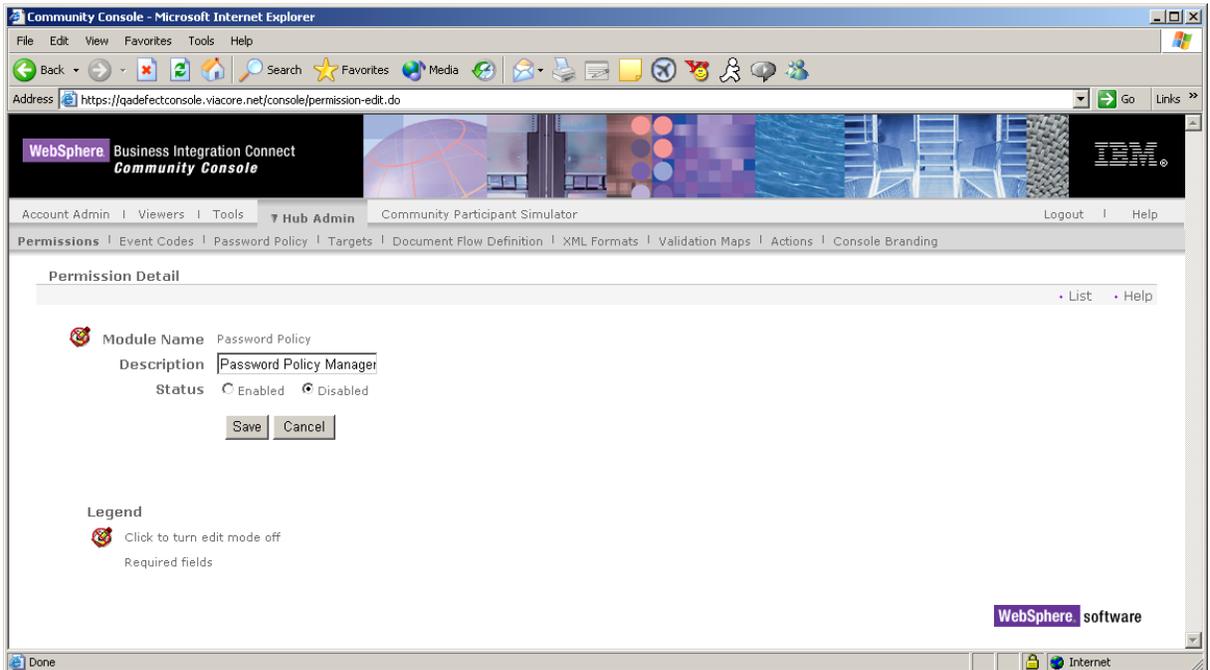


Figure 2-7. Permission Detail Screen

4. Complete the following parameters in the screen:

Table 2-3. Permission Details

Parameter	Description
Module Name	Read-only field that shows the name of the module that corresponds to the permission.
Description	A description of the permission, which is displayed on the Permission List screen.
Status	Enables or disables the permission. <ul style="list-style-type: none">• If enabled, a module can be viewed and access rights controlled by the operator, manager, and participant admin users.• If disabled, the module will not be viewable in the console navigation, and will not appear as a selectable module within the Group Permission screen. (Permissions can also be enabled or disabled directly from the Permission List – see “Enabling or disabling permissions quickly” on page 24).

5. Click **Save**.

Enabling or disabling permissions quickly

You can change the permission status of a module from the Permission List screen by clicking Enabled or Disabled in the status column.

- If enabled, a module can be viewed and access rights controlled by the operator, manager, and participant admin users.
 - If disabled, the module will not be viewable in the console navigation, and will not appear as a selectable module within the Group Permission screen.
1. Click **Hub Admin** on the main menu and **Permissions** on the horizontal navigation bar. The Console displays the Permission List screen (see [Figure 2-5 on page 22](#)).
 2. Click **Enabled** or **Disabled** under the **Status** column on the Permission List screen. If the status is **Enabled**, a dialog box asks whether you want to disable permissions. If the status is **Disabled**, a dialog asks whether you want to enable permissions.
 3. To change the module's permission status, click **OK**. If you click **OK**, the Permission List screen displays the module's new status.

Configuring targets

The Target List screen provides location information that enables the Document Manager to fetch documents from the appropriate system location based on the transport type of the incoming document. You can create separate target configurations based on transport type. The Document Manager can then poll the document repository locations of multiple Web, FTP, and POP mail servers — including internal directories and JMS queues — for incoming documents. Once the Document Manager retrieves a document from the location based on a pre-defined target, the routing infrastructure can process the document based on channel configuration.

Creating a new target

To create a new target for incoming documents, use the following procedure.

1. Click **Hub Admin** on the main menu and **Targets** on the horizontal navigation bar. The Console displays the Target List screen (see [Figure 2-8 on page 25](#)).

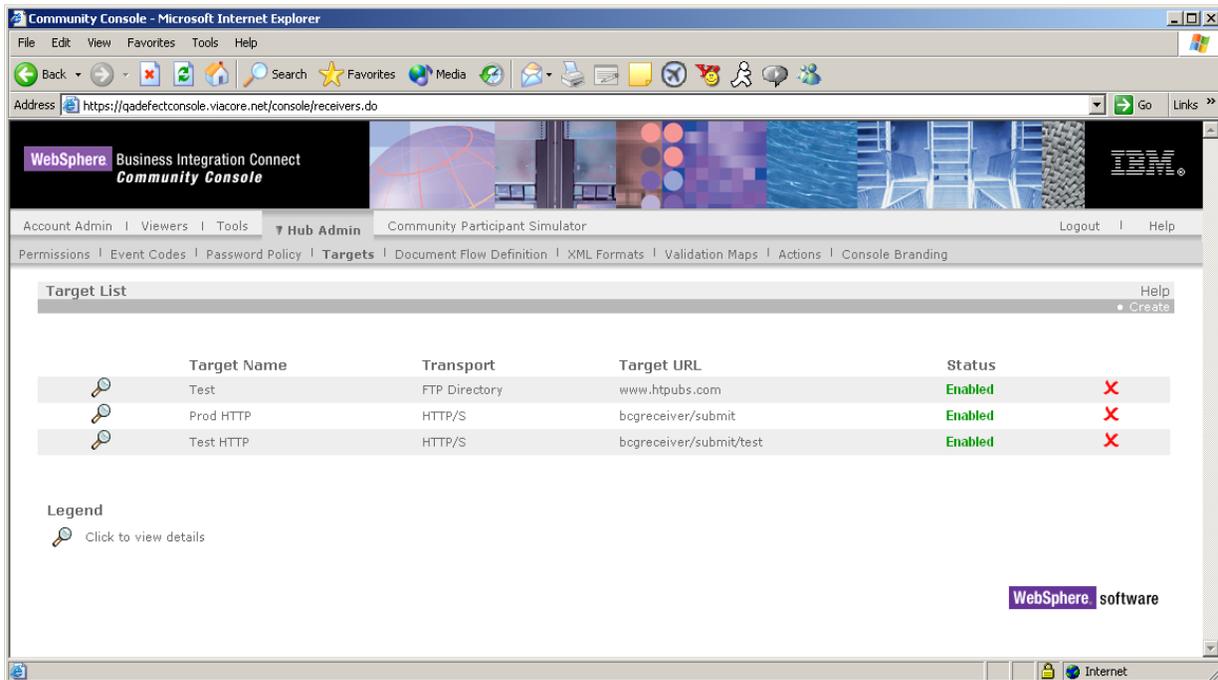


Figure 2-8. Target List Screen

2. Click **Create**. The Console displays the Target Details screen (see [Figure 2-9](#)).

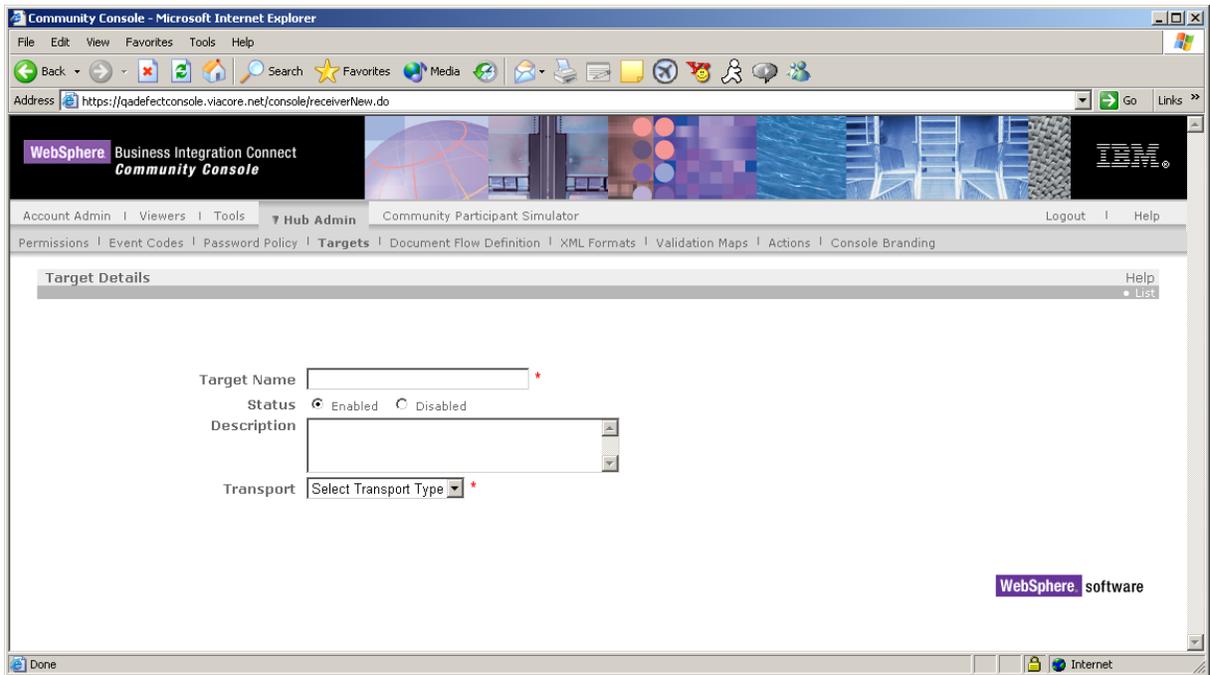


Figure 2-9. Target Details Screen

3. Complete the following parameters in the screen:

Table 2-4. Target Details

Parameter	Description
Target Name	Name used to identify the target.
Status	Allow (Enabled) or deny (Disabled) the system to access this target.
Description	Text that describes the function or other characteristic of this target.
Transport	One of the following transport types: <ul style="list-style-type: none"> • FTP Directory — see “FTP Directory” on page 26 • JMS — see “JMS” on page 27 • POP3 — see “POP3” on page 28 • HTTP/S — see “HTTP/S” on page 29 • File Directory — see “File Directory” on page 29

FTP Directory

If you selected **FTP Directory** as the transport, perform the following procedure.

1. Complete the following parameters in the screen:

Table 2-5. FTP Directory

Parameter	Description
FTP Root Directory	Location of the root directory where the FTP directory tree will be built. For example: /data/router/ftp
File Unchanged Interval	Number of seconds the file size must remain unchanged before the Document Manager retrieves it for processing.
Thread Nbr	Number of documents the Document Manager will process simultaneously.
Exclude File Ext	File extension for documents the Document Manager will exclude from processing. Examples may include exe, txt, or doc.

2. Click **Add**. The Document Manager ignores all documents with the displayed file extension. Click **Remove** to delete a file extension from the exclusion list.

NOTE: Do not type a dot in front of the file name extension (for example, .exe or .txt). Just type the characters that denote the file extension.

3. (Optional) Configure the schedule the Document Manager uses to poll documents from the FTP directory.
4. Click **Save**.

JMS

If you selected **JMS** as the transport, perform the following procedure.

1. Click **new** to create the required Gateway Type for this target. All incoming documents to this target will be assigned the displayed Gateway Type. To change an existing Gateway Type, click **edit**.

2. Complete the following parameters in the screen:

Table 2-6. JMS Values

Parameter	Description
JMS Provider URL	URL of name service used to find JMS queue. Examples: JMS WebSphere MQ - file:/D:/JNDI-Directory JBoss - jnp://hplxdev2:1099
User Id	User ID required to access JMS queue. Leave blank if not used.
Password	Password associated to user ID above. Leave blank if not used.
JMS Queue Name	Name of JMS queue.
JMS Factory Name	Name of Java™ class the JMS provider will use to generate connection to JMS queue.
Provider URL Package	Name of classes (or JAR file) that Java uses to understand JMS Context URL.
JNDI Factory Name	Factory name used to connect to name service.
Time Out	Number of milliseconds that target will monitor JMS queue.
Thread Nbr	Number of documents the Document Manager will process simultaneously.

3. Click **Save**.

POP3

If you selected **POP3** as the transport, perform the following procedure.

1. Click **new** to create the required Gateway Type for this target. All incoming documents to this target will be assigned the displayed Gateway Type. To change an existing Gateway Type, click **edit**.

2. Complete the following parameters in the screen:

Table 2-7. POP3 Values

Parameter	Description
POP3 Server	The name of the POP3 server to be used.
Port Number	Port number assigned to POP3. The default value is recommended.
User Id	User ID required to access port. Leave blank if not used.
Password	Password associated to user ID above. Leave blank if not used.
Time Out	Number of milliseconds that target will monitor the URI.
Thread Nbr	Number of documents the Document Manager will process simultaneously.

3. (Optional) Configure the schedule the Document Manager uses to poll documents from the directory.
4. Click **Save**.

HTTP/S

If you selected **HTTP/S** as the transport, perform the following procedure.

1. Click **new** to create the required Gateway Type for this target. All incoming documents to this target will be assigned the displayed Gateway Type. To change an existing Gateway Type, click **edit**.
2. For **URI**, type the Web address for incoming documents. This address must start with /bcgreceiver. Example: /bcgreceiver/Receiver
3. For **Max Sync Timeout**, type the number of milliseconds a synchronous connection will remain open. For **Max Sync Sim Conn**, type the maximum number of synchronous connections the system will allow.

NOTE: Sync Routing values are global across all HTTP/S targets. Changing these values for a single HTTP/S target affects all HTTP/S targets in the system.

4. Click **Save**.

File Directory

If you selected **File Directory** as the transport, perform the following procedure.

1. Click **New** to create the required gateway type for this target. Note that you can change an existing gateway type by clicking **Edit**.

2. Complete the following parameters in the screen:

Table 2-8. File Directory Values

Parameter	Description
Document Root Path	Location of the root directory where the directory tree will be built.
Poll Interval	Number of seconds the document manager will use for polling documents from the directory.
File Unchanged Interval	Number of seconds the file size must remain unchanged before the Document Manager retrieves it for processing.
Thread Nbr	Number of documents the Document Manager will process simultaneously.

3. (Optional) Configure the schedule the Document Manager uses to poll documents from the directory.
4. Click **Save**.

Viewing and editing target details

The following procedure describes how to view details for a target. As part of this procedure, you can edit the target's parameters.

1. Click **Hub Admin** on the main menu and **Targets** on the horizontal navigation bar. The Console displays the Target List screen (see [Figure 2-8 on page 25](#)).
2. Click the  icon next to the target whose details you want to view. The Console displays the Target Details screen (see [Figure 2-10 on page 31](#)).

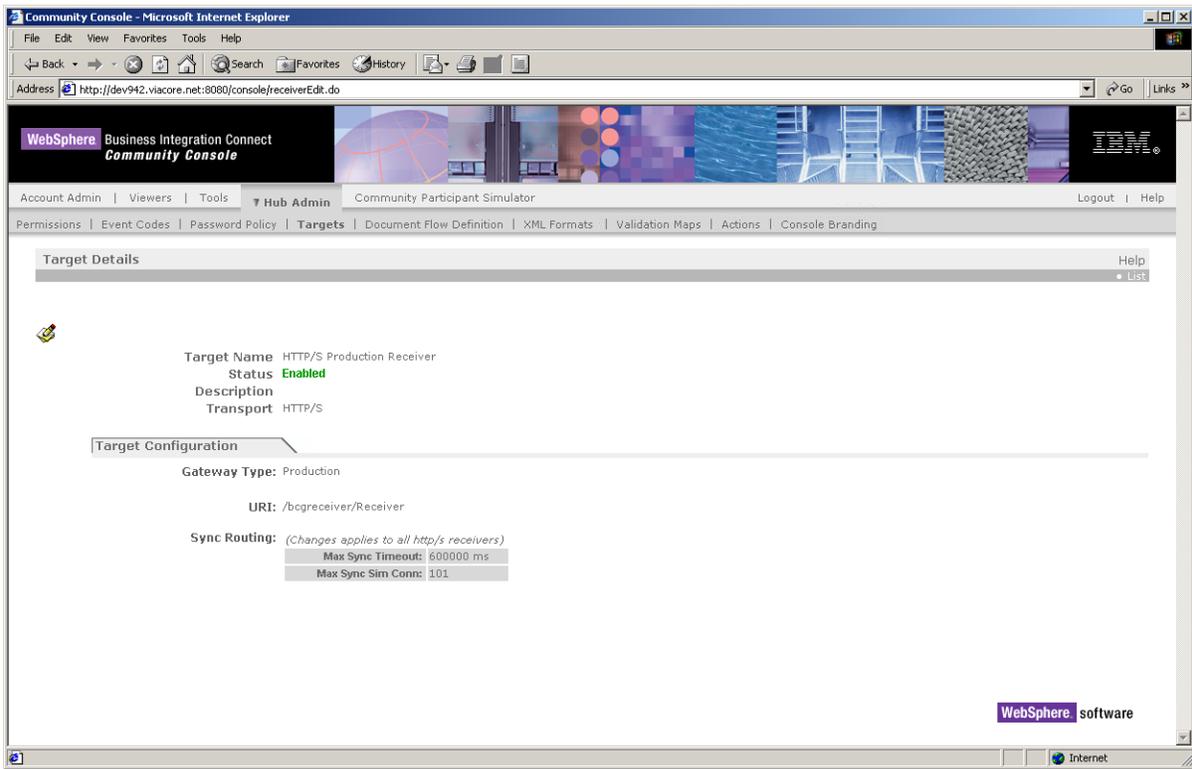


Figure 2-10. Target Details Screen

3. To edit the parameters of the target, click the  icon. The Console displays the Target Details screen (see [Figure 2-11 on page 32](#)).

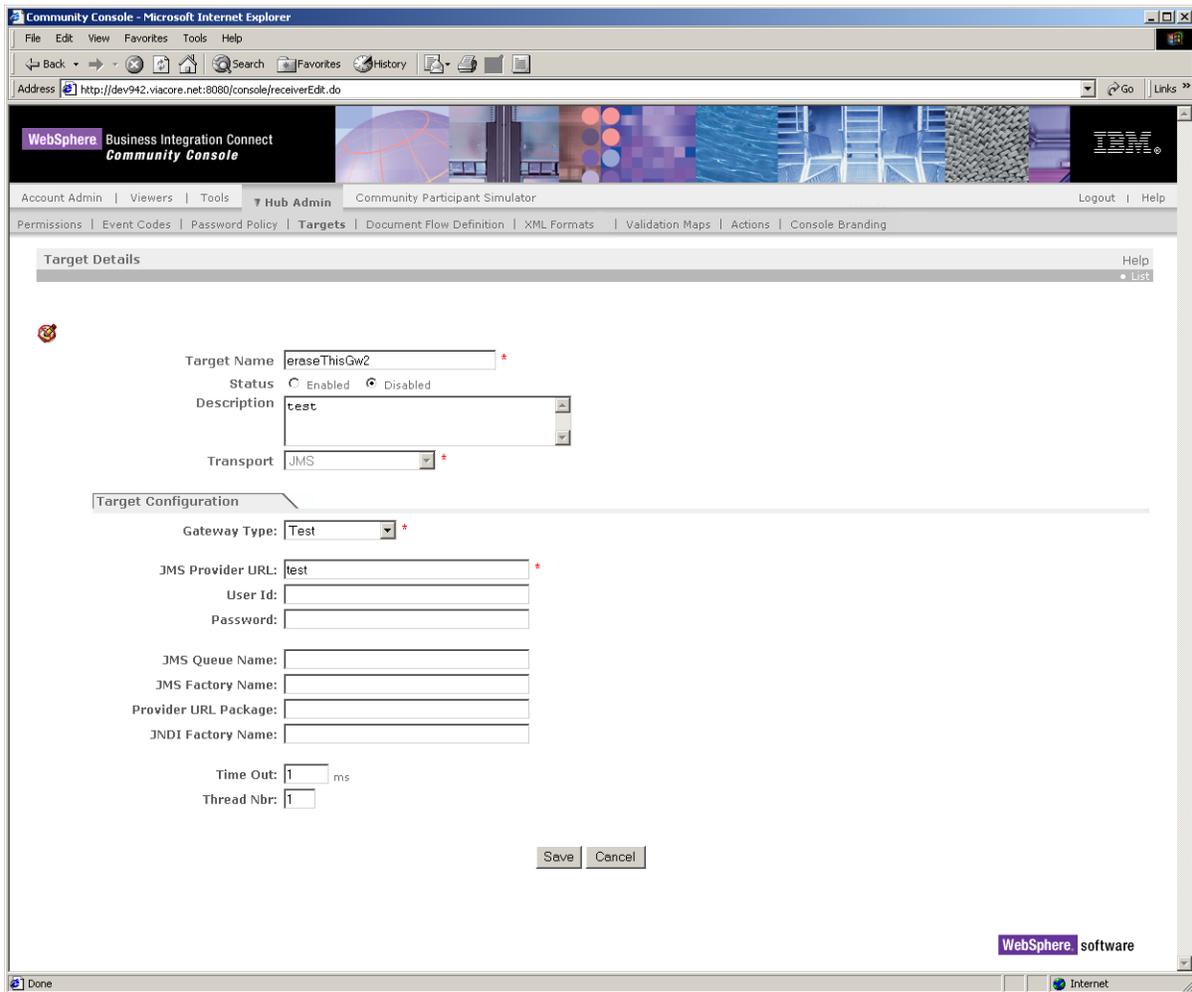


Figure 2-11. Screen for Editing a Target

4. Complete the parameters in the screen (see [Table 2-4 on page 26](#)) and the appropriate target configuration screen ([Table 2-5 on page 27](#), [Table 2-6 on page 28](#), [Table 2-8 on page 30](#), or [Table 2-7 on page 29](#)).
5. Click **Save**.

Enabling or disabling targets

You can enable or disable targets from the Target List screen by clicking **Enabled** or **Disabled** in the **Status** column. To do this:

1. Click **Hub Admin** on the main menu and **Targets** on the horizontal navigation bar. The Console displays the Target List screen (see [Figure 2-8 on page 25](#)).
2. Click **Enabled** or **Disabled** next to the target whose status you want to change.

Deleting targets

You can delete targets that you do not need anymore. Note that the deletion occurs immediately. There is no warning message asking you to confirm this step.

1. Click **Hub Admin** on the main menu and **Targets** on the horizontal navigation bar. The Console displays the Target List screen (see [Figure 2-8 on page 25](#)).

NOTE: The target in the following step is immediately deleted without a warning message. Be sure that you want to delete the target.

2. Click the  icon next to the target you want to delete.

Configuring Document Flow Definitions and download packages

A Document Flow Definition is a collection of “meta-information” that defines the document-processing capabilities of the system. For the system to process a business document, two or more Document Flow Definitions must be linked to create a node. A node contains all the necessary information the system needs to receive, process, and route documents to the hub-community.

Because of the many different types of business processes, protocols, and delivery standards available in the B2B industry, the system can contain different node configurations to meet the various business-processing requirements of the Community Manager and Participants. To ensure that the system meets these requirements, the Console’s Document Flow Definition module is used to create each Document Flow Definition, define its capabilities, and link them together to create nodes. By creating multiple nodes, the system can meet the document-processing needs of the entire hub-community.

Understanding Document Flow Definitions

The following sections describe the theory of operation behind Document Flow Definitions.

Business Integration Connect has the following types of Document Flow Definitions to define its document-processing capabilities:

- **Package** — specifications describing document format, packaging, encryption, and content-type identification.
- **Protocol** — structure and location of information within the document needed for processing and routing.
- **Document Flow** — the business transaction between the Community Manager and Participant. A business transaction may contain multiple documents.

- Activity — the business function a Document Flow performs.
- Action — the actual electronic documents exchanged in the business transaction.

For convenience, WebSphere Business Integration Connect contains several pre-configured Document Flow Definitions. [Table 2-9](#) lists the preconfigured Document Flow Definitions.

Table 2-9. Preconfigured Document Flow Definitions

Package	
AS1	Applicability Statement 1 standard
AS2 1.0 / 1.1	Applicability Statement 2 standard
Backend Integration	Proprietary standard used for custom back-end integration
Protocol	
Binary	General use protocol used for pass-through routing of binary documents requiring no validation or transformation
XML Event	General protocol used for custom back-end integration
Document Flow	
Binary	Document flow used for pass-through routing of binary documents
XML Event	Document flow used for routing custom document status events

Document Flow Definition components

Each Document Flow Definition has the following components:

- Definition — to contain the name, version, Document Flow Type, and a general description of the Document Flow Definition.
- Attributes — to contain information about the Document Flow Definition's functionality. The system uses the attribute information to perform various document-processing and routing functions such as validation, checking for encryption, and retry count.
- Context — to identify other Document Flow Definitions linked together to form a node. The complete node is what defines the capabilities (or Document Flow Definition context) of the system for the routing and processing of incoming documents.

If you create a new Document Flow Definition, you must define all three components before the system can use the Document Flow Definition to create connections

Document Flow Definition interaction

Once Document Flow Definitions are created and linked to form nodes, the interaction between various nodes determines what connections the system creates between the Community Manager and Participants. This interaction between nodes provides the mechanism for the system to perform document transformation, validation, and pass-through routing.

Creating Document Flow Definitions

Creating Document Flow Definitions involves the following steps:

1. Creating a custom Document Flow Definition or uploading a complete node. See [“Creating custom definitions,”](#) below.
2. Setting attributes. See [“Setting Document Flow Definition attributes”](#) on page 42.
3. Editing attribute values. See [“Editing attribute values”](#) on page 45 and [“Editing RosettaNet values”](#) on page 45.
4. Enabling the Document Flow Definition. See [“Enabling a Document Flow Definition”](#) on page 46.
5. Creating Document Flow Definition interactions. See [“Creating document flow interactions”](#) on page 46.

Creating custom definitions

To manually create Document Flow Definitions for RosettaNet Partner Interface Processes (PIPs) and custom XML processes, use the following procedure.

TIP: Use the pre-installed binary package as an example when creating a simple Document Flow Definition.

1. Click **Hub Admin** on the main menu and **Document Flow Definition** on the horizontal navigation bar. The Console displays the Document Flow Definitions screen (see [Figure 2-12 on page 36](#)).

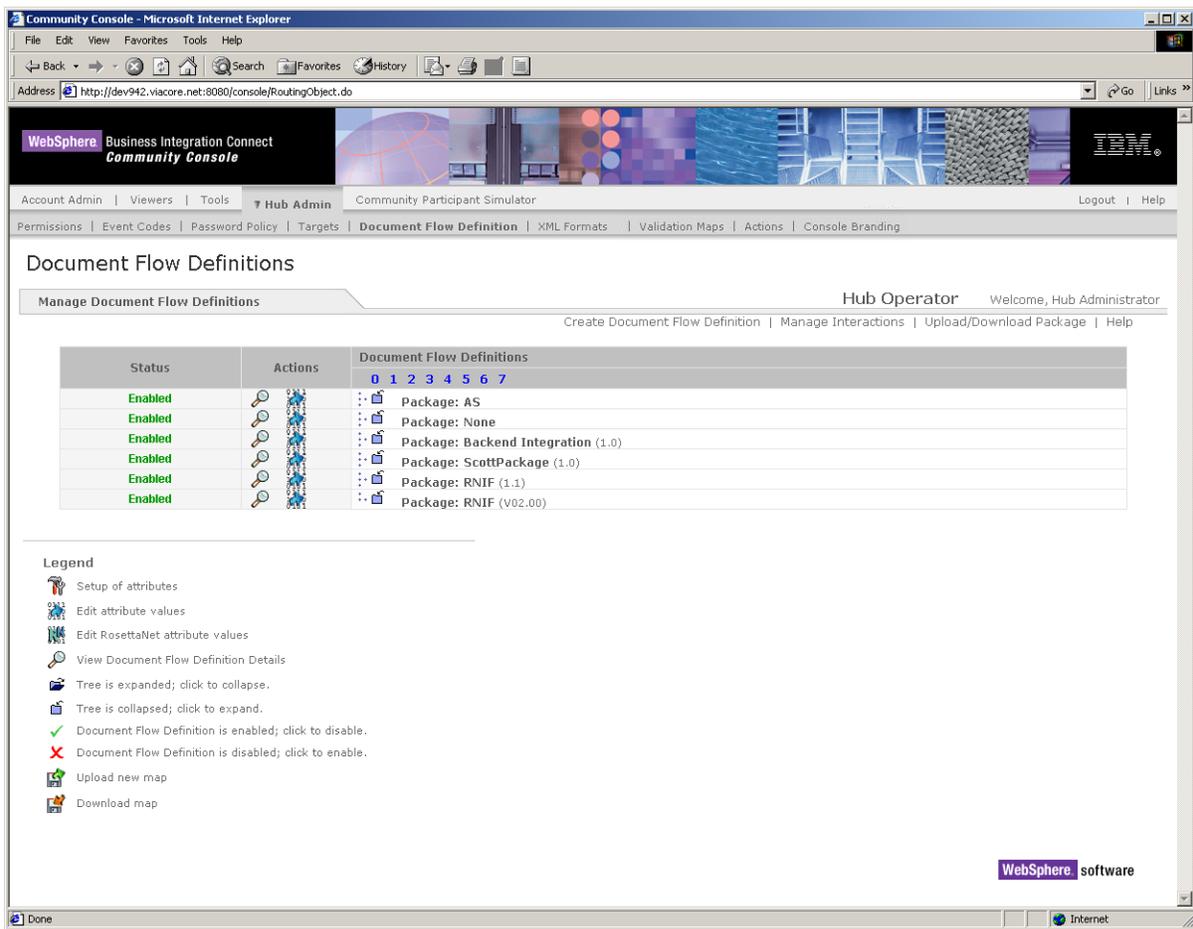


Figure 2-12. Document Flow Definitions Screen

2. Click **Create Document Flow Definition**. The Console displays the Manage Document Flow Definitions screen (see [Figure 2-13 on page 37](#)).

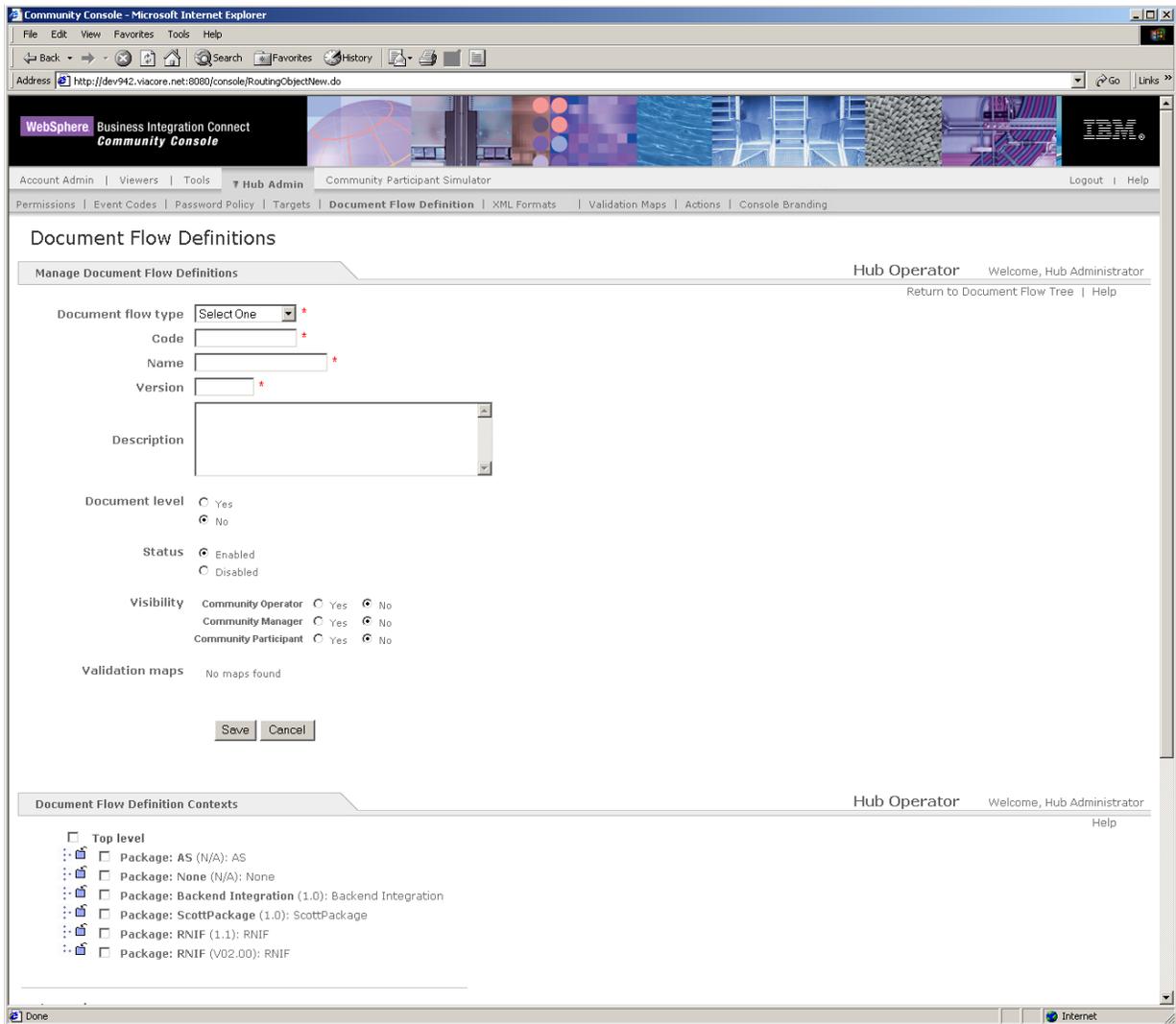


Figure 2-13. Manage Document Flow Definitions Screen

3. Complete the following parameters in the screen:

Table 2-10. Document Flow Definition Contents

Parameter	Description
Document Flow type	<p>Select Package, Protocol, document flow, Activity, or Action:</p> <ul style="list-style-type: none"> • Package – specifications describing document format, packaging, encryption, and content-type identification. • Protocol – structure and location of information within the document needed for processing and routing. • Document Flow – the required order of sub-transactions needed to complete a business transaction. • Activity – the business function a process performs. • Action – the source document sent in a document flow. • Signal – the document sent in response to an action.
Code	<p>Codified value of what object is in document content. For example:</p> <ul style="list-style-type: none"> • Protocol: RNSC, RosettaNet, or Binary. • Document Flow: 2A12, 3A4, 7B6, etc. • Activity, Action, and Signal: Use the value specified in the RosettaNet PIP specification. <p>For Activity and Action, Document Flow Definitions, Code and Name must be the same value.</p>
Name	<p>Name used to identify Document Flow Definition. For Activity and Action, Document Flow Definitions, the Code and Name must be the same value.</p>
Version	<p>Version of Document Flow Definition found in document content (for example, V02.00, 1.1).</p>
Description	<p>Text that describes function of Document Flow Definition.</p>
Document level	<p>Limits the system to create interactions only at the Document Flow level. An interaction or connection created at a level other than the Document Flow level will not function.</p> <p>Select Yes if the Document Flow Definition you are creating represents the Document Flow in the node hierarchy. Examples include: 3A4, 3B7, 0A1, and Binary.</p> <p>Select No for all other definition levels within the node: Package, Protocol, Activity, Action, and Signal.</p>
Status	<p>Select Enabled to make Document Flow Definition available to the system.</p>
Visibility	<p>Select Console visibility based on user type. For more information about user types, see the online help topic “Creating custom definitions.”</p>
Validation maps	<p>Displays the validation map associated to this definition. The Console displays the message “No maps found” until a validation map has been assigned.</p>

NOTE: Outbound EDI from Manager to Participant must use the Backend Integration rather than the None package. This is because the EDI message is sent as binary data, and the None package does not have any HTTP custom headers. The HTTP custom headers tell the Document Manager how to route the message.

