

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



Community Console User 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 133.

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.

Contents

About this book - - - - - 5

| | |
|---|---|
| Who should read this book - - - - - | 5 |
| Conventions and terminology used in this book - - - - - | 5 |
| Typographic conventions - - - - - | 5 |
| Terms - - - - - | 5 |
| Getting help - - - - - | 7 |
| Online Help - - - - - | 7 |
| Customer service - - - - - | 8 |
| Company web site - - - - - | 8 |

Chapter 1. Introduction - - - - - 9

| | |
|---|----|
| What is a hub-community? - - - - - | 9 |
| Community Operator - - - - - | 9 |
| Community Manager - - - - - | 9 |
| Community Participant - - - - - | 9 |
| Community Console users - - - - - | 9 |
| Hub-community configurations - - - - - | 12 |
| Community Console's administrative users and their privileges - - - - - | 15 |
| Logging In and Out of the Console - - - - - | 17 |
| Community Console icons - - - - - | 18 |
| Using the Community Console - - - - - | 21 |
| Links to modules and features - - - - - | 22 |

Chapter 2. Managing community connections and users:

Account Admin - - - - - 23

| | |
|--|----|
| Managing your Participant profile - - - - - | 24 |
| Viewing and editing your Participant profile - - - - - | 24 |
| Managing gateways - - - - - | 26 |
| Performing gateway tasks - - - - - | 26 |
| Viewing a list of gateways - - - - - | 26 |
| Viewing or editing gateway details - - - - - | 27 |
| Creating a gateway - - - - - | 28 |
| View, select, or edit your default gateways - - - - - | 30 |
| Managing FTP - - - - - | 31 |
| Community Console FTP configuration - - - - - | 31 |
| Setting up FTP - - - - - | 33 |
| Creating your FTP account - - - - - | 35 |

| | |
|---|----|
| Changing FTP password or account status for ProFTPD users - - - - - | 36 |
| Managing B2B capabilities - - - - - | 37 |
| Managing certificates - - - - - | 40 |
| Performing certificate tasks - - - - - | 43 |
| Viewing a list of digital certificates - - - - - | 43 |
| Viewing and editing digital certificate details - - - - - | 43 |
| Uploading and defining a digital certificate - - - - - | 44 |
| Disabling a digital certificate - - - - - | 45 |
| Managing users - - - - - | 46 |
| Performing user tasks - - - - - | 46 |
| Viewing or editing user details - - - - - | 46 |
| Assigning users to groups - - - - - | 49 |
| Creating a new user - - - - - | 49 |
| Managing groups - - - - - | 51 |
| Performing group tasks - - - - - | 51 |
| Viewing group memberships and assigning users to groups - - - - - | 52 |
| Viewing, editing, or assigning group permissions - - - - - | 53 |
| Viewing or editing group details - - - - - | 53 |
| Creating a new group - - - - - | 54 |
| Deleting a group - - - - - | 55 |
| Managing contacts - - - - - | 56 |
| Performing contact tasks - - - - - | 56 |
| Viewing or editing contact details - - - - - | 56 |
| Adding a contact to an alert - - - - - | 58 |
| Creating a new contact - - - - - | 62 |
| Removing a contact - - - - - | 63 |
| Managing addresses - - - - - | 64 |
| Performing address tasks - - - - - | 64 |
| Editing an address - - - - - | 64 |
| Creating a new address - - - - - | 65 |
| Deleting an address - - - - - | 66 |
| Managing alerts - - - - - | 67 |
| Performing alert tasks - - - - - | 68 |
| Viewing or editing alert details and contacts - - - - - | 68 |
| Searching for alerts - - - - - | 71 |
| Adding a new contact to an existing alert - - - - - | 71 |

| | | | |
|---|-----------|---|------------|
| Creating a volume-based alert and adding contacts - - - - - | 73 | Chapter 4. Analyzing document flow: | |
| Creating an event-based alert and adding contacts - - - - - | 76 | Tools - - - - - | 103 |
| Disabling or enabling an alert - - - - - | 80 | Document Analysis - - - - - | 104 |
| Removing an alert - - - - - | 80 | Document States - - - - - | 104 |
| | | Viewing documents in the system - - | 104 |
| Chapter 3. Viewing events and documents: Viewers - - - - - | 81 | Viewing process and event details - - | 106 |
| Event Viewer - - - - - | 82 | Document Volume Report - - - - - | 107 |
| Event types - - - - - | 83 | Create a Document Volume Report - | 107 |
| Performing Event Viewer tasks - - - - | 83 | Exporting the Document Volume Report - - - - - | 109 |
| Searching for events - - - - - | 83 | Printing reports - - - - - | 109 |
| Viewing event details - - - - - | 85 | Test Participant Connection - - - - - | 110 |
| AS1/AS2 Viewer - - - - - | 87 | Test Participant connection - - - - - | 110 |
| Performing AS1/AS2 Viewer tasks - - | 87 | Web Server result codes - - - - - | 111 |
| Searching for messages - - - - - | 87 | | |
| Viewing message details - - - - - | 89 | Chapter 5. Community Participant Simulator - - - - - | 115 |
| RosettaNet Viewer - - - - - | 92 | Initiate and view document flow - - - - | 118 |
| Performing RosettaNet Viewer tasks - | 92 | Searching for an open document - - | 119 |
| Searching for RosettaNet processes - | 92 | Responding to an open document - - | 119 |
| Viewing RosettaNet process details - - | 94 | Removing an open document - - - - | 120 |
| Viewing raw documents - - - - - | 95 | | |
| Document Viewer - - - - - | 96 | Glossary - - - - - | 121 |
| Performing Document Viewer tasks - - | 96 | | |
| Searching for documents - - - - - | 96 | Notices and Trademarks - - - - | 133 |
| Viewing document details, events, and raw document - - - - - | 99 | Notices - - - - - | 133 |
| Viewing data validation errors - - - - | 100 | Programming interface information - - - - - | 135 |
| | | Trademarks and service marks - - - - | 135 |

About this book

IBM® WebSphere® Business Integration Connect is an electronic document processing system used to manage a business-to-business (B2B) trading community. B2B has evolved over recent years to help businesses conduct many types of automated transactions (for example, purchase orders and invoices), quickly, conveniently, and economically.

The parties involved in an IBM WebSphere Business Integration Connect's trading or hub-community are the Community Manager, Community Operator, and Community Participants (also referred to as Participants). Each of these parties have administrative users with different levels of privileges. In addition, the administrative users will add regular users with specific console access privileges.

This guide walks introduces the Community Manager and Participants to the product's console.

Who should read this book

This document describes how a Community Manager or Participant configures and uses IBM WebSphere Business Integration Connect to manage the exchange of business documents.

Conventions and terminology used in this book

Typographic conventions

This document uses the following conventions:

| | |
|---------------------------|--|
| bold | Indicates a selection on a screen. |
| 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. |
| <i>italics</i> | Indicates a variable. |

Terms

The following terms are unique to this product and document processing. Additional terms appear in this guide's [Glossary, page 121](#).

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 WebSphere Business Integration Connect and to manage the flow of your company's business documents to and from your Community Manager or 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 WebSphere 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 individuals responsible for the configuration and overall health and maintenance of the system, hub-wide.

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

Community Participant: The Participant sends business transactions to and receives business transactions from the Community Manager. The Participants can access features that support their role in the community.

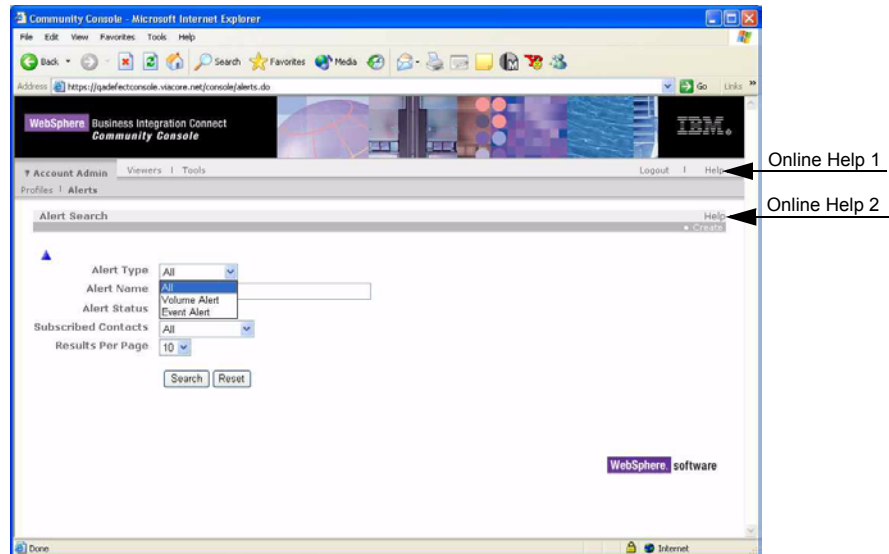
RosettaNet PIP (Partner Interface Process): A model that depicts the activities, decisions, and Partner Role Interactions that fulfill a business transaction between two Partners in a given supply chain. (In WebSphere Business Integration Connect, Partners are called Participants.) Each Participant involved 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

Online Help is available on the right side of each screen.



The Community Console

- Click the top Help (Online Help 1 in the above illustration) to display the entire online Help system for the console.
- Click the bottom Help (Online Help 2 in the above illustration) to display online Help that is specific to the screen that you are viewing.

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. Introduction

What is a hub-community?

IBM WebSphere Business Integration Connect's hub-community consists of three entities connected to a central hub for the real-time exchange of business documents: Community Operator, Community Manager, and Participants.

Community Operator

The Community Operator is a company responsible for managing the day-to-day operation of the hub-community. The Community Operator maintains the hardware and software infrastructure of the hub-community on a 24x7 basis. Responsibilities include:

- Troubleshooting and repair.
- Ensuring that the hub-community is properly configured for all Participants.
- Assisting in the configuration of new Participants to the hub-community.
- Strategic planning for future growth to ensure the hub-community operates at peak efficiency.

The role of the Community Operator can be contracted to a third party company within the hub-community, or the Community Manager who purchased Business Integration Connect can elect to perform the function of the Community Operator.

Community Manager

The Community Manager is the primary company and driving force within the hub-community. This company is responsible for the purchase and construction of the hub-community, including definition of the electronic business processes transacted between them and their Community Participants.

The Community Manager can also choose to be the Community Operator.

Community Participant

Participants are the companies that do business with the Community Manager via the hub-community. Participants must complete a configuration process to connect to the hub-community. Once connected, Participants can exchange electronic business documents with the Community Manager.

Community Console users

Each entity (Community Operator, Community Manager, or Participant) requires secure visibility into the activities of the hub-community via the Community Console. Note that the level of visibility is different for each entity.

To achieve visibility, each entity grants access to the WebSphere Business Integration Connect to one or more users. Access is based on two criteria: the entity (Community Operator, Community Manager, or Participant), and the role that the individual will perform.

Some users are granted administrative access privileges to the console. Administrative access privileges are required by those who are responsible for system configuration. Other users are granted access privileges based on specific requirements. For example, analysts might routinely audit the system's workload and performance, but only require access to specific console features.

Table 1-1. The hub-community's Community Console users

| | Community Operator | Community Manager | Community Participant |
|-------------------------|-----------------------------|--------------------------|------------------------------|
| Administrative Users | Hub Admin Operator Admin | Manager Admin | Participant Admin |
| Non-administrative User | Operator User | Manager User | Participant User |

Community Console administrative users

Based on the criteria noted above, the hub-community includes the following administrative user types:

- Hub Admin
- Operator Admin
- Manager Admin
- Participant Admin

Users who are given these administrative roles can grant console access to other users on a need to know basis.