If using a custom XML protocol in a Backend Integration package, the Document Manager overrides the protocol and uses the x-aux values contained in the document HTTP/S header to determine the protocol, protocol version, process, and process version (see the example below). However, if using a custom XML format combined with a non Backend Integration package such as AS1, AS2, None, or RNIF, the system determines the protocol, protocol version, process, and process version from the element path defined in the XML format guideline.

Example HTTP/S header:

```
From HTTP/S Post set headers=%headers% x-aux-protocol: XML x-aux-protocol-version:
1.0 x-aux-sender-id: 987654321 x-aux-receiver-id: 102420488 x-aux-process-type:
XML_DTD x-aux-process-version: 1.0 x-aux-production: true x-aux-system-msg-id:
GWYN_OBID_H2_DTD_00000004
```

4. For **Document Flow Definition Contexts**, select a higher level Document Flow Definition with which this definition will be associated to create a node.
-

NOTE: Document flow definition contexts must be in the appropriate top-down order for the node to work:

1. Package
 2. Protocol
 3. Document Flow
 4. Activity
 5. Action
 6. Signal
-

5. Click **Save**.

Uploading and downloading a package

To upload a Document Flow Definition package, use the following procedure.

NOTE: To upload RosettaNet Implementation Framework (RNIF) PIPs, upload the following packages:

- Package_RNIF_1.1.zip
- Package_RNIF_V02.00.zip
- Package_RNSC_1.0_RNIF_1.1.zip
- Package_RNSC_1.0_RNIF_V02.00.zip

These packages were installed when you installed Business Integration Connect. They reside in the directory `./B2BIntegrate`. After you upload these packages, you can upload RNIF PIPs.

1. Click **Hub Admin** on the main menu and **Document Flow Definition** on the horizontal navigation bar. The Console displays the Document Flow Definitions screen (see [Figure 2-12 on page 36](#)).
2. Click **Upload/Download Package**. The Console displays the Upload/Download Packages screen (see [Figure 2-14](#)).

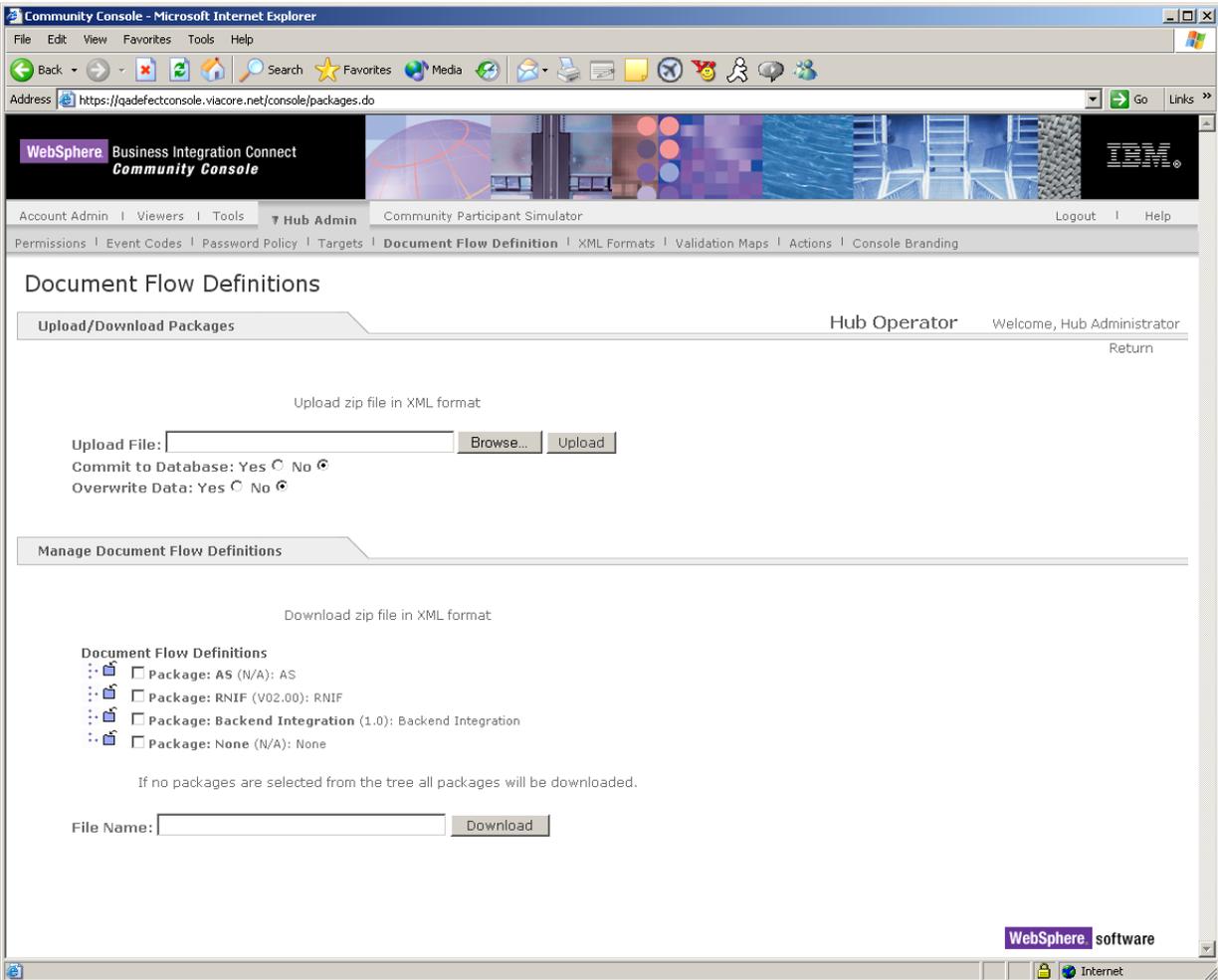


Figure 2-14. Upload/Download Packages Screen

- Complete the following parameters in the screen:

Table 2-11. Upload/Download Package

Parameter	Description
Upload File	Type the path and name of the ZIP archive you want to use for the company logo or browse and select the file. The file within the ZIP archive must be within a directory titled Packages. For example: Packages/AS1.xml.
Commit to Database	Click Yes or No : <ul style="list-style-type: none"> Click Yes to upload the PIP package into the system database. Click No to upload the PIP package in test mode (package is not installed) and use the system-generated messages displayed in the Messages box to troubleshoot upload errors.
Overwrite Data	Click Yes to replace a package currently in the database or No to add the package to the database.

- Click **Upload**. The package is installed into the system.

NOTE: When a new PIP is uploaded, the attribute values for that PIP does not replace the values of the same attributes that already exist at the protocol and package level. However, if the uploaded PIP contains attributes are not present in the existing protocol or package level, the attributes are added.

Downloading a package to a local computer

To download a package to a local computer, use the following procedure.

- Click **Hub Admin** on the main menu and **Document Flow Definition** on the horizontal navigation bar. The Console displays the Document Flow Definitions screen (see [Figure 2-12 on page 36](#)).
- Click **Upload/Download Package**. The Console displays the Upload/Download Packages screen (see [Figure 2-14 on page 40](#)).
- Click the  icon and expand the node to the appropriate Document Flow Definition. Select the box for the Document Flow Definition you want to download. To download all packages, leave all boxes unchecked.
- For **File Name**, type a name for the zip archive that contains the Document Flow Definition data.
- Click **Download** to download the ZIP archive to the destination desired.

NOTE: When extracting the files from the ZIP archive, use the Extract feature in the ZIP application to maintain the files in their proper directory structure. This guarantees that the files can be successfully uploaded to the system after making any modifications.

When a new PIP is uploaded, the attribute values for that PIP does not replace the values of the same attributes that already exist at the protocol and package level. However, if the uploaded PIP contains attributes are not present in the existing protocol or package level, the attributes are added.

Setting Document Flow Definition attributes

Attributes are the information that gives the Document Flow Definition its functionality. The system uses the attribute information for various document processing and routing functions such as validation, checking for encryption, and retry count.

To increase the efficiency of managing Document Flow Definitions and nodes, the attributes for a particular Document Flow Definition can be inherited by the lower level Document Flow Definitions within a node in a hierarchical (top-down) fashion. The highest level Document Flow Definition is the Package, and package attributes are considered global since they can be inherited by all the other Document Flow Definitions within the node. The following illustrates the hierarchical relationship of the Document Flow Definitions within a single node:



Attributes set at the Package level are inherited by the Protocol, Document Flow, Activity, Action, and Signal levels automatically. If Package-level attributes have been set and their values defined, the system applies those same attributes to all the lower level definitions in that same node automatically, even though you have not defined the lower level attributes.

You can override inherited attributes by setting and adding values to the lower level definitions individually. For example, an attribute set at the Package level can be changed at the Protocol or Document Flow levels. Due to the inherited nature of attributes, an attribute that is changed at the Protocol level is inherited by the lower Document Flow, Activity, Action, and Signal levels.

When creating a new Document Flow Definition, the attributes associated with the Document Flow Definition must first be defined. After the attribute is defined, the actual values for the attribute can be added.

NOTE: All attributes are set with default values for the pre-installed and uploaded RosettaNet PIP packages. Use of the default values is recommended.

To set Document Flow Definition attributes, use the following procedure.

1. Click **Hub Admin** on the main menu and **Document Flow Definition** on the horizontal navigation bar. The Console displays the Document Flow Definitions screen (see [Figure 2-12 on page 36](#)).
2. Click the  icon to individually expand a node to the appropriate Document Flow Definition level or select a number from 0-7 to expand all displayed Document Flow Definition nodes to the selected level.
3. Click the  icon to view the attributes for the selected Document Flow Definition.
4. Under **Document Flow Definition Contexts**, perform one of the following steps:
 - Select attributes from a pre-defined list. See [“Selecting attributes from a list,”](#) below.
 - Copy attributes from a Document Flow Definition at a similar hierarchical level within the same node into a new Document Flow Definition. See [“Cloning from an existing object in the current context,”](#) below.

Selecting attributes from a list

To select attributes from a list, use the following procedure.

1. Click **Select attributes from a list**.
2. Click the  icon to view the attribute list.
3. Select the attributes that will be used for this Document Flow Definition. If an attribute is selected that matches the attribute of the Document Flow Definition above it in the same node, the attribute values of the higher level Document Flow Definition is inherited.
4. Click **Save**.

Cloning from an existing object in the current context

The following procedure describes how attributes from a Document Flow Definition at a similar hierarchical level within the same node can be copied into a new Document Flow Definition. For example, the attributes for the RNSC protocol can only be cloned from another protocol, such as RosettaNet or CanonicalXML, if they exist within the same package (node). However, the Console also displays all the nodes in the system where that same Document Flow Definition is used. For example, if RNSC is used as a protocol in the AS and Backend Integration packages, the Console displays both of those nodes and their corresponding definitions as options from which to clone.

1. Click **Clone from an existing object in this context**.
2. Click the  icon to view the attribute list.
3. Under **Document Flow Definition Peers**, click **Clone** for the document flow definition you want to clone. The attributes are added to the new Document Flow Definition.

NOTE: The selected Document Flow Definition must be enabled to copy its attributes.

For all two-way PIPS such as a 3A4, the system uses the following attributes for the confirmation action:

- Time To Acknowledge,
- Retry Count
- Signature Required
- Encryption
- Validation Map

All other attributes selected are ignored.

Editing attribute values

After you define the attributes for a Document Flow Definition, use the following procedure to edit the values for each attribute.

1. Click **Hub Admin** on the main menu and **Document Flow Definition** on the horizontal navigation bar. The Console displays the Document Flow Definitions screen (see [Figure 2-12 on page 36](#)).
2. Click to individually expand a node to the appropriate Document Flow Definition level or select a number from 0-7 to expand all displayed Document Flow Definition nodes to the selected level.
3. Under **Actions**, click the  icon adjacent to the Document Flow Definition whose attributes have been previously defined. The Console displays a list of defined attributes under **Document Flow Context Attributes**.
4. Select the appropriate attribute values in the **Update** column or click the box under the **Reset** column to return the attribute value to its default setting.
5. Click **Save**.

Editing RosettaNet values

After you define the attributes for a Document Flow Definition, use the following procedure to edit the RosettaNet values.

1. Click **Hub Admin** on the main menu and **Document Flow Definition** on the horizontal navigation bar. The Console displays the Document Flow Definitions screen (see [Figure 2-12 on page 36](#)).
2. Click to individually expand a node to the appropriate Document Flow Definition level or select a number from 0-7 to expand all displayed Document Flow Definition nodes to the selected level.
3. Under **Actions**, click the  icon adjacent to the Document Flow Definition whose attributes have been previously defined. The Console displays a list of defined attributes under **RosettaNet Attributes**.
4. Complete the following parameters under **RosettaNet Attributes**. (These attributes are defined automatically when a PIP is uploaded to the system.)

NOTE: If the Console displays the message “No attributes were found,” the attributes have not been defined. See [“Setting Document Flow Definition attributes” on page 42](#) for information about how to define attributes.

If the Console displays this message for a lower-level definition, the definition may still work, since it inherits the attributes of the higher level definition. Adding attributes and their values overrides the inherited attributes, changing its functionality.

5. Click **Save**.

Enabling a Document Flow Definition

To activate or deactivate a Document Flow Definition, use the following procedure.

1. Click **Hub Admin** on the main menu and **Document Flow Definition** on the horizontal navigation bar. The Console displays the Document Flow Definitions screen (see [Figure 2-12 on page 36](#)).
2. Click to individually expand a node to the appropriate Document Flow Definition level or select a number from 0-7 to expand all displayed Document Flow Definition nodes to the selected level.
3. Under the **Status** column, click **Enabled** to place the Document Flow Definition offline or **Disabled** to place the Document Flow Definition online.

NOTE: If a package Document Flow Definition is disabled, all lower-level Document Flow Definitions in that node are also disabled, regardless of whether their individual status was enabled.

If a lower-level Document Flow Definition is disabled, all remaining definitions within the same package remain enabled.

If a Document Flow Definition is disabled, all preexisting connections and attributes continue to work. The disabled Document Flow Definition only restricts the creation of new connections.

4. When a message asks whether you are sure, click **OK** to proceed or **Cancel** to abort.

Creating document flow interactions

The Document Flow Definitions screen provides a **Manage Interactions** link that lets you create the mechanism the system uses for transforming one Document Flow Definition into another. By creating interactions between similar document flows using different protocols, the system can transform for example, a Participant's purchase order request in their proprietary XML format to a RosettaNet 3A4 purchase order request used by the Community Manager.

Once the interactions are created in the system for all the documents being exchanged between the Community Manager and Participants, the system automatically creates a connection between the Manager and Participant for each Document Flow Definition their internal systems are capable of supporting.

Each Participant in the hub-community uses B2B Capabilities to define the Document Flow Definitions their internal systems are able to support (see the WebSphere Business Integration Connect Community Console User Guide for information about using B2B Capabilities).

Creating a document flow interaction is based on two guidelines:

- A document flow interaction must be created for every action. An individual document (or message) exchanged in a document flow. (or document) that is exchanged within a document flow if each document requires a transformation map.
- A document flow interaction is required for any transaction requiring a connection between the Community Manager and Participant.

The following examples show the number of interactions required for a particular document flow:

Table 2-12. Interaction Example 1

Participant		Manager
Package: AS2 (1.0)		Package: AS2 (1.0)
Protocol: RNSC (1.0)		Protocol: RNSC (1.0)
Document Flow: 3B3 Distribute Shipment Status (R01.00)	Document flow interaction	Document Flow: 3B3 Distribute Shipment Status (R01.00)
 No transformation map		

Table 2-13. Interaction Example 2

Participant		Manager
Package: RNIF (2.0)		Package: Builder
Protocol: RNSC (1.0)		Protocol: RNSC (1.0)
Document Flow: 3A4 Request Purchase Order (W02.00)	Document flow interaction	Document Flow: 3A4 Request Purchase Order (W02.00)
 No transformation map		

Table 2-14. Interaction Example 3

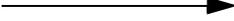
Participant		Manager
Package: Builder		Package: RNIF (2.0)
Protocol: Custom XML		Protocol: RosettaNet (1.1)
Document Flow: Purchase Order		Document Flow: 3A4 (W02.00)
Activity: Request Purchase Order	Four document flow interactions with four transformation maps	Activity: Request Purchase Order
Action: Purchase Order Request		Action: Purchase Order Request
Action: Receipt Acknowledgment		Action: Receipt Acknowledgment

Table 2-14. Interaction Example 3 (continued)

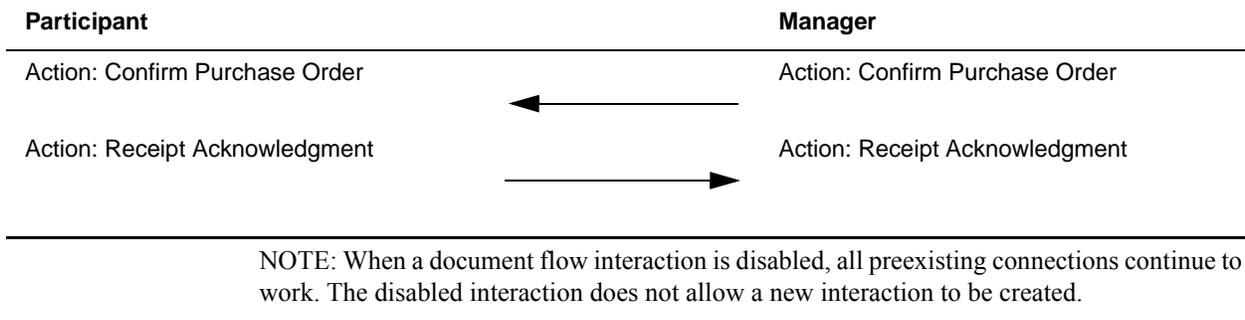


Table 2-15 lists the supported document flow interactions.

Table 2-15. Supported Document Flow Control Definitions

From	To	From Package	To Package	From Protocol	To Protocol
Participant	Manager	RNIF 1.1	Backend Integration	RN	RNSC
Participant	Manager	RNIF 1.1	Backend Integration	RN	XML
Participant	Manager	RNIF 1.1	Backend Integration	RN	RN
Participant	Manager	RNIF 2.0	Backend Integration	RN	RNSC
Participant	Manager	RNIF 2.0	Backend Integration	RN	XML
Participant	Manager	RNIF 2.0	Backend Integration	RN	RN
Participant	Manager	None	Backend Integration	Binary	Binary
Participant	Manager	None	Backend Integration	XML	XML
Manager	Participant	Backend Integration	RNIF 1.1	RNSC	RN
Manager	Participant	Backend Integration	RNIF 2.0	RNSC	RN
Participant	Manager	AS2	Backend Integration	Binary	Binary
Participant	Manager	AS2	Backend Integration	XML	XML
Manager	Participant	Backend Integration	AS2	Binary	Binary
Manager	Participant	Backend Integration	AS2	XML	XML

Table 2-15. Supported Document Flow Control Definitions (continued)

From	To	From Package	To Package	From Protocol	To Protocol
Manager	Participant	Backend Integration	None	Binary	Binary
Manager	Participant	Backend Integration	None	XML	XML
Manager	Participant	Backend Integration	RNIF 1.1	XML	RN
Manager	Participant	Backend Integration	RNIF 2.0	XML	RN

Creating valid flow interactions

To create valid flow interactions, use the following procedure.

1. Click **Hub Admin** on the main menu and **Document Flow Definition** on the horizontal navigation bar. The Console displays the Document Flow Definitions screen (see [Figure 2-12 on page 36](#)).
2. Click **Manage Interactions**. The Console displays the Valid Document Flow Interactions screen (see [Figure 2-15](#)).

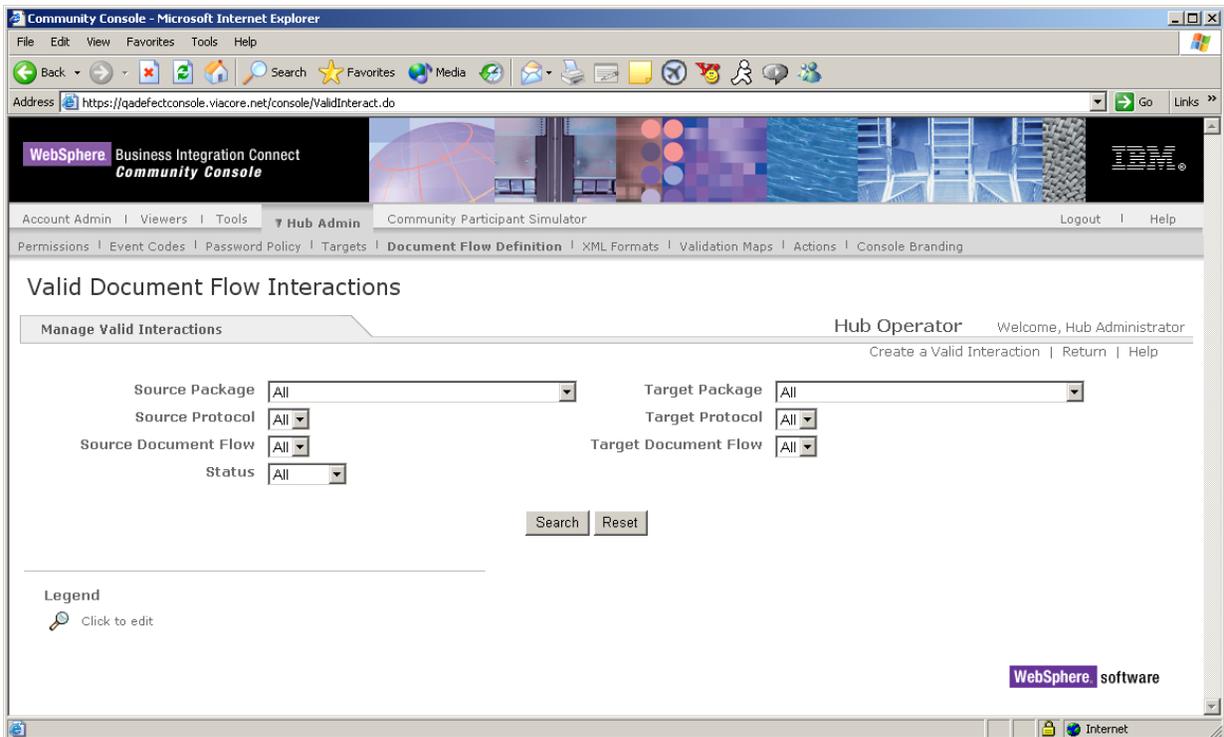


Figure 2-15. Valid Document Flow Interactions Screen

3. Click **Create a Valid Interaction**. The Console displays the Create a Valid Interaction screen (see Figure 2-16)

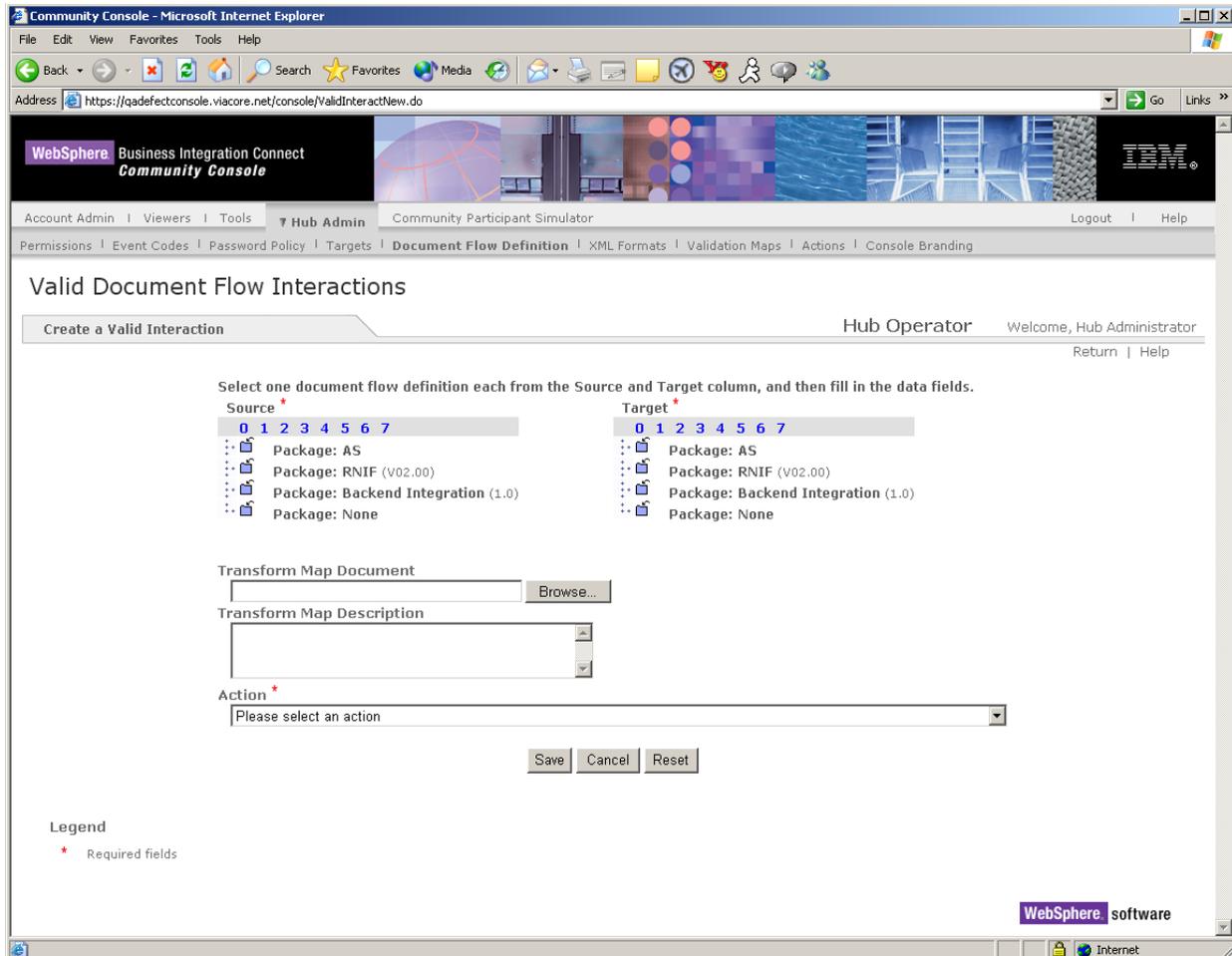


Figure 2-16. Create a Valid Interaction Screen

4. Click to individually expand a node to the appropriate Document Flow Definition level or select a number from 0-7 to expand all displayed Document Flow Definition nodes to the selected level.
5. Under **Transform Map Document**, click the **Browse** button. Navigate to the appropriate document and double-click it. The path and name of the document appear in the text box next to the **Browse** button.
6. Under **Transform Map Description**, type an optional description.
7. Under **Action**, select the action that is to be performed.
8. Click **Save**.

Searching for interactions

To search for valid interactions that meet your search criteria, use the following procedure.

1. Click **Hub Admin** on the main menu and **Document Flow Definition** on the horizontal navigation bar. The Console displays the Document Flow Definitions screen (see [Figure 2-12 on page 36](#)).
2. Click **Manage Interactions**. The Console displays the Valid Document Flow Interactions screen (see [Figure 2-15 on page 49](#)).
3. Enter your search criteria.
4. Click **Search**. The system finds all interactions that meet your search criteria (see [Figure 2-17](#)).

The screenshot shows the 'Valid Document Flow Interactions' page in the IBM Business Integration Connect Community Console. The page has a search filter section with dropdown menus for Source Package, Source Protocol, Source Document Flow, Status, Target Package, Target Protocol, and Target Document Flow. Below the filters are 'Search' and 'Reset' buttons. A pagination bar shows 'Page 1 of 2' and 'Total Rows: 13'. The main content area is a table with columns for 'Enabled', 'Edit', 'Source', 'Transformation Map', and 'Target'. Five rows of interactions are listed, each with a green checkmark in the 'Enabled' column and a magnifying glass icon in the 'Edit' column.

Enabled	Edit	Source	Transformation Map	Target
✓		Package: AS AS (N/A) Protocol: Binary Binary (1.0) Document Flow: Binary Binary (1.0)	Transformation Map:	Package: Backend Integration Backend Integration (1.0) Protocol: Binary Binary (1.0) Document Flow: Binary Binary (1.0)
✓		Package: Backend Integration Backend Integration (1.0) Protocol: Binary Binary (1.0) Document Flow: Binary Binary (1.0)	Transformation Map:	Package: AS AS (N/A) Protocol: Binary Binary (1.0) Document Flow: Binary Binary (1.0)
✓		Package: AS AS (N/A) Protocol: Binary Binary (1.0) Document Flow: Binary Binary (1.0)	Transformation Map:	Package: None None (N/A) Protocol: Binary Binary (1.0) Document Flow: Binary Binary (1.0)
✓		Package: None None (N/A) Protocol: Binary Binary (1.0) Document Flow: Binary Binary (1.0)	Transformation Map:	Package: AS AS (N/A) Protocol: Binary Binary (1.0) Document Flow: Binary Binary (1.0)
✓		Package: RNIIF RNIIF (V02.00) Protocol: RosettaNet RosettaNet (V02.00) Document Flow: 3AT Notify of Purchase Order Update (V02.02) Activity: Notify of Purchase Order Update Notify of Purchase Order Update (N/A) Action: Purchase Order Update Notification Action Purchase Order Update	Transformation Map:	Package: Backend Integration Backend Integration (1.0) Protocol: RINSC RINSC (1.0) Document Flow: 3AT Notify of Purchase Order Update (V02.02) Activity: Notify of Purchase Order Update Notify of Purchase Order Update (N/A) Action: Purchase Order Update Notification Action Purchase Order Update

Figure 2-17. Example of Matching Interactions that Match Search Criteria

5. To disable an interaction, click the  icon next to the interaction you want to disable. When a precautionary message asks whether you are sure, click **OK** to continue or **Cancel** to abort.

If you click **OK**, the icon changes to . You can click this icon to re-enable the interaction (you will be prompted with the same precautionary message).

6. To edit an interaction, click the  next to the interaction. A window appears with controls for editing the interaction. Perform your edits and click **Save**.

Configuring validation maps

Business Integration Connect uses the concept of “validation maps” to validate documents. This concept lets you upload or download field-level validation maps (or schema) and associate them to types of documents, such as failure notification, 3A4 Purchase Order Requests, and 3A4 Purchase Order Confirmations. By associating a validation map to an action level definition, the system can validate the structure of incoming RosettaNet or XML documents.

Displaying the Manage Maps screen

Validation map activities are performed from the Manage Maps screen. To display the Manage Maps screen, click **Hub Admin** on the main menu and **Validation Maps** on the horizontal navigation bar. The Console displays the Manage Maps screen (see [Figure 2-18 on page 53](#)).