Hub Admin: Community Operator Administrative User

The Hub Admin is the Community Operator administrative user who has super-user console privileges. As a result, the Hub Admin has access to all of the console's modules and features. These privileges give this user the tools necessary to perform configuration and management functions in the hub-community.

The Hub Admin assumes slightly different roles in the two types of hub-community configurations. In the first configuration, there are three separate, distinct entities: the Community Operator (a third party), the Community Manager, and Participants. The distinction between the Hub Admin user and the other user types is particularly clear in this configuration.



In the second configuration, the Community Manager performs the role of Community Operator. In this case, the Hub Admin user type and the Manager Admin user type are usually combined into the same function. (To learn more about the Manager Admin, see the following section.)



For more information about the two types of hub-community configurations, see [“Hub-community configurations” on page 12](#).

Operator Admin

The Operator Admin is the second Community Operator’s administrative user. This user has access to all of the console’s features except those in the Hub Admin module.

Manager Admin

The Manager Admin is the Community Manager’s administrative user. The Manager Admin manages access to the console by employees within the Community Manager’s company. The Manager Admin is also responsible for the functionality required for document exchange with the hub-community’s Participants.

Participant Admin

The Participant Admin is the Participant’s administrative user. The Participant Admin’s role is similar to the Manager Admin’s role. The Participant Admin manages access to the console by employees within the Participant’s company. The Participant Admin is also responsible for the functionality required for document exchange with the Community Manager.

Community Console non-administrative users

Operator user

The Operator User, a regular user rather than an administrative user, receives access to the console from the Hub Admin. The Operator User uses the console to view specific business document processing information based on the user's role in the Community Operator's company.

Manager user

The Manager User, a regular user rather than an administrative user, receives access to the console from the Manager Admin. The Manager User uses the console to view specific business document processing information based on the user's role in the Community Manager's company.

Participant user

The Participant User, a regular user rather than an administrative user, receives access to the console from the Participant Admin. The Participant User uses the console to view specific business document processing information based on the user's role in the Participant's company.

Hub-community configurations

There are two types of hub-community configurations. Before installation, the Community Manager decides which configuration the hub-community will use.

The first configuration consists of three separate entities: Community Manager, Participants, and a third party Community Operator (see [Table 1-2 on page 13](#)). In the second configuration, the Community Operator and Community Manager roles are performed by the Community Manager ([Table 1-3 on page 14](#)). As a result, the Hub Admin and Manager Admin administrative user roles are combined into one, the Hub-Manager Admin.

The following tables illustrate the relationship between hub-community configurations, entities, and user types.

Table 1-2. Hub-Community with Community Manager, Participants, and a third party Community Operator.

| Entity | User | Description |
|--------------------|-------------------|--|
| Community Operator | Hub Admin | Super administrative user in the hub-community. Responsible for initial setup and configuration of the hub-community. Creates Participants, but is not responsible for Participant configuration. Responsible for overall management of the hub-community. |
| | Operator Admin | This user can access all console features except those in the Hub Admin module. |
| | Operator User | Responsibilities can include managing, analyzing, reporting, and troubleshooting business documents between Community Manager and Participants. |
| Community Manager | Manager Admin | Responsible for Community Manager configuration. Manages access to the console by employees within the Community Manager's company. Responsible for the functionality required for document exchange with the hub-community's Participants |
| | Manager User | Responsibilities can include managing, analyzing, reporting, and troubleshooting business documents with the Participants. |
| Participant | Participant Admin | Responsible for Participant configuration. Manages access to the console by employees within the Participant's company. Responsible for the functionality required for document exchange with the Community Manager. |
| | Participant User | Responsibilities can include managing, analyzing, reporting, and troubleshooting business documents with the Community Manager. |

Table 1-3. Hub Community with Community Manager acting as Community Operator, and Participants.

| Entity | User | Description |
|----------------------------|-------------------|---|
| Community Manager-Operator | Hub-Manager Admin | <p>Super administrative user in the hub-community.</p> <p>Responsible for initial setup and configuration of the hub-community. Creates Participants, but is not responsible for Participant configuration.</p> <p>Responsible for overall management of the hub-community.</p> <p>Manages access to the console by employees within the Community Manager-Operator's company.</p> <p>Responsible for the functionality required for document exchange with the hub-community's Participants.</p> |
| | Manager User | <p>Responsibilities can include managing, analyzing, reporting, and troubleshooting business documents with the Participants.</p> |
| Participant | Participant Admin | <p>Responsible for Participant configuration.</p> <p>Manages access to the console by employees within the Participant's company.</p> <p>Responsible for the functionality required for document exchange with the Community Manager.</p> |
| | Participant User | <p>Responsibilities can include managing, analyzing, reporting, and troubleshooting business documents with the Community Manager.</p> |

Community Console's administrative users and their privileges

The table that follows identifies each administrative user's privileges. Note that when any user logs on to the console, the console only displays features that the user can access.

Table 1-4. Community Console's administrative users and their privileges

| Module or Feature | Community Operator | | Community Manager | Participant |
|-----------------------------------|--------------------|----------------|-------------------|-------------------|
| | Hub Admin | Operator Admin | Manager Admin | Participant Admin |
| Account Admin Module | | | | |
| Participant Management | x | x | x | x |
| Certificate Management | x | x | x | x |
| Gateway Management | x | x | x | x |
| User Management | x | x | x | x |
| Group Management | x | x | x | x |
| Contact Management | x | x | x | x |
| Address Management | x | x | x | x |
| Participant Connection Management | x | x | | |
| Exclusion List Management | x | x | | |
| Alert Management | x | x | x | x |
| B2B Management | x | x | x | x |
| FTP Management | x | x | x | x |
| Viewers Module | | | | |
| | | x | | |
| Event Viewer | x | x | x | x |
| RosettaNet Viewer | x | x | x | x |
| AS1/AS2 Viewer | x | x | x | x |
| Document Viewer | x | x | x | x |
| • Data Validation | x | x | x | x |
| • Original Raw Document | x | x | x | x |
| • Translated Raw Document | x | x | x | |
| Gateway Queue | x | x | | |
| Tools Module | | | | |
| | | x | | |
| Document Analysis | x | x | x | x |
| Document Volume Report | x | x | x | x |
| Test Participant Connection | x | x | x | x |

Table 1-4. Community Console's administrative users and their privileges

| Module or Feature | Community Operator | | Community Manager | Participant |
|---|---|----------------|-------------------|-------------------|
| | Hub Admin | Operator Admin | Manager Admin | Participant Admin |
| Hub Admin Module | Available to Community Operator's Hub Admin only. | | | |
| Permission Management | x | | | |
| Password Policy Management | x | | | |
| Event Code Management | x | | | |
| Action Management | x | | | |
| Document Flow Definition Management | x | | | |
| Validation Map Management | x | | | |
| Target Management | x | | | |
| Console Branding Management | x | | | |
| XML Formats Management | x | | | |
| Community Participant Simulator Module | | | | |
| Initiate Process | x | x | x | |
| View Open Processes | x | x | x | |

Logging In and Out of the Console

To display the Community Console:

Recommended screen resolution is 1024x768.

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

1. Open a Web browser and enter the following URL:

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

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

The browser displays the console's login screen.

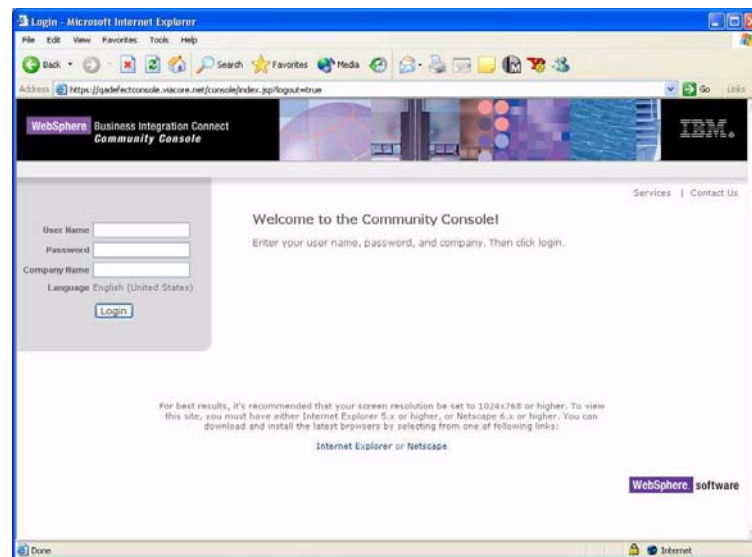


Figure 1-1. The Community Console's login screen

In most cases, your Community Operator has sent you the user name, initial password, and company name that you will use to log in to the Community Console. You will need this information for the following procedure. If you have not received this information, contact your Community Operator.

To log in to the Community Console (these instructions are for the Community Manager as well as Participants):

1. Enter the User Name for your company.
2. Enter the Password for your company.
3. Enter your Company Name, for example, IBM.
4. Click **Login**. When you log in the first time, you must create a new password.
5. Enter a new password, then enter the new password a second time in the Verify text box.
6. Click **Save**. The system displays the console's initial entry screen.

To log out of the Community Console:

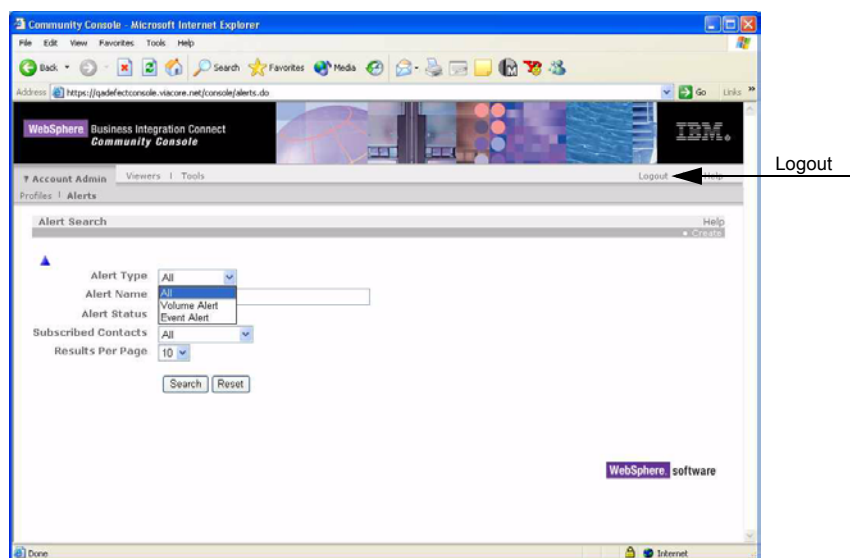


Figure 1-2. Logout Link

1. Click the **Logout** link at the top of any console screen (see [Figure 1-2 on page 18](#)). The system logs you out and returns you to the console's Login screen.

Community Console icons

The icons in the table below are unique to the WebSphere Business Integration Connect Community Console.

Table 1-5. Community Console icons

| Icon | Description |
|------|---------------------------------|
| ★ | Required field. |
| 🔍 | Click to view details. |
| 🔎 | Search. |
| ✓ | Selected (active). |
| 👥 | Click to view group membership. |
| 👤 | Click to view memberships. |
| 🔑 | Click to view permissions. |

Table 1-5. Community Console icons







































| Icon | Description |
|---|--|
|  | Click to edit details. |
|  | Click to turn edit off. |
|  | Click to remove selected item. |
|  | Generate certificate. |
|  | Participant. |
|  | All Participants. |
|  | Calendar. |
|  | Indicates that gateway is disabled. |
|  | Tree is collapsed. |
|  | Tree is expanded. |
|  | Attributes. |
|  | Set up attributes. |
|  | Edit RosettaNet attribute values. |
|  | Edit attribute values. |
|  | Create new capability. |
|  | Indicates document contains an attachment. |
|  | Click to display raw document. |
|  | Document currently in progress. |
|  | Document processing was successful. |
|  | Translated document. |
|  | Document failed processing. |
|  | Click to view validation errors. |

Table 1-5. Community Console icons

| Icon | Description |
|---|------------------------------------|
|  | View process. |
|  | MDN has been processed. |
|  | MDN waiting. |
|  | Retries exceeded. |
|  | Add or update. |
|  | Click to view details. |
|  | Show all documents. |
|  | Duplicate document. |
|  | Synchronous document. |
|  | Click to export report. |
|  | Click to continue. |
|  | Click to pause. |
|  | Click to stop. |
|  | Click to export a report. |
|  | Print document, report, and so on. |
|  | Click to view the Help system. |

Using the Community Console

After you configure WebSphere Business Integration Connect, you will use two console tools on a regular basis: the Event Viewer and Document Analysis.

Use the Event Viewer, in the Viewers module, to research events. Most types of documents are resent multiple times, so when a document fails and generates an alert, it is something that you should investigate and correct to prevent similar failures in the future.

You can locate a specific event and then research why it occurred. The Event Viewer allows you to search for events by time, date, event type, event code, and event location. The Hub Admin can also search by Participant, Source IP, and Event IP.

NOTE: Not all users will have access to Debug events.

The data that the Event Viewer generates helps you identify the event and the document that created the event. You can also view the raw document, which identifies the field, value, and reason for the error.

The second most commonly used tool is Document Analysis, a feature in the Tools module. It is used to find out how many documents were received, how many are in progress, and of those completed, how many failed and how many were successful. Use this tool to drill down to the specific documents that failed to find out why they failed.

The console's Account Admin module are used primarily when you are setting up Business Integration Connect and thereafter for maintenance.

Links to modules and features

The following table includes links to the documentation for each of the console's modules and features.

Table 1-6. WebSphere Business Integration Connect's Modules and Features

| Module and Module Features | Location |
|-----------------------------------|--------------------------|
| Account Admin | Page 23 |
| Managing your Participant profile | Page 24 |
| Managing gateways | Page 26 |
| Managing FTP | Page 31 |
| Managing B2B capabilities | Page 37 |
| Managing certificates | Page 40 |
| Managing users | Page 46 |
| Managing groups | Page 51 |
| Managing contacts | Page 56 |
| Managing addresses | Page 64 |
| Managing alerts | Page 67 |
| Viewers | Page 81 |
| Event Viewer | Page 82 |
| RosettaNet Viewer | Page 92 |
| AS1/AS2 Viewer | Page 87 |
| Document Viewer | Page 96 |
| Tools | Page 103 |
| Document Analysis | Page 104 |
| Document Volume Report | Page 107 |
| Test Participant Connection | Page 110 |
| Community Participant Simulator | Page 115 |
| Upload Document | Page 117 |
| View Open Document Flows | Page 118 |

Chapter 2. Managing community connections and users: Account Admin

The features in the Account Admin module control how IBM WebSphere Business Integration Connect is used, and by whom.

For example, you can control access to the Community Console and each of its features. You can control who receives alerts when important events occur. Examples of events include Participant Connection Not Found, RosettaNet Validation Error, and Document Delivery Failed.

You will also use this module to maintain your Participant profile, certificates, gateways, users, groups, contacts, addresses, alerts, FTP server, and B2B capabilities. (B2B capabilities define the types of business processes your system can send and receive.) If you were involved in the configuration process, you are already familiar with these features.

Table 2-1. Account Admin features

| What feature do you want to use? | See |
|-----------------------------------|-------------------------|
| Managing your Participant profile | page 24 |
| Managing gateways | page 26 |
| Managing FTP | page 31 |
| Managing B2B capabilities | page 37 |
| Managing certificates | page 40 |
| Managing users | page 46 |
| Managing groups | page 51 |
| Managing contacts | page 56 |
| Managing addresses | page 64 |
| Managing alerts | page 67 |

Managing your Participant profile

Use the Account Admin Participants feature to view and edit the information that identifies your company to the system.

Participants can edit all attributes in their profile except the Participant Login Name used for login, and the Participant Type. Participants can also add and remove Business IDs and IP addresses. IP addresses include Production and Test.

This feature also includes an option to reset all user passwords. You might want to use this feature if you feel that user passwords have been compromised.

Viewing and editing your Participant profile

1. Click **Account Admin** on the main menu.
2. Click **Profiles** on the horizontal navigation bar.
3. Click **Community Participants**. The system displays your profile.

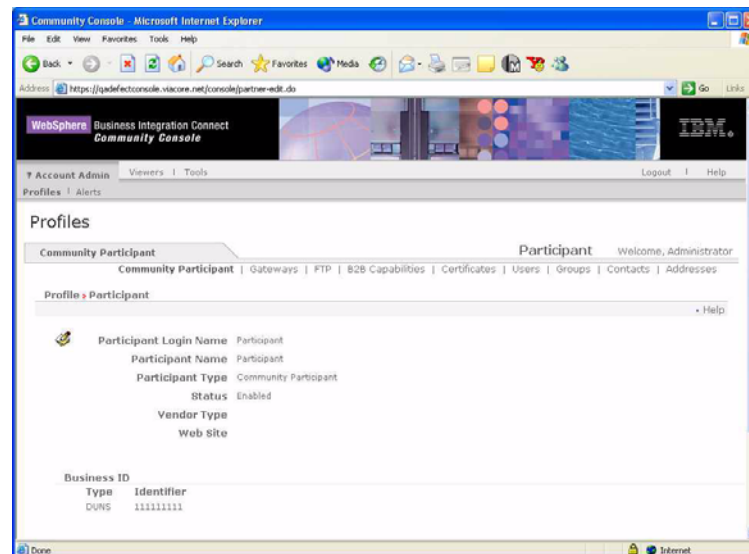


Figure 2-1. Participant profile

4. Click  to edit. The system displays the Participant Detail screen.

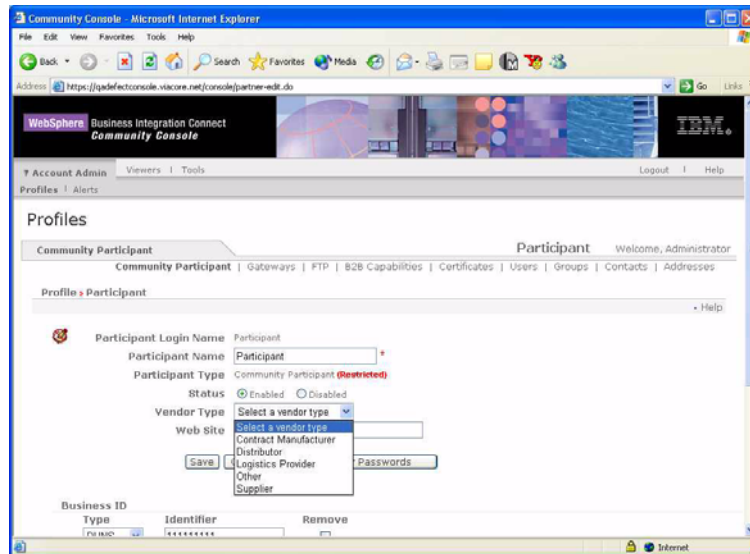


Figure 2-2. Edit Participant profile

5. Edit your profile, as required (some values cannot be edited). For an explanation of the values, see the following table.

Table 2-2. Values on Participants screens

| Value | Description |
|------------------------|---|
| Participant Login Name | Identifies the Participant to the system. Maximum of 15 characters. Cannot include the following special characters: , . ! # ; : \ / & ?. Participants cannot edit this value. |
| Participant Name | The name the Participant wants displayed to the hub-community. Maximum of 30 characters. |
| Participant Type | Community Operator, Participant, or Community Manager. Participants cannot edit this value. |
| Community Manager | Name of Community Manager. |
| Status | Enabled or Disabled. If disabled, Participant is not visible in search criteria and drop-down lists. |
| Vendor Type | Identifies the Participant's role, for example, Contract Manufacturer or Distributor. |
| Web Site | Identifies the Participant's web site. |
| Business ID | DUNS, DUNS+4, or Freeform number that the system uses for routing. You can add additional business ID numbers. <ul style="list-style-type: none"> DUNS numbers must equal nine digits and DUNS+4 thirteen digits. Freeform ID numbers accept up to 60 alpha, numeric, and special characters. |
| IP Address | <ul style="list-style-type: none"> Gateway Type, for example, CPS Participant. IP Address of Participant. |

6. Click **Save**.

Managing gateways

RESTRICTIONS: Some gateway values are dependent on the selected transport protocol. Restrictions are noted in the values table and procedures.

A gateway is a B2B network point that acts as the entrance to another network. A gateway can resolve data translation and compatibility issues to ensure data transfer. Used in conjunction with participant connections, which define the connection between two specific community members' environments, gateways control the successful routing of business documents.

Business Integration Connect uses gateways to identify addressing and the source and destination configurations.

You must create and maintain a default gateway. If you do not, you cannot create connections. You cannot delete your default gateway because this action disables the gateway's channel. You can, however, change your default gateway from one gateway to another. The Gateways screen identifies your default gateway.

Use the Gateways feature to add gateways and to view information used to route documents to their proper destination. You can view Target URI, transport protocol, and gateway status from this feature.

The information required to add a gateway depends on the type of transport that the gateway will use.

Performing gateway tasks

Table 2-3. Gateway Tasks

| What do you want to do? | See |
|---|-------------------------|
| View a list of gateways | page 26 |
| View or edit gateway details | page 27 |
| Create a gateway | page 28 |
| View, select, or edit your default gateways | page 30 |



Viewing a list of gateways

To view a list of gateways in the system:

1. Click **Account Admin** on the main menu.
2. Click **Gateways**. The system displays the Gateway List screen.

Viewing or editing gateway details

IMPORTANT: If you disable a gateway, you also disable the participant connection associated with the gateway. The gateway will not function. If you set the gateway to offline, documents will queue until the gateway is put back online.

1. Click **Account Admin** on the main menu.
2. Click **Gateways**. The system displays the Gateway List screen.
3. Click  to view gateways details.
4. Click  to edit gateway details.