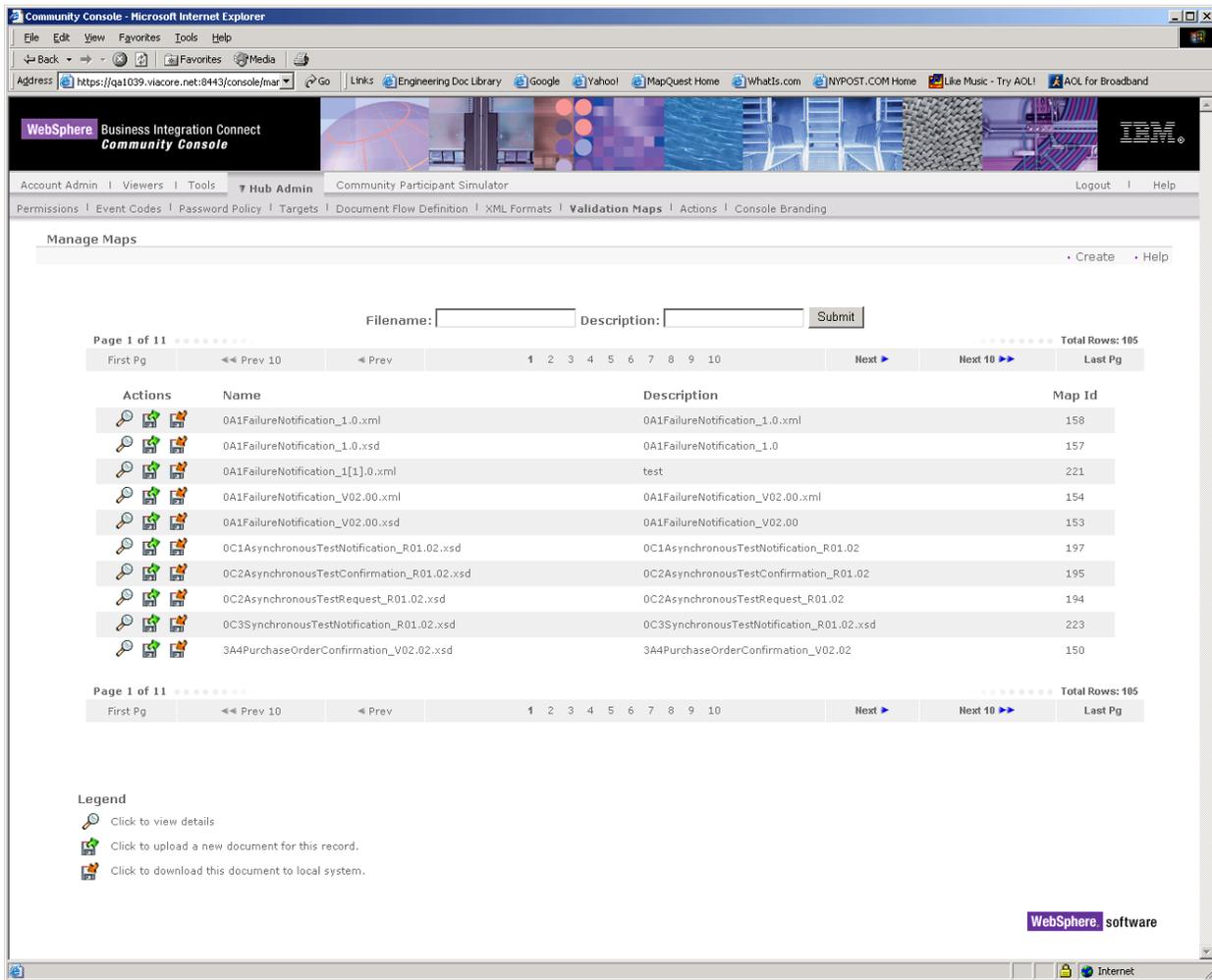


Figure 2-18. Manage Maps Screen

Each row in the Manage Maps screen shows name and description of the document and the map ID with which it is associated. The Manage Maps screen can consist of more rows than can fit on a single screen. The number of rows is displayed in the top-right and bottom-right areas of the screen. If there are more rows than can fit on a single screen, the system creates additional screens to hold this information. To view these other screens, the Manage Maps screen provides controls at the top and bottom of the screen to navigate to other screens.

Table 2-16. Manage Maps Navigational Control

Control	Description
First Pg	Click to go to the first screen.
◀◀ Prev 10	Click to view the previous 10 rows.

Table 2-16. Manage Maps Navigational Control (continued)

Control	Description
	Click to go to the previous screen.
	Click a number to go to the desired screen. The current number is shown in bold .
	Click to go to the next screen.
	Click to view the next 10 rows.
	Click to go to the last screen.

Adding a validation map to a Document Flow Definition

To add a new validation map to a Document Flow Definition, use the following procedure.

1. Click **Hub Admin** on the main menu and **Validation Maps** on the horizontal navigation bar. The Console displays the Map Update screen (see [Figure 2-18 on page 53](#)).
2. Click **Create**. The Console displays the Map Update screen (see [Figure 2-19](#)).

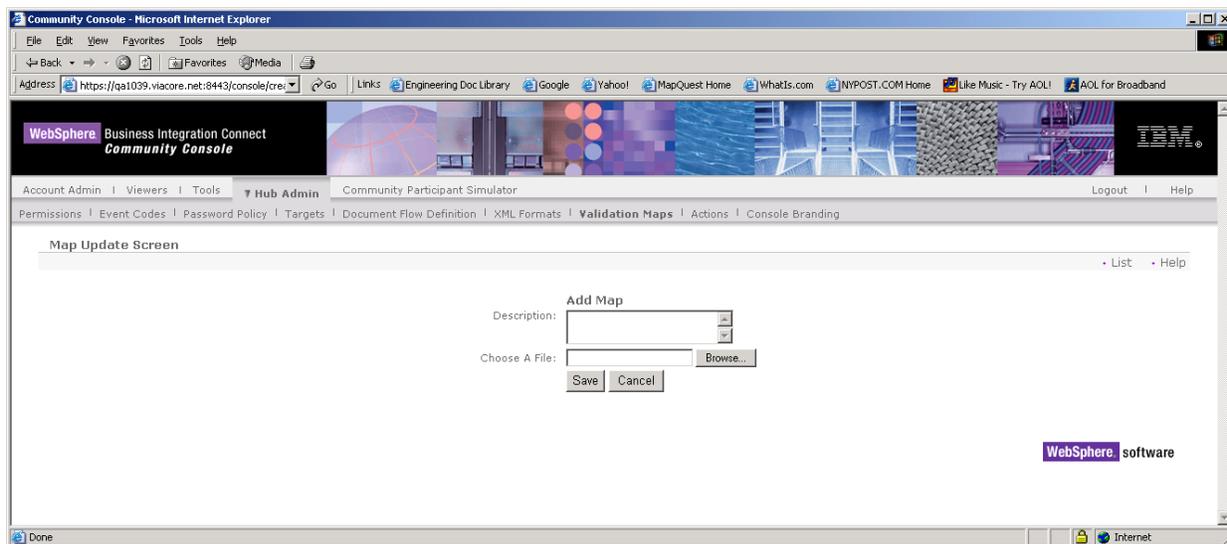


Figure 2-19. Map Update Screen

3. Complete the following parameters in the screen:

Table 2-17. Manage Maps Screen

Parameter	Description
Description	Text that describes the map you want to add.
Choose A File	Type the path and name of the map you want to use for the company logo or browse and select the file.

4. Click **Save**.

NOTE: Be sure that the validation map is in the proper XML format. The system does not distinguish between a proper or improper document type.

Updating a validation map

To update a validation map currently in the system, use the following procedure.

1. Click **Hub Admin** on the main menu and **Validation Maps** on the horizontal navigation bar. The Console displays the Manage Maps screen (see [Figure 2-18 on page 53](#)).
2. Click the  icon to download the validation map to your local computer and update the map as needed.
3. Click the  icon to load the updated map to the system

Associating a map to a Document Flow Definition

To associate a validation map to a Document Flow Definition, use the following procedure.

1. Click **Hub Admin** on the main menu and **Validation Maps** on the horizontal navigation bar. The Console displays the Manage Maps screen (see [Figure 2-18 on page 53](#)).
2. Click the  icon next to the validation map you want to associate to the Document Flow Definition. The Console displays the Manage Maps screen (see [Figure 2-20](#)).

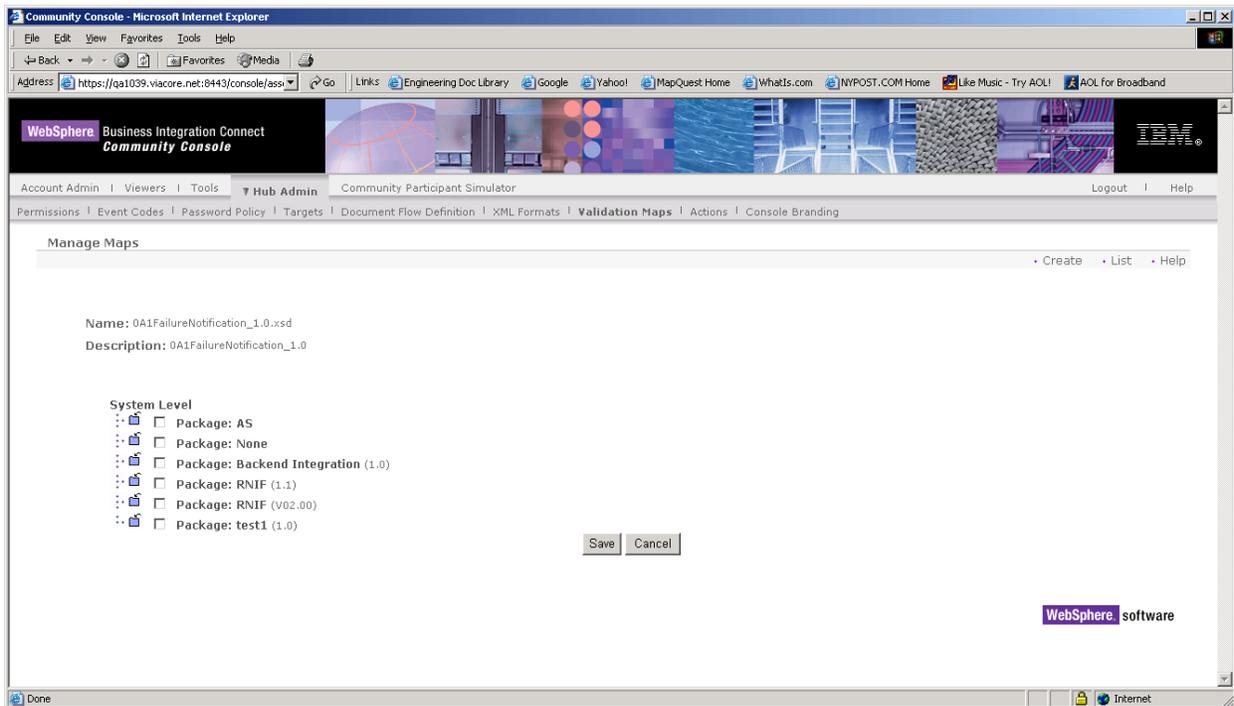


Figure 2-20. Manage Maps Screen

3. Click the  icon and expand the node to the Action (or document) level.
4. Select the **Action** box to associate the validation map to the Action Document Flow Definition.
5. Click **Save**.

NOTE: Once you associate a validation map to a Document Flow Definition, the map cannot be disassociated. This prevents the deactivation of existing connections based on the Document Flow Definition.

Managing XML formats

XML, or Extensible Markup Language, is the universal format for structured documents and data on the World Wide Web. XML is increasingly becoming the general standard document format of structured data. Using the Manage XML Protocols screen, you can create and manage custom XML formats that can be added to Document Flow Definitions.

An XML format defines the paths within a set of XML documents. Using this information, you can create and manage custom XML formats that can be added to the system as a Document Flow Definition. An XML format defines the paths within a set of XML documents. This enables the Document Manager to retrieve the values that uniquely identify an incoming document and access information within the document necessary for proper routing and processing.

NOTE: When using a custom XML format within the Backend Integration package, the Document Manager will override the protocol and use the x-aux values contained in the document HTTP/S header to determine the protocol, protocol version, document flow, and document flow version (see example below). However, if using a custom XML format combined with a non Backend Integration package such as AS1, AS2, None, or RNIF, the system will normally determine the protocol, protocol version, document flow, and document flow version from the element path defined in the XML format guideline.

Example HTTP/S header:

```
From HTTP/S Post set headers=%headers% x-aux-protocol: XML x-aux-protocol-version:
1.0 x-aux-sender-id: 987654321 x-aux-receiver-id: 102420488 x-aux-process-type:
XML_DTD x-aux-process-version: 1.0 x-aux-production: true x-aux-system-msg-id:
GWYN_OBID_H2_DTD_00000004
```

Creating an XML format

To create an XML format, use the following procedure.

1. Click **Hub Admin** on the main menu and **XML Formats** on the horizontal navigation bar. The Console displays the Manage XML Formats screen (see [Figure 2-21 on page 58](#)).

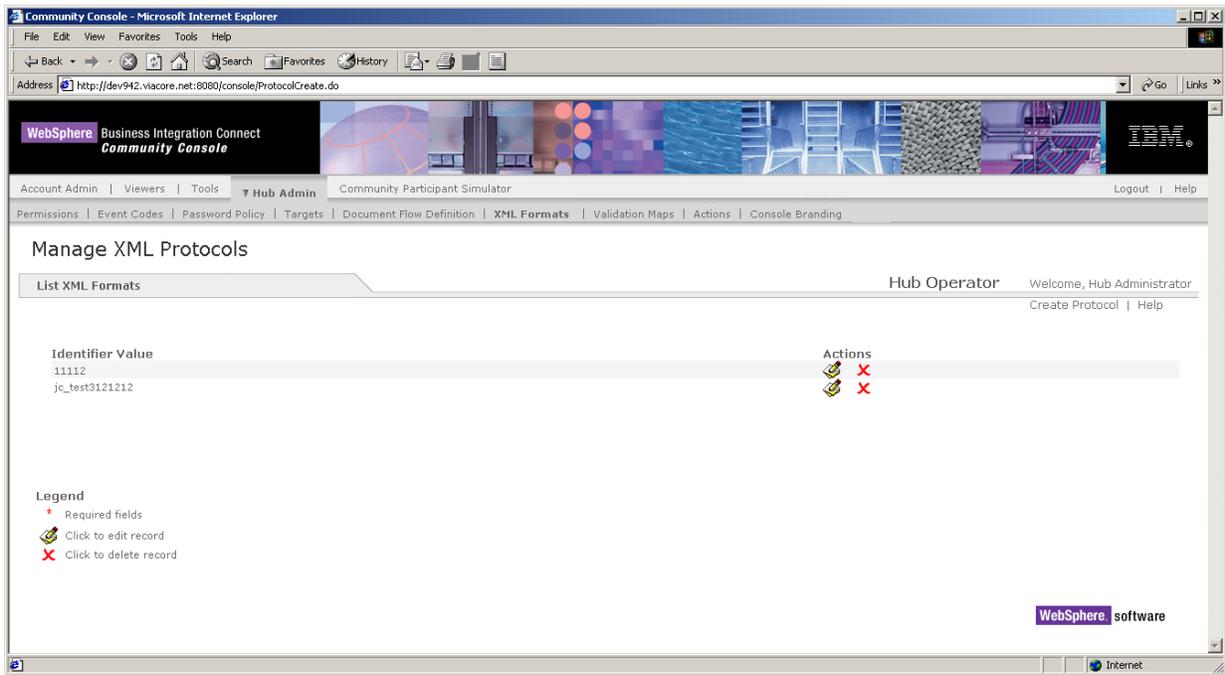


Figure 2-21. Manage XML Formats Screen

2. Click **Create XML Format**. The Console displays the View XML Format screen (see [Figure 2-22 on page 59](#)).

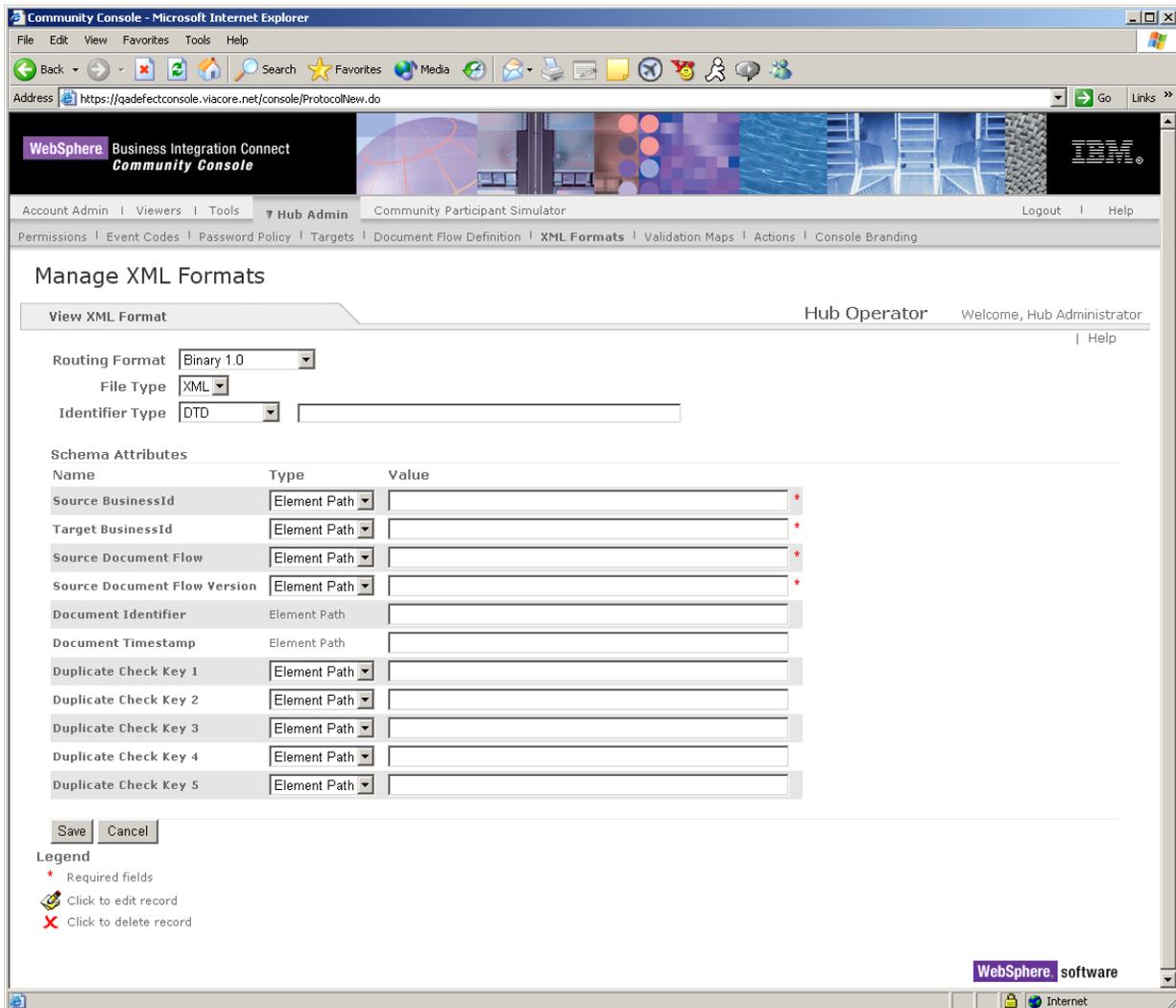


Figure 2-22. View XML Format Screen

- Complete the following parameters in the screen:

Table 2-18. View XML Format

Parameter	Description
Routing Format	The Document Flow Definition with which this protocol will be associated. This definition must be created before creating the XML format (see “Configuring Document Flow Definitions and download packages” on page 33).
File Type	XML is the only option.
Identifier Type	The element used to identify the incoming document type: DTD, Name Space, or Root Tag.

Table 2-18. View XML Format (continued)

Parameter	Description
Source / Target BusinessId	Path of the Business ID. For Type, select: <ul style="list-style-type: none">• Element Path – path to Business ID in document.• Constant – actual Business ID value in document.
Source Document Flow	An expression that defines the path to the document flow within the XML document. For Type, select: <ul style="list-style-type: none">• Element Path – path to value in document.• Constant – actual value in document.
Source Document Flow Version	An expression that defines the path to the version value within the XML document. For Type, select: <ul style="list-style-type: none">• Element Path – path to value in document.• Constant – actual value in document.
Document Identifier	Path for the document ID number.
Document Timestamp	Path for the document creation timestamp.
Duplicate Check Key 1 – 5	Paths for identifying the routing of a duplicate document. For Type, select: <ul style="list-style-type: none">• Element Path – path to check key value in document.• Constant – actual check key value in document.

4. Click **Save**.

Editing XML format values

There may be times when you need to edit XML format values. To edit these values, use the following procedure.

1. Click **Hub Admin** on the main menu and **XML Formats** on the horizontal navigation bar. The Console displays the Manage XML Formats screen (see [Figure 2-21 on page 58](#)).
2. Click the  icon next to the XML format you want to edit. The Console displays the View XML Protocol screen, with the values that have already been defined for the selected XML protocol (see [Figure 2-11 on page 32](#)).
3. Change the appropriate values. If you need assistance, see [Table 2-18](#).
4. Click **Save**.

Deleting an XML format

If you no longer need an XML format, use the following procedure to delete it.

NOTE: No warning message is displayed prior to deleting an XML format. Therefore, be sure you do not need an XML format before you delete it.

IMPORTANT: Deleting an XML format disables any pre-existing connection based on that protocol. Any document exchanged using that connection fails with an Unknown Document event. However, the Document Flow Definition associated with the deleted protocol remains in the system.

1. Click **Hub Admin** on the main menu and **XML Formats** on the horizontal navigation bar. The Console displays the Manage XML Formats screen (see [Figure 2-21 on page 58](#)).
2. Click the  icon next to the XML format you want to delete. The XML format is deleted.

Enabling or disabling Actions

The Actions screen is a read-only screen that shows the steps the system uses when processing documents. To display the Actions screen, click **Hub Admin** on the main menu and **Actions** on the horizontal navigation bar.

Figure 2-23 shows an example of an Actions screen. The following parameters are displayed for each action:

- Action Name — name used to identify action based on activities the action will perform.
- Status — when enabled, the action is available to the hub-community for creating or updating a connection.

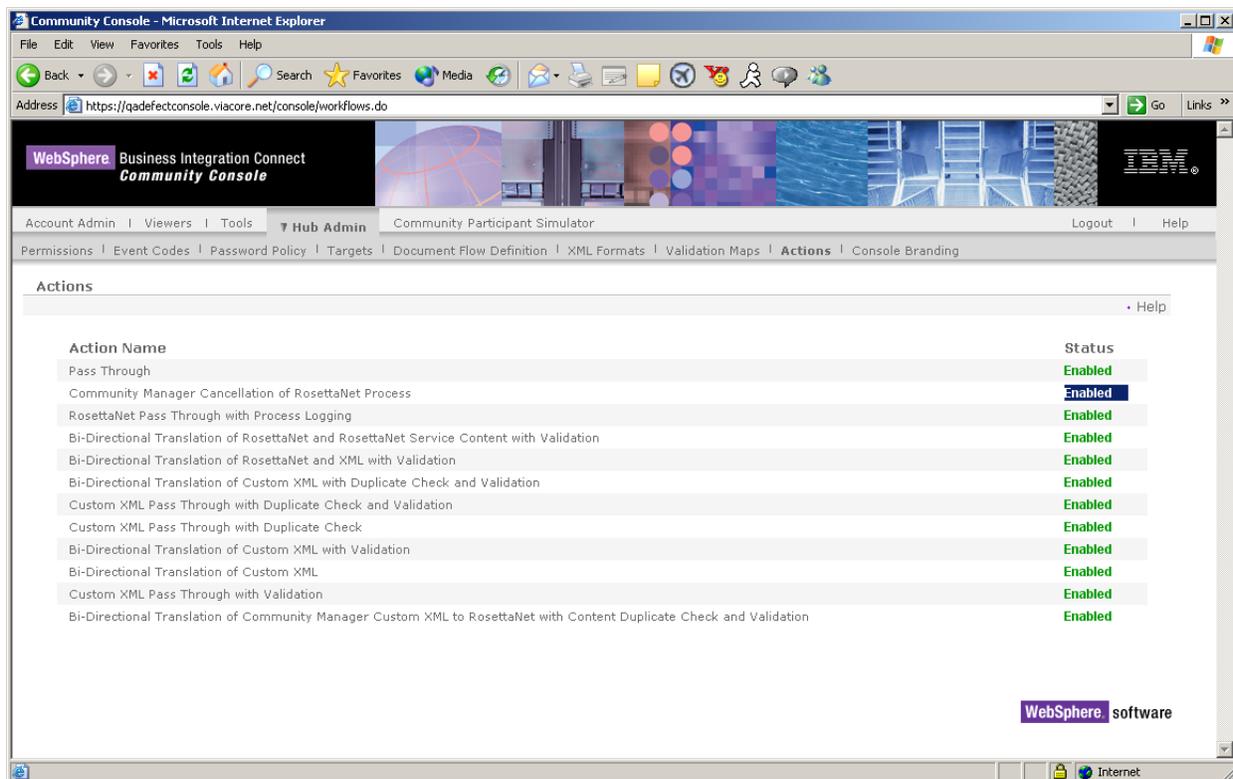


Figure 2-23. Actions Screen

Managing event codes

When an event occurs within the Business Integration Connect, an event code is generated. Using the Event Codes screen, you can see the event codes that have been generated and export them to other applications.

Viewing and editing permission details

The following procedure describes how to view details for an event code. As part of this procedure, you can edit the visibility and alertable status of the event code and view the severity of the code.

1. Click **Hub Admin** on the main menu and **Event Codes** on the horizontal navigation bar. The Console displays the Event Codes screen (see [Figure 2-24](#)).

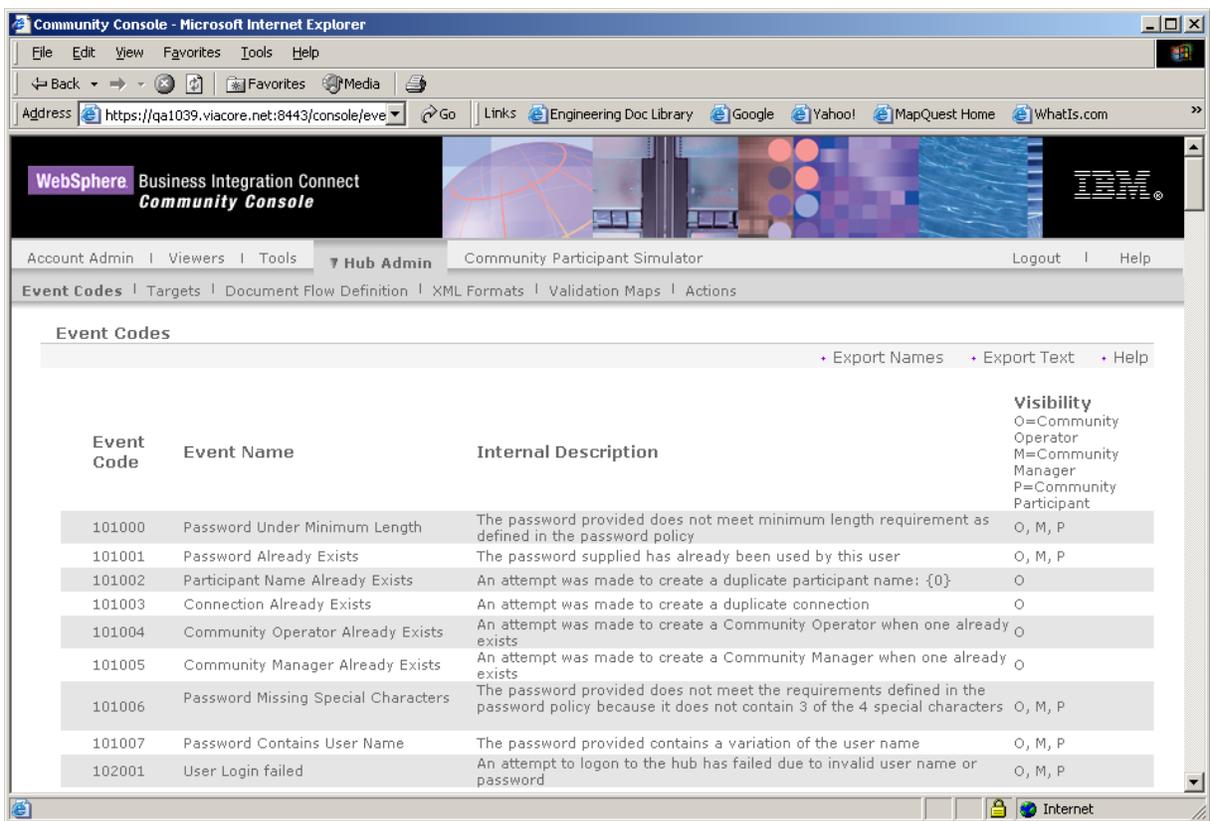


Figure 2-24. Event Codes Screen

2. Click the  icon next to the event code whose details you want to view. The Console displays the Event Code Details screen (see [Figure 2-25 on page 64](#)).

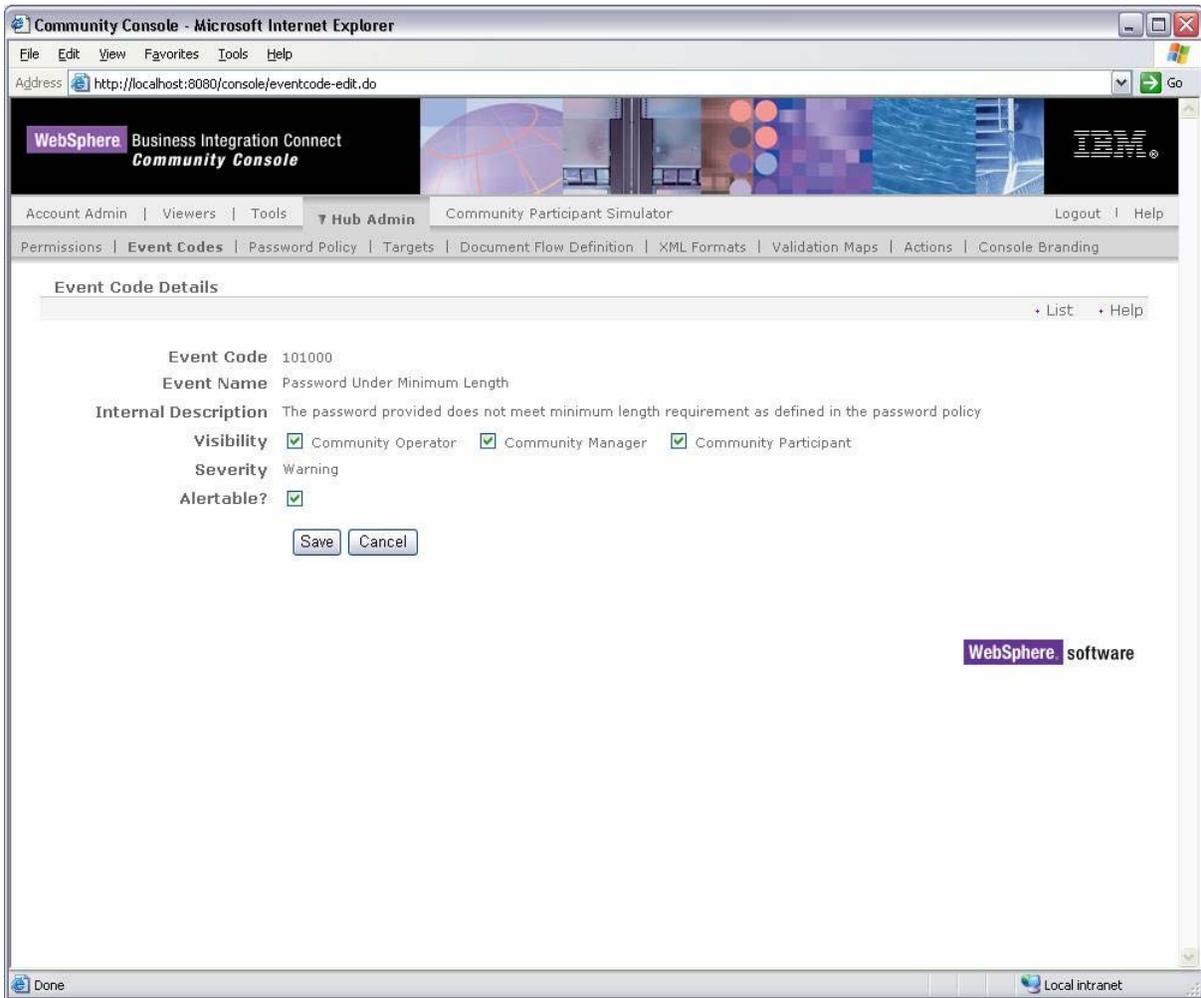


Figure 2-25. Event Code Details Screen

3. Complete the following parameters in the screen:

Table 2-19. Event Code Details

Parameter	Description
Event Code	Read-only field that shows the unique number for this event code.
Event Name	Read-only field that shows the name used to identify event in relation to action that triggered the event.
Internal Description	Read-only field that describes the circumstances that triggered the event.
Visibility	Check the users that will be able to view the event code: Community Operator, Manager, or Participant.

Table 2-19. Event Code Details (continued)

Parameter	Description
Severity	<p>Read-only field that shows the seriousness associated with this event code, from Debug (least serious) to Critical (most serious):</p> <ul style="list-style-type: none">• Debug – used for low-level system operations and support. Visibility and use are subject to the permission level of the user.• Info – generated when a system operation ends successfully. These events are also used to provide the status of documents being processed. Informational events require no user action.• Warning – occurs due to non-critical anomalies in document processing or system functions that allow the operation to continue.• Error – occurs due to anomalies in document processing that cause the process to end.• Critical – generated when services end due to system failure. Critical events require intervention by support personnel.
Alertable	<p>When checked, the event appears in the Event Name drop-down list on the Define tab of the Alert screen. This allows an alert to be set for this event. The procedure for associating an alert with an event is described in the WebSphere Business Integration Connect Community Console User Guide.</p>

Saving event code names

The Event Codes screen provides two ways to save event codes:

- Click **Export Names** to save only the event names in the event list.
- Click **Export Text** to save the internal descriptions in the event list in text format.

To save event names or internal descriptions, use the following procedure:

1. Click **Hub Admin** on the main menu and **Event Codes** on the horizontal navigation bar. The Console displays the Event Codes screen (see [Figure 2-24 on page 63](#)).
2. Click **Export Names** or **Export Text**, depending on what you want to export. The Console displays the File Download screen.
3. Click **OK**.
4. When prompted, save the exported file.

Chapter 3. Account Admin Activities

This chapter describes how to perform the following Account Admin activities:

- [“Managing Participant profiles,”](#) below
- [“Managing gateway configurations”](#) on page 79
- [“Creating an FTP account”](#) on page 85
- [“Managing certificates”](#) on page 88
- [“Managing B2B capabilities”](#) on page 94
- [“Managing Participant connections”](#) on page 98
- [“Managing Exclusion Lists”](#) on page 108

These Account Admin activities can be performed by the Hub Admin, Manager Admin, and Participant Admin users, with the following limitations:

- **Managing Participants:** Manager Admin and Participant Admin users cannot create Participants and edit Participant Type, Parent, and Action parameters.
- **Managing Gateway:** Manager Admin and Participant Admin users can edit a subset of parameters.

Managing Participant profiles

The Account Admin Participants feature allows Hub Admin users to create, view, and edit Participant profile. A Participant profile identifies companies to the system.

NOTE: Participant Admin and Manager Admin users can only edit their own Participant Profile.

Creating Participants

Hub Admin users can create new Participants using the following procedure.

1. Click **Account Admin** on the main menu and **Profiles** on the horizontal navigation bar. If the Participant Search screen is not displayed, click **Community Participants** to display it (see [Figure 3-1 on page 68](#)).

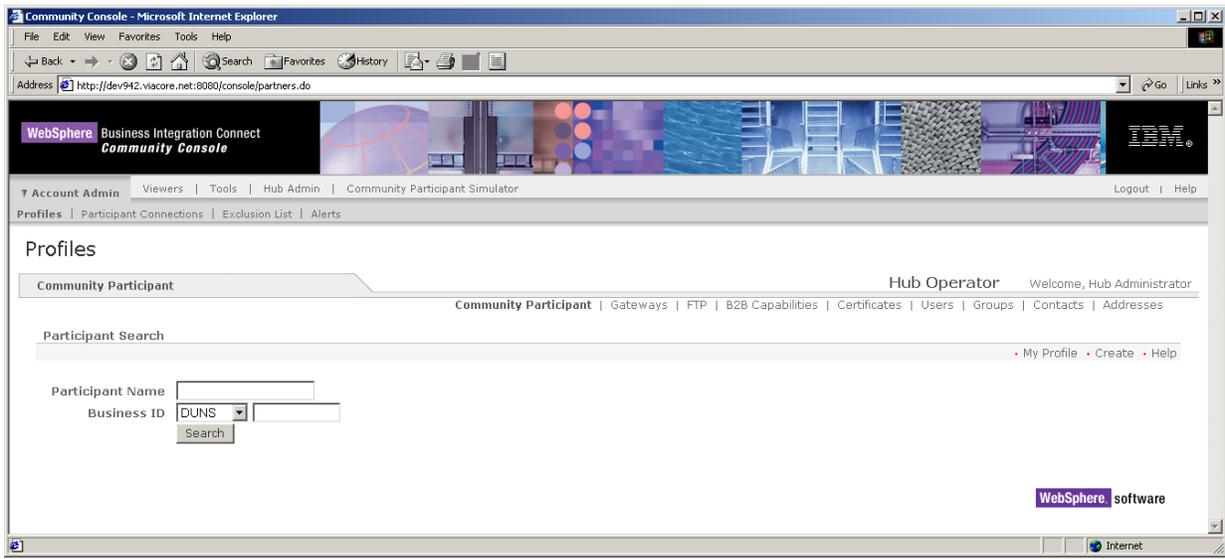


Figure 3-1. Participant Search Screen

2. Click **Create**. The Console displays the Participant Detail screen (see [Figure 3-2 on page 69](#)).

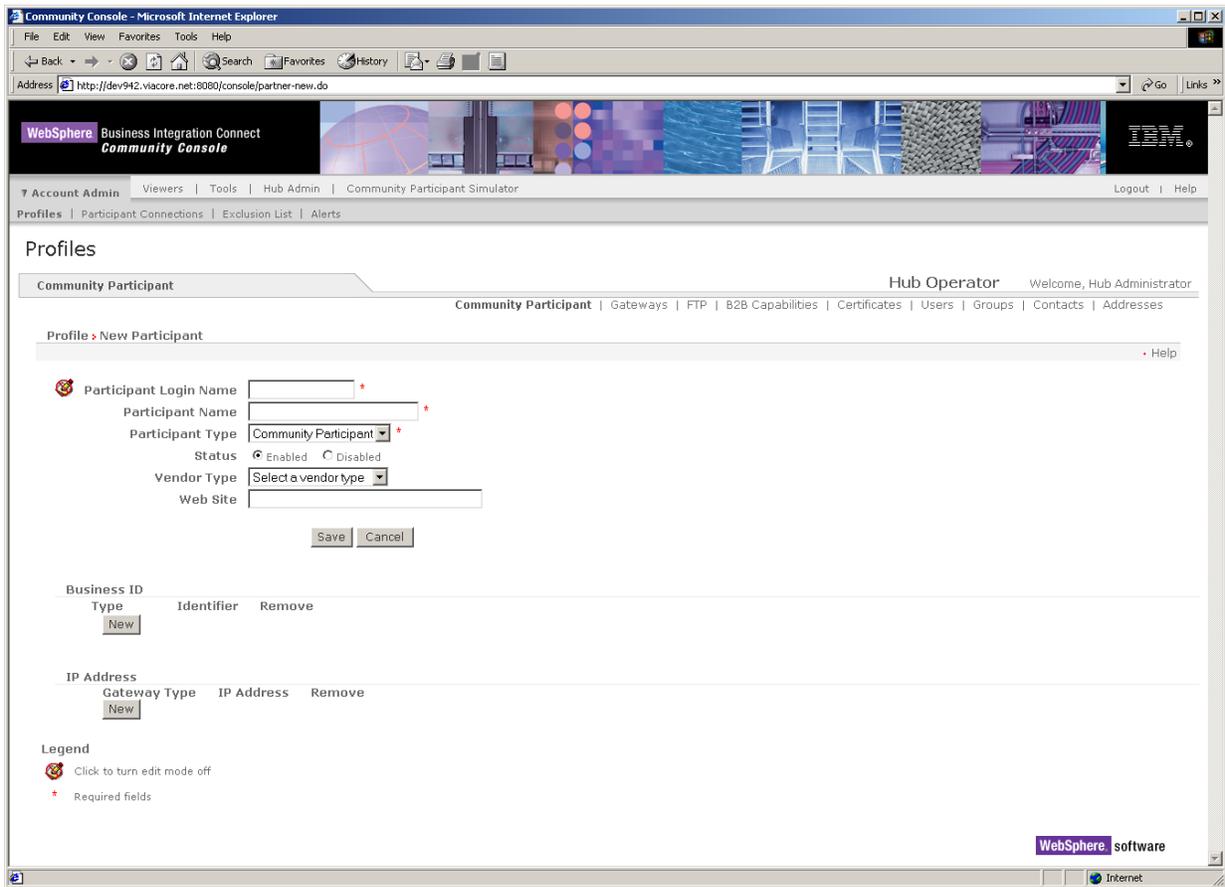


Figure 3-2. Participant Detail Screen

- Complete the following parameters in the screen:

Table 3-1. Participant Detail Screen Parameters

Parameter	Description
Participant Login Name / Participant Name	Name that identifies the trading entity to the system. Both the company name and a modified version used for login are used.
Participant Type	Community Operator, Participant, or Community Manager. <ul style="list-style-type: none"> The Community Operator is responsible for managing day-to-day operation of the hub-community. This can include maintaining the hardware and software infrastructure, ensuring the hub-community is properly configured for use, and assisting with the adding of new Participants. The Community Participant is the individual company conducting business with the Community Manager via the hub-community. The Community Manager is responsible for purchasing and building the hub-community. This can include defining the electronic business processes exchanged between them and their Participants. <p>The system supports one Community Operator and one Community Manager. Trying to create a second Community Operator or Community Manager displays the error message "An error occurred while saving this record."</p>
Participant Status	Enabled or Disabled. If disabled, the Participant will be absent from all search criteria and drop-down menus in the Tools and Viewers modules.
Vendor Type	Business function. Vendor Type is used during provisioning.
Web Site	Participant Web site. Web site is used during Provisioning.
Business ID	DUNS, DUNS+4, or Freeform number that the system uses to route documents. <ul style="list-style-type: none"> DUNS numbers must equal nine digits. DUNS+4 numbers must equal 13 digits. Freeform ID numbers accept up to 60 alpha, numeric, and special characters.
IP Address	Gateway type and corresponding IP address for receiving incoming documents.

- Under **Business ID**, click **New**. The Console displays the fields in [Figure 3-3 on page 71](#). Then specify a business ID type and type the appropriate identifier.

NOTE: To remove an identifier from the system, type the identifier and check **Remove**. The identifier will be removed when you click **Save**.

Observe the following guidelines when typing the identifier:

- DUNS numbers must equal nine digits.

- DUNS+4 must equal 13 digits.
- Freeform ID numbers accept up to 60 alphanumeric and special characters.

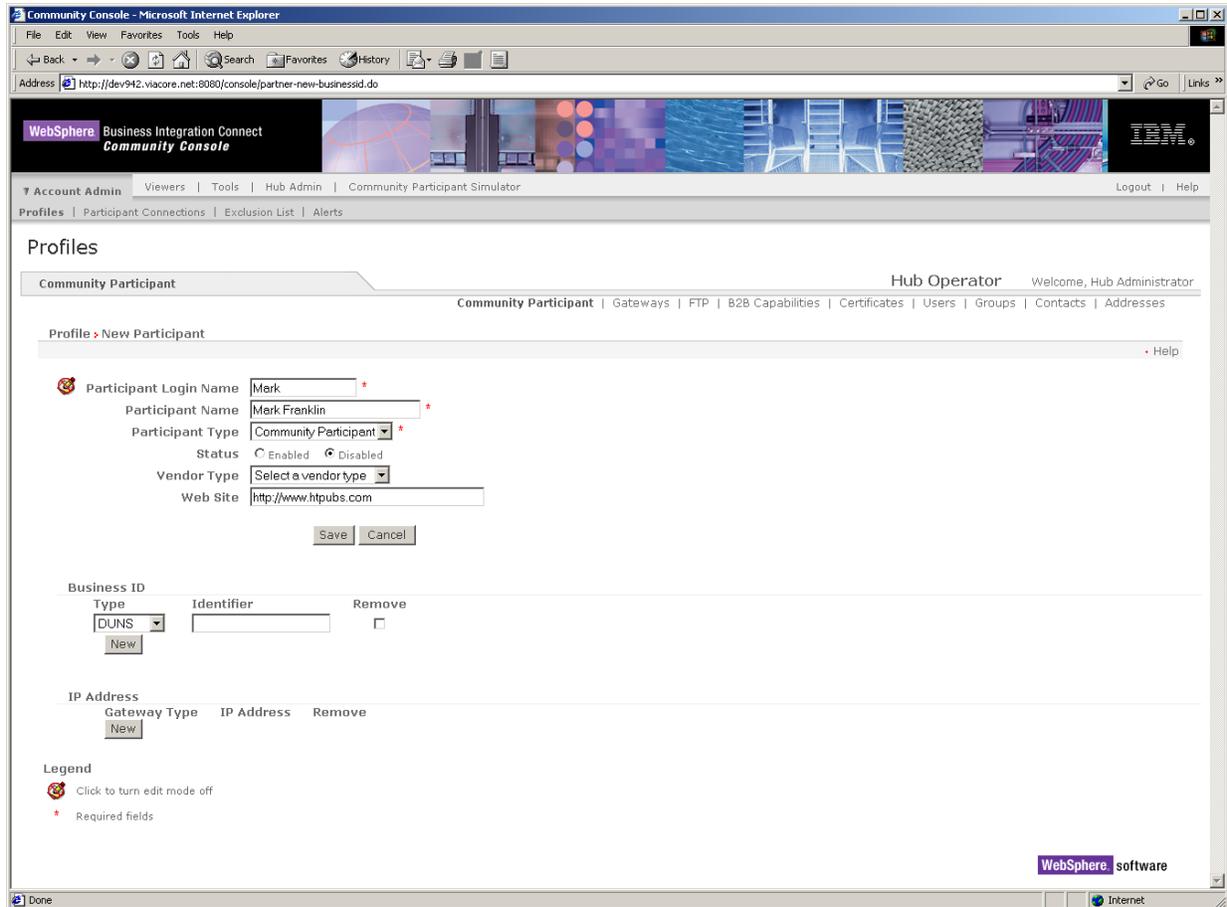


Figure 3-3. Typing a Business ID

5. Under **IP Address**, click **New**. The Console displays the fields in [Figure 3-4 on page 72](#). Then specify the gateway type and type the Participant's IP address(es).

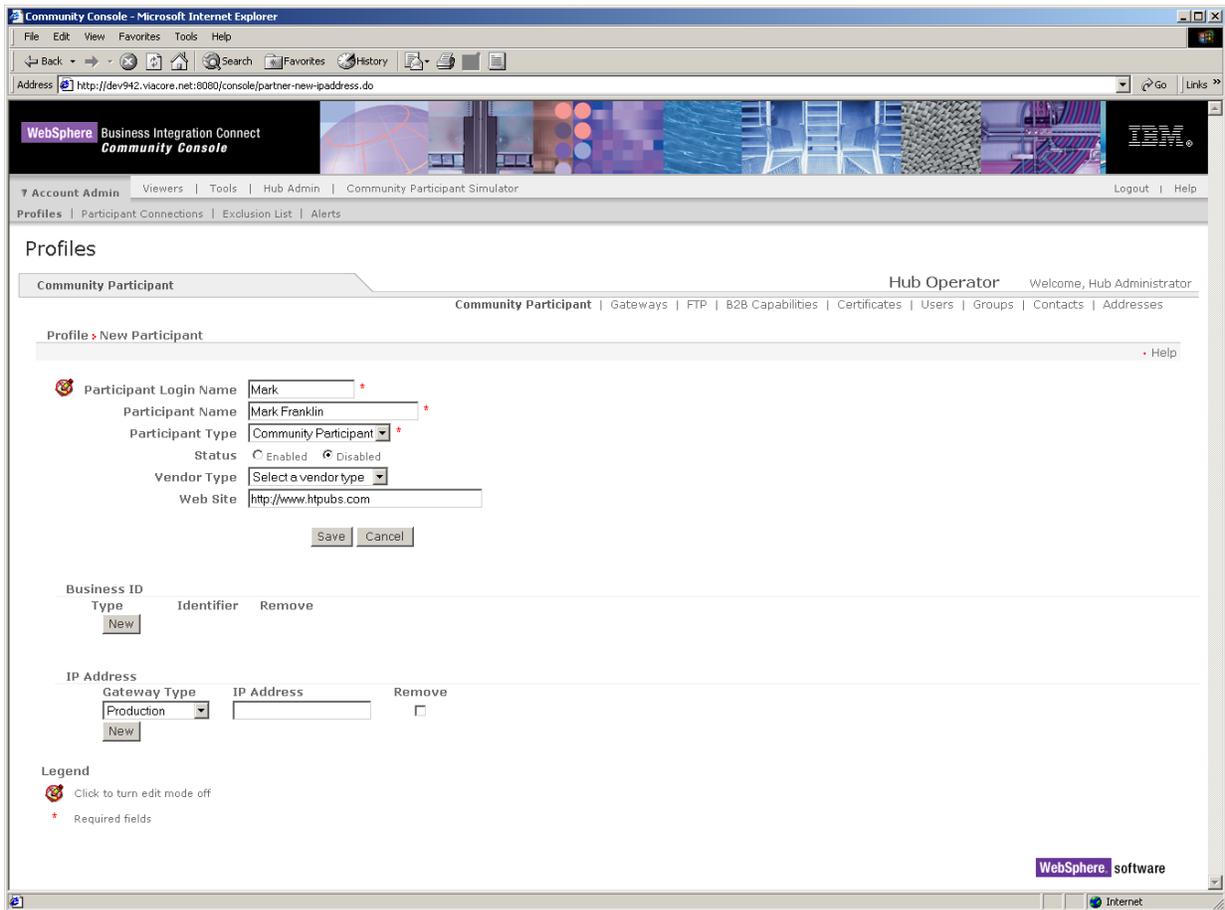


Figure 3-4. Typing an IP Address

6. Click **Save**.

NOTE: The system supports one Community Operator and one Community Manager. Trying to create a second Community Operator or Community Manager displays the error message "An error occurred while saving this record."

Viewing and editing Participant profiles

There might be times when you need to modify a Participant profile. Use the following procedure to view and edit Participant profiles.

1. Click **Account Admin** on the main menu and **Profiles** on the horizontal navigation bar. If the Participant Search screen is not displayed, click **Community Participants** to display it (see [Figure 3-1 on page 68](#)).
2. Click **Search**.

3. Click the  icon next to the Participant whose details you want to view. The Console displays the Participant Details screen (see [Figure 3-5 on page 73](#)).

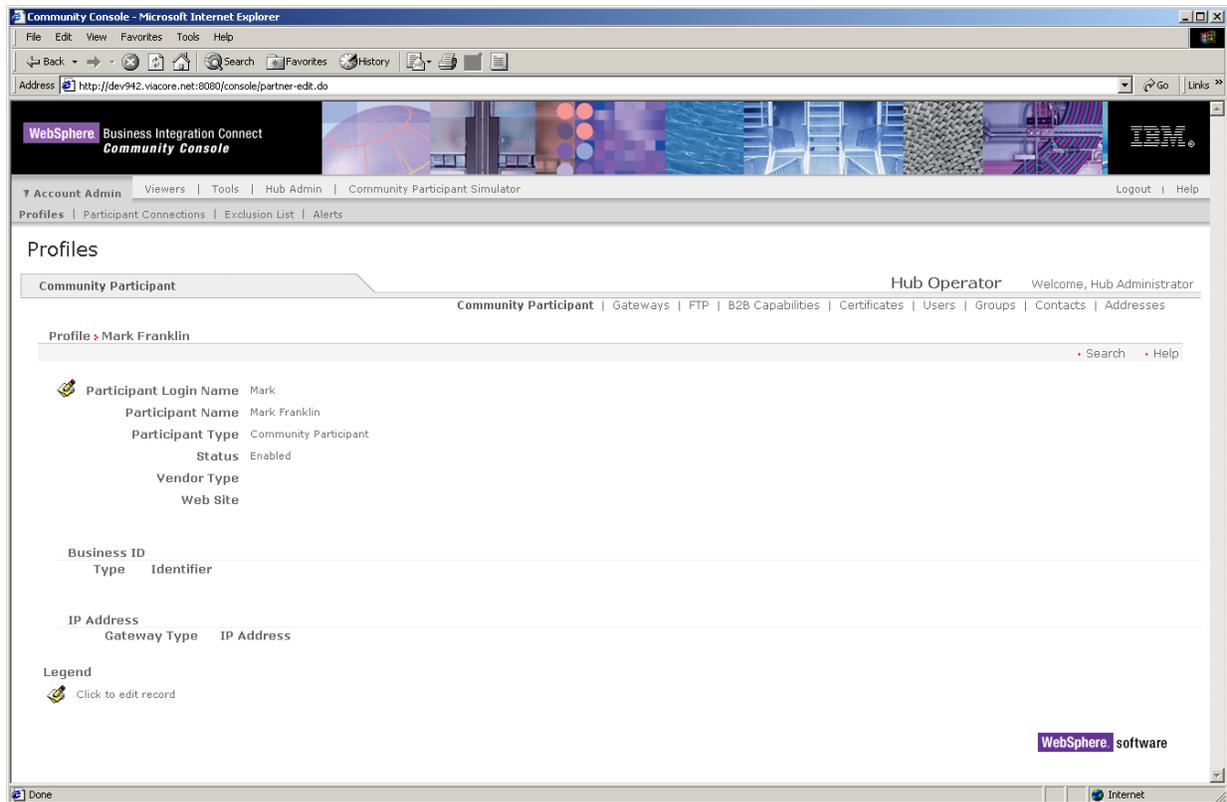


Figure 3-5. Example of Viewing Profile Details

4. To edit the profile details, click the  icon. The Console displays the screen in [Figure 3-6 on page 74](#).

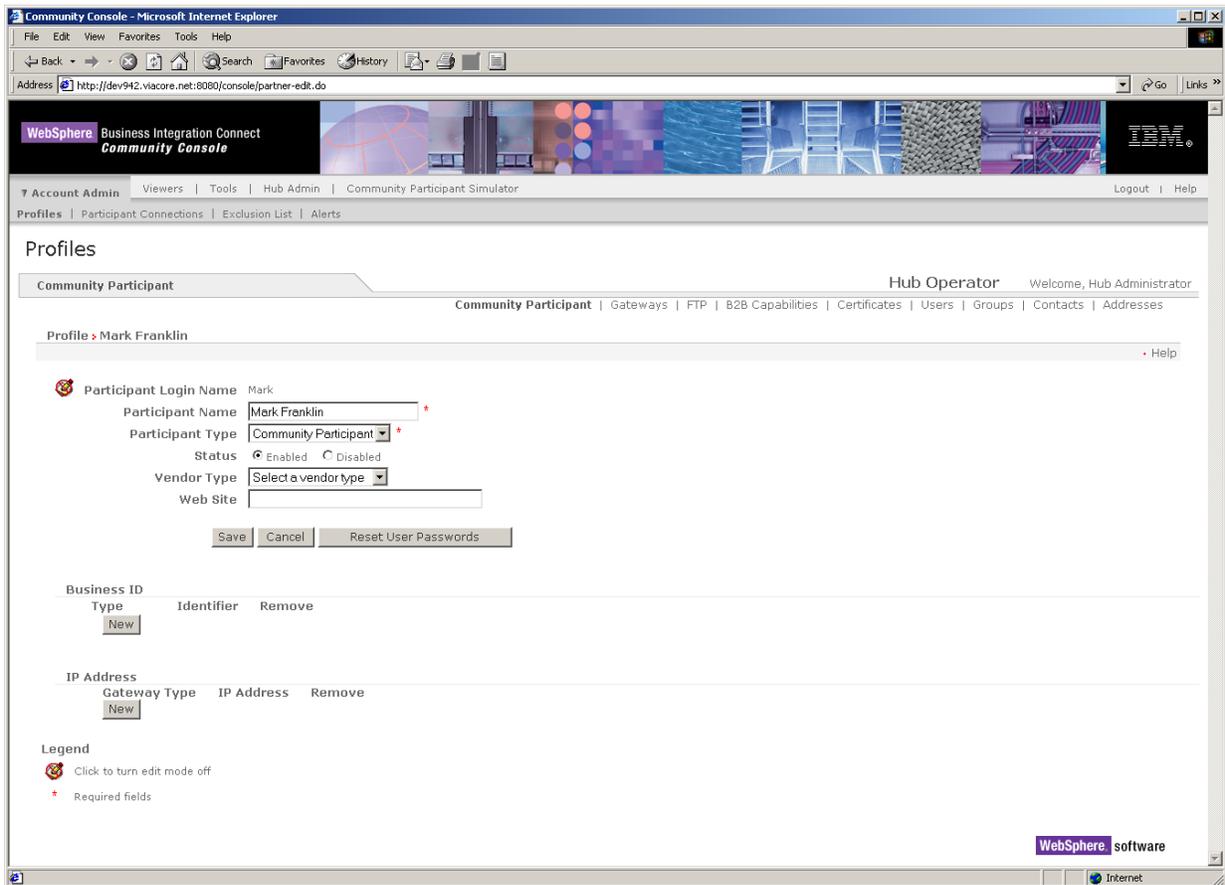


Figure 3-6. Editing Profile Details

5. Modify the Participant profile as necessary (see [Table 3-1](#)).

NOTE: If you click **Reset User Passwords**, the Console displays the message in [Figure 3-7](#). Click **OK** to proceed (the Console displays the message in [Figure 3-8 on page 75](#)) or click **Cancel** to retain the passwords. If you clicked **OK**, click it again to reset the passwords or click **Cancel** to not reset them.



Figure 3-7. Reset User Password Message



Figure 3-8. Are You Sure Message

6. When you finish, click **Save**.

Searching for Participants

The Participants screen allows the system to find Participants that meet your search criteria.

1. Click **Account Admin** on the main menu and **Profiles** on the horizontal navigation bar. If the Participant Search screen is not displayed, click **Participants** to display it (see [Figure 3-1 on page 68](#)).
2. Type the Participant name or business ID in the appropriate text boxes.
3. Click **Search**. The system finds that Participants that match your criteria. [Figure 3-9 on page 76](#) shows an example of this screen.

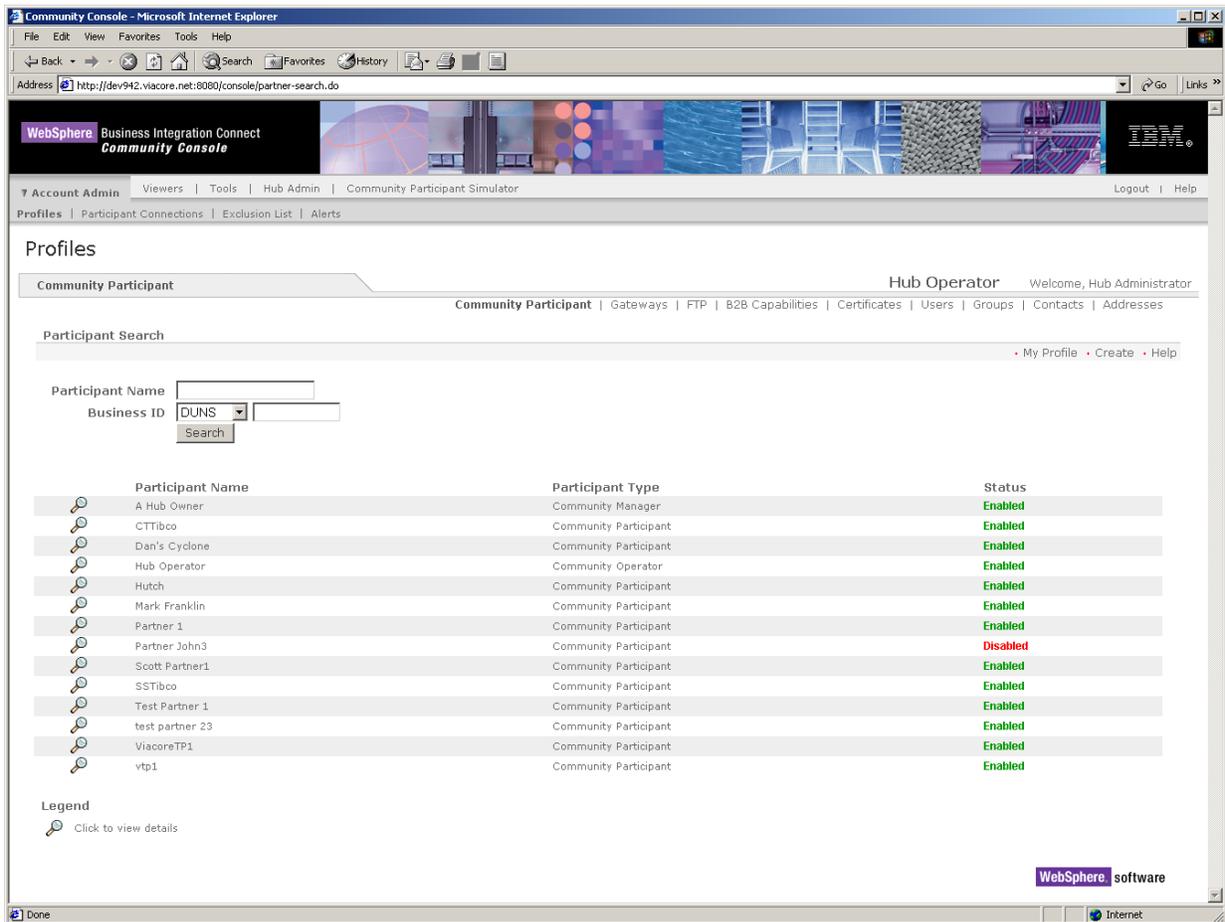


Figure 3-9. Example of Searching for Participants

4. To change the Participant's status, click **Enabled** or **Disabled** in the **Status** column.
5. To view the details for a Participant, click the  icon next to the Participant.
6. To edit the Participant profile, click the  icon and see [Table 3-1 on page 70](#).
7. When you finish, click **Save**.

Viewing your profile

To view your profile, use the following procedure.

1. Click **Account Admin** on the main menu and **Profiles** on the horizontal navigation bar. If the Participant Search screen is not displayed, click **Community Participants** to display it (see [Figure 3-1 on page 68](#)).

2. Click **My Profile**. The Console displays the My Profile screen (see [Figure 3-10 on page 77](#)).

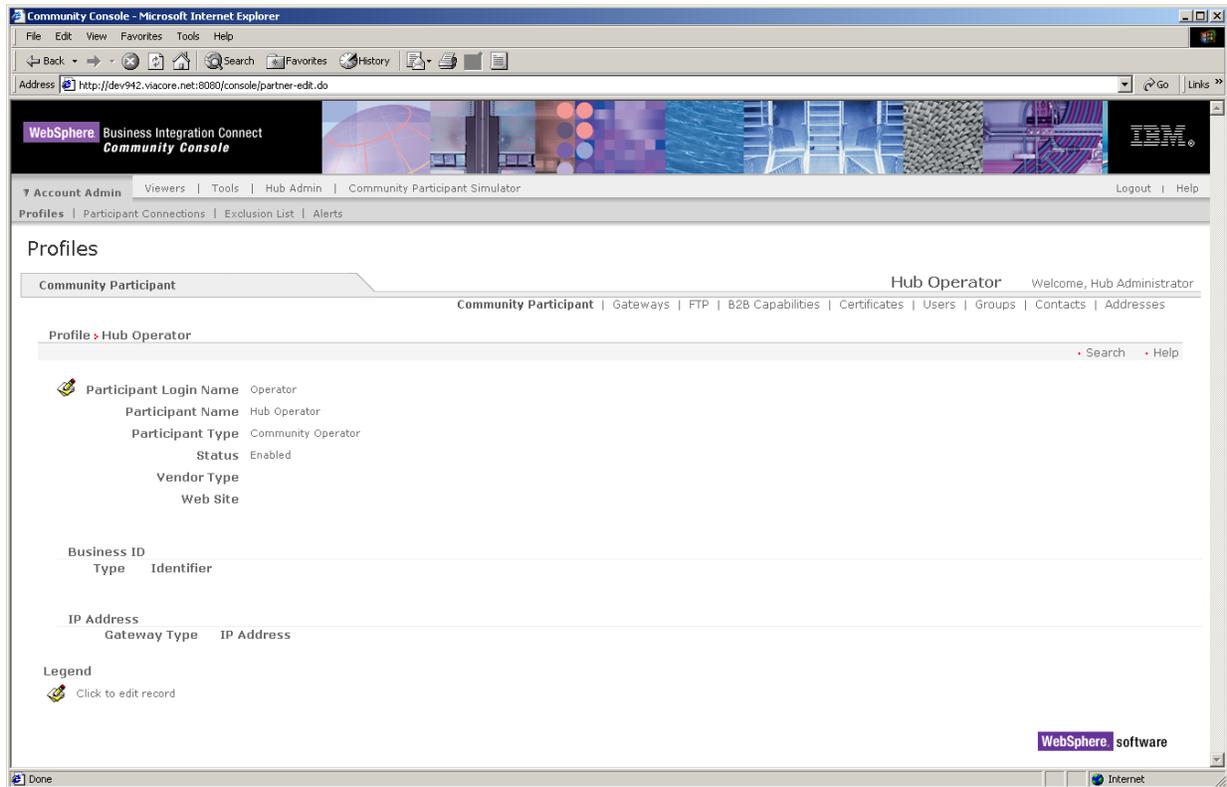


Figure 3-10. My Profile Screen

3. To edit your profile, click the  icon. The Console displays the screen in [Figure 3-11 on page 78](#).
4. Edit your profile (see [Table 3-1 on page 70](#)).
5. When you finish, click **Save**.

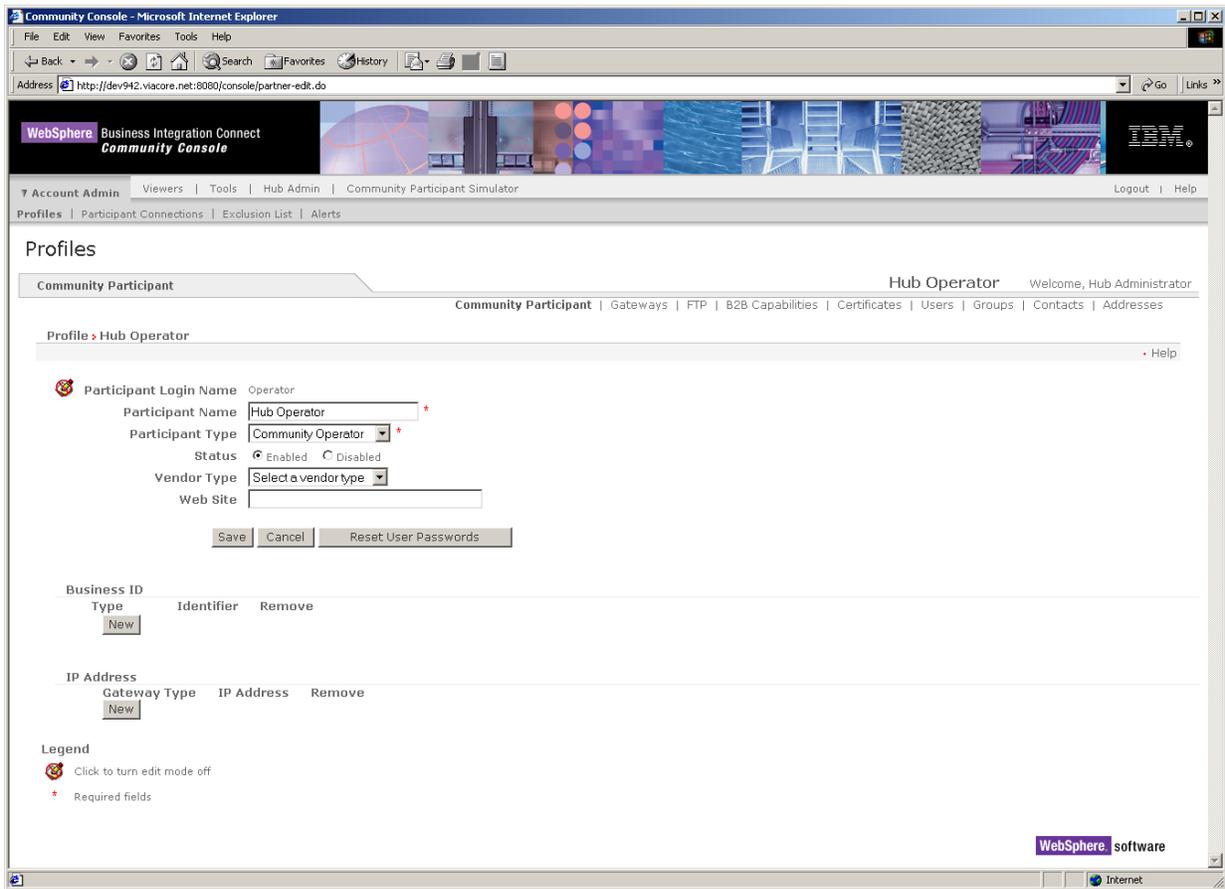


Figure 3-11. Editing Your Profile

Managing gateway configurations

Use gateways to manage the transport information used in routing documents to their proper destination in the hub-community. The outbound Transport protocol determines which information is used during gateway configuration.