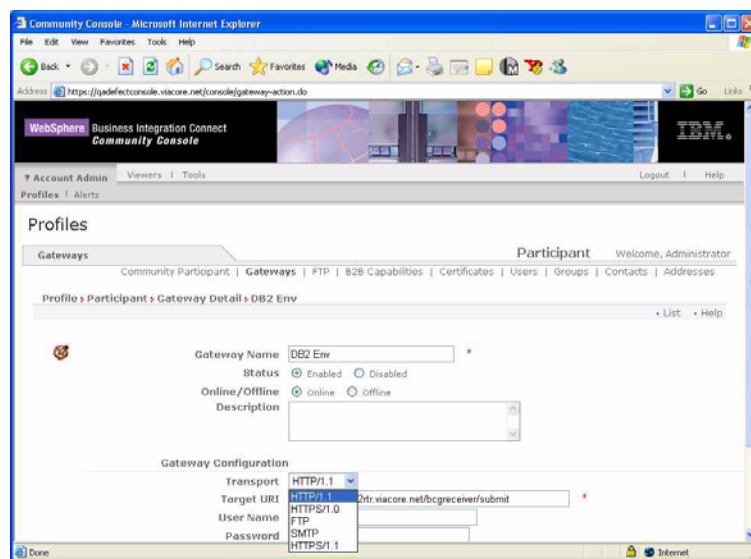


Figure 2-3. Gateway Detail (Edit)

5. Edit information as required. The following table describes gateway values.

Table 2-4. Values on the gateway screen

| Value | Description |
|-------------------|--|
| Gateway Name | Name of gateway. |
| Transport | Protocol used to route documents. |
| Target URI | URI of destination. |
| Online or Offline | If offline, documents are queued until the gateway is placed online. |
| Status | Enabled or Disabled. Documents routing through a gateway with a disabled status fail processing. |
| Default | Identifies the default gateway. |

6. Click **Save**.

Creating a gateway

To create a new gateway:

1. Click **Account Admin** on the main menu.
2. Click **Gateways**. The system displays the Gateway List screen.
3. Click **Create** on the sub-menu. The system displays the Gateway Detail screen.

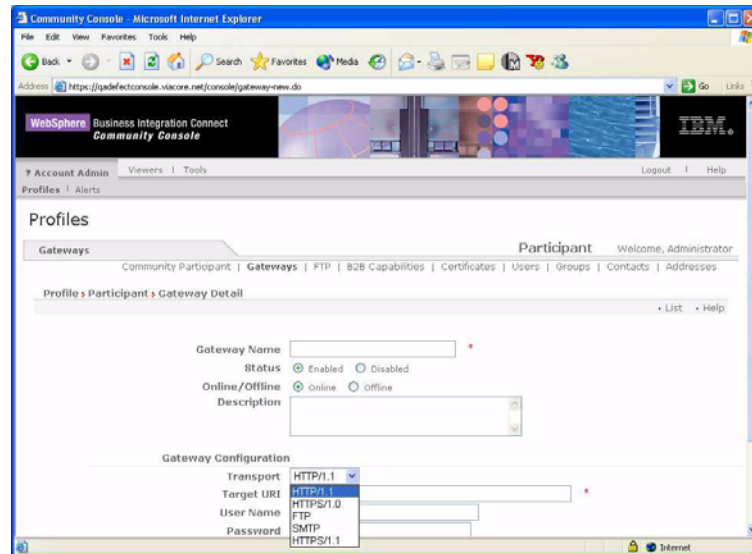


Figure 2-4. Gateway Detail (Create)

4. Enter a unique name for the gateway.
5. Select the gateway's status: Enabled or Disabled. Documents fail to process if they are routed through a gateway with a disabled status. When you disable a gateway, you also disable the participant connection associated with the gateway.
6. Select Online or Offline. If offline, documents are queued until the gateway is placed online.
7. Enter a description of the gateway.
8. Select that gateway's transport method (for example, HTTP 1.1 or SMTP).

Table 2-5. Required information for each transport method

| Transport | HTTP | HTTPS | FTP | JMS | SMTP |
|----------------------------|---|---|---|---|---|
| Transport Protocol Version | 1.1 only | 1.0 or 1.1 | - | - | - |
| Target URI | Must match http://... | Must match https://... | Must match ftp://... | - | Must match mailto:... |
| User Name for URI | Required if authentication is required. | Required if authentication is required. | Required if authentication is required. | Required if authentication is required. | Required if authentication is required. |
| Password for URI | Required if authentication is required. | Required if authentication is required. | Required if authentication is required. | Required if authentication is required. | Required if authentication is required. |
| Authentication Required | Optional - basic authentication | Optional - basic authentication | Required | Optional | Optional |

9. Enter the gateway's Target URI in one of the following formats (not required for JMS):
http://<URI>
https://<URI>
10. Enter the User Name for the URI (not required for JMS). This is required whenever authentication is required. When using FTP, this is the log in for a Participant's FTP server.
11. Enter the Password for the URI (not required for JMS). This is required whenever authentication is required.

IMPORTANT: When you are using JMS for Transport, the Target URI is the URL for the JNDI service.

For MQ JMS, the format of the Target URI is as follows:
file:/// <user defined MQ JNDI bindings path>.

This directory contains the MQ .bindings file for file-based JNDI. Note the three slashes after file.

12. Select **Yes** or **No** to require authentication. This is required for FTP, often required for JMS. If required for JMS, user name and password are also required.
13. If you are a Participant, or if you are a Community Manager and you did not select JMS as the Transport method, click **Save**. If you are a Community Manager and selected JMS, continue to the next step.
14. Enter the required information for JMS (for example, JMS Factory Name).
15. Click **Save**. To add additional gateways, repeat these steps.

View, select, or edit your default gateways

To view, select, or edit your default gateway:

1. Click **Account Admin** on the main menu.
2. Click **Gateways**. The system displays the Gateway List screen.
3. Click **View Default Gateway** on the sub-menu. The system displays the Default Gateway List screen.
4. Use the drop-down lists to select or change one or more default gateways.
5. Click **Save**.

Managing FTP

If you do not plan to use Business Integration Connect's FTP functionality, you can disregard this section. The Community Operator may disable this feature if your company is not using FTP.

FTP is a file transfer protocol used to copy files to and from remote computer systems on the Internet. Business Integration Connect can receive inbound documents through FTP.

All XML sent by a Participant to Business Integration Connect must be XML documents that have all of the required routing information in the content of the document. All other documents are treated as binary documents for pass-through routing.

Business Integration Connect is configured to support ProFTPD. ProFTPD must be installed and configured before you create an FTP account. If you use a different FTP server, additional manual setup is required.

Community Console FTP configuration

The Hub Admin uses the Community Console to perform the following tasks:

- Enable or disable FTP for Participants.
- Set the password for the FTP login.

If you are a Participant and you are using ProFTPD, after you install and configure ProFTPD, you can enable your own FTP account through the console (this feature is not available if you are using a non-ProFTPD server). However, documents cannot be received by the Community Manager until the Hub Admin creates a target to receive documents through FTP.

When your FTP account is enabled, Business Integration Connect performs the following tasks:

- Creates a user account in the FTP server. The FTP login name is the Participant's login name and the initial password is auto-generated.
- Creates a home FTP login for the Participant. The home directory is the login name of the Participant.
- Creates binary and document sub-directories under the Participant's home directory, and a sub-directory below both the binary and document sub-directories for each gateway type configured in the product. For more information about the FTP directory structure, see ["FTP server directory structure" on page 32](#).

The Community Console allows Participants to view the information they need to transfer files using FTP. This includes the following information:

- The user name to log in to the FTP server (not editable).
- Account status (Enabled or Disabled). Participants can view and change their FTP account status.
- Password for FTP account (editable).
- The hostname of the Community Manager's FTP server. For example: ftp.myHub.com <ftp://ftp.myHub.com> (not editable).

Participants can update the password used to log in to the FTP server. Note that this password is different from the password the Participant uses to log in to the console. When updating the password, Business Integration Connect's password policy is enforced.

FTP server directory structure

When FTP is enabled for a Participant, the system creates the following directory structure under the Participant's default FTP login directory:

```
binary
  <GatewayType>
  <GatewayType>
  <and so on>
documents
  <GatewayType>
  <GatewayType>
  <and so on>
```

The default configuration defines Test and Production destination types, resulting in the following directory structure:

```
Binary
  Production
  Test
Documents
  Production
  Test
```

The Participant transfers files to IBM WebSphere Business Integration Connect by putting the file in the directory corresponding to the correct document type (Binary or Documents) and correct destination type (in the example above, Production or Test).

It is assumed that all documents placed in a destination type directory under the Documents directory are documents that include all routing information within the document. These are limited to custom XML formats defined in the product. It is the responsibility of the Participant to ensure that the files they transfer using FTP do not clash with any existing files.

All documents placed in a destination type directory under the Binary directory must follow specific file naming conventions.

Binary file naming convention

Files sent by FTP and placed in a destination type sub-directory under the Participant's Binary sub-directory must conform to the following naming convention that identifies the file's destination:

<To Business Identifier>.<unique name>

The following is a description of each part of the file name:

- *<To Business Identifier>* represents one of the business identifiers associated with the destination Participant.
- *.* is the period character.

- *<unique name>* is any set of valid file name characters, and can contain the '.' (period) character. The unique name ensures that the full file name does not conflict with the names of any other transferred files.

The complete list of valid file name characters is dependent on the FTP server and operating system where the product is installed.

The system does not process Binary files other than ensure that the sending community member has permission (that is, a connection) to send to the destination community member. The system passes the binary file exactly as received to the destination community member.

Setting up FTP

Business Integration Connect is configured to support the ProFTPD server. When you use ProFTPD, Business Integration Connect creates separate FTP user accounts that are only used for Business Integration Connect FTP access. In addition, ProFTPD runs Business Integration Connect's FTP scripts automatically; no manual modifications are required.

Most FTP servers use system accounts as FTP user accounts. If you use an FTP server other than ProFTPD, you are responsible for user account management and you must edit several scripts with a text editor. The scripts create a user by adding a line to the password file, change the password in the password file, and modify the FTP directory to say active or inactive.

There may be other FTP servers that are similar to ProFTPD. If you use a different FTP server to run the Business Integration Connect scripts, unmodified or with limited modifications, the FTP server must support a separate password file. If not, you must modify the scripts and the FTP server to make it work.

Using the same user for FTP and Business Integration Connect eliminates permission issues.

Perl is required for ProFTPD support in the console. Perl is installed by default on Linux. Before setting up FTP, verify that Perl, preferably 5.6, is installed on the systems running the console.

Setting up FTP using the ProFTPD server

Business Integration Connect is configured to use the ProFTPD server. If you use a different FTP server, see [“Setting up FTP using the ProFTPD server” on page 33](#).

Business Integration Connect automates user creation for ProFTPD. Rather than using system accounts for FTP user logins, ProFTPD creates separate user accounts.

Setting up FTP using the ProFTPD server is a two-part process:

1. Download and install ProFTPD server. The product can be installed in any directory, as long as the directory allows Business Integration Connect read-write permissions, and the configuration points to the shared directory, \$SHARED_STORAGE.

The following URL at LinuxQuestions.org explains how to install ProFTPD for Linux:

<http://www.linuxquestions.org/questions/answers.php?action=viewarticle&artid=17>

2. Edit the *ServerAdmin*, *AuthUserFile*, *Include \$SHARED_STORAGE/ftp/ftp.ipac1*, *user*, *group*, *DirFakeUser*, and *DirFakeGroup* values in the proFTPD configuration file, *proftpd.conf*:
 - ***ServerAdmin***. Replace email@mycompany.com with your e-mail address.
 - ***AuthUserFile***. Point this value to \$SHARED_STORAGE/ftp/conf/ftp.passwd.
 - ***Include \$SHARED_STORAGE/ftp/conf/ftp.ipac1***. Include file for IP filtering. See ProFTPD documentation for file format.
 - ***user***. Set to the user that Business Integration Connect runs as.
 - ***group***. Set to the group that Business Integration Connect runs as.
 - ***DirFakeUser***. Use the follow setting to enable globally:
DirFakeUser on ~
 - ***DirFakeGroup***. Use the following setting to enable globally:
DirFakeGroup on ~
3. Disable any other authentication method such as PAM Authentication (this is set as the default in the ProFTPD configuration file).
4. Set up the FTP target directory on the Targets screen, identifying FTP as the transport mode. For more information, see the IBM WebSphere Business Integration Connect [Administrator Guide](#).