Viewing and editing gateways

Use the following procedure to view the gateways configured for the system and edit them.

1. Click **Account Admin** on the main menu and **Profiles** on the horizontal navigation bar.
2. Click **Gateways**. The Console displays the list of gateways (see [Figure 3-12](#)).

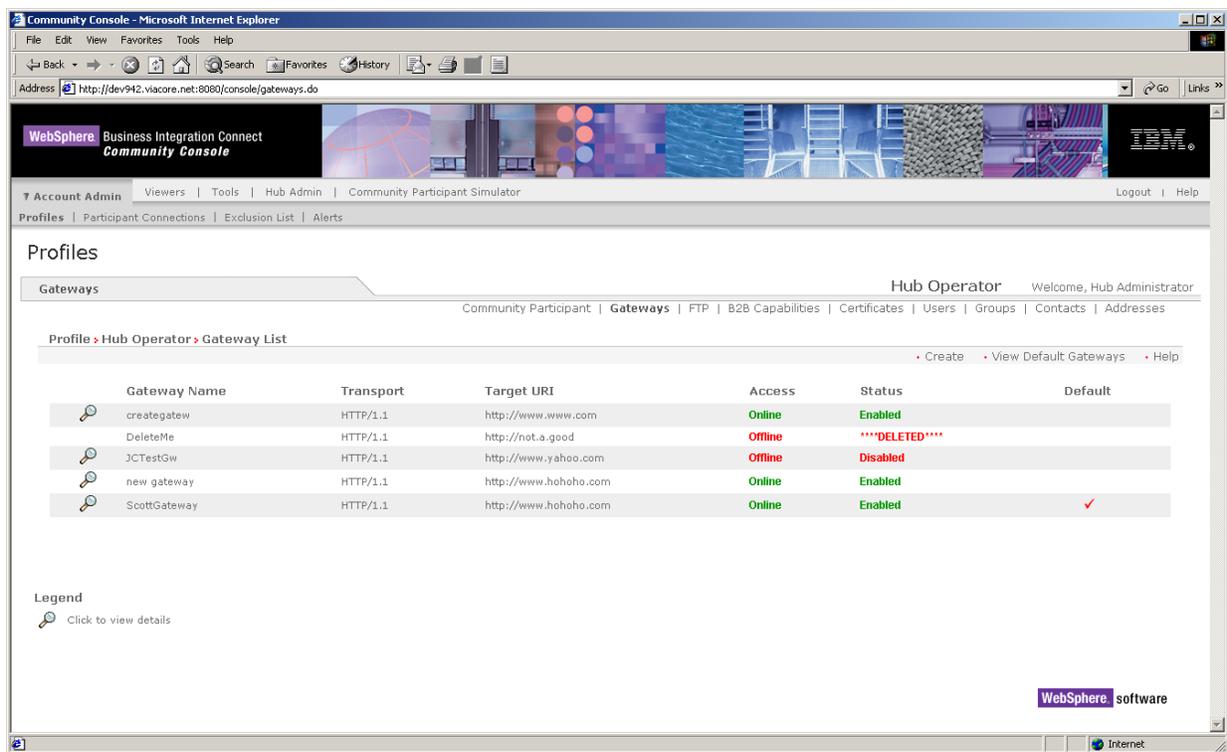


Figure 3-12. Sample Gateway List Screen

3. To change the access of a gateway, click **Online** or **Offline** under the **Access** column.
4. To change the status of a gateway, click **Enabled** or **Disabled** under the **Status** column.
5. To view gateway details, click the  icon next to a gateway. The Console displays the Gateway Detail screen (see [Figure 3-13 on page 80](#)).

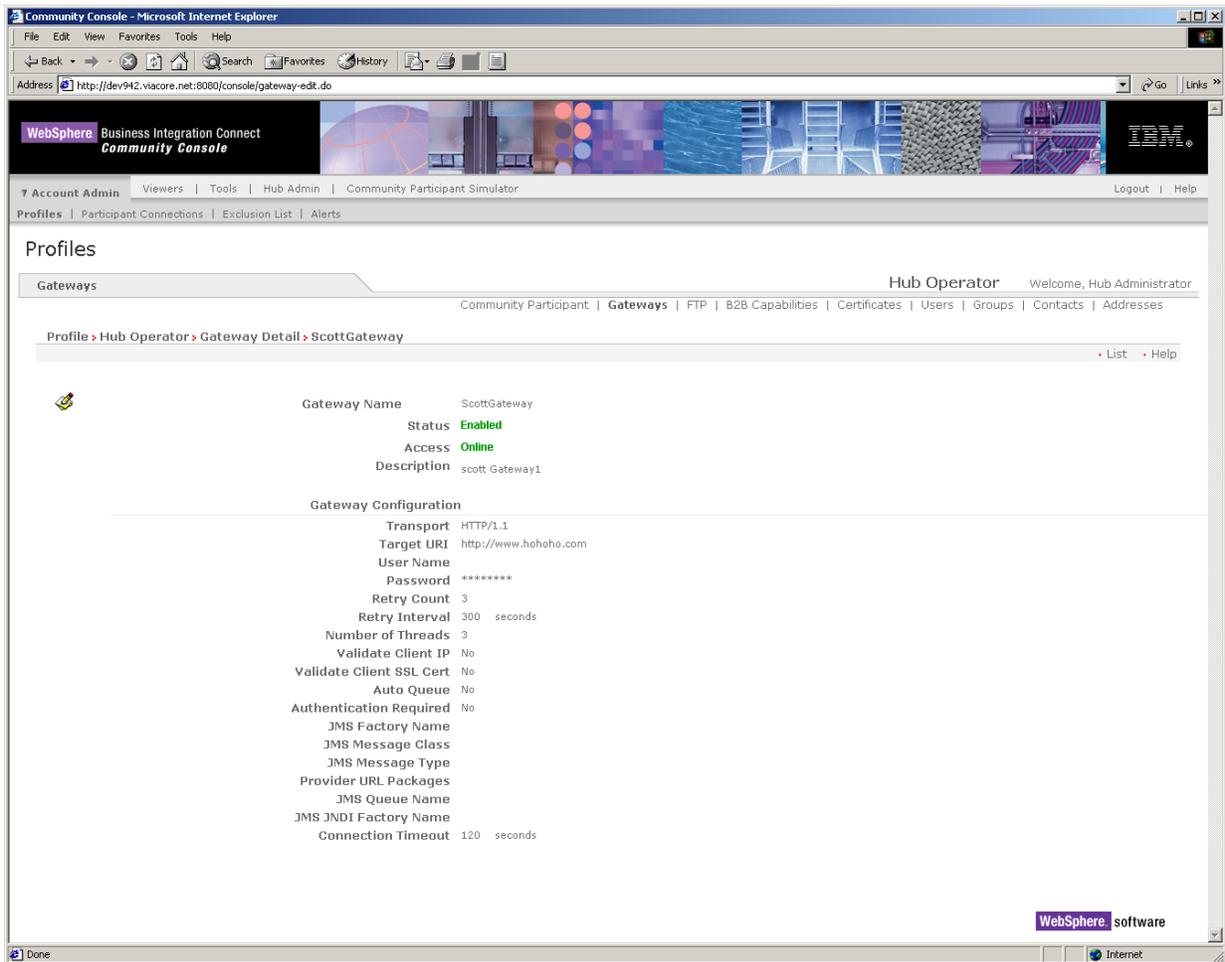


Figure 3-13. Gateway Detail Screen

- To edit the gateway details, click the  icon. The Console displays the Gateway Detail screen (see [Figure 3-14 on page 81](#)). Edit the parameters in the screen (see [Table 3-2 on page 81](#)), then click **Save**.

Alternatively, you can delete this gateway by clicking **Delete**.

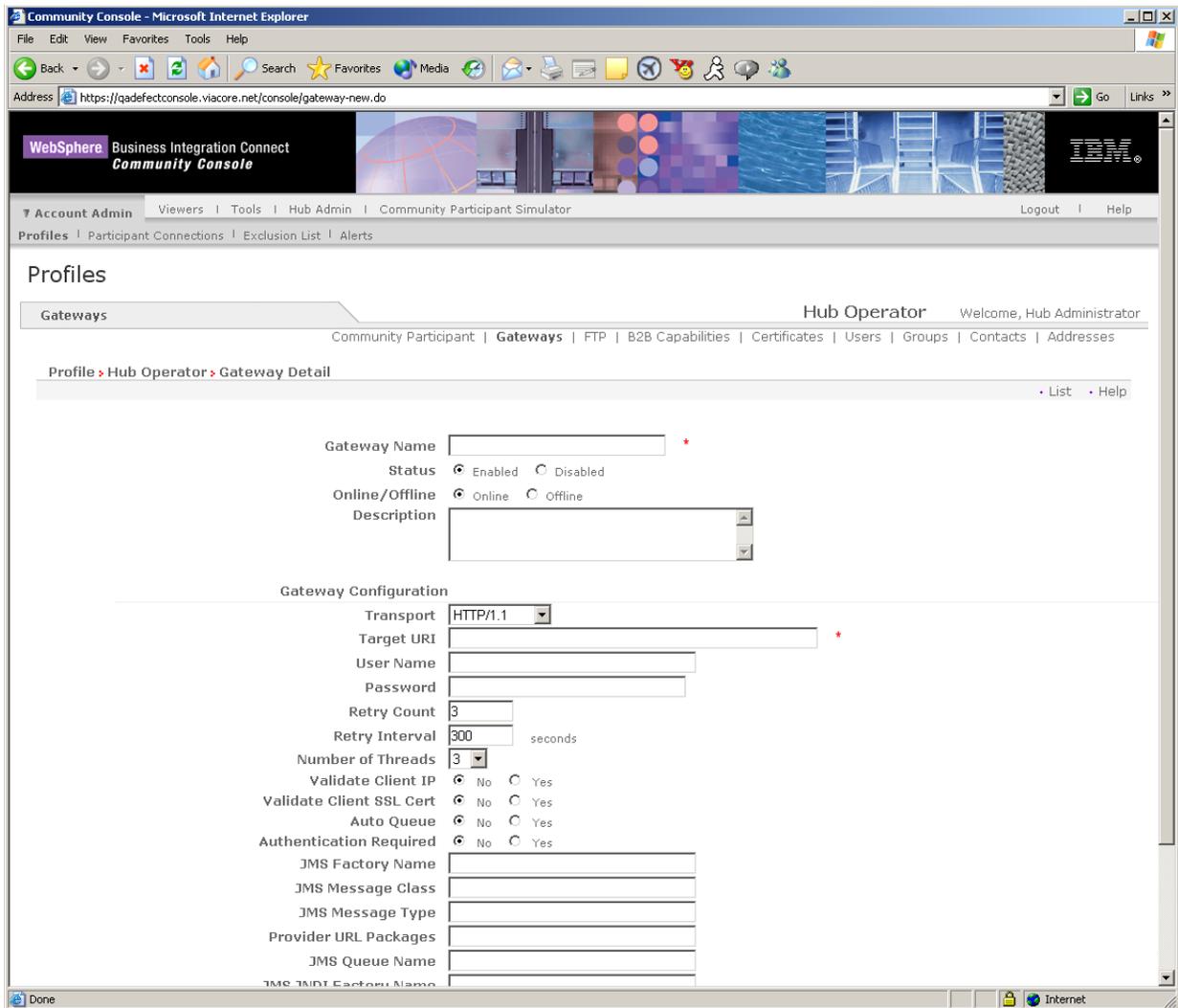


Figure 3-14. Gateway Detail Screen

Table 3-2. Gateway Detail Screen

Parameter	Description
Gateway Name	Name used to identify the gateway.
Status	Indicate whether the gateway is enabled or disabled. If disabled, documents passing through the gateway fail processing.
Online / Offline	Indicate whether the gateway is online or offline. If offline, documents are queued until the gateway is placed online.
Description	Optional description of the gateway.
Gateway Configuration	
Transport	Protocol for routing documents (see “Information required for gateway configuration” on page 84).

Table 3-2. Gateway Detail Screen (continued)

Parameter	Description
Target URI	Uniform Resource Identifier (URL) of the Participant.
User Name	User name for secure access through the Participant firewall.
Password	Password for secure access through the Participant firewall.
Retry Count	Maximum number of times the system tries to send a document before failing it. Default value is 3.
Retry Interval	Number of seconds the system pauses before trying to resend a document that was not sent successfully. Default value is 300 (5 minutes).
Number of Threads	Number of threads allocated for routing a document. Default value is 3. This parameter is available to Hub Admin users only.
Validate Client IP	Validates the IP address of the sending partner before processing the document.
Validate Client SSL Cert	Validates the sending Participant's digital certificate against the DUNS number associated with the document before processing the document.
Auto Queue	If enabled, documents are placed in a temporary repository if the gateway is placed offline. If disabled and the gateway is placed offline, the document fails to route and an error occurs.
Authentication Required	If enabled, user name and password are supplied with JMS messages.
JMS Factory Name	Name of the Java class the JMS provider will use to generate connection to the JMS queue.
JMS Message Class	Class of message.
JMS Message Type	Type of JMS message.
Provider URL Package	Name of classes or JAR file that Java uses to understand JMS Context URL.
JMS Queue Name	Queue name where JMS messages are stored.
JMS JNDI Factory Name	Factory name used to connect to the name service.
Connection Timeout	Number of seconds the JMS session remains active. Default value is 120 (2 minutes).

Viewing default gateways

Use the following procedure to view default gateways configured for the system and edit them.

1. Click **Account Admin** on the main menu and **Profiles** on the horizontal navigation bar.
2. Click **Gateways**. The Console displays the list of gateways (see [Figure 3-12 on page 79](#)).
3. Click **View Default Gateways**. The Console displays a list of all gateway types with their associated gateway.
4. To view information associated with a default gateway, click the  icon next to the gateway. The Console displays a Gateway Detail screen (see [Figure 3-15 on page 83](#)).

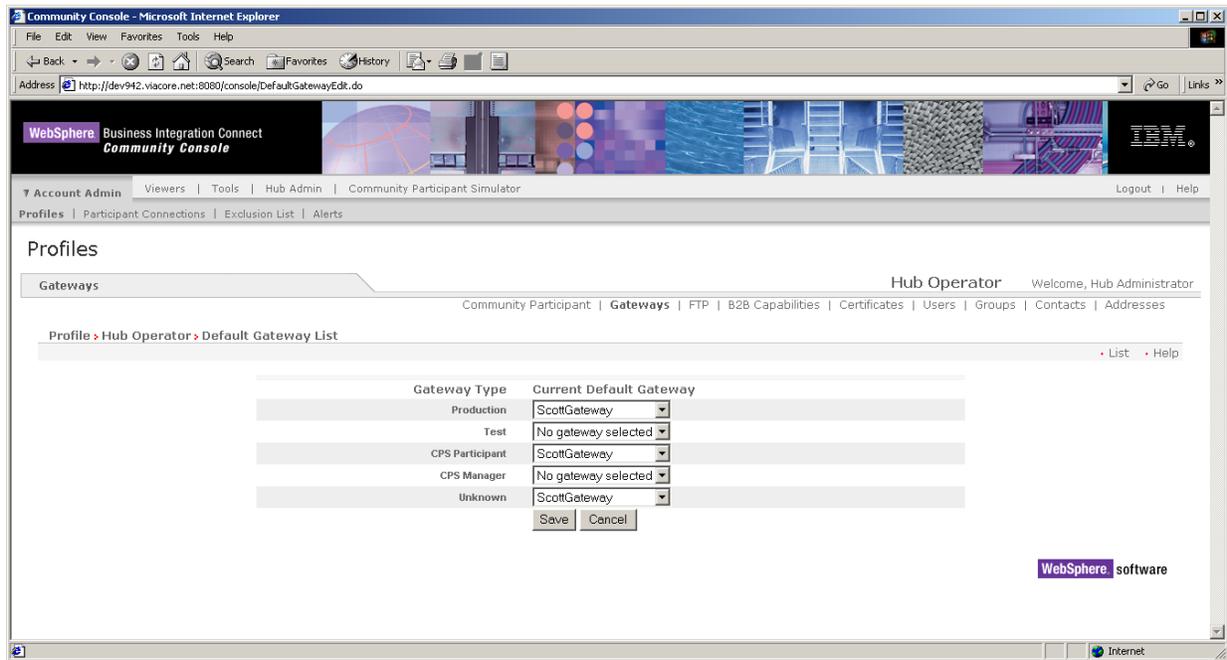


Figure 3-15. Default Gateway Screen

5. Edit the information as desired, then click **Save**.
6. Alternatively, you can delete this default gateway by clicking **Delete**.

Creating gateways

To create gateways, use the following procedure.

1. Click **Account Admin** on the main menu and **Profiles** on the horizontal navigation bar.
2. Click **Gateways**. The Console displays a list of gateways (see [Figure 3-12 on page 79](#)).
3. Click **Create**. The Console displays the Gateway Detail screen (see [Figure 3-15 on page 83](#)).
4. Complete the parameters in the screen (see [Table 3-2 on page 81](#)).
5. Click **Save**.

Deleting gateway configurations

If you no longer need a gateway configuration, use the following procedure to delete it. A precautionary message does not appear before you delete a gateway configuration. Therefore, be sure you do not need the gateway configuration before you delete it.

1. Click **Account Admin** on the main menu and **Profiles** on the horizontal navigation bar.
2. Click **Gateways**. The Console displays a list of gateways (see [Figure 3-12 on page 79](#)).
3. Click the  icon next to the gateway you want to delete. The Console displays the Gateway Detail screen (see [Figure 3-13 on page 80](#)).
4. Click the  icon.
5. Click **Delete**.

Information required for gateway configuration

The transport type selected determines the information needed for gateway setup. The boxes marked with an X require configuration information, boxes marked with the letter O are optional.

Transport	HTTP	HTTPS	FTP	JMS	File Directory	SMTP
Target URI	X	X	X		X	X
User Name	O	O	O	O	O	O
Password	O	O	O	O	O	O
Retry Count	X	X	X	X	X	X
Retry Interval	X	X	X	X	X	X
Number of Threads	X	X	X	X	X	X
Validate Client IP	O	O	O			
Validate Client SSL Cert		O				
Auto Queue	O	O	O	O		O
Authentication Required	O	O	X	O		O
JMS Factory Name				X		
JMS Message Class				X		
JMS Message Type				X		
Provider URL Package				X		
JMS Queue Name				X		
JMS JNDI Factory Name				X		
Connection Timeout	X	X	X			

NOTE: The ability to edit certain gateway configuration values varies with the permission level of the user.

Creating an FTP account

The File Transfer Protocol (FTP) is a protocol used on the Internet for sending files. Documents sent by Participants to the WebSphere Business Integration Connect system are routed through the FTP server ProFTPD. Using the FTP module, you can create an account for routing documents using ProFTPD.

To use ProFTPD with Business Integration Connect:

- ProFTPD must be installed and configured prior to creating an FTP account.
- Perl 5.6 is required for ProFTPD support within the Community Console.

NOTE: FTP documents routed to the system with a disabled status or incorrect password are rejected.

Specifying an FTP server

To define an FTP server for Business Integration Connect, use the following procedure.

1. Click **Account Admin** on the main menu and **Profiles** on the horizontal navigation bar.
2. Click **FTP**. The Console displays the FTP Configuration screen (see [Figure 3-16](#)).

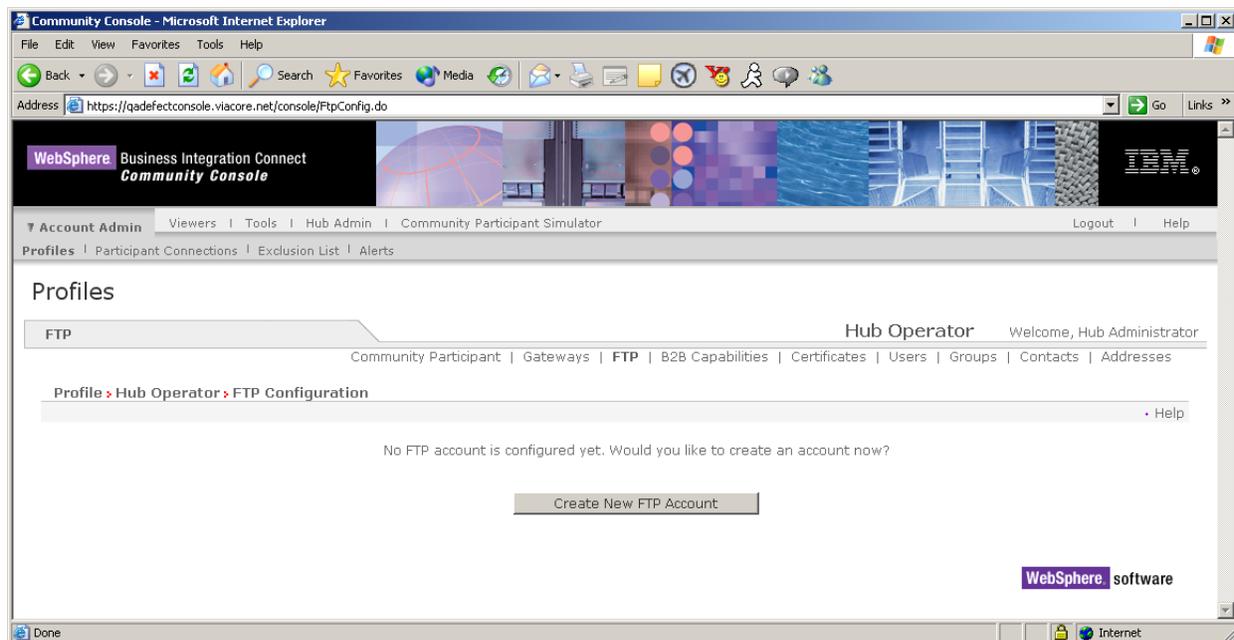


Figure 3-16. FTP Configuration Screen

3. Click **Create New FTP Account**. The system creates the account with a system-supplied password.

- To change the password or status, click the  icon. The Console displays the FTP screen (see [Figure 3-17 on page 86](#)).

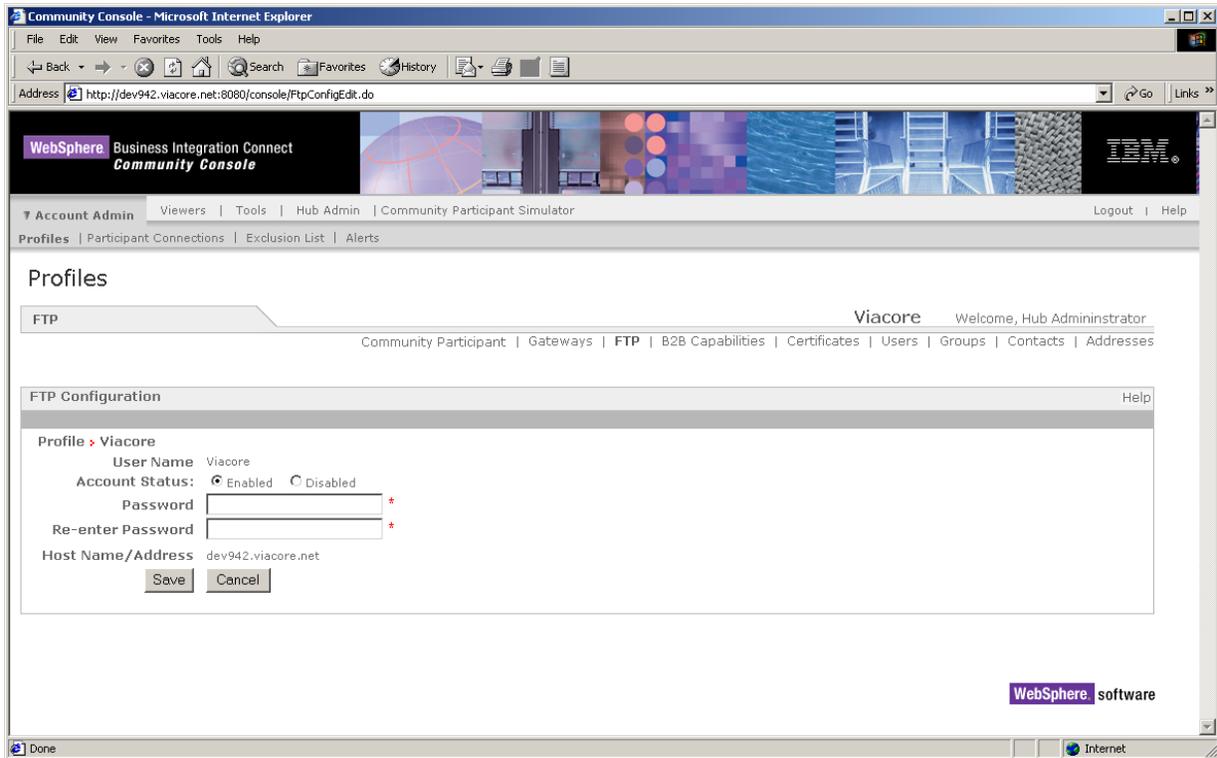


Figure 3-17. FTP Configuration Screen

- Complete the following parameters in the screen:

Table 3-3. FTP Configuration Screen

Value	Description
Account Status	Allows you to enable or disable your FTP account.
Password	Password for access to the FTP directory. For security, each password character is displayed as an asterisk (*).
Re-enter Password	Same entry as Password. For security, each password character is displayed as an asterisk (*).

- Click **Save**.

Editing FTP details

To change the FTP password or status, use the following procedure.

1. Click **Account Admin** on the main menu and **Profiles** on the horizontal navigation bar.
2. Click **FTP**. The Console displays the FTP Configuration screen (see [Figure 3-18](#)).

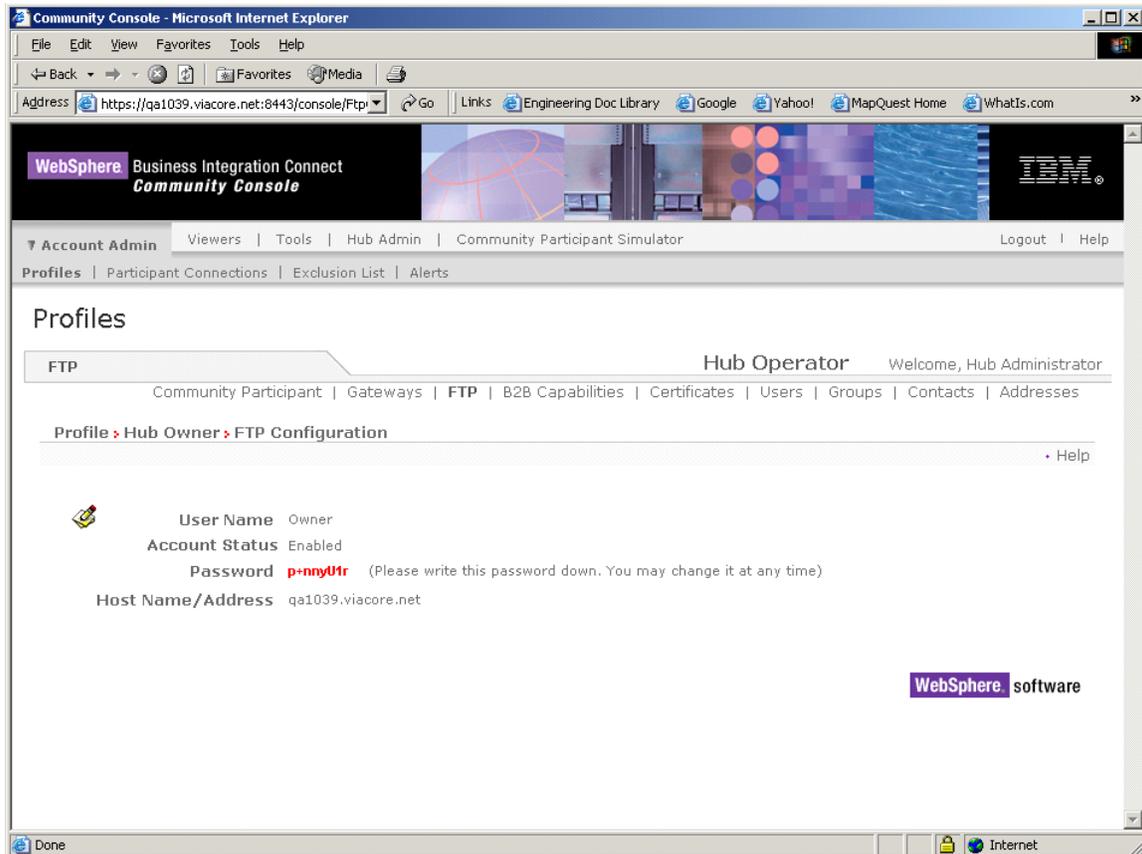


Figure 3-18. FTP Configuration Screen

3. Click the  icon.
4. Complete the following parameters in the screen:

Table 3-4. FTP Configuration Screen

Value	Description
Account Status	Allows you to enable or disable your FTP account.

Table 3-4. FTP Configuration Screen (continued)

Value	Description
Password	Password for access to the FTP directory. For security, each password character is displayed as an asterisk (*).
Re-enter Password	Same entry as Password. For security, each password character is displayed as an asterisk (*).

5. Click **Save**.

Managing certificates

A digital certificate is an online identification credential, similar to a driver's license or passport. It verifies an individual with a "guarantee of identity." Part of a digital certificate is digital signatures. Digital signatures are calculations based on an electronic document using public-key cryptography. Through this process, the digital signature is tied to the document being signed, as well as to the signer, and cannot be reproduced. With the passage of the federal digital signature bill, digitally signed electronic transactions have the same legal weight as transactions signed in ink.

Business Integration Connect uses digital certificates to verify the authenticity of business document transactions between the Community Manager and Participants. They are also used for encryption and decryption. Digital certificates were uploaded and identified during the configuration process.

NOTE: Before you can use the procedures in this section, the certificates must be loaded into the system. For more information, refer to "[Administering Certificates](#)" on page 121.

Viewing and editing digital certificates

Use the following procedure to view a list of the digital certificates that have been defined for the system and edit them.

1. Click **Account Admin** on the main menu and **Profiles** on the horizontal navigation bar.
2. Click **Certificates**. The Console displays the Digital Certificate List (see [Figure 3-19 on page 89](#)).

NOTE: Red digital certificate dates indicate that the certificate has expired or is not yet valid.

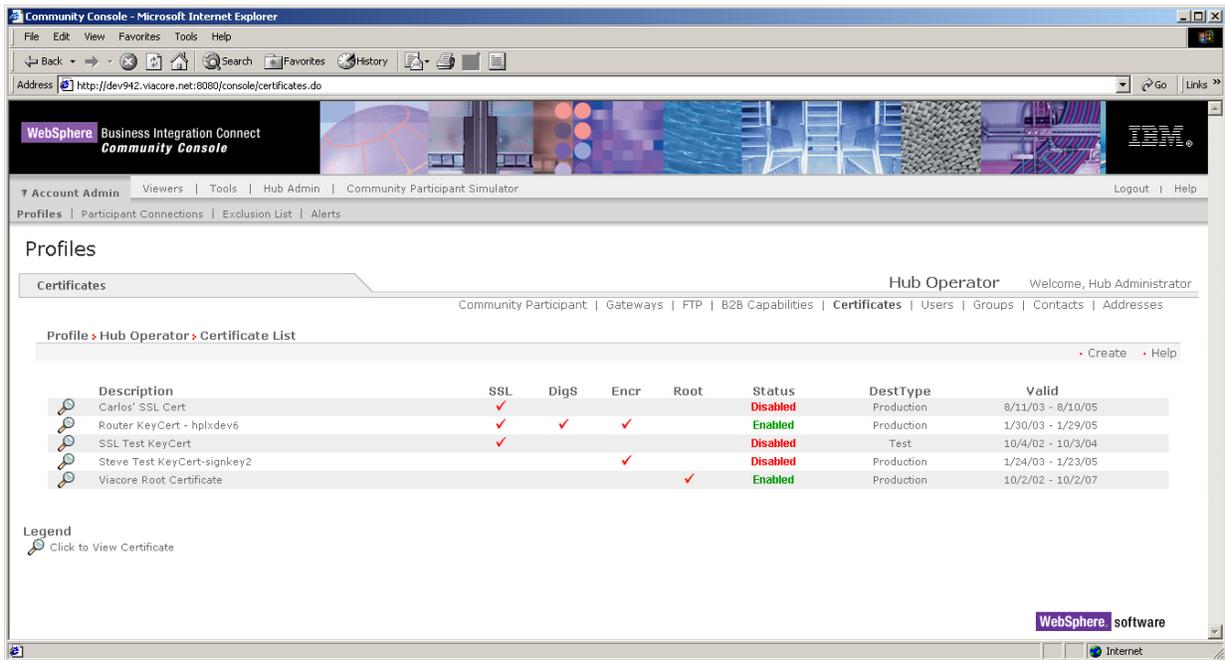


Figure 3-19. Example of Digital Certificate List

- To view details about a certificate, click the  icon next to the certificate. The Console displays the Viewing Certificate Details screen (see [Figure 3-20 on page 90](#)).