Guidelines for using different FTP servers

If you do not use ProFTPD, you must assume user management for your FTP server. This requires that you either modify the Business Integration Connect scripts, or edit the scripts manually. Business Integration Connect scripts modify the FTP server's configuration. The values that you must edit are the user name and password. When a user requests FTP server access, you will give them a normal system account.

If you want to use the Community Console's FTP feature, you must modify the scripts to suit your FTP server.

Your FTP server can be installed in any directory, as long as the directory allows Business Integration Connect read-write permissions, and the configuration points to the shared directory.

Business Integration Connect FTP scripts, their functions, and values you must edit

FTP values are stored in your FTP server's configuration file.

Business Integration Connect FTP scripts are located in the `../common/ftp/bin/` directory.

The following table describes the purpose of each script. You can modify your scripts (recommended) or manually edit your FTP password file. Your FTP password file is identified in your FTP configuration file.

Table 2-6. FTP scripts and their functions

| Script | Function |
|-----------------------------|---|
| con_createFtpAcct.pl | Creates an FTP account by adding a line to the FTP password file. See the text that follows this table for an example of an FTP password file. |
| con_createFtpDirectories.pl | Creates the FTP account directories on the shared storage location. If you are a non-ProFTPD user, your FTP server installer created your FTP account directory. |
| con_disableFtpAcct.pl | Disables the account by modifying the FTP password file entry for an account. |
| con_enableFtpAcct.pl | Enables the account by modifying the FTP password file entry for the account. |
| con_modifyFtpAcct.pl | Changes the account's password of an existing account. |

The following are sample entries in an FTP password file.

```
Username1:2ES.ehig1fRHqvc:2002:100::/opt/IBM/WBIC/shared/vms/receiver/ftp/use
rname1:/bin/bash
```

```
Username2:979HSRGpv1WI6:2003:100::/opt/IBM/WBIC/shared/vms/receiver/ftp/use
rname2:/bin/bash
```

The following is a description of the fields in these entries:

Table 2-7. Description of fields in FTP password file

| Field | Description |
|---------|------------------------|
| Field 1 | The account login |
| Field 2 | Encrypted password |
| Field 3 | User ID |
| Field 4 | Group ID |
| Field 5 | Not Used |
| Field 6 | Account home directory |
| Field 7 | shell - not used |


Creating your FTP account

To create your FTP account:

1. Click **Account Admin** on the main menu.
2. Click **Profiles** on the horizontal menu bar.
3. Click **FTP**. The system advises you that your FTP is not configured.
4. Click **Create New Account**.
5. Select **Enabled** for Account Status.
6. Enter a password. This is the password you use to log in to your FTP server. (The FTP login name is your Participant login name.) Note that this password is different from the password used to log in to the console. When you enter your password, your FTP server's password policy is enforced.
7. Re-enter the password.
8. Click **Save**.

Changing FTP password or account status for ProFTPD users

To change the password of your FTP configuration:

1. Click **Account Admin** on the main menu.
2. Click **Profiles** on the horizontal menu bar.
3. Click **FTP**. The system displays your FTP profile on the FTP Configuration screen.
4. Click  to edit FTP details. The system displays an editable version of your FTP profile.
5. Change your account status, if desired.
6. Change your password, if desired. This is the password you use to log in to your FTP server. (The FTP login name is your Participant login name.) Note that this password is different from the password used to log in to the console. When you change your password, your FTP server's password policy is enforced.
7. If you changed your password, re-enter the new password.
8. Click **Save**.

Managing B2B capabilities

NOTE: In smaller installations, this process might be performed by the Hub Admin.

Use this feature to view and edit predefined hub-wide B2B capabilities, and to enable additional local B2B capabilities, if required.

A B2B capability identifies a specific type of business process that can be exchanged between you and other community members. B2B or document processing capabilities are defined using document flow definitions. A document flow definition gives the system all of the necessary information to receive, process, and route documents between community members.

Each capability consists of up to five different document flow definitions:

Package. Describes document format, packaging, encryption, and content-type identification.

Protocol. Identifies structure and location of information in the document. The system needs this information to process and route the document.


Document flow. Identifies the business process that will be processed between the Community Manager and its Participants.

Activity. The business function the process performs.

Action. The individual documents that make up a complete business process. The documents are processed between the Community Manager and Participant.

Each document flow definition contains attributes (that is, information) that define the definition's functionality. An attribute is a piece of information that is associated with a specific document flow. The system uses this information for various functions such as validating the documents or checking for encryption.

To review and edit your system B2B capabilities:

1. Click **Account Admin** on the main menu.
2. Click **Profiles** on the horizontal navigation bar.
3. Click **B2B Capabilities**. The system displays the B2B Capabilities screen.
 - If a folder appears next to a package and Enabled appears in the Enabled column, the Hub Admin has enabled this capability for you.
 - A check mark below Set Source or Set Target tells you that you can use this capability in that role (that is, as the source, target, or both).
 - The  icon tells you that you are not enabled as a source or target.
 - The Enabled column displays the status of the package: Enabled or Disabled.

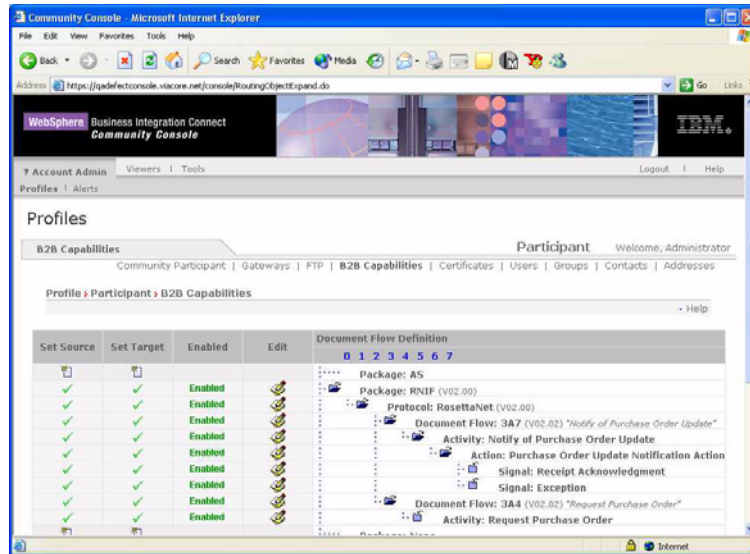



Figure 2-5. B2B Capabilities

4. Click **Enabled** to enable a capability, then click the folder. All lower levels are automatically activated.
5. Set your capability to initiate (**Set Source**), receive (**Set Target**), or initiate and receive the document flow context. In a 2-way PIP, Set Source and Set Target are the same for all actions, regardless of the fact that the request originates from one Participant and the corresponding confirmation originates from another.
6. Click  to view and, if desired, change lower level document flow definitions (for example Protocol or Document Flow). You can also change a document flow definition's attributes (for example, Time to Perform or Retry Count). When you use this screen for the first time, attributes are set at the global level. However, you can reset them at the local level, if desired. Setting an attribute at the local level overrides the global setting in your environment, but it does not change the global setting.

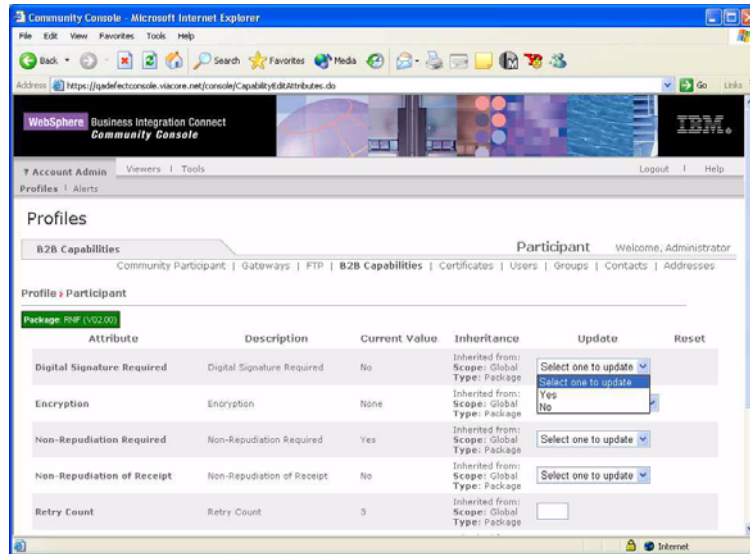


Figure 2-6. Editing B2B Capabilities

- If you make a change at any level, it is propagated to all lower levels.
- You can select and edit an individual folder below a package, if desired. A change made in this manner is not propagated to lower levels.
- You can override the built-in “select all” option by deselecting from the bottom up.
- Signals, for example, receipt acknowledgements, are specific to RosettaNet. There are three signals under each action: Receipt Acknowledge, General Exception, and Receipt Acknowledgement Exception. You can set attributes for signals.
- Set the capability to initiate (Set Source), receive (Set Target), or initiate and receive for each lower level document flow definition.

If you changed an attribute, click **Save**.

Managing certificates

Digital certificates are used to verify the authenticity of business document transactions between the Community Manager and Participants. They are also used for encryption and decryption. Use this screen to edit existing and add new digital certificates to Business Integration Connect.

After you upload your certificates, they are viewable from the console.

You can create certificate expiration alerts that will notify you when a certificate is about to expire. For more information, see [“Managing alerts” on page 67](#). Expired certificates are saved in the IBM WebSphere Business Integration Connect database; they cannot be deleted from the system.

Certificate terms

Certificate authority (CA). An authority that issues and manages security credentials and public keys for message encryption. When an individual or company requests a digital certificate, a CA checks with a registration authority (RA) to verify information given to them by the individual or company. If the RA verifies the submitted information, the CA issues a certificate.

Examples of a CA include VeriSign and Thawte.

Digital certificate. A digital certificate is the electronic version of an ID card. It establishes your identity when you perform B2B transactions over the Internet. Digital certificates are obtained from a Certificate Authority (CA) and consist of three things:

- The public-key portion of your public and private key pair.
- Information that identifies you.
- The digital signature of a trusted entity (CA) attesting to the validity of the certificate.

Digital signature. A digital code created with a private key. Digital signatures allow members of the hub-community to authenticate transmissions through signature verification. When you sign a file, a digital code is created that is unique to both the contents of the file and your private key. Your public key is used to verify your signature.

Encryption. A method of scrambling information to render it unreadable to anyone except the intended recipient, who must decrypt the information to read it.

Decryption. A method of unscrambling encrypted information so that it becomes legible again. The recipient's private key is used for decryption.

Key. A digital code used to encrypt, sign, decrypt, and verify files. Keys come in key pairs, a private key and a public key.

Non-repudiation. To prevent the denial of previous commitments or actions. For B2B electronic transactions, digital signatures are used to validate the sender and time stamp the transaction. This prevents the parties involved from claiming that the transaction was not authorized or not valid.

Private key. The secret portion of a key pair. This key is used to sign and decrypt information. Only you have access to your private key. Your private key is also used to generate a unique digital signature based on the contents of the document.

Public key. The public portion of a key pair. This key is used to encrypt information and verify signatures. A public key can be distributed to other members of the hub-community. Knowing a person's public key does not help anyone discover the corresponding private key.

Self-signed key. A public key that has been signed by the corresponding private key for proof of ownership.

X.509 certificate. A digital certificate used to prove identity and public key ownership over a communication network. It contains the issuer's name (that is, the CA), the user's identifying information, and the issuer's digital signature.

Your certificate identifies your organization and the time period that the certificate is valid.

Description

Digital certificates help companies identify themselves when they conduct business over the Internet. They are used the same way an I.D. card or driver's license is used. When Company A presents their certificate to Company B, the certificate verifies Company A's identity.

The following is a simplified example of how digital certificates are issued and used.

Company A and Company B want to conduct business transactions with each other over the Internet. Company B, who has a digital certificate and key pair (public and private keys), requests a copy of Company A's certificate and public key.

Company A, who does not have a digital certificate, contacts a Certificate Authority (CA) and requests a digital certificate. The CA verifies Company A's identity and issues the company a digital certificate. The certificate includes a key pair (public and private keys), the digital signature of the CA, and information that identifies Company A (the company's name and digital signature). The certificate also includes a serial number and expiration date.

Company A and Company B exchange digital certificates and public keys. Both parties now trust each other and are willing to conduct Internet transactions with each other.

The different types of digital certificates are described in the following section.

Certificate types and supported formats

All certificates must be in either DER in binary form, or in ASCII Privacy Enhanced Mail (PEM) format. The certificates can be converted from one format to another.

There are several types of certificates:

- **SSL Client certificate (Participants and Community Manager).** A transport certificate. If your outbound transport is HTTPS, you will need an SSL Client certificate. In most cases the SSL Client certificate must be signed by a CA. If the certificate is used in a test environment, it can be self-signed.

You must upload the certificate to Business Integration Connect through the console and send a copy of the certificate to the Hub Operator.

- **Encryption certificate (Participants and Community Manager).** If hub-community members will encrypt files, you will need an encryption-decryption certificate.

You must upload the certificate to Business Integration Connect through the console and send a copy of the certificate to the Hub Operator.

- **Digital signature certificate (Participants and Community Manager).** If you are digitally signing or verifying digitally signed documents, you will need a digital signature certificate in DER format. In most cases this certificate must be signed by a CA. If the certificate is used in a test environment, it can be self-signed.

You must upload the certificate to Business Integration Connect through the console and send a copy of the certificate to the Hub Operator.

- **VTP certificate (Community Manager).** This certificate is used by Business Integration Connect's Document Manager for the Community Participant Simulator feature. For more information, see ["Preparing for the test process" on page 115](#). This certificate is copied to the file system rather than uploaded through the console.

VTP certificates copied to the file system are active for all Participants created through the console. They are used to validate signed documents received from the Community Participant Simulator. Additionally, certificates copied to the file system are not viewable through the console.

Client authentication

If client authentication is not required, the following must occur:

- If the hub-community web server's certificate is a self-signed certificate, Participant's must have a copy of that certificate.
- If the hub-community web server's certificate is from a Certificate Authority, the Participants must have a copy of the CA root certificate.

If client authentication is required, the following must occur:

- If the hub-community web server's certificate is a self-signed certificate, Participant's must have a copy of that certificate.
- If the hub-community web server's certificate is from a Certificate Authority, the Participants must have a copy of the CA root certificate.
- The target server must have a copy of the Participant's certificate if it is self-signed and loaded in the trust keystore.
- The target server must have a copy of the certificate authorities certificate if the certificate is authenticated from a CA and loaded in the trust keystore.

Performing certificate tasks

Table 2-8. Certificate tasks

| What do you want to do? | See |
|--|-------------------------|
| View a list of digital certificates. | page 43 |
| View and edit digital certificate details. | page 43 |
| Upload and define a digital certificate. | page 44 |
| Disabling a digital certificate. | page 45 |

Viewing a list of digital certificates

To view a list of digital certificates:

1. Click **Account Admin** on the main menu.
2. Click **Certificates**. The system displays a list of existing digital certificates.



NOTE: If a certificate has expired, the certificate's dates are displayed in red.

Table 2-9. Values on the Certificate List screen

| Value | Description |
|--------------|---|
| Description | Unique name of certificate. |
| SSL | A check mark appears if this is an SSL certificate. |
| DigS | A check mark appears if this is a digital signature certificate. |
| Encry | A check mark appears if this is an encryption certificate. |
| Status | Enabled or disabled. |
| Gateway Type | Used with SSL certificates only. Identifies the destination that the certificate is used for. |
| Valid | Time period for which the certificate is valid. |

Viewing and editing digital certificate details

To view and edit digital certificate details:

1. Click **Account Admin** on the main menu.
2. Click **Certificates**. The system displays a list of existing digital certificates.
3. Click  to view certificate details. The system displays the Certificate Details screen.
4. Click  to edit the certificate. Participants can edit everything in their profile except Participant Name (for login) and Participant Type.
5. Edit as required.
6. Click **Save**.

Uploading and defining a digital certificate

To upload and define a digital certificate:

1. Click **Account Admin** on the main menu.
2. Click **Profiles** on the horizontal navigation bar.
3. Click **Certificates**. The system displays the Certificate List screen.
4. Click **Create** on the sub-menu. The system displays the Create New Certificate screen.

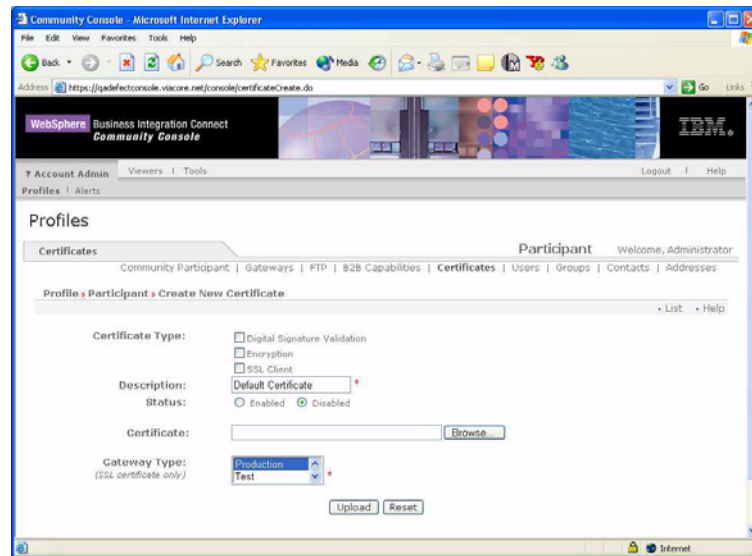




Figure 2-7. Create New Certificate

5. Select the Certificate Type: Digital Signature Validation, Encryption, or SSL Client. You can upload multiple digital signature and SSL certificates. However, you can only upload one encryption certificate.
 - **Digital signature certificate.** If you are digitally signing or verifying digitally signed documents, you will need a digital signature certificate.
 - **Encryption certificate.** If hub-community members will encrypt files, you will need an encryption-decryption certificate.
 - **SSL Client certificate.** A transport certificate. If your outbound transport is HTTPS, you will need an SSL Client certificate.
6. Enter a unique name (Description) for the certificate in the Certificate Name text box.
7. Select Enabled or Disabled.
8. Click **Browse** and navigate to the digital certificate.
9. Select the Gateway Type, for example, CPS Participant (SSL certificates only). This feature allows you to select a certificate based on destination.
10. Click **Upload**.

Disabling a digital certificate

To disable a digital certificate:

1. Click **Account Admin** on the main menu.
2. Click **Certificates**. The system displays a list of existing digital certificates.
3. Click  to view certificate details. The system displays the Certificate Details screen.
4. Click  to edit the certificate.
5. Click **Disabled**.
6. Click **Save**.

Managing users

Use this feature to create, view, and edit user profiles. The system uses user profiles to control console access, alert delivery, and user visibility.

A user profile includes the user's name and contact information (e-mail address and telephone numbers), login status (Enabled or Disabled), as well as the user's alert status (Enabled or Disabled), and visibility (Local or Global).

- If a user's login status is Enabled, the user can log in to the Community Console. If a user's login status is Disabled, the user cannot log in to the Community Console.
- If a user's alert status is Enabled, the user can receive alert notifications. If a user's alert status is Disabled, the user cannot receive alert notifications.
- If the user's visibility is Local, the user is only visible to your organization. If a user's visibility is Global, the user is visible to the entire hub-community.

You can also auto-generate a password for a user.

Performing user tasks

Table 2-10. User tasks

| What do you want to do? | See |
|----------------------------|-------------------------|
| View or edit user details. | page 46 |
| Assign users to groups. | page 49 |
| Create a new user. | page 49 |

Viewing or editing user details

NOTE: You can use this feature to assign or auto-generate a new password for a user.

To view or edit user details:

1. Click **Account Admin** on the main menu.
2. Click **Profiles** on the horizontal navigation bar.
3. Click **Users**. The system displays the User List screen.

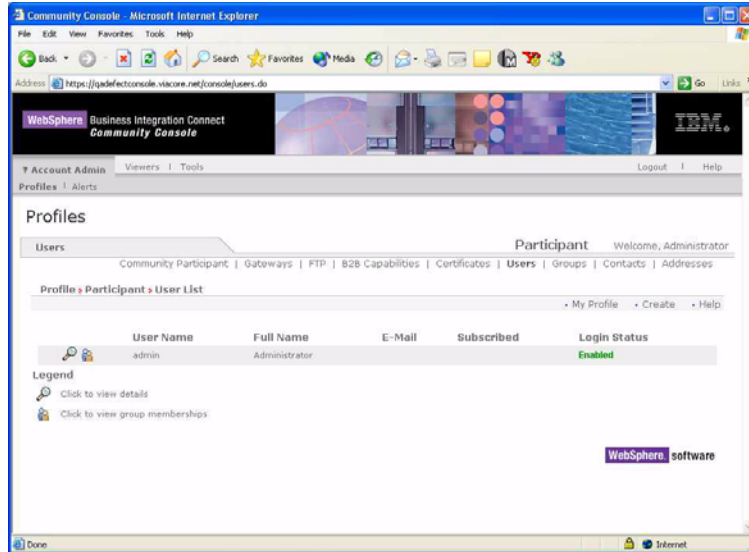




Figure 2-8. User List

The following table describes the values on the User List screen.