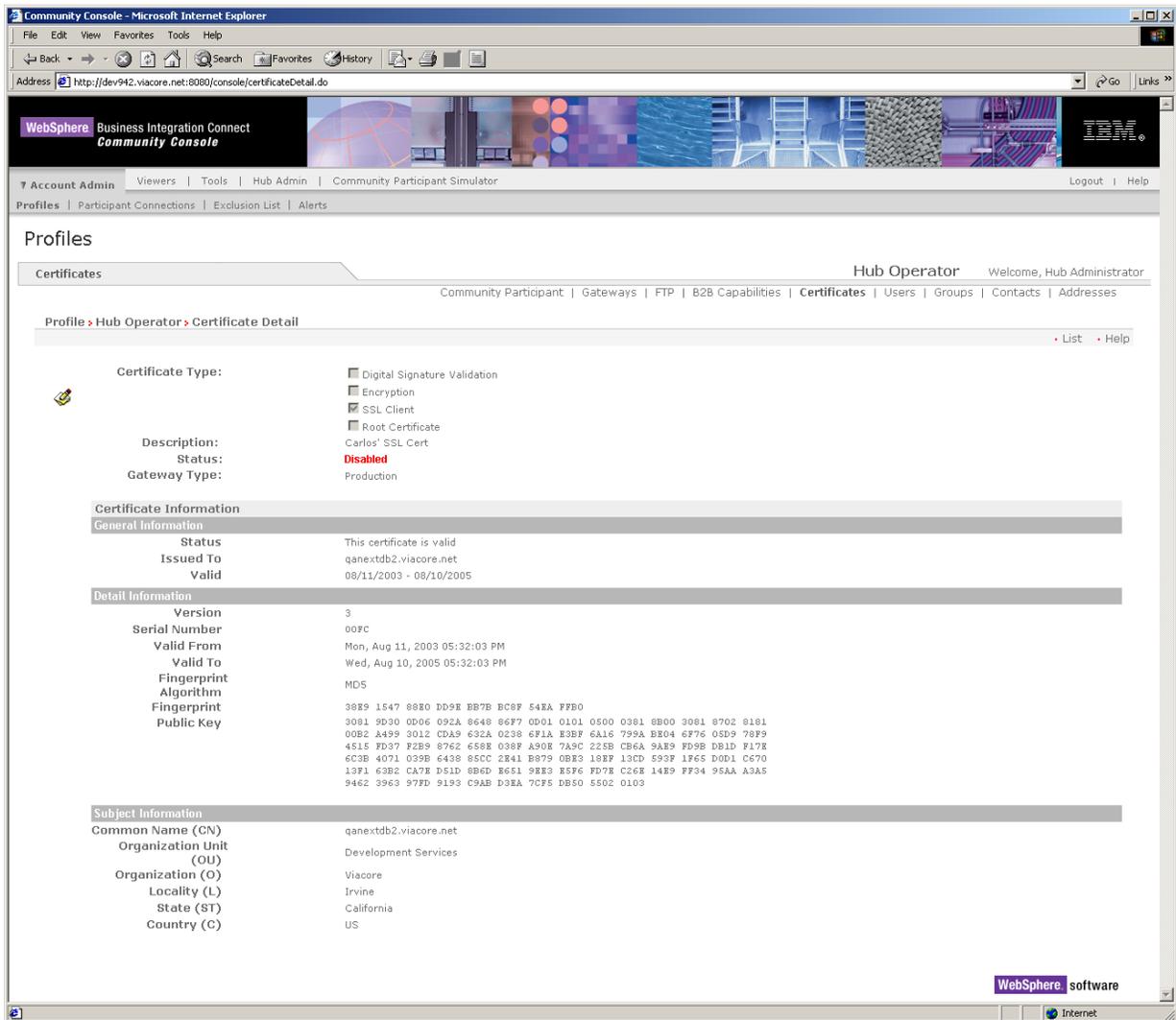


Figure 3-20. Viewing Certificate Details

- To edit the digital certificate, click the  icon. The Console displays the Certificate Detail screen (see Figure 3-21 on page 91).

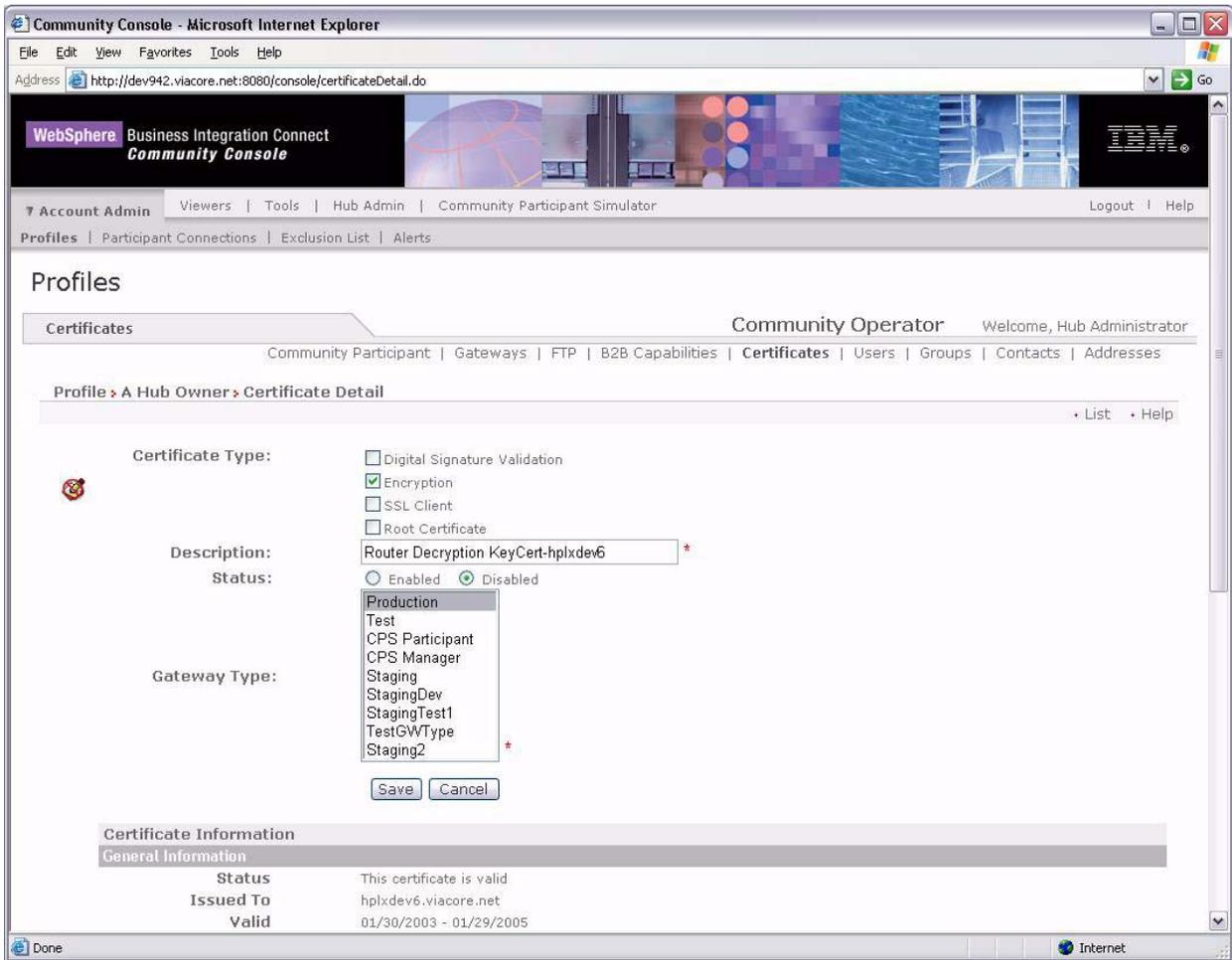


Figure 3-21. Certificate Detail Screen

5. Complete the following parameters in the screen, then click **Save**. Alternatively, you can delete the certificate by clicking **Delete**.

Table 3-5. Digital Certificate Parameters

Parameter	Description
Certificate Type	Type of digital certificate: <ul style="list-style-type: none">• Digital Signature Validation – authenticates the digital signature on documents coming from a Participant.• Encryption — contains the public key for encrypting outgoing documents to a Participant.• SSL Client — authenticates a Participant's certificate used for initiating an SSL connection.• Root Certificate — certificate issued from certifying authority for establishing certificate chain.
Description	Text that describes the certificate.
Status	Enables or disables the certificate.
Gateway Type	Select the type of gateway associated with the certificate.

Creating digital certificates

To create digital certificates, use the following procedure.

1. Click **Account Admin** on the main menu and **Profiles** on the horizontal navigation bar.
2. Click **Certificates**. The Console displays the Digital Certificate List (see [Figure 3-19 on page 89](#)).

NOTE: Red digital certificate dates indicate that the certificate has expired or is not yet valid.

3. Click **Create**. The Console displays the Create New Certificate screen (see [Figure 3-22 on page 93](#)).

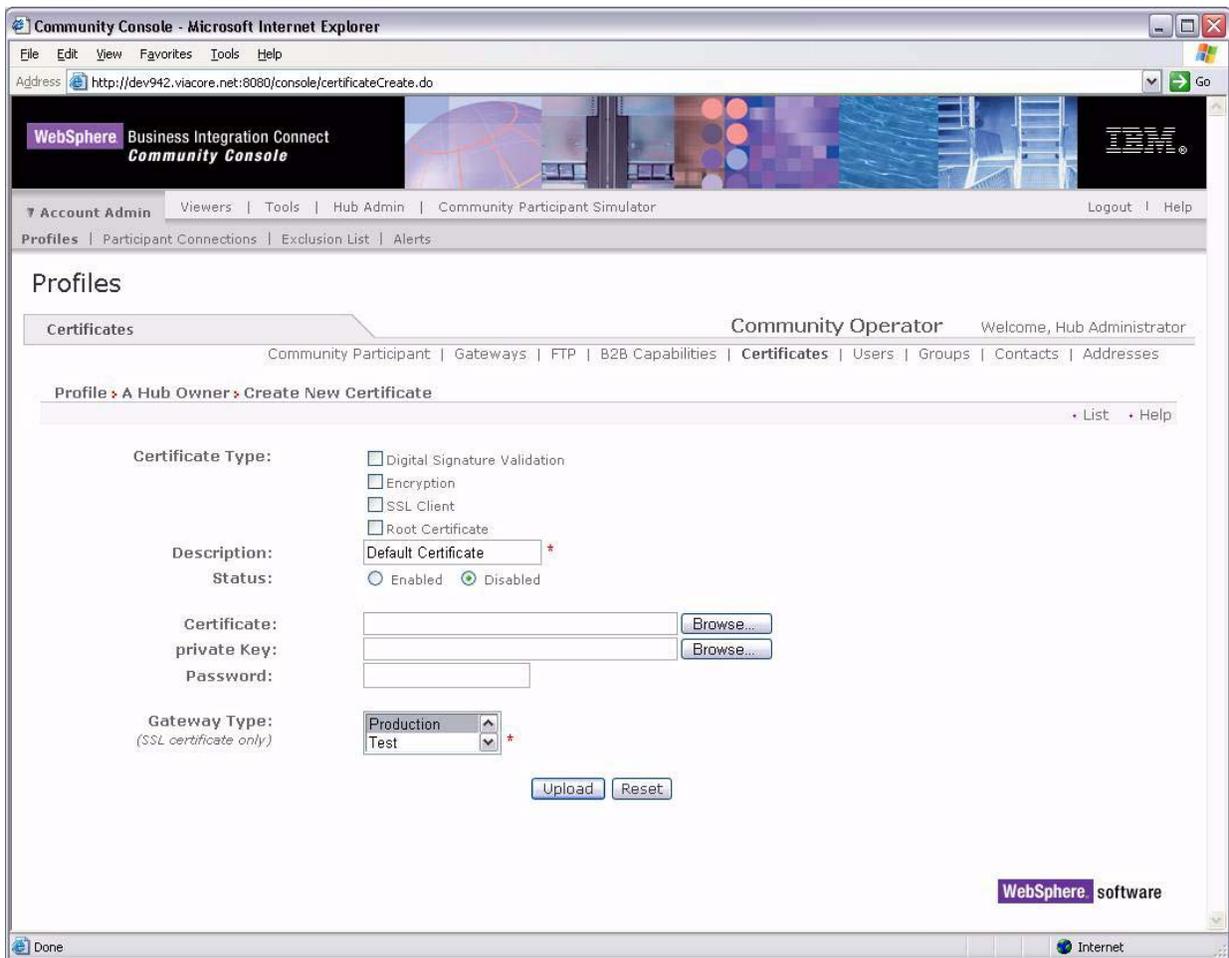


Figure 3-22. Create New Configuration Screen

4. Complete the following parameters in the screen:

Table 3-6. Digital Certificate Parameters

Parameter	Description
Certificate Type	Type of digital certificate: <ul style="list-style-type: none"> • Digital Signature Validation – authenticates the digital signature on documents coming from a Participant. • Encryption — contains the public key for encrypting outgoing documents to a Participant. • SSL Client — authenticates a Participant's certificate used for initiating an SSL connection. • Root Certificate — certificate issued from certifying authority for establishing certificate chain.
Description	Text that describes the certificate.

Table 3-6. Digital Certificate Parameters (continued)

Parameter	Description
Status	Enables or disables the certificate.
Certificate	Type the path and name of the certificate you want to use or browse and select the certificate.
private Key	Type the path and name of the private key you want to use for this certificate or browse and select the private key.
Password	Type the password you want to use.
Gateway Type	If you are creating an SSL certificate, select the type of gateway associated with the certificate.

NOTE: If a connection requires a digital certificate, and all certificates for that connection are disabled, the document fails processing.

5. Click **Upload**.

Disabling a digital certificate

If you do not want to use a digital certificate, use the following procedure to disable it.

1. Click **Account Admin** on the main menu and **Profiles** on the horizontal navigation bar.
2. Click **Certificates**. The Console displays the Digital Certificate List (see [Figure 3-19 on page 89](#)).
3. Click the  icon next to the certificate you want to disable.
4. Click the  icon to edit certificate details.
5. For **Status** select **Disabled**.
6. Click **Save**.

Managing B2B capabilities

The B2B industry consists of various business processes, protocols, and delivery standards. Business Integration Connect supports these different business-collaboration types using the concepts of Document Flow Definitions and nodes. With Document Flow Definitions and nodes, the Participant types his or her B2B capabilities into the system, so connections can be created for document routing and processing.

The core of Business Integration Connect is B2B connectivity between disparate business processes, protocols, and delivery standards. The system handles these requirements using Document Flow Definitions and nodes. Participants use the B2B Capabilities feature to define their B2B capabilities using Document Flow Definitions and nodes.

A Document Flow Definition is a collection of “meta-information” that defines the document-processing capabilities of the Participant. For the system to process a business document, two or more Document Flow Definitions must be linked to create a node. A node contains all the necessary information the system needs to receive, process, and route documents between the Participant and Manager.

Because of the different types of business processes, protocols, and delivery standards available in the B2B industry, the system contains different node configurations to meet the various business-processing requirements of the Community Manager and Participants. To ensure that the system meets these requirements, you can use the B2B Capabilities feature to associate a Participant's B2B capabilities to a Document Flow Definition. The system then uses values added to each Document Flow Definition to manage the Participant's B2B capabilities.

Types of Document Flow Definitions

The system uses up to five different Document Flow Definitions to define its document-processing capabilities:

- **Package** — specifications describing document format, packaging, encryption, and content-type identification.
- **Protocol** — structure and location of information within the document needed for processing and routing.
- **Document Flow** — the business transaction between the Community Manager and Participant.
- **Activity** — the business function a document flow performs.
- **Action** — the actual electronic documents exchanged in a document flow.

The Participant normally sets his or her B2B capabilities at the Action level.

Document Flow Definition attributes

Each Document Flow Definition contains attributes (or information) that determine its functionality. The system uses the attribute information for various document processing and routing functions such as validation, checking for encryption, retry count, etc. The attributes for each Document Flow Definition are set with default values. The user can change these values based on their own document routing and processing requirements.

Setting B2B capabilities

Use the following procedure to set the B2B capabilities of your system.

1. Click **Account Admin** on the main menu and **Profiles** on the horizontal navigation bar.
2. Click **B2B Capabilities**. The Console displays the B2B capabilities screen (see [Figure 3-23 on page 96](#)). The right side of the screen shows the packages, protocols, and business processes supported by the system as Document Flow Definitions (for more information, see [“Understanding Document Flow Definitions” on page 33](#)).

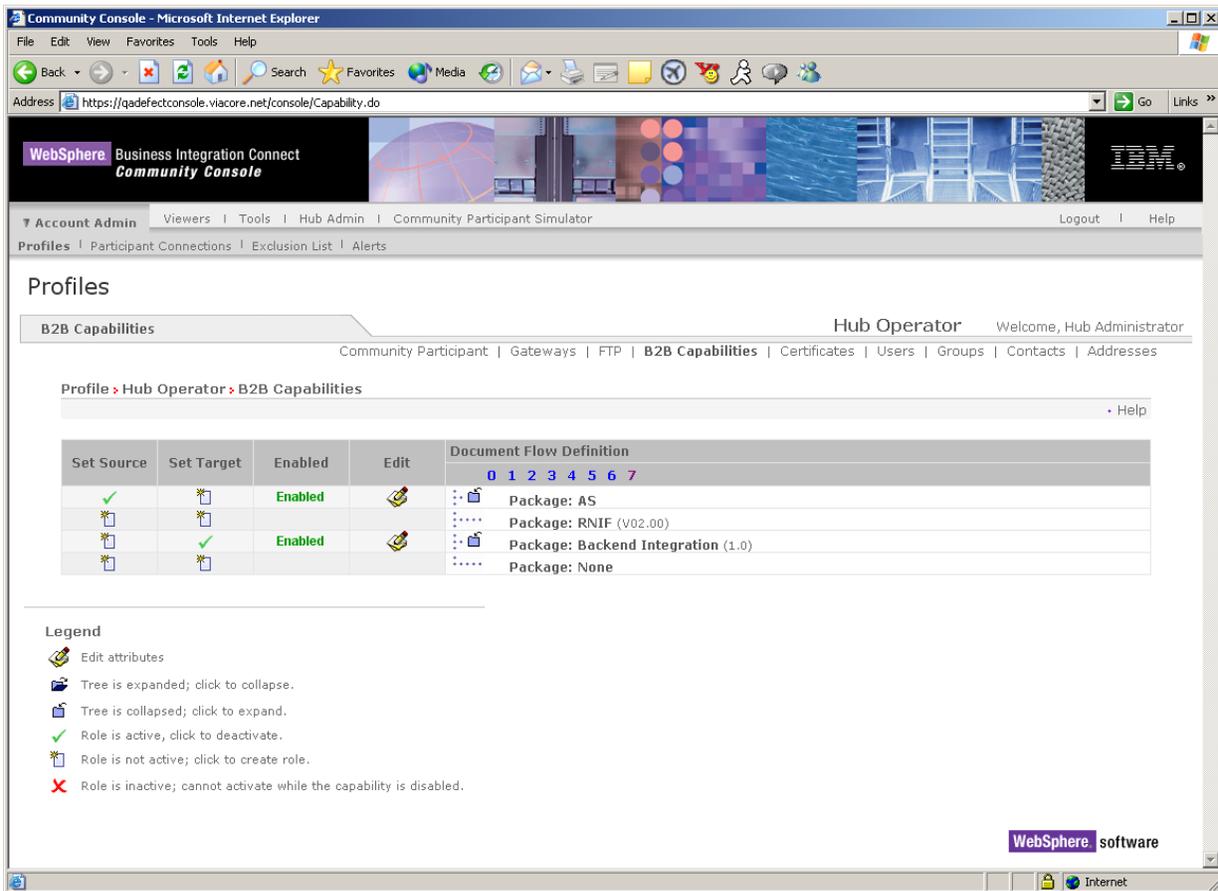


Figure 3-23. B2B Capabilities Screen

- Click the icon under the **Set Source** column for the Packages on the right that contain business processes you will send to the Community Manager.
- Click the icon under **Set Target** for the Packages that contain business processes you will receive from the Community Manager.
- Select both if you will send and receive those same processes. The Console displays a icon if the Document Flow Definition is enabled.

NOTE: The selection of **Set Source** will be the same for all actions in 2-way PIP regardless that the request will originate from one Participant and the corresponding confirmation from another. This also applies to **Set Target**.

- Click the icon at the Package level to expand an individual node to the appropriate Document Flow Definition level or select a number from 0-7 to expand all displayed Document Flow Definition nodes to the selected level.
- Again, select the **Set Source**, **Set Target**, or both roles for the lower Protocol, Document Flow, Action, and Activity levels for each Document Flow Definition your system supports.

TIP: If a definition is activated at the Document Flow level, both the Action and Activity definitions will be activated automatically.

5. (Optional) Click **Enabled** under the **Enabled** column to place a Document Flow Definition offline. Click **Disabled** to place online.

NOTE: If a package Document Flow Definition is disabled, all lower-level Document Flow Definitions in that same node are also disabled, regardless of whether their individual status was enabled.

If a lower-level Document Flow Definition is disabled, all higher-level definitions within the same node remain enabled.

When a Document Flow Definition is disabled, all preexisting connections and attributes continue to function. The disabled Document Flow Definition only restricts the creation of new connections.

6. (Optional) Click the  icon to display the screen in [Figure 3-24 on page 98](#). Then edit the attribute values for each Document Flow Definition.
7. Click **Save**.

Changing B2B attribute values

Attributes values give a Document Flow Definition its functionality. The system uses the attribute values for various document processing and routing functions such as validation, checking for encryption, retry count, synchronous or asynchronous communication, etc. Changes to the attribute values for a higher-level Document Flow Definition will be inherited by the lower-level definitions within the same node.

To change the attribute values in a Document Flow Definition, use the following procedure.

1. Click **Account Admin** on the main menu and **Profiles** on the horizontal navigation bar.
2. Click **B2B Capabilities**. The Console displays the B2B capabilities screen (see [Figure 3-23 on page 96](#)).
3. Click to individually expand a node to the appropriate Document Flow Definition level or select a number from 0-7 to expand all displayed Document Flow Definition nodes to the selected level.
4. Click the  icon to display the screen in [Figure 3-24 on page 98](#). Then modify the appropriate attribute values in the **Update** column.

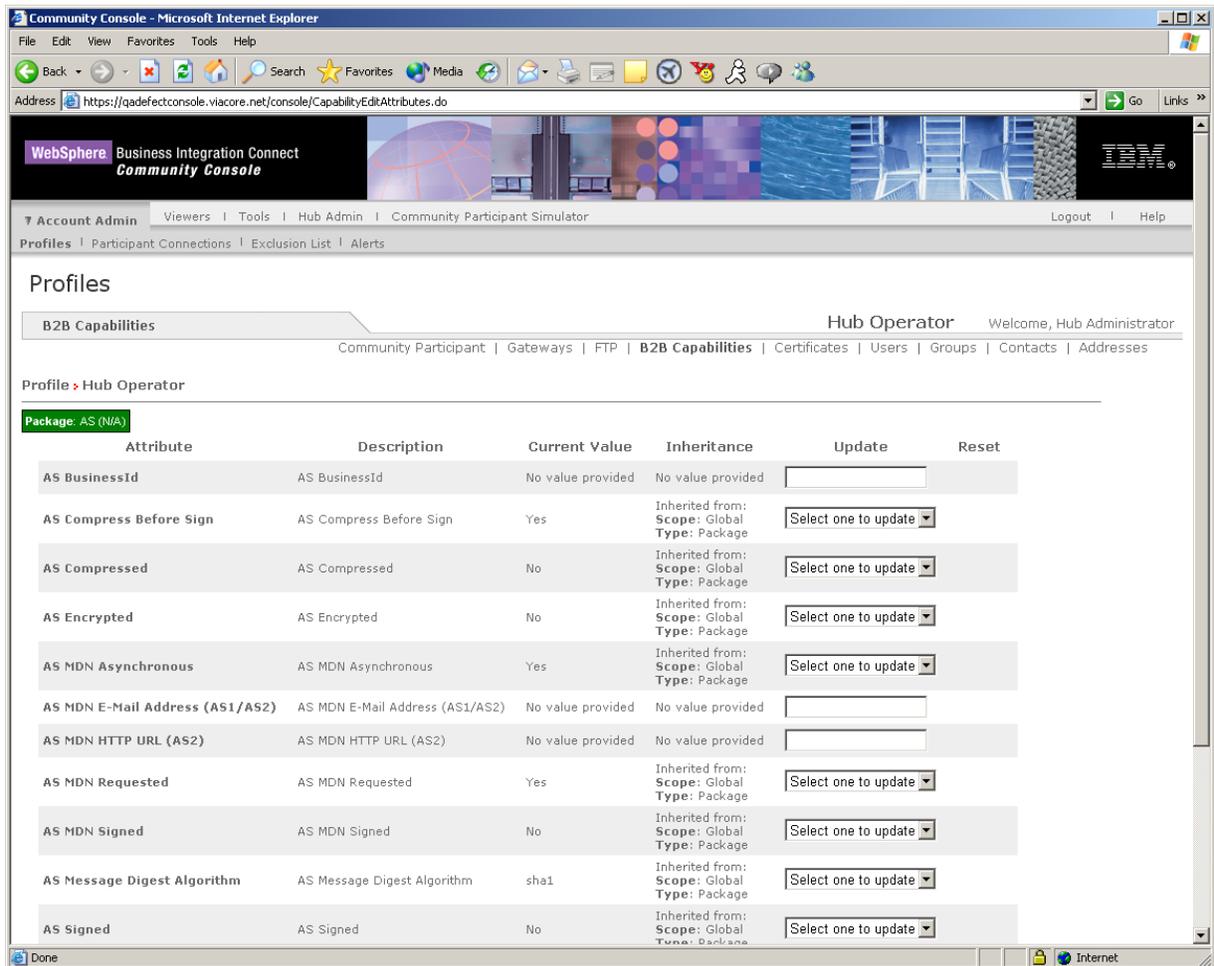


Figure 3-24. Screen for Changing B2B Attribute Values

5. Click **Save**.

Managing Participant connections

Participant connections are the mechanism that enables the system to process and route documents between the Community Manager and its various Participants. Connections contain the information necessary for the proper exchange of each document flow including RosettaNet TPA attributes, transport protocol, document processing action, gateway type, and Participant gateway. A document cannot be routed unless a connection exists between the Community Manager and one of its Participants.

The system automatically creates connections between the Community Manager and Participants based on their B2B capabilities. The data typed in the B2B Capabilities module of the Community Console determines the functionality of each available connection. The configuration of each connection can be modified to fit the needs of the hub-community.

Connection components

Individual connections are composed of four components:

- Attributes
- Action
- Gateway
- Gateway type

Once the system creates a connection, all four components can be modified to tailor its routing and processing functionality. [Table 3-7](#) describes each component.

Table 3-7. Manage Participant Components

Component	Description
Attributes	Attributes are the information the connection uses for various document processing and routing functions such as validation, checking for encryption, and retry count. To increase the efficiency when creating connections, the attributes for a new connection are inherited from the B2B capabilities of the Manager and Participant automatically.
Action	Action is the sequence of steps the system uses to process a particular document. Each connection typically consists of one or more steps, including transformation, duplicate check, validation, or pass-through routing. You can select the appropriate action for each connection.
Gateway	Each gateway contains the URL, transport protocol, and routing configuration data of the target Participant. A gateway is assigned to each gateway type within the connection.
Gateway Type	Gateway type identifies the nature of a document being exchanged. A connection can contain multiple types of gateways to accommodate the routing and processing of the same document to more than one system. This improves connection efficiency by multiplying the use of a single connection for production, test, or routing to multiple systems within one organization.

Connection duplication

The system avoids the inadvertent duplication of connections by uniquely identifying each connection based on the following parameters:

- Target
- Source
 - Source package & version
 - Source protocol & version
 - Source process & version

In the following example, for instance, the system will not activate two connections using the same source participant and attributes with the same target participant — even though the target participant is using the RosettaNet protocol in one connection and the RNSC protocol in the other. In this case, the connection containing the target RosettaNet protocol must be deactivated before the system allows the other connection containing the target RNSC protocol to be used.



Searching for connections

To access connections, you search for them. There are two ways to search for connections:

- Using the Managing Connections screen to search for connections by selecting the source and target. See “[Performing a basic search for connections](#),” below.
- Using the system’s Advanced Search facility to specify additional search criteria including Business ID, initiating and receiving packages and protocols, and initiating and receiving document flows. See “[Performing an advanced search for connections](#)” on page 104.

Performing a basic search for connections

Use the following procedure to perform a basic search for connections. When selecting a Source and a Target, observe the following guidelines:

- The Source and Target must be unique.
 - Do not mix a production gateway with a test gateway when selecting Source and Target; otherwise, an error occurs. Both the Source and the Target must be production or test gateways.
1. Click **Account Admin** on the main menu and **Participant Connections** on the horizontal navigation bar. The Console displays the Manage Connections screen (see [Figure 3-25](#)).

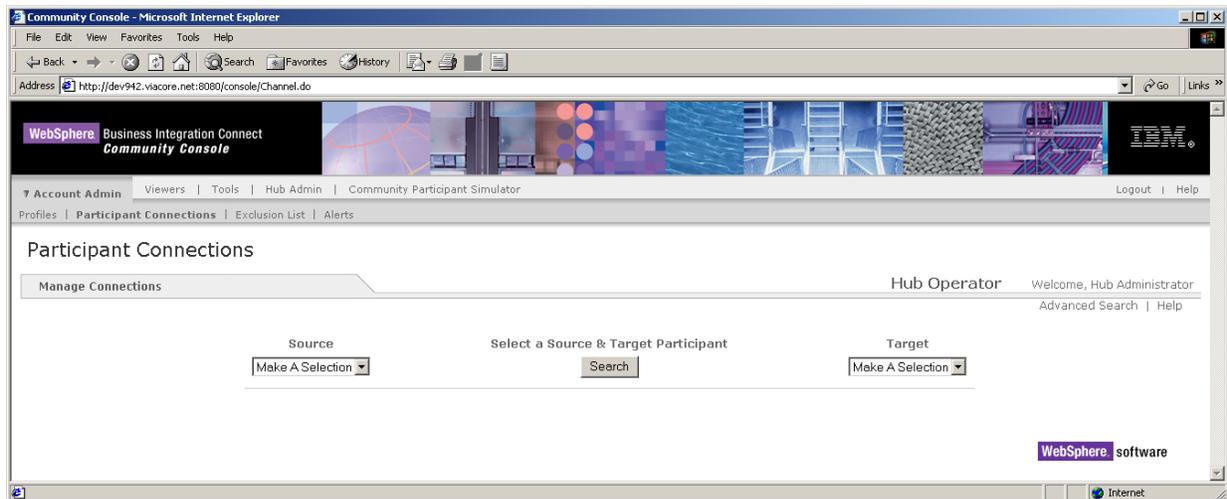


Figure 3-25. Manage Connections Screen

2. Under **Source**, select a Source.
3. Under **Target**, select a Target.

NOTE: To create a new connection, the Source and Target must be unique.

4. Click **Search**. The system finds the connections that match your criteria (see [Figure 3-26 on page 102](#)).

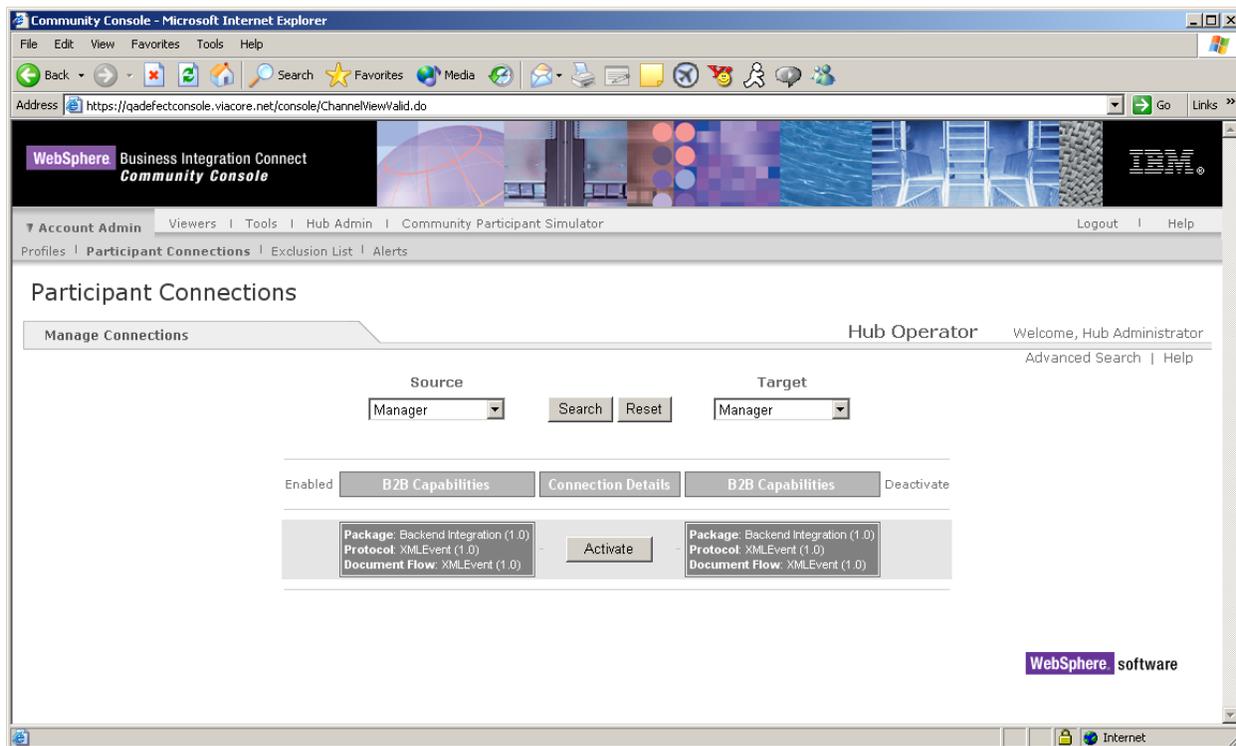


Figure 3-26. Example of Finding Connections That Match Your Search Criteria

5. To activate a connection, click **Activate**. The Console displays the Manage Connections screen (see [Figure 3-27 on page 103](#)). This screen shows the package, protocol, and document flow for the source and target. It also provides buttons you can click to view and change partner-connection status and parameters.

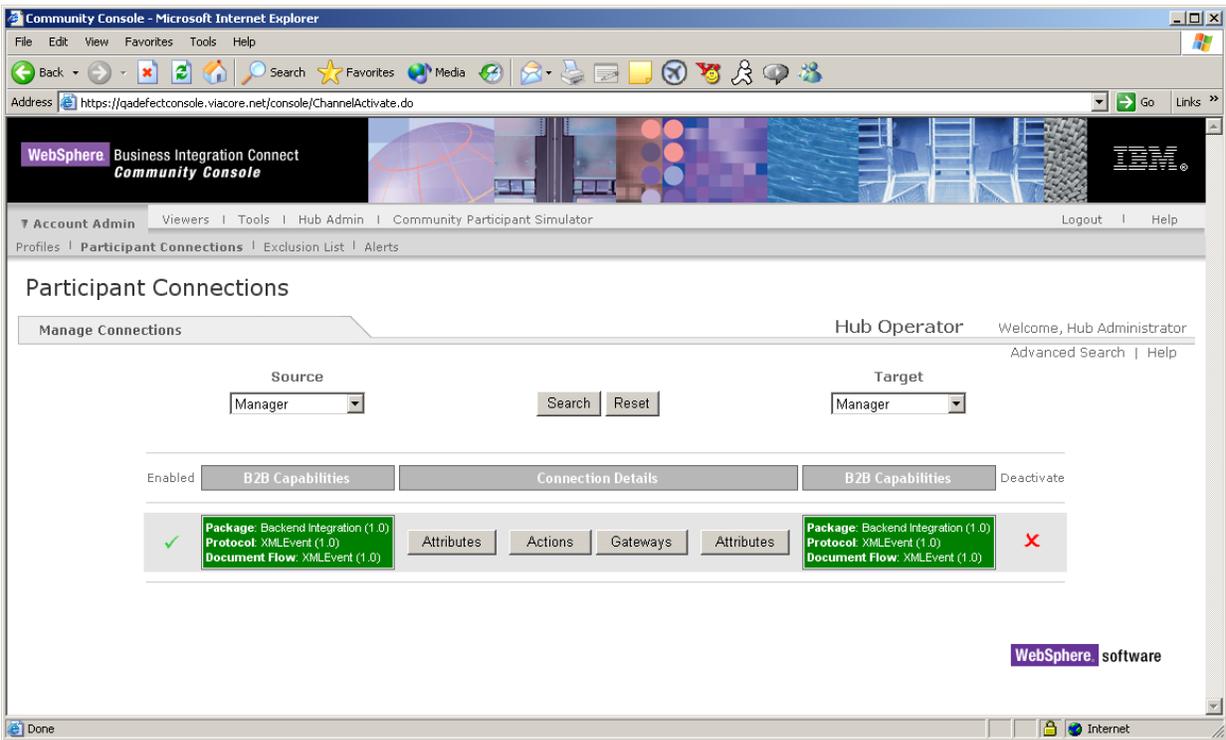


Figure 3-27. Manage Connections Screen

6. Click the appropriate item as necessary:

- Clicking the  disables a connection.
- Clicking the  enables a connection.
- Clicking **Attributes** displays the Connection Attributes screen, where you can view and change connection attributes. For more information, see [“Changing Participant attribute values” on page 107](#).
- Clicking **Actions** displays the Connection Details screen, where you can view and change the Action. For more information, see [“Selecting a new action” on page 107](#).
- Clicking **Gateways** displays the Connection Management Gateway screen, where you can view and change the source or target gateway. For more information, see [“Changing the source or target gateway” on page 108](#).

Performing an advanced search for connections

Use the following procedure to conduct an advanced search for connections. When selecting a Source and a Target, observe the following guidelines:

- The Source and Target must be unique.
 - Do not mix a production gateway with a test gateway when selecting Source and Target; otherwise, an error occurs. Both the Source and the Target must be production or test gateways.
1. Click **Account Admin** on the main menu and **Participant Connections** on the horizontal navigation bar. The Console displays the Manage Connections screen (see [Figure 3-25 on page 101](#)).
 2. Click **Advanced Search**. The Console displays the Advanced Search screen (see [Figure 3-28](#)).

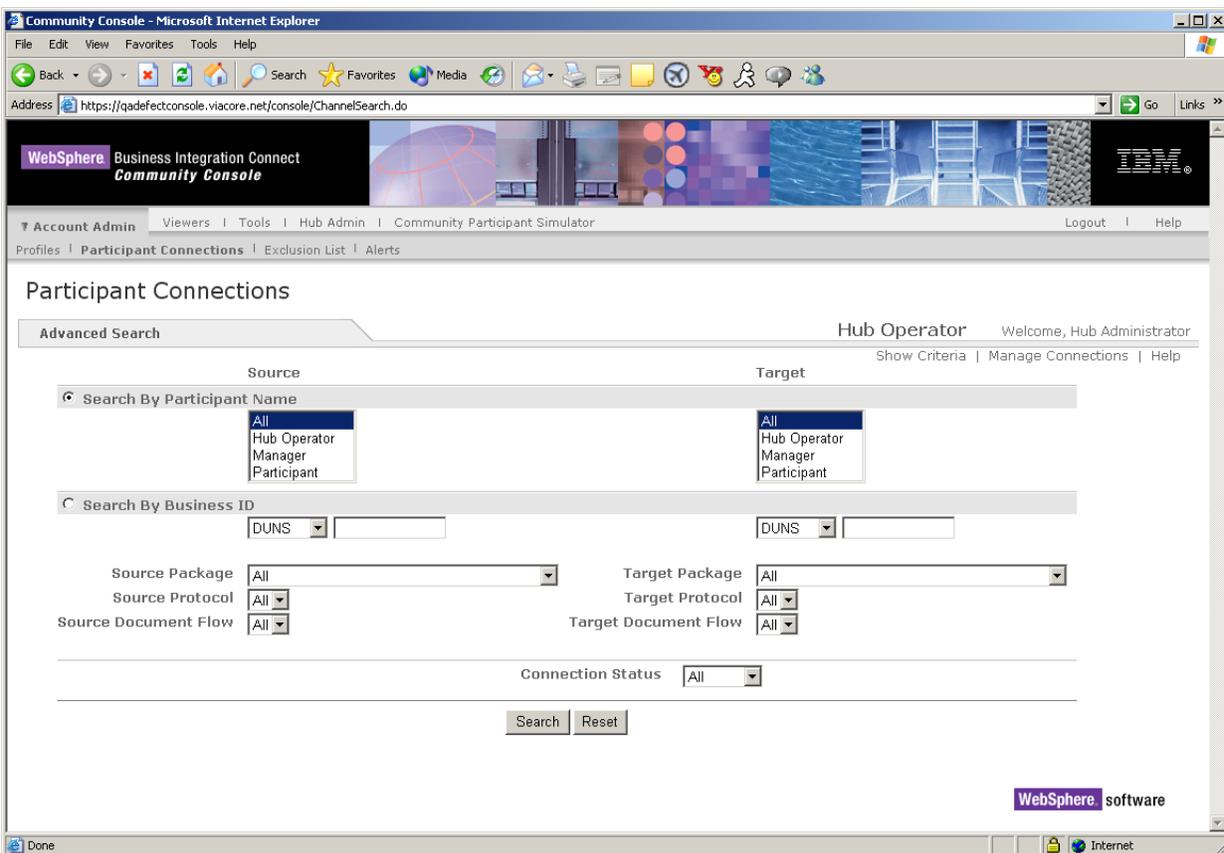


Figure 3-28. Advanced Search Screen

3. Complete the following parameters in the screen:

Table 3-8. Advanced Search Screen

Parameter	Description
Search By Participant Name	Names of the Source and Target.
Search By Business ID	Business IDs of the Source and Target. Includes DUNS, DUNS+4, and Freeform.
Source Package	Package used by the Source.
Target Package	Package used by the Target.
Source Protocol	Protocol used by the Source.
Target Protocol	Protocol used by the Target.
Source Document Flow	Document Flow used by the Source.
Target Document Flow	Document Flow used by the Target.
Connection Status	Allows you to search for enabled, disabled, or enabled and disabled connections.

4. Click **Search**. The system finds the connections that match your criteria (see [Figure 3-26 on page 102](#)).

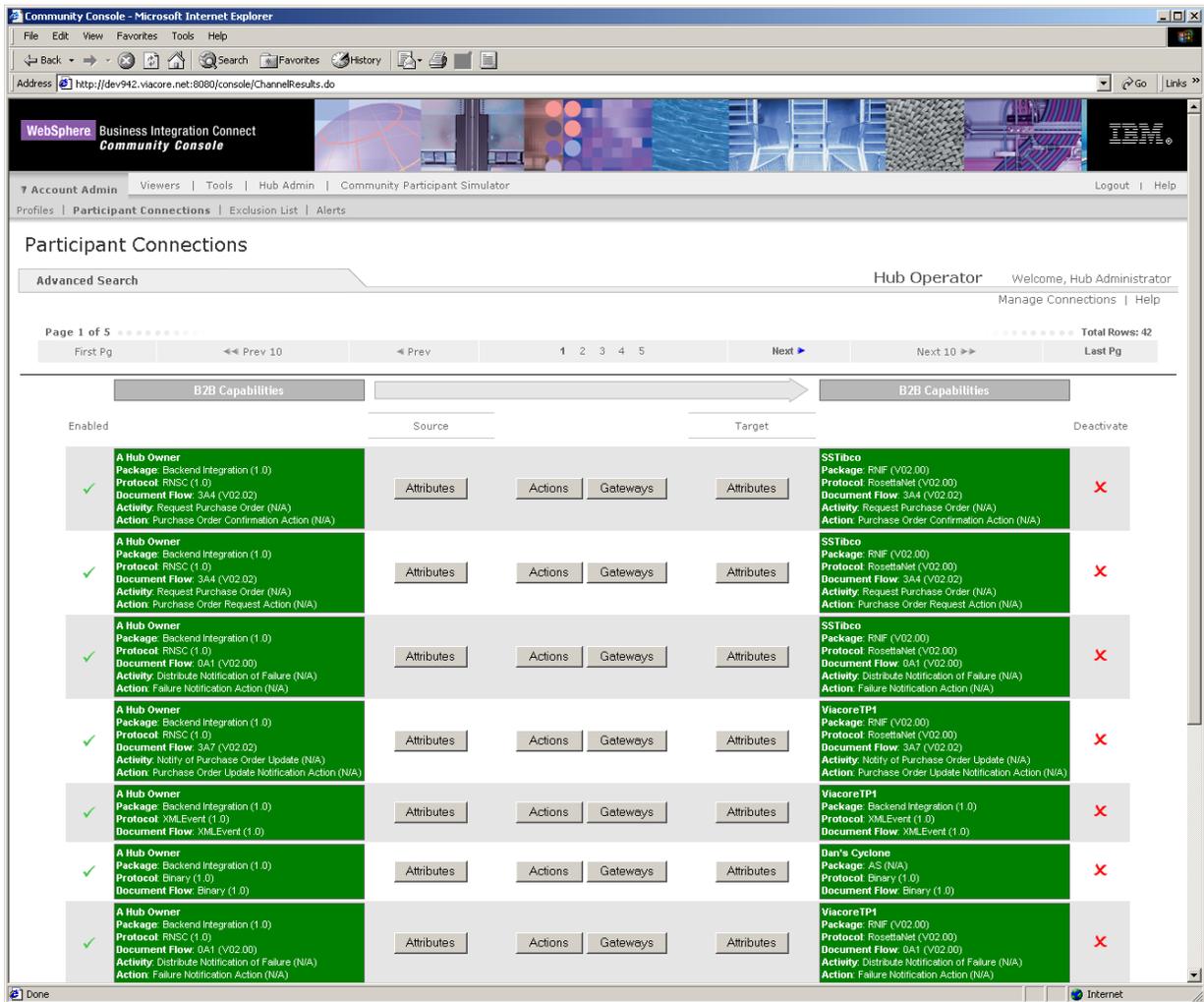


Figure 3-29. Example of the System Finding Connections

Changing connection configurations

To change the configuration of a connection, use the following procedure.

1. Click **Account Admin** on the main menu and **Participant Connections** on the horizontal navigation bar. The Console displays the Manage Connections screen (see [Figure 3-25 on page 101](#)).
2. Perform a basic search for connections (see [“Performing a basic search for connections” on page 101](#)) or advanced search for connections ([“Performing an advanced search for connections” on page 104](#)).
3. See the appropriate section:
 - To change Participant attribute values, see [“Changing Participant attribute values,”](#) below.
 - To select a new action, see [“Selecting a new action,”](#) below.
 - To change the source or target gateway, see [“Changing the source or target gateway” on page 108](#).
 - To disable or activate a configuration, see [“Disabling or deactivating a connection” on page 108](#).

Changing Participant attribute values

To change Participant attribute values, use the following procedure.

1. Click **Attributes** for either the Source or Target Participant.
2. In the **Scope** drop-down list, select **Connection** if the attribute changes will apply to all the gateway types associated with the connection, or select a gateway type to which the changes will apply.
3. Click the  icon and expand the node to the Document Flow Definition whose attribute values will be changed.
4. Update the attribute value as needed.
5. Click **Save**.

Selecting a new action

To select a new action, use the following procedure.

1. Click **Actions**.
2. Select the new action from the drop-down list.
3. Click **Save**.

Changing the source or target gateway

To change the source or gateway target, use the following procedure.

1. Click **Gateways**.
2. Select the source or target gateway from the drop-down list.
3. Click **Save**.

Disabling or deactivating a connection

To disable a connection, click the  in the **Enabled** column. The connection display color changes to red, indicating that the connection has been disabled. To re-enable the connection, click the  icon.

To deactivate a connection, click the  icon. The connection display color changes to gray and the icon disappears. To re-enable the connection, click **Activate**.

Managing Exclusion Lists

An Exclusion List lets the Community Operator configure the Document Manager to restrict notifications sent to the Manager from its trading partners. Trading partners are identified by name and business ID.

The following notifications can be selected for routing restriction:

- 0A1 - Notification of Failure — sent to the Manager by a Participant that cannot complete a particular document flow.
- Backend Event — a system-generated XML file sent to the Manager to notifying him or her that their Participant has received a business document successfully.

Adding Participants to the Exclusion List

Use the following procedure to add a Participant to the Exclusion List.

1. Click **Account Admin** on the main menu and **Exclusion List** on the horizontal navigation bar. The Console displays the Exclusion List screen (see [Figure 3-30 on page 109](#)).

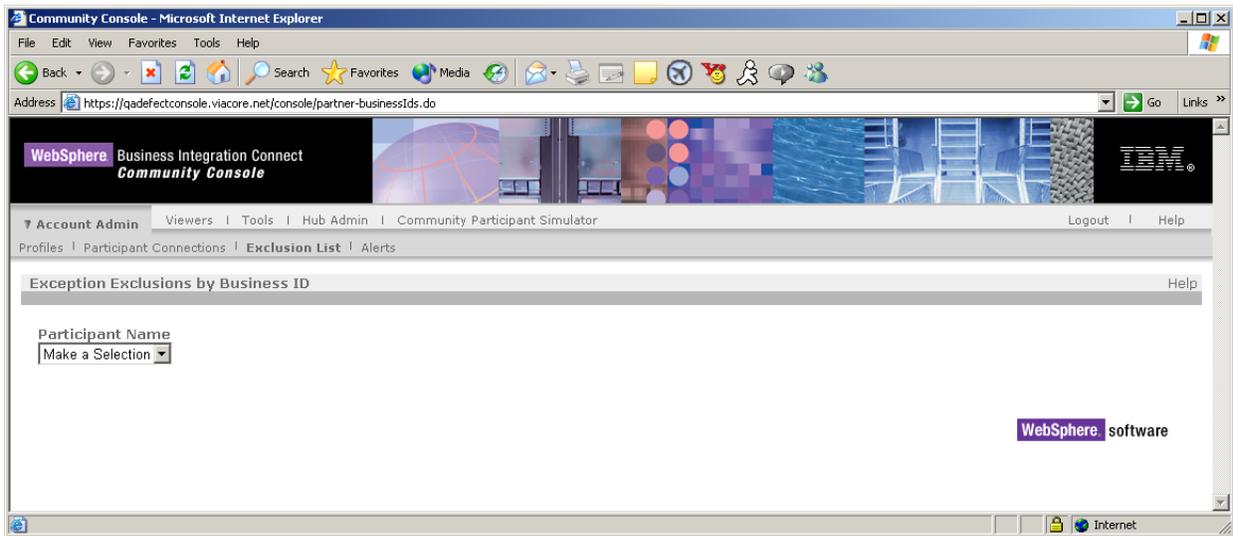


Figure 3-30. Exclusion List Screen

2. Select a Participant from the **Participant Name** drop-down list. The Console displays a list of Participants and their business ID and exclusion status (see Figure 3-31 on page 109). **Send All Notifications** is selected by default.

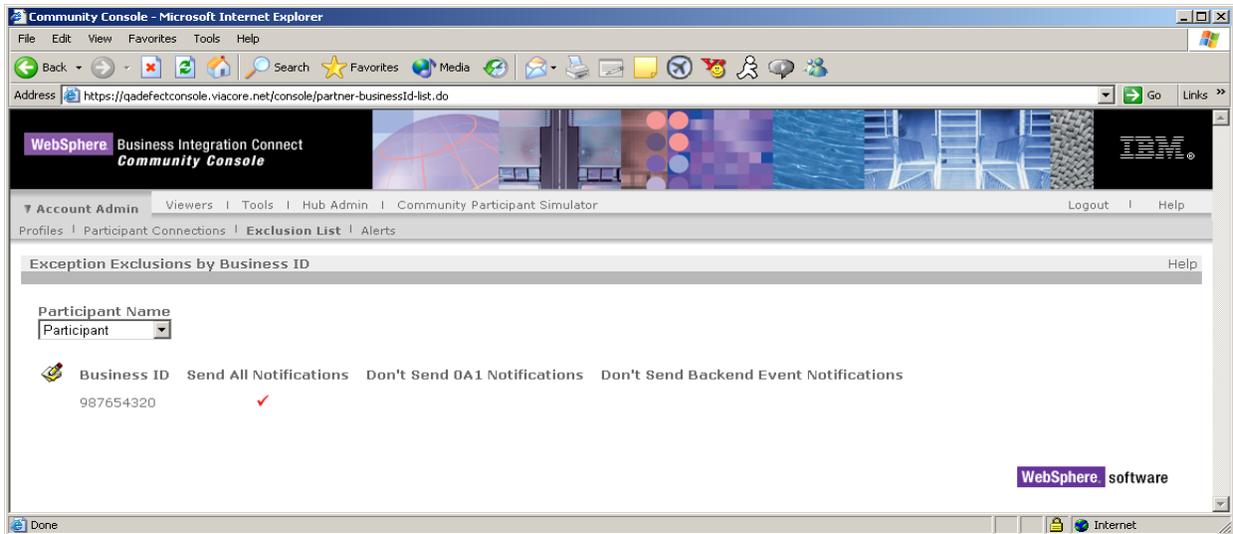


Figure 3-31. Example of Participants and Their Corresponding Business IDs and Exclusion Status

Editing the Exclusion List

There might be times when you need to edit the Exclusion List. For example, you might want to restrict a notification from being routed to the Community Manager.

1. Click **Account Admin** on the main menu and **Exclusion List** on the horizontal navigation bar. The Console displays the Exclusion List screen (see [Figure 3-30 on page 109](#)).
2. Select a Participant from the **Participant Name** drop-down list. The Console displays a list of Participants and their business ID and exclusion status (see [Figure 3-31 on page 109](#)).
3. Click the  icon next to the notification you want to edit. The screen in [Figure 3-32](#).

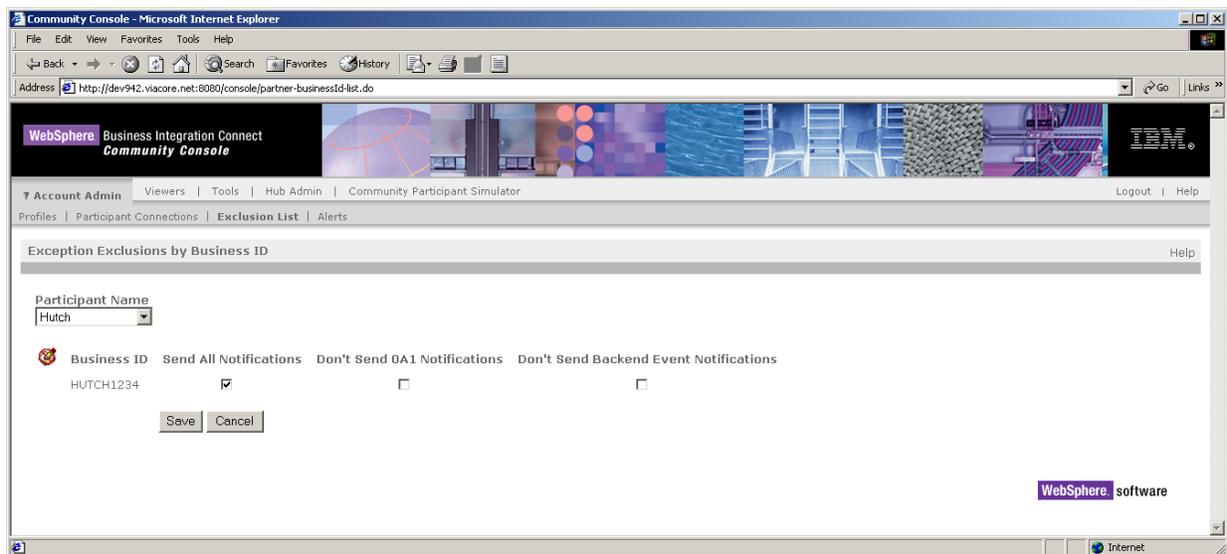


Figure 3-32. Screen for Editing Participant IDs

4. Check the check box below the notification to restrict the notification from being routed to the Community Manager. Select **Send All Notifications** to remove all routing restrictions.
5. Click **Save**.

Chapter 4. Using the Gateway Queue

The Gateway Queue lets you view documents queued for delivery from any gateway in the system. It also allows you to view all gateways that have documents queued for delivery, display and remove documents in a queue, and enable or disable gateways.

The Gateway Queue can be used to ensure that time-sensitive documents are not left standing in the queue. It can also be used to ensure that the maximum number of documents to be queued is not exceeded. Using the Gateway Queue, you can:

- See a list of all gateways containing documents queued for delivery
- View a document that has been in a gateway queue for an extended amount of time (30 seconds or more). This may indicate a problem with the document itself. You can also view document details to troubleshoot or delete documents from the queue.
- View gateway details to ensure proper operation. Documents backing up in a gateway queue can indicate a fault in the delivery manager or gateway.
- Confirm gateway status. An offline gateway causes documents to collect in the queue until the gateway is placed online. Gateway status does not affect connection functionality. Documents continue to be processed and placed in the queue for delivery.

Viewing the gateway list

To view a list of documents residing in the gateway, use the following procedure.

1. Click **Viewers** on the main menu and **Gateway Queue** on the horizontal navigation bar. The Console displays the Gateway Queue screen (see [Figure 4-1 on page 112](#)).

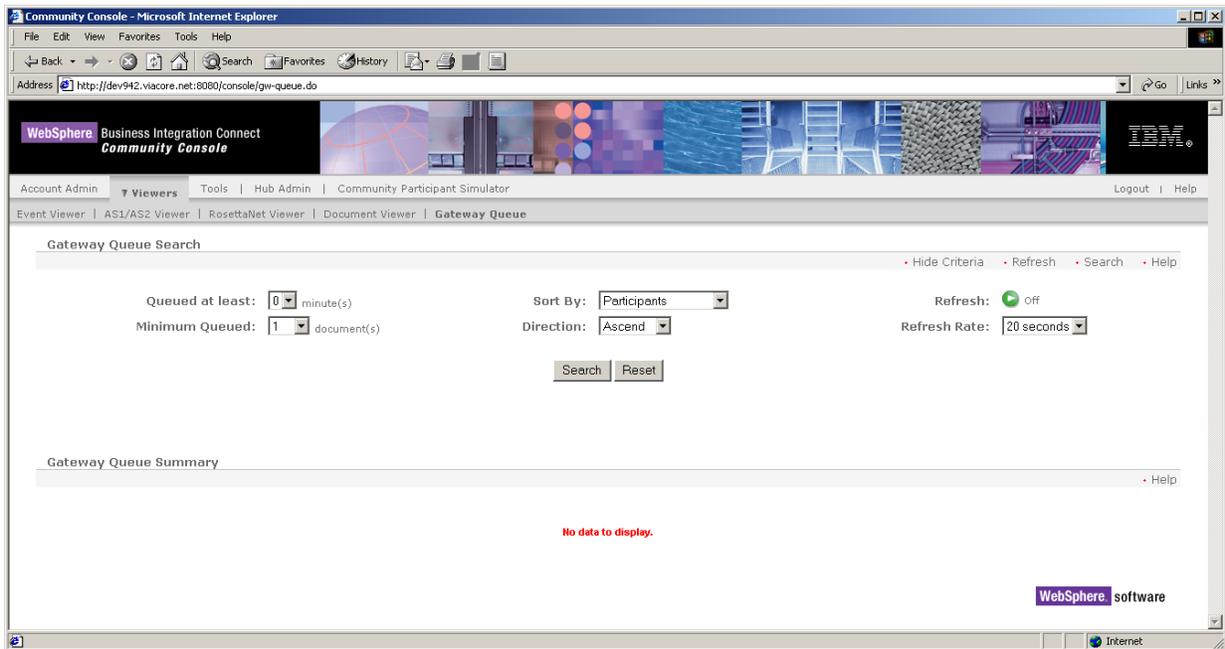


Figure 4-1. Gateway Queue Screen

2. Complete the following parameters in the screen:

Table 4-1. Gateway Queue Screen

Criteria	Description
Queued at least	Minimum number of minutes a document has been waiting in gateway queue. For example, if six minutes is selected, all gateways containing documents that have been waiting for delivery six minutes or more will be displayed. Default is 0.
Minimum Queued	Minimum number of documents in a gateway queue. Default is 1.
Sort By	Sort search results by Participant (default), Gateway Name, or Last Sent Timestamp.
Direction	Click Ascend to display documents starting with the oldest time stamp or end of the alphabet, or Descend to display documents starting with the most recent time stamp or beginning of the alphabet.
Refresh	Turn refresh on or off (default).
Refresh Rate	Number of seconds the Console waits before updating displayed data.

- Click **Search**. The system finds all documents in the gateway that match your search criteria. [Table 4-2 on page 113](#) shows the information returned from the search.

Table 4-2. Results After Gateway Queue Search

Criteria	Description
Participant	Trading partner associated with gateway.
Gateway	Name of the gateway.
Queued	Number of documents in the gateway queue waiting for delivery. Link to gateway details.
State	Shows whether the gateway is online or offline.
Last Sent	Last date and time when a document was sent to the gateway successfully.

- For the Console to display a gateway, the gateway must meet all the requirements of the search criteria in an “and” fashion.

Viewing queued documents

To have the system search for queued documents that meet your search criteria, use the following procedure.

- Click **Viewers** on the main menu and **Gateway Queue** on the horizontal navigation bar. The Console displays the Gateway Queue screen (see [Figure 4-1 on page 112](#)).
- Click **Search**.
- Complete the following parameters in the screen:

Table 4-3. Search Criteria for the Gateway Queue

Parameter	Description
Participant	Name of the partner receiving the document.
Gateway	Name of the gateway.
Reference ID	Unique identification number assigned to document by system.
Document ID	Unique identification number assigned to document by source participant.
Sort By	Sorts search results by Participant (default), Reference ID, Document ID, or time document entered gateway queue.
Direction	Click Ascend to display documents starting with the oldest time stamp or end of the alphabet, or Descend to display documents starting with the most recent time stamp or beginning of the alphabet.

4. To view in-depth document details, click **Reference ID**. For information about the in-depth information displayed when viewing document details, see the topic “About document viewer” in the online help.

Removing documents from the queue

The following procedure describes how to remove documents from the delivery queue. You must be logged in as Hub Admin to delete documents from the queue.

1. Click **Viewers** on the main menu and **Gateway Queue** on the horizontal navigation bar. The Console displays the Gateway Queue screen (see [Figure 4-1 on page 112](#)).
2. Click **Search**.
3. Complete the parameters in the screen (see [Table 4-3 on page 113](#)).
4. Click the  icon.

Viewing gateway details

To view information about a particular gateway, including a list of documents in the queue, use the following procedure.

1. Click **Viewers** on the main menu and **Gateway Queue** on the horizontal navigation bar. The Console displays the Gateway Queue screen (see [Figure 4-1 on page 112](#)).
2. Type the search criteria (see [Table 4-1 on page 112](#)).
3. Click **Search**. A list of gateways appears.
4. Click the document count link in the **Queued** column. Gateway details and a list of queued documents appear.

Changing gateway status

To place a gateway online or offline, use the following procedure.

1. Click **Viewers** on the main menu and **Gateway Queue** on the horizontal navigation bar. The Console displays the Gateway Queue screen (see [Figure 4-1 on page 112](#)).
2. Type the search criteria (see [Table 4-1 on page 112](#)).
3. Click **Search**. A list of gateways appears.
4. Click the document count link in the **Queued** column. Gateway details and a list of queued documents appear.
5. Click **Online** in **Gateway Info** to place a gateway offline or click **Offline** to place gateway online. (You must be logged in as Hub Admin to change gateway status.)

Chapter 5. Troubleshooting

This chapter provides troubleshooting information you can use to identify and resolve problems. Topics in this chapter include:

- [“Optimizing database query performance” on page 115](#)
- [“Avoiding out-of-memory errors” on page 115](#)
- [“Reprocessing events and business documents that fail to log to the database” on page 116](#)
- [“Poor performance and system events are not working” on page 117](#)
- [“Shutting down” on page 117](#)
- [“Starting the system after a machine shutdown” on page 118](#)
- [“Restarting the Document Manager after a crash” on page 119](#)

Optimizing database query performance

The RUNSTATS command updates the database query access plan for each table and index. To optimize database query performance, run RUNSTATS at least once a week when IBM WebSphere Business Integration Connect application and database activity is at a minimum. As database traffic increases, run RUNSTATS more frequently — up to once a day.

NOTE: Since RUNSTATS updates database system information, deadlock timeouts potentially can occur under specific circumstances. Therefore, it is recommended that the WebSphere Business Integration Connect application be quiesced and database access be limited to running RUNSTATS.

Avoiding out-of-memory errors

To improve routing performance and avoid out-of-memory errors, use the following scripts to change the initial and maximum heap size:

Query current heap size:

- ```
/opt/IBM/WBICConnect/console/was/bin/wsadmin.sh -conntype NONE -f $LOCATION_OF_SCRIPTS$/queryJVMAattrs.jacl
```

Set min/max heap size:

- ```
/opt/IBM/WBICConnect/console/was/bin/wsadmin.sh -conntype NONE -f $LOCATION_OF_SCRIPTS$/setJVMAattrs.jacl
```

Change the heap size to the recommended values by editing `setJVMAattrs.jacl`.

Default:

- `Xms=50`
- `Xmx=256`

First recommendation:

- `Xms=256`
- `Xmx=512`

Second recommendation:

- `Xms=256`
- `Xmx=1024`

Reprocessing events and business documents that fail to log to the database

If an event or doc in the `DATALOGQ` JMS queue fails three attempts to log to the database, it is inserted into the `DATALOGERRORQ` JMS queue to allow for later reprocessing when the problem has been resolved.

To reprocess these failed events and documents, use the manual utility `reprocessDbLoggingErrors.sh`. This utility dequeues all the events and docs from `DATALOGERRORQ` and re-queues them into `DATALOGQ`, so the normal `DocumentLogReceiver` will log them to the database again.

The utility stops after it processes all the existing events and documents in `DATALOGERRORQ`. Any events and document that fails to log ends up in `DATALOGERRORQ` again; however, this time, the utility ensures that the event or document is reprocessed only once (that is, the utility does not enter an endless loop with failing events and documents).

To run the `reprocessDbLoggingErrors.sh` utility:

1. Verify that the `env` variables are correctly defined in `reprocessDbLoggingErrors.sh` on any Document Manager machine:

```
REPROCESSOR_HOME=/opt/apps/router
JAVA_HOME=$REPROCESSOR_HOME/java
LOG_REPROCESSOR_CLASSES=$REPROCESSOR_HOME/classes
```

2. Run the utility from the command line.

Poor performance and system events are not working

If the system is performing very slowly and system events are not working, there may be a problem with the WebSphere MQ publish/subscribe broker.

1. Open the file `/var/mqm/qmgrs/<queue manager name>/qm.ini` and look for the following:

```
MaxActiveChannels=1000Broker:
```

If you see this entry, replace the `Channels` and `Broker` parameters with the following:

```
Channels:
```

```
MaxChannels=1000
```

```
MaxActiveChannels=1000
```

```
Broker:
```

```
SyncPointIfPersistent=yes
```

2. Save your changes
3. Shut down Business Integration Connect (see [“Shutting down,”](#) below).
4. Stop WebSphere MQ by:

- a. Stopping the publish/subscribe broker:

```
endmqbrk -m <hostname>.queue.manager
```

- b. Stopping the listener:

```
endmqlsr -m <hostname>.queue.manager
```

- c. Stopping the queue manager:

```
endmqm <hostname>.queue.manager
```

5. Create and start WebSphere MQ, using the instructions in the WebSphere Business Integration Connect Installation Guide. However, do not perform steps 2 through 4 in the procedure.
6. Restart Business Integration Connect, using the instructions in the WebSphere Business Integration Connect Installation Guide.

Shutting down

When shutting down the system, shut down the Receiver before shutting down the Document Manager. This safeguard prevents documents from entering the system while the Document Manager is shutting down. A shutdown can take up to 15 minutes if there is a large number of documents being processed.

Starting the system after a machine shutdown

The following sections describe how to start the system components if the machine where they reside has been out of service. You must first start DB2 and WebSphere MQ before you can start the Business Integration Connect components.

Starting DB2

To start DB2, use the following procedure.

1. Change to the database owner (db2inst1 if the default was used):

```
su - db2inst1
```

2. Start the database instance:

```
db2start
```

Starting WebSphere MQ

To start WebSphere MQ, use the following procedure.

1. Change to the WebSphere MQ user:

```
su - mqm
```

2. Start the queue manager:

```
strmqm <hostname>.queue.manager
```

3. Start the listener:

```
runmqtsr -t tcp -p <port number> -m <hostname>.queue.manager &
```

4. Wait about 10 seconds and press Enter to return to the command prompt.

5. Start the JMS Broker (the publish-subscribe broker):

```
strmqbrk -m <hostname>.queue.manager
```

Starting the Community Console, Receiver, and Document Manager

To start the Community Console, Receiver, and Document Manager, use the following procedure.

1. Change to the general Business Integration Connect user:

```
su - bcguser
```

2. Navigate to the Community Console script directory:

```
cd <installation location>/console/was/bin
```

where <installation location> is where Business Integration Connect is installed.

3. Start the Community Console:

```
./startServer.sh server1
```
4. Navigate to the Receiver script directory:

```
cd <installation location>/receiver/was/bin
```
5. Start the Receiver:

```
./startServer.sh server1
```
6. Navigate to the Document Manager script directory:

```
cd <installation location>/router/was/bin
```
7. Start the Document Manager:

```
./startServer.sh server1
```

Restarting the Document Manager after a crash

If the Document Manager should crash, use the following procedure to restart it. This procedure ensures that all documents that have been received will be processed.