Table 2-11. Values on User List screen

| Value | Description |
|--------------|--|
| User Name | Console login name. |
| Full Name | Full name of user. |
| E-Mail | E-mail address used for alert notification. |
| Subscribed | If this option is checked, one or more alerts are assigned to the user. If the user is removed from the system, all alert subscriptions to this user are also removed. |
| Login Status | Enabled status allows the user to log in to the console. |

4. Click  to view a user's details.
5. Click  to edit a user's details.

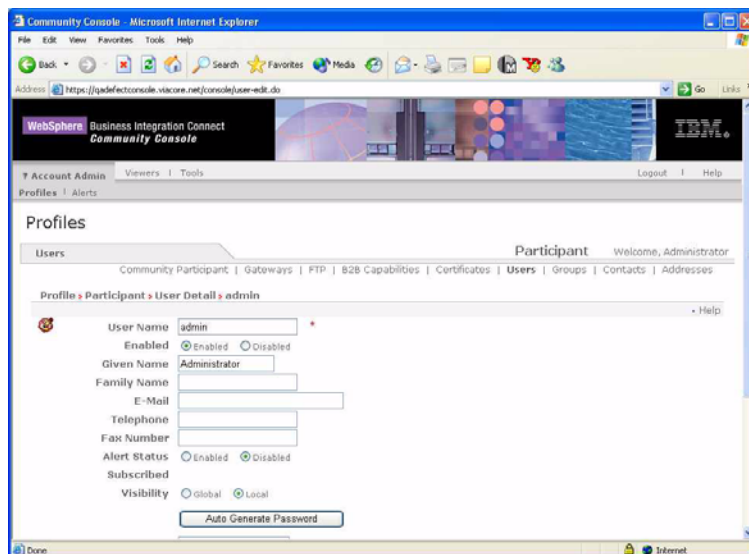


Figure 2-9. User Details (Edit)

6. Edit information as required. The following table describes the values on the User Details screen.



Table 2-12. User details

| Value | Description |
|------------------------|---|
| User Name | Login name for console user. |
| Enabled | Enable or Disable console access. |
| Given Name | First Name of user. |
| Family Name | Last name of user. |
| E-mail | E-mail address used for alert notification. |
| Telephone | Telephone number of user. |
| Fax Number | Fax number of user. |
| Alert Status | When this option is Enabled, this user receives all subscribed alerts. Select Disabled to stop this user from receiving all alerts. |
| Subscribed | This value is system populated. |
| Visibility | <ul style="list-style-type: none"> Local. User is only visible to your organization. Global. User is visible to the entire hub-community. |
| Auto-Generate Password | Automatically generates a password for the user. |
| Password | Manually password entry. |
| Re-enter Password | Second entry of manual password. |

7. Click **Save**.

Assigning users to groups

To assign users to groups:

1. Click **Account Admin** on the main menu.
2. Click **Profiles** on the horizontal navigation bar.
3. Click **Users**. The system displays the User List screen.
4. Click  to view the target user's group membership details.
5. Click  to edit the user's group memberships.

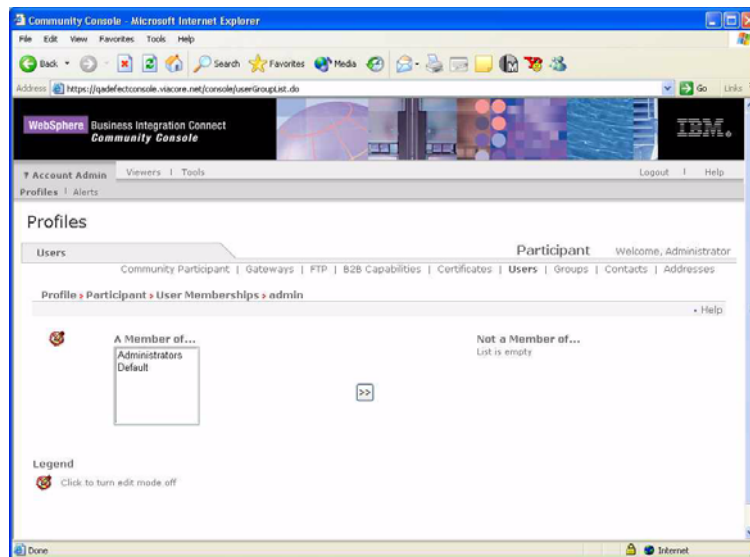



Figure 2-10. User Memberships (Edit)

6. Select a group and use arrow keys to assign a user to or remove a user from a group.
7. Click  when you finish editing.

Creating a new user

Use this feature to add a new user. After you define your users and groups, you can add users to groups.

To create a new user:

1. Click **Account Admin** on the main menu.
2. Click **Profiles** on the horizontal navigation bar.
3. Click **Users**. The system displays the User List.
4. Click **Create** in the sub-menu. The system displays the User Detail screen.

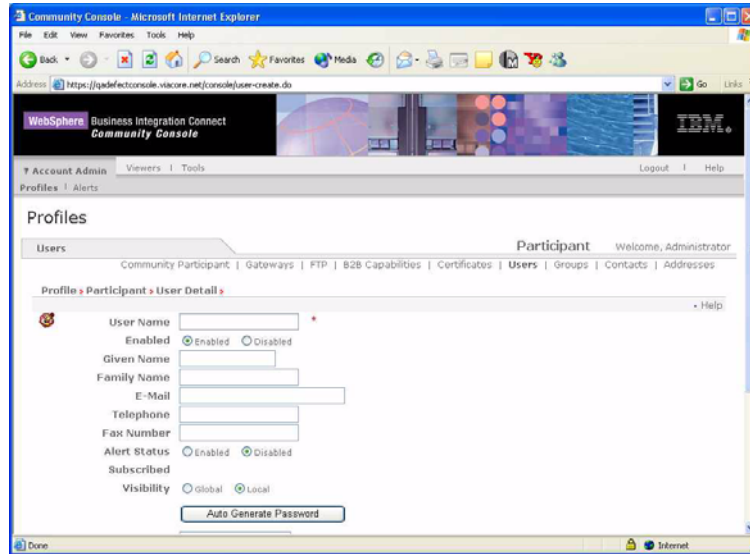


Figure 2-11. User Detail (Create)

5. Enter the user name (login name for the user).
6. Select if you want to Enable or Disable console access for this user.
7. Enter the user's name (Given Name and Family Name.)
8. Enter the e-mail address that the system will use to send alert notifications to the user.
9. Enter the user's telephone and fax numbers.
10. Select if you want to Enable or Disable alert notification for this user. When enabled, the user receives all subscribed alerts. When disabled, the users does not receive alerts.

NOTE: The Subscribed value is system populated.

11. Select if the user is only visible to your organization (Local), or visible to the entire hub-community (Global).
12. Click **Auto Generate Password** to generate a password automatically. If you choose to select a password for this user, enter the password in the Password and Re-enter Password text boxes.
13. Click **Save**. Repeat these steps to add additional users.

Managing groups

Use the Group feature to perform the following tasks:

- Create groups.
- Assign console permissions to the group.
- Assign users to groups.

Use this feature to create a group for a specific type of user, with specific console privileges. For example, you might want to create a group Testers for users who are assigned to test connectivity during the testing cycle. After you create group Testers, you would assign permissions to the group based on the console features the group’s users must have access to during the testing cycle. The third step of the process is to assign users to the Testers group.

- Permissions are assigned to groups.
- Users are members of one or more groups.

The system automatically creates the Administrator and Default groups with the following default permission settings:

Table 2-13. Administrator and default groups default permission settings

| Group | Default Permission Settings |
|---------------|--|
| Administrator | Read-write for all Community Console modules |
| Default | Read only for all Community Console modules |

Default permission settings can be overridden by the Hub Admin and Participant Admin.

RESTRICTIONS: Administrator and Default groups are system generated and cannot be edited or deleted. The Community Operator has an additional group, Hub Admin.

Performing group tasks

Table 2-14. Group tasks

| What do you want to do? | See |
|--|-------------------------|
| View group memberships and assign users to groups. | page 52 |
| View, edit, or assign group permissions. | page 53 |
| View or edit group details. | page 53 |
| Create a new group. | page 54 |
| Delete a group. | page 55 |

Viewing group memberships and assigning users to groups

To view group memberships or assign users to groups:

1. Click **Account Admin** on the main menu.
2. Click **Profiles** on the horizontal navigation bar.
3. Click **Groups**. The system displays the Group List screen.

Table 2-15. Values on the Group List screen

| Value | Description |
|-------------|---------------------------|
| Name | Group name. |
| Description | Description of group. |
| Group Type | Type, for example System. |

4. Click  to view a list of users in a group. If this icon does not appear, there are no members in the group. Click Memberships in the sub-menu.

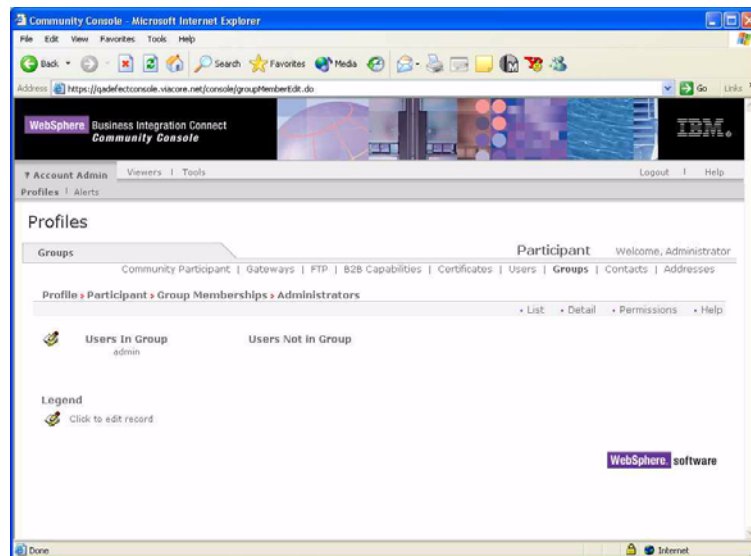





Figure 2-12. Group Memberships (Edit)

5. Click  to edit users in a group.
6. Use arrow keys to assign users to the group.
7. Click  to save and exit.

Viewing, editing, or assigning group permissions

To view, edit, or assign group permissions:

1. Click **Account Admin** on the main menu.
2. Click **Profiles** on the horizontal navigation bar.
3. Click **Groups**. The system displays the Group List screen.
4. Click  to view a group's permissions. The system displays a list of the selected group's permissions.

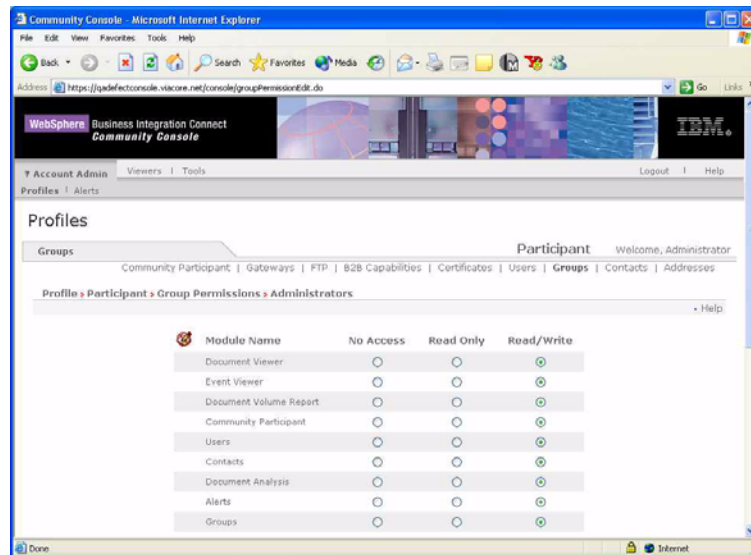




Figure 2-13. Group Permissions (Edit)

5. Select **No Access**, **Read Only**, or **Read/Write** for each feature.
6. Click **Save**.

Viewing or editing group details

To view or edit group details:

1. Click **Account Admin** on the main menu.
2. Click **Profiles** on the horizontal navigation bar.
3. Click **Groups**. The system displays the Group List screen.
4. Click  to view group details (Name and Description). The system displays the Group Detail screen.
5. Click  to edit group details (you cannot edit system generated groups).
6. Edit as required.
7. Click **Save**.

RESTRICTIONS: Administrator and Default groups are system generated and cannot be edited or deleted. The Community Operator has an additional group, Hub Admin.

Creating a new group

To create a new group:

1. Click **Account Admin** on the main menu.
2. Click **Profiles** on the horizontal navigation bar.
3. Click **Groups**. The system displays the Group List screen.
4. Click **Create** on the sub-menu. The system displays the Group Detail screen.