1. Check the `router_in` directory for any files that have the extension `vmd_locked`.
2. If there are files that have the extension `vmd_locked` that are more than two minutes old, rename the to extension `vmd`.

NOTE: If there are multiple instances of DocumentManager running, there are files with the `vmd_locked` extension that are being actively processed by the other instances of the Document Manager. Do not rename those files.

3. Depending on the state of processing a document, it is possible that a document will fail with an event 210031 “Unable to nonrep document.” If this occurs, the files for the document will reside in the directory `router_in/reject`. If this happens, rename the file with the extension `vmd` with the extension `vmd_restart`. Then move the files for the document to the directory `router_in dir` for processing.

Appendix A. Administering Certificates

With Business Integration Connect, you can install and use the following types of certificates for inbound and outbound transactions:

- SSL (server side)
- SSL (client)
- Digital signature
- Encryption

As the Hub Admin or Operator Admin, you use Business Integration Connect's Community Console to install all of the required certificates for Business Integration Connect storage and you can use the ikeyman tool for WebSphere Application Server (WAS) storage.

NOTE: When a Participant's certificate expires, it is the Participant's responsibility to obtain a new certificate. The Console's Alert feature includes certificate expiration alerts for certificates stored in Business Integration Connect. For more information, see the IBM WebSphere Business Integration Connect Community Console User Guide.

You can use one certificate for multiple purposes. For inbound SSL, however, the private key and associated certificate must be in formats suitable for both Business Integration Connect and WAS storage.

Certificate Overview

Table 1 summarizes the way certificates are used in Business Integration Connect.

Table A--1. Certificate Summary Information

Message Delivery Method (Note 1)	Hub Owner Certificate	Obtain Certificate from Partner	CA (Note 2)	Give Certificate to Partner (Note 3)	Comments
Inbound SSL	Server side certificate (WAS Keystore)	If Client side is being used. (WAS Truststore) Note 4	(WAS Truststore)	Hub owner certificate if self-signed or the CA root certificate if it is CA authenticated.	
Outbound SSL	If Client side is being used. (Business Integration Connect)	Hub owner certificate if self-signed or the CA root certificate if it is CA authenticated.	WebSphere Business Integration Connect	Hub owner certificate if self-signed or the CA root certificate if it is CA authenticated.	
Inbound Encrypt	Private key (Business Integration Connect)	N/A	N/A	Hub owner certificate	For decrypting the message
Inbound Signature	N/A	Certificate for validating the certificate used for the digital signature (Business Integration Connect)	WebSphere Business Integration Connect	N/A	For verification
Outbound Encrypt	Use certificate obtained from trading partner (certificate is installed in partner's profile)	N/A	N/A	Hub owner certificate	
Outbound Signature	Private key (Business Integration Connect)	N/A	N/A	Optional, depending on partner	

- Note 1: Inbound - message coming into Business Integration Connect from a partner. Outbound - message going out of Business Integration Connect to a partner.
- Note 2: If the certificate is CA issued then issuing CA certificate must be obtained and stored. This applies to either the Hub owner certificate or the Partners certificate.
- Note 3: If a private key is involved then this certificate corresponds to the private key.
- Note 4: If a CA certificate is used, only the CA needs to provide a certificate (the Partner does not need to provide one).

Understanding terms and concepts

The following terms are specific to the creation and use of certificates in the Business Integration Connect environment:

- **ikeman** — a key management utility used to create key databases, public and private key pairs, and certificate requests (CSR). You can also use ikeman to create self-signed certificates.
- **keystore** — a file that contains your public and private keys.
- **truststore** — a key database file that contains the public keys for your partner's self signed and the CA certificates. The public key is stored as a signer certificate. For commercial CA, the CA root certificate is added. The truststore file can be a more publicly accessible key database file that contains all the trusted certificates.

Creating and installing certificates

The following sections describe how to create and install certificates that you want to use with WebSphere Business Integration Connect.

Creating and installing inbound SSL certificates

If your community is not using SSL, neither you nor your Participants need an inbound or outbound SSL certificate.

This server certificate is used by the Receiver and Community Console when it receives documents from Participants through SSL. It is the certificate that the Receiver presents to identify the hub to the Participant. This server certificate can be self-signed, or it can be signed by a CA. In most cases you will use a CA certificate to increase security. You might use a self-signed certificate in a test environment. Use ikeman to generate a certificate and key pair. Refer to documentation available from IBM for more information about using ikeman.

IBM WebSphere Application Server is embedded in Business Integration Connect. WebSphere Application Server handles all inbound SSL connections. The installation provides a keystore and truststore for the Receiver and for the Console. The names are:

- receiver.jks
- receiverTrust.jks
- console.jks
- consoleTrust.jks

The default password for accessing all four stores is WAS. The embedded WebSphere Application Server is configured to use these four stores.

NOTE: The following Unix command can be used to change the password of the keystore file:

```
/opt/IBM/WBICconnect/console/was/java/bin/keytool -storepasswd  
-new $NEW_PASSWORD$ -keystore $KEYSTORE_LOCATION$ -storepass  
$CURRENT_PASSWORD$ -storetype JKS
```

After you generate the certificate and key pair, use the certificate for inbound SSL traffic for all Participants. If you have multiple Receivers or Community Consoles, copy the resultant keystore to each instance. If the certificate is self signed, provide this certificate to the Participants. To obtain the certificate, use `ikeyman` to extract the certificate to a file.

NOTE: There is an incompatibility between certificates that `ikeyman` and WebSphere Business Integration Connect can use. If you use the same certificate for inbound SSL and business data encryption, you first need to use the `createCert.sh` script to generate the certificates and then use `ikeyman` to import the created `pkcs12` file into the keystore.

NOTE: Use `ikeyman` to delete the WebSphere "dummy" server certificate. If this certificate is not removed, it will be presented to the partner during SSL session establishment.

If you also use SSL Client Authentication, obtain either the participant's self signed certificate or the certificate provided by a CA and install it in the appropriate truststore. After installing the certificate, configure the application server to use client authentication by running the `bcgClientAuth.jacl` script.

There is an additional feature that can be used with SSL Client Authentication. This feature is enabled via the Community Console. For HTTPS, WebSphere Business Integration Connect checks certificates against the Business IDs in the inbound documents. To use this feature, create the Participant's profile, then select the `Validate Client SSL Certificate` option on the Participant's Gateway screen. For more information, see [“Managing gateway configurations” on page 79](#).

If you use self-signed server certificates, use the following procedure.

1. Use `ikeyman` to generate a self signed certificate and a key pair for the Receiver or Community Console keystore. The `ikeyman` utility is located in the `was/bin` directory. It is included with WebSphere Application Server, which is embedded in Business Integration Connect. Instructions for running `ikeyman` can be found in documentation available from IBM.
2. Use `ikeyman` to extract to a file the certificate that will contain your public key.
3. Use e-mail to distribute the server certificate to all Participants.

If the certificate is signed by a CA, use the following procedure.

1. Use `ikeyman` to generate a certificate request and a key pair for the Receiver. The `ikeyman` utility is located in the `was/bin` directory. It is included with WebSphere Application Server, which is embedded in Business Integration Connect. Instructions for running `ikeyman` can be found in documentation available from IBM.
2. Submit a Certificate Signing Request (CSR) to a CA.
3. When you receive the signed certificate from the CA, use `ikeyman` to place the signed certificate into the keystore.
4. Distribute the signing CA certificate to all Participants.

For client authentication, use the following procedure:

1. Obtain your Participants' certificates.
2. Install the certificate into the truststore using `ikeyman`.

NOTE: When you add more Participants to your hub-community, you can use `ikeyman` to add their certificates to the truststore. If a Participant leaves the community, you can use `ikeyman` to remove the Participant's certificates from the truststore

Outbound SSL certificate

If your community is not using SSL, you do not need an inbound or outbound SSL certificate.

When you use SSL to send outbound documents to your Participants, the Participants request from you a server certificate. If a Participant's certificate is self signed, use the Console to import it into Business Integration Connect. If the certificate is CA signed, you need only import the CAs certificate into the Console.

NOTE: The same CA certificate can be used for multiple participants. The certificate must be in X.509 DER format.

If SSL client authentication is required, the Participant will, in turn, request a certificate from Business Integration Connect. For Business Integration Connect to present the certificate to the Participant, use the Console to import your certificate into Business Integration Connect. You can generate the certificate using the `createCert.sh` script in the `was/bin` directory. If the certificate is a self signed certificate, it must be provided to the Participant. If a CA signed certificate, the CA must be given to the Participant.

To set up for server authentication from the Participant, install the Partner's self-signed or CA signed certificate through the console's certificate feature. The certificate must be in binary format using DER encoding. You perform this task logged in to the console as the Hub Operator, and install the certificate in your own profile.

If client authentication is not required by the Participant, use the following procedure.

1. Use the `createCert.sh` script in the `was/bin` directory to generate a self-signed certificate in X.509 format and a private key in PKCS 8 format.
2. Install the self-signed certificate and key through the Console's certificate feature. You perform this task logged in to the Console as the Hub Operator, and install the certificate in your own profile.
3. Send your self-signed certificate or CA to all Participants.

Inbound signature certificate

The Document Manager uses your inbound signed certificate to verify the sending party when it receives documents. The Participants send their self-signed signature certificates in X.509 DER format to you. You, in turn, install the Participants' certificates through the Console.

To install the certificate, use the following procedure.

1. Receive the Participant's signature certificate in X.509 DER format.
2. Install the certificates through the Console's certificate feature. You perform this task logged in to the console as the Hub Operator, and install the certificate in the Participant's profile, denoting the certificate as a signature certificate.
3. If the certificate was signed by a CA and the CAR root certificate is not installed in the Hub Admin account, install the CA certificate through the Console's certificate feature. You perform this task logged in to the console as the Hub Operator, and install the certificate in your own profile.

NOTE: You do not have to perform the previous step if the CA certificate is already installed.

4. Enable at the package (highest level), Partner, or connection level (lowest level). Your setting can override other settings at the connection level. The connection summary will inform you if any required attribute is missing.

Outbound signature certificate

The Document Manager uses this certificate when it sends outbound, signed documents to Participants. The same certificate and key are used for all ports and protocols.

1. Use the createCert.sh script in the was/bin directory to generate a self-signed certificate and private key in PKCS 8 format.
2. Install the certificate and key through the console's certificate feature. You perform this task logged in to the console as the Hub Operator, and install the certificate in your profile, denoting the certificate as a signature certificate
3. Distribute the certificate to your Participants. The preferred method for distribution is to send the certificate in a zip file that is password protected, by e-mail. Your Participants must call you and request the password for the zip file.
4. Enable at package (highest level), Partner, or connection level (lowest level). Your setting can override other settings at the connection level. The connection summary will inform you if any required attribute is missing.

Inbound encryption certificate

This certificate is used by the Receiver to decrypt encrypted files received from Participants. The Receiver uses our private key to decrypt the documents. Encryption is used to keep anyone other than the sender and intended recipient from viewing documents in transit.

1. Use the createCert.sh script in the was/bin directory to generate a self-signed certificate in X.509 format and a private key in PKCS 8 format.
2. Install the certificate and key through the console's certificate feature. You perform this task logged in to the console as the Hub Operator, and install the certificate in your profile, denoting the certificate as an encryption certificate.

3. Distribute the certificate to your Participants. They are required to import the file into their B2B product for use as an encryption certificate. Advise them to use it when they want to send encrypted files to the Community Manager. If your certificate is CA signed, provide the CA certificate as well.
4. Enable at package (highest level), Partner, or connection level (lowest level). Your setting can override other settings at the connection level. The connection summary will inform you if any required attribute is missing.

Outbound encryption certificate

The outbound encryption certificate is used when the hub sends an encrypted document to a Participant. Business Integration Connect encrypts the document with the Participant's public key, and the Participant decrypts the document with their private key.

1. Obtain the Participant's encryption certificate. The certificate must be in X.509 DER format.
2. Install the certificate through the console's certificate feature. You perform this task logged in to the console as the Hub Operator, and install the certificate in the Participant's profile, denoting the certificate as an encryption certificate.
3. If the certificate is signed by a CA, and you do not have the CA's certificate installed in the system, log in to the console as Hub Operator and install this certificate in your own profile. You need only load a CA's certificate once.
4. Enable at package (highest level), Partner, or connection level (lowest level). Your setting can override other settings at the connection level. The connection summary will inform you if any required attribute is missing.

Configuring SSL for the Console and Receiver

To configure SSL for the Console and Receiver in Business Integration Connect, use the following procedure.

1. Obtain the following information:
 - The full path names of the key file and the trust file; for example:
`/opt/receiver/etc/KeyFile.jks` and `/opt/receiver/etc/TrustFile.jks`
You must enter these names correctly. In the Linux environment, these names are case-sensitive.
 - The new passwords for each file.
The format of each file. This must be chosen from one of the values JKS, JCEK, or PKCS12. Enter this value in upper-case exactly as shown.
 - The path to the script file named `bcgssl.jacl`.
2. Open a Console window and change to `<server-root>/bin`. The server does not need to be running to change the passwords.

3. Enter the following command, substituting the values that are enclosed in $\langle \rangle$. All values must be entered.

```
./wsadmin.sh -f <jacl-path>/bcgssl.jacl -conntype NONE install  
<keyFile pathname> <keyFile password> <keyFile format> <trustFile  
pathname> <trustFile password> <trustFile format>
```

4. Start the server. If the server fails to start, it may be due to an error when running `bcgssl.jacl`. If you make a mistake, you can rerun the script to correct it.
5. If you used `bcgClientAuth.jacl` to set the `clientAuthentication SSL` property, reset it after using `bcgssl.jacl`. This is because `bcgssl.jacl` overwrites any values that may have been set for `clientAuthentication` with the value `false`.

Index

A

Account Admin activities [67](#)

- adding Participants to the Exclusion List [108](#)
- changing B2B attribute values [97](#)
- changing connection configurations [107](#)
- changing Participant attribute values [107](#)
- changing the source or target gateway [108](#)
- connection components [99](#)
- connection duplication [99](#)
- creating an FTP account [85](#)
- creating digital certificates [92](#)
- creating gateways [83](#)
- creating Participants [67](#)
- deleting gateway configurations [84](#)
- disabling a digital certificate [94](#)
- disabling or deactivating a connection [108](#)
- Document Flow Definition
 - attributes [95](#)
- editing FTP details [87](#)
- editing the Exclusion List [110](#)
- information for gateway configuration [84](#)
- managing B2B capabilities [94](#)
- managing certificates [88](#)
- managing exclusion lists [108](#)
- managing gateway configurations [79](#)
- managing Participant connections [98](#)
- managing Participant profiles [67](#)
- performing a basic search for connections [101](#)
- performing an advanced search [104](#)
- searching for connections [101](#)
- searching for Participants [75](#)
- selecting a new Action [107](#)
- setting B2B capabilities [95](#)
- specifying an FTP server [85](#)
- types of Document Flow Definitions [95](#)
- viewing and editing digital certificates [88](#)
- viewing and editing gateways [79](#)

- viewing and editing Participant profiles [72](#)
- viewing default gateways [82](#)
- viewing your profile [76](#)

Account, creating an FTP [85](#)

Actions

- enabling or disabling [62](#)
- selecting a new [107](#)

Activities

- Account Admin [67](#)
- Hub Admin [15](#)

Adding

- a validation map to a Document Flow Definition [54](#)
- Participants to the Exclusion List [108](#)

Advanced search

- for connections [104](#)
- screen [104](#)

Alert Management, search for alerts [94](#)

Alert Search, search criteria [86, 87](#)

Are You Sure Message [75](#)

Associating a map to Document Flow Definition [55](#)

Attributes

- changing B2B [97](#)
- changing Participant values [107](#)
- Document Flow Definition [95](#)
- selecting Document Flow Definition [43](#)
- setting Document Flow Definition [42](#)

Avoiding out-of-memory errors [115](#)

B

B2B attributes, changing [97](#)

B2B capabilities

- managing [94](#)
- screen [96](#)
- setting [95](#)

Basic search, for connections [101](#)

Branding the Community Console [15](#)

C

Certificates

- creating [92](#)

- Details screen [91](#)
 - disabling [94](#)
 - managing [88](#)
 - viewing and editing [88](#)
 - Changing
 - B2B attribute values [97](#)
 - connection configurations [107](#)
 - gateway status [114](#)
 - Participant attribute values [107](#)
 - the source or target gateway [108](#)
 - Cloning from an existing object in the current context [43](#)
 - Community Console
 - branding [15](#)
 - icons [12](#)
 - logging in [9](#)
 - logging out [13](#)
 - navigating through [11](#)
 - stopping [14](#)
 - Company
 - logo uploading [18](#)
 - Website [6](#)
 - Components
 - connections [99](#)
 - Document Flow Definition [34](#)
 - Configurations
 - changing connection [107](#)
 - deleting gateway [84](#)
 - gateway required information [84](#)
 - managing gateway [79](#)
 - Configuring
 - Document Flow Definitions [33](#)
 - download packages [33](#)
 - permissions [21](#)
 - targets [25](#)
 - validation maps [52](#)
 - Connections
 - changing configurations [107](#)
 - components [99](#)
 - disabling or deactivating [108](#)
 - duplication [99](#)
 - managing Participant [98](#)
 - performing a basic search [101](#)
 - searching for [101](#)
 - Console Branding screen [17](#)
 - Crash, restarting after [119](#)
 - Creating
 - a new target [25](#)
 - an FTP account [85](#)
 - an XML format [57](#)
 - custom definitions [35](#)
 - digital certificates [92](#)
 - Document Flow Definitions [35](#)
 - document flow interactions [46](#)
 - gateways [83](#)
 - New Configuration screen [93](#)
 - Participants [67](#)
 - Custom Document Flow Definitions [35](#)
 - Customer Service [6](#)
- ## D
- Database query performance, optimizing [115](#)
 - Database, reprocessing events and business documents [116](#)
 - Deactivating a connection [108](#)
 - Default
 - Gateway screen [83](#)
 - gateways [82](#)
 - Deleting
 - an XML format [61](#)
 - gateway configurations [84](#)
 - targets [33](#)
 - Details, viewing gateway [114](#)
 - Digital certificates
 - creating [92](#)
 - disabling [94](#)
 - managing [88](#)
 - viewing and editing [88](#)
 - Disabling
 - a connection [108](#)
 - a digital certificate [94](#)
 - actions [62](#)

- permissions quickly [24](#)
- targets [33](#)
- Displaying the Manage Maps screen [52](#)
- Document Flow Definition
 - adding a validation map [54](#)
 - associating a validation map [55](#)
 - attributes [42, 95](#)
 - cloning from existing object [43](#)
 - components [34](#)
 - configuring [33](#)
 - creating [35](#)
 - creating custom [35](#)
 - creating interactions [46](#)
 - downloading a package to a local computer [41](#)
 - enabling [46](#)
 - interaction [34](#)
 - screen [36](#)
 - selecting attributes [43](#)
 - types [95](#)
 - understanding [33](#)
 - uploading and downloading a package [39](#)
- Document processing terms [5](#)
- Documents
 - removing from the queue [114](#)
 - reprocessing [116](#)
 - viewing queued [113](#)
- Download packages, configuring [33](#)
- Downloading
 - a Document Flow Definition package [39](#)
 - a package to a local computer [41](#)
 - sample images [16](#)
- DUNS numbers [70](#)
- DUNS+4 [70](#)

E

- Editing
 - digital certificates [88](#)
 - FTP details [87](#)
 - gateways [79](#)
 - Participant profiles [72](#)
 - password policy details [18](#)

- permission details [21, 63](#)
- profile details [74](#)
- target details [30](#)
- the Exclusion List [110](#)
- XML format values [60](#)
- your profile [78](#)
- Enabling
 - a Document Flow Definition [46](#)
 - actions [62](#)
 - permissions quickly [24](#)
 - targets [33](#)
- Event codes
 - managing [63](#)
 - saving names [65](#)
- Events, reprocessing [116](#)
- Example
 - digital certificate List [89](#)
 - Participants and their corresponding business IDs and exclusion status [109](#)
 - searching for Participants [76](#)
 - system finding connections [106](#)
 - viewing profile details [73](#)
- Exclusion List
 - adding Participants [108](#)
 - editing [110](#)
 - managing [108](#)
 - screen [109](#)
- Existing object, cloning from current context [43](#)

F

- Fail to log, reprocessing events and business documents [116](#)
- File directory [29](#)
- File Transfer Protocol, creating an account [85](#)
- Folders [121](#)
- Format, creating an XML format [57](#)
- Freeform ID numbers [70](#)
- FTP
 - Configuration screen [85, 86, 87](#)
 - creating an account [85](#)
 - directory [26](#)

- editing details [87](#)
- specifying a server [85](#)

G

Gateway

- changing source or target [108](#)
- changing status [114](#)
- creating [83](#)
- deleting configurations [84](#)
- Detail screen [80, 81](#)
- managing configurations [79](#)
- Queue screen [112](#)
- removing documents from the queue [114](#)
- required configuration information [84](#)
- using Queue [111](#)
- viewing and editing [79](#)
- viewing default [82](#)
- viewing details [114](#)
- viewing queued documents [113](#)
- viewing the list [111](#)

Getting Help [6](#)

H

Header background, uploading [18](#)

Help [6](#)

HTTP/S [29](#)

Hub Admin activities [15](#)

- adding a validation map to a Document Flow Definition [54](#)
- associating a map to Document Flow Definition [55](#)
- branding the Community Console [15](#)
- cloning from an existing object in the current context [43](#)
- configuring Document Flow Definitions and download packages [33](#)
- configuring permissions [21](#)
- configuring targets [25](#)
- configuring validation maps [52](#)
- creating a new target [25](#)
- creating an XML format [57](#)
- creating custom definitions [35](#)

- creating Document Flow Definitions [35](#)
- creating document flow interactions [46](#)
- deleting an XML format [61](#)
- deleting targets [33](#)
- displaying the Manage Maps screen [52](#)
- Document Flow Definition
 - components [34](#)
- Document Flow Definition interaction [34](#)
- downloading a package to a local computer [41](#)
- downloading sample images [16](#)
- editing XML format values [60](#)
- enabling a Document Flow Definition [46](#)
- enabling or disabling actions [62](#)
- enabling or disabling permissions quickly [24](#)
- enabling or disabling targets [33](#)
- file directory [29](#)
- FTP directory [26](#)
- HTTP/S [29](#)
- JMS [27](#)
- managing event codes [63](#)
- managing password policy [18](#)
- managing XML formats [57](#)
- POP3 [28](#)
- saving event code names [65](#)
- selecting attributes from a list [43](#)
- setting Document Flow Definition attributes [42](#)
- understanding Document Flow Definitions [33](#)
- updating a validation map [55](#)
- uploading a header background and company logo [18](#)
- uploading and downloading a package [39](#)
- viewing and editing password policy details [18](#)
- viewing and editing permission details [21, 63](#)
- viewing and editing target details [30](#)

I

Icons in the Community Console [12](#)

Image

- downloading sample [16](#)
- specifications [16](#)

Information required for gateway configuration [84](#)

Interaction

- creating document flow [46](#)
- Document Flow Definition [34](#)

J

JMS [27](#)

L

- Logging in [9](#)
- Logging out [13](#)

M

Machine shutdown, starting the system after [118](#)

Manage

- Connections screen [101](#)
- Document Flow Definitions screen [37](#)
- Maps screen [53, 56](#)
- XML Formats screen [58](#)

Managing

- B2B capabilities [94](#)
- certificates [88](#)
- event codes [63](#)
- exclusion lists [108](#)
- gateway configurations [79](#)
- Participant connections [98](#)
- Participant profiles [67](#)
- password policy [18](#)
- XML formats [57](#)

Map Update screen [54](#)

My Profile screen [77](#)

N

- Navigating through Community Console [11](#)
- New action, selecting [107](#)
- New target, creating [25](#)

O

- Online Help [6](#)
- Optimizing database query performance [115](#)
- Out-of-memory errors, avoiding [115](#)

P

Package

- downloading to a local computer [41](#)
- uploading and downloading [39](#)

Participant

- adding to Exclusion Lists [108](#)
- advanced search for connections [104](#)
- basic search for connections [101](#)
- changing attribute values [107](#)
- connection components [99](#)
- connection duplication [99](#)
- creating [67](#)
- Detail screen [69](#)
- managing connections [98](#)
- managing profiles [67](#)
- Search screen [68](#)
- searching [75](#)
- searching for connections [101](#)
- viewing and editing profiles [72](#)
- viewing profile [76](#)

Password

- Policy details screen [20](#)
- Policy screen [19](#)
- viewing and editing policy details [18](#)

Performing

- advanced search for connections [104](#)
- basic search for connections [101](#)

Permission

- configuring [21](#)
- Detail screen [23](#)
- enabling or disabling quickly [24](#)
- List screen [22](#)
- viewing and editing details [21, 63](#)

Poor performance and system events are not working [117](#)

POP3 [28](#)

Profile

- managing Participant [67](#)
- viewing [76](#)

Q

- Queue, removing documents from [114](#)
- Queued documents, viewing [113](#)

R

- Removing documents from the queue [114](#)
- Reprocessing events and business documents [116](#)
- Reprocessing events and business documents that fail to log to the database [116](#)
- Required information, gateway configuration [84](#)
- Reset user password message [74](#)
- Restarting the Document Manager [119](#)
- Restarting the Document Manager after a crash [119](#)
- Router and Receiver, stopping [14](#)
- Router, restarting [119](#)
- Router, restarting after a crash [119](#)

S

- Sample Gateway List screen [79](#)
- Sample images, downloading [16](#)
- Saving event code names [65](#)
- Screens
 - Advanced search [104](#)
 - Are You Sure Message [75](#)
 - B2B Capabilities [96](#)
 - Certificate Detail [91](#)
 - Console Branding [17](#)
 - Create New Configuration [93](#)
 - Document Flow Definitions [36](#)
 - Editing a Target [32](#)
 - Editing Participant IDs [110](#)
 - Editing Profile Details [74](#)
 - Editing Your Profile [78](#)
 - Example of Digital Certificate List [89](#)
 - Example of Participants and Their Corresponding Business IDs and Exclusion Status [109](#)
 - Example of Searching for Participants [76](#)
 - Example of the System Finding Connections [106](#)
 - Example of Viewing Profile Details [73](#)
 - Exclusion List [109](#)
 - FTP Configuration [85, 86, 87](#)

- Gateway default [83](#)
- Gateway Detail [80, 81](#)
- Gateway Queue [112](#)
- Manage Connections [101](#)
- Manage Document Flow Definitions [37](#)
- Manage Maps [53, 56](#)
- Manage XML Formats [58](#)
- Map Update [54](#)
- My Profile [77](#)
- Participant Detail [69](#)
- Participant Search [68](#)
- Password Policy [19](#)
- Password Policy Details [20](#)
- Permission Detail [23](#)
- Permission List [22](#)
- Reset User Password Message [74](#)
- Sample Gateway List [79](#)
- Target Details [26, 31](#)
- Target List [25](#)
- Typing a Business ID [71](#)
- Typing an IP Address [72](#)
- Upload/Download Packages [40](#)
- View XML Format [59](#)
- Viewing Certificate Details [90](#)

Search

- advanced for connections [104](#)
- Alert Search criteria [86, 87](#)
- basic for connections [101](#)
- for alerts [94](#)

Searching

- for connections [101](#)
- for Participants [75](#)

Selecting

- a new action [107](#)
- attributes from a list [43](#)

Server, specifying an FTP [85](#)

Setting

- B2B capabilities [95](#)
- Document Flow Definition attributes [42](#)

Shutting down [117](#)

- Source gateway, changing [108](#)
- Specifying an FTP server [85](#)
- Starting WebSphere Business Integration Connect [9](#)
- Status, change gateway [114](#)
- Stopping
 - Community Console [14](#)
 - Document Manager and Receiver [14](#)
- System events not working [117](#)

T

- Target
 - changing gateway [108](#)
 - configuring [25](#)
 - creating new [25](#)
 - deleting [33](#)
 - Details screen [26, 31](#)
 - enabling or disabling [33](#)
 - List screen [25](#)
 - viewing and editing details [30](#)

- Terms [5](#)

- Transport
 - file directory [29](#)
 - FTP [26](#)
 - HTTP/S [29](#)
 - JMS [27](#)
 - POP3 [28](#)

- Troubleshooting [115](#)
 - avoiding out-of-memory errors [115](#)
 - optimizing database query performance [115](#)
 - poor performance and system events are not working [117](#)
 - reprocessing [116](#)
 - reprocessing events and business documents that fail to log to the database [116](#)
 - restarting the Document Manager [119](#)
 - restarting the Document Manager after a crash [119](#)
 - shutting down [117](#)
 - starting the system after a machine shutdown [118](#)

- Types of Document Flow Definitions [95](#)

- Typing
 - business ID [71](#)

- IP address [72](#)

U

- Understanding Document Flow Definitions [33](#)
- Updating a validation map [55](#)
- Upload/Download Packages screen [40](#)
- Uploading
 - company logo [18](#)
 - Document Flow Definition package [39](#)
 - header background [18](#)
- Using the Gateway Queue [111](#)

V

- Validation maps
 - adding to a Document Flow Definition [54](#)
 - associating a map to Document Flow Definition [55](#)
 - configuring [52](#)
 - displaying the Manage Maps screen [52](#)
 - updating [55](#)
- View XML Format screen [59](#)
- Viewing
 - certificate details [90](#)
 - default gateways [82](#)
 - digital certificates [88](#)
 - gateway details [114](#)
 - gateway list [111](#)
 - gateways [79](#)
 - Participant profile [72, 76](#)
 - password policy details [18](#)
 - permission details [21, 63](#)
 - queued documents [113](#)
 - target details [30](#)

W

- WBIC terms [5](#)
- WebSphere Business Integration Connect
 - starting [9](#)
 - starting after machine shutdown [118](#)
- WebSphere Business Integration Connect – Express folders [121](#)

X

XML

creating a format [57](#)

deleting a format [61](#)

editing format values [60](#)

managing formats [57](#)

Notices and Trademarks

Notices

IBM may not offer the products, services, or features discussed in this document in all countries. Consult your local IBM representative for information on the products and services currently available in your area. Any reference to an IBM product, program, or service is not intended to state or imply that only that IBM product, program, or service may be used. Any functionally equivalent product, program, or service that does not infringe any IBM intellectual property right may be used instead. However, it is the user's responsibility to evaluate and verify the operation of any non-IBM product, program, or service.

IBM may have patents or pending patent applications covering subject matter described in this document. The furnishing of this document does not give you any license to these patents. You can send license inquiries, in writing, to:

IBM Director of Licensing
IBM Corporation
North Castle Drive
Armonk, NY 10504-1785
U.S.A.

The following paragraph does not apply to the United Kingdom or any other country where such provisions are inconsistent with local law: INTERNATIONAL BUSINESS MACHINES CORPORATION PROVIDES THIS PUBLICATION "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF NON-INFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. Some states do not allow disclaimer of express or implied warranties in certain transactions, therefore, this statement may not apply to you.

This information could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein; these changes will be incorporated in new editions of the publication. IBM may make improvements and/or changes in the product(s) and/or program(s) described in this publication at any time without notice.

Any references in this information to non-IBM Web sites are provided for convenience only and do not in any manner serve as an endorsement of those Web sites. The materials at those Web sites are not part of the materials for this IBM product and use of those Web sites is at your own risk.

IBM may use or distribute any of the information you supply in any way it believes appropriate without incurring any obligation to you.

Licensees of this program who wish to have information about it for the purpose of enabling: (i) the exchange of information between independently created programs and other programs (including this one) and (ii) the mutual use of the information which has been exchanged, should contact:

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

Such information may be available, subject to appropriate terms and conditions, including in some cases, payment of a fee.

The licensed program described in this document and all licensed material available for it are provided by IBM under terms of the IBM Customer Agreement, IBM International Program License Agreement, or any equivalent agreement between us.

Any performance data contained herein was determined in a controlled environment. Therefore, the results obtained in other operating environments may vary significantly. Some measurements may have been made on development-level systems and there is no guarantee that these measurements will be the same on generally available systems. Furthermore, some measurement may have been estimated through extrapolation. Actual results may vary. Users of this document should verify the applicable data for their specific environment.

Information concerning non-IBM products was obtained from the suppliers of those products, their published announcements or other publicly available sources. IBM has not tested those products and cannot confirm the accuracy of performance, compatibility or any other claims related to non-IBM products. Questions on the capabilities of non-IBM products should be addressed to the suppliers of those products.

This information contains examples of data and reports used in daily business operations. To illustrate them as completely as possible, the examples may include the names of individuals, companies, brands, and products. All of these names are fictitious and any similarity to the names and addresses used by an actual business enterprise is entirely coincidental.

All statements regarding IBM's future direction or intent are subject to change or withdrawal without notice, and represent goals and objectives only.

COPYRIGHT LICENSE:

This information contains sample application programs in source language, which illustrates programming techniques on various operating platforms. You may copy, modify, and distribute these sample programs in any form without payment to IBM, for the purposes of developing, using, marketing or distributing application programs conforming to the application programming interface for the operating platform for which the sample programs are written. These examples have not been thoroughly tested under all conditions. IBM, therefore, cannot guarantee or imply reliability, serviceability, or function of these programs. You may copy, modify, and distribute these sample programs in any form without payment to IBM for the purposes of developing, using, marketing, or distributing application programs conforming to IBM's application programming interfaces.

Programming interface information

Programming interface information is intended to help you create application software using this program.

General-use programming interfaces allow you to write application software that obtain the services of this program's tools.

However, this information may also contain diagnosis, modification, and tuning information. Diagnosis, modification and tuning information is provided to help you debug your application software.

Warning: Do not use this diagnosis, modification, and tuning information as a programming interface because it is subject to change.

Trademarks and service marks

The following terms are trademarks of International Business Machines Corporation in the United States, other countries, or both:

IBM
the IBM logo
CrossWorlds
DB2
DB2 Universal Database
MQSeries
Passport Advantage
WebSphere

Microsoft, Windows, and the Windows logo are trademarks of Microsoft Corporation in the United States, other countries, or both.

Intel and Xeon are trademarks or registered trademarks of Intel Corporation in the United States, other countries, or both.

Solaris, Java, and all Java-based trademarks are trademarks of Sun Microsystems, Inc. in the United States, other countries, or both.

Other company, product or service names may be trademarks or service marks of others.