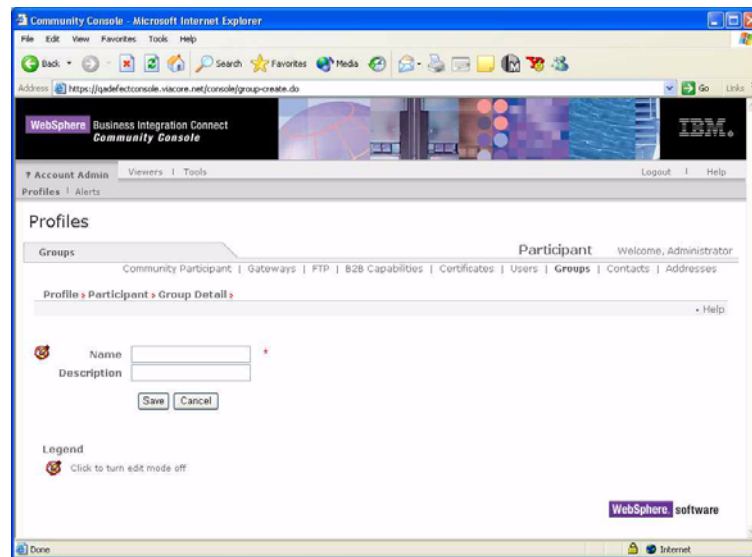




Figure 2-14. Group Detail (Create)

5. Enter the new group's **Name** and **Description**.
6. Click **Save**. To add additional groups, repeat these steps.

Deleting a group

To delete a group:

1. Click **Account Admin** on the main menu.
2. Click **Profiles** on the horizontal navigation bar.
3. Click **Groups**. The system displays the Group List screen.
4. Click  to view group details. The system displays the Group Details screen.
5. Click  to edit group details.
6. Click **Delete**. Confirm that you want to delete.

RESTRICTIONS: Administrator and Default groups are system generated and cannot be edited or deleted.

Managing contacts

Use the Contacts feature to create contact information for key personnel. You will use this contact information to identify who should receive notification when events occur and the system generates alert notifications.

Depending on the size of your organization, you will probably want to notify different contacts when different types of events occur. For example, when a document fails validation, security personnel should be notified so that they can evaluate the problem. When the Community Manager's transmissions exceed normal boundaries, your network administrator should be notified to ensure that the system is handling the increase in transmissions efficiently.

After you create your contacts, you will return to the Alert feature to link the appropriate contacts to each alert that you created.

Performing contact tasks

Table 2-16. Contact tasks

| What do you want to do? | See |
|-------------------------------|-------------------------|
| View or edit contact details. | page 56 |
| Add a contact to an alert. | page 58 |
| Create a new contact. | page 62 |
| Remove a contact. | page 63 |

Viewing or editing contact details

To view or edit contact details:


1. Click **Account Admin** on the main menu.
2. Click **Profiles** on the horizontal navigation bar.
3. Click **Contacts**. The system displays a list of current contacts.

The following table identifies the values that appear on the Contacts screen.

Table 2-17. Values on Contact List screen

| Value | Description |
|--------------|--|
| Full Name | Full name of contact. |
| Contact Type | Describes the role of the contact, for example, B2B Lead or Business Lead. |
| E-Mail | E-mail address used for alert notification. |

Table 2-17. Values on Contact List screen

| Value | Description |
|--------------|---|
| Visibility | <ul style="list-style-type: none">Local - Contact is only visible to your organization.Global - Contact is visible to the Community Operator and Community Manager. Both of these parties can subscribe the contact to alerts. |
| Subscribed | If this option is selected, one or more alerts are assigned to this contact. If the contact is removed from the system, all alert subscriptions to this contact are removed from the system. |
| Alert Status | When the Alert Status is enabled, this contact receives all subscribed alerts. |
| Delete | Click  to delete appropriate contact. |



- Click  to view contact details. The system displays the Contact Detail screen.
- Click  to edit contact details.
- Edit information as required. The following table describes contact values.

Table 2-18. Contact details

| Value | Description |
|--------------|---|
| Given Name | Contact's first name. |
| Family Name | Contact's last name. |
| Address | Contact's address, include street, city, state, and postal code. |
| Contact Type | Describes the role of the contact, for example, B2B Lead or Business Lead. |
| E-mail | Contact's e-mail address for alert notification. |
| Telephone | Contact's telephone number. |
| Fax Number | Contact's fax number. |
| Alert Status | When this option is enabled, this contact receives all subscribed alerts. Select Disable to stop this contact from receiving all alerts. |
| Subscribed | This value is system populated. |
| Visibility | <ul style="list-style-type: none">Local - Contact is only visible to your organization.Global - Contact is visible to the Community Operator and Community Manager. Both of these parties can subscribe the contact to alerts. |

- Click **Save**.

Adding a contact to an alert

To add a contact to an alert:

1. Click **Account Admin** on the main menu.
2. Click **Alerts** on the horizontal navigation bar. The system displays the Alert Search screen.

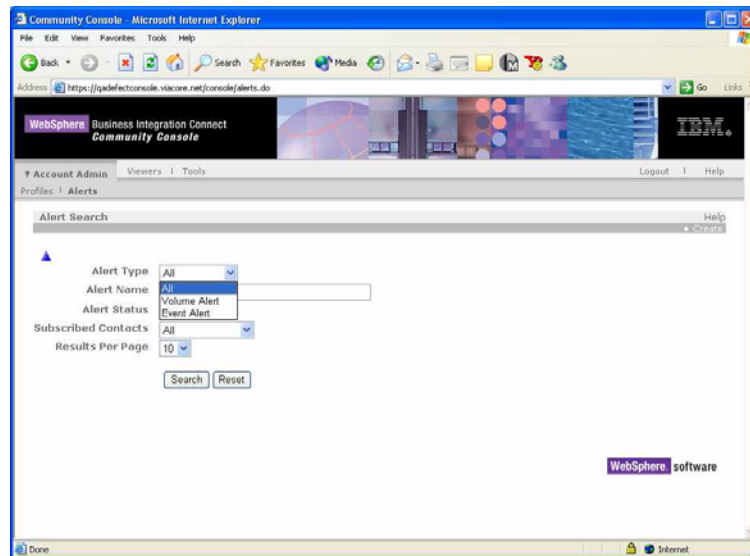


Figure 2-15. Alert Search

3. Enter the Alert Name. If you do not know the Alert Name, select search criteria from the drop-down lists.
4. Click **Search**. The system displays the Alert Search Results screen with a list of alerts that meet your search criteria.

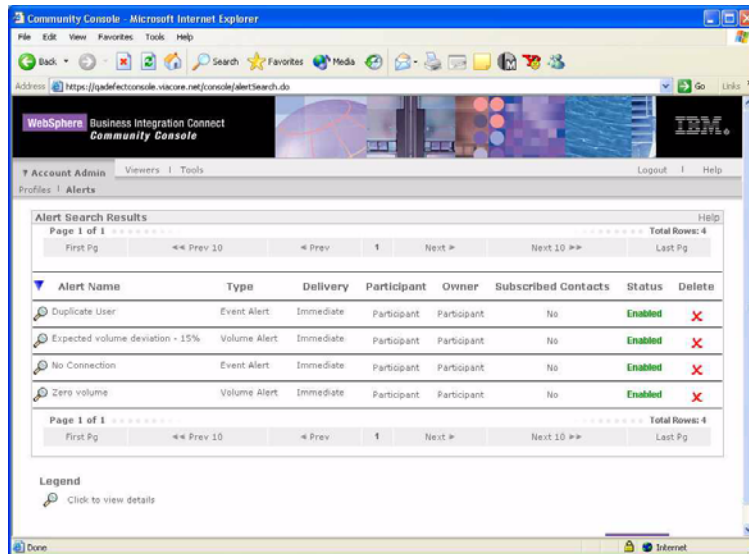


Figure 2-16. Alert Search Results

5. Locate the alert and click to view the target alert's details. The system displays the Alert: Events or Alert: Volume screen.
6. Click to edit alert details.

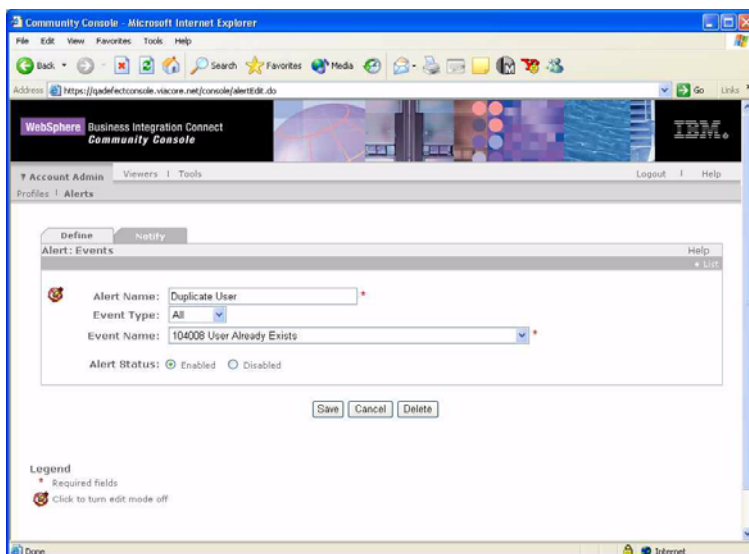


Figure 2-17. Alert: Events (Edit)

7. Click the **Notify** tab. The system displays the Notify for Alerts screen.

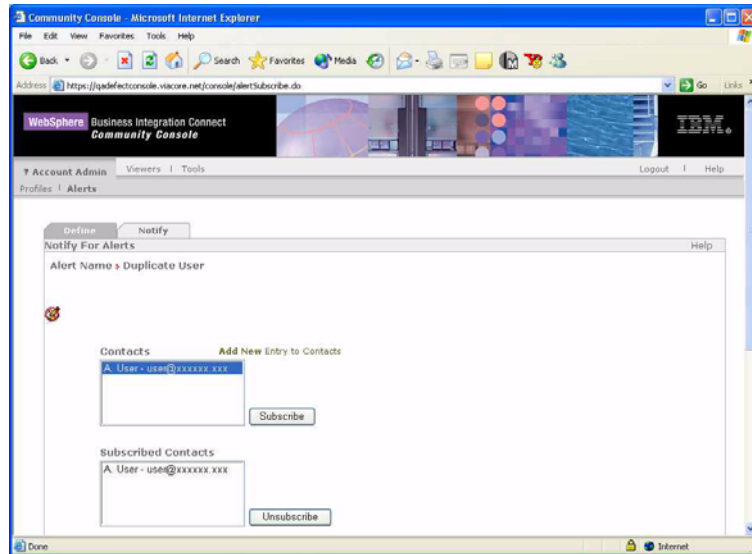


Figure 2-18. Notify for Alerts (Edit)

8. Select the contact in the Contacts box and click **Subscribe**. The system displays the contact's name in the Subscribed Contacts box. If you are adding the contact to a volume alert, skip the next step.

9. Select the Mode of Delivery (does not apply to volume alerts):

- **Send alerts immediately.** When you select this option, the system sends alert notifications to the contact when the alert occurs. Use this option for critical alerts.
- **Batch Alerts By.** When you select this option, you can specify when you want the contact to receive alert notifications. Use this option for non-critical alerts.

The two options in this section, Count and Time, are not mutually exclusive.

If you select the Count option, you must always select the Time option.

- If the number of alerts (Count) is reached during the time limit that you have selected (Time), the system generates an alert notification.
- If an alert occurs but the number of alerts (Count) is not reached during the time limit that you have selected (Time), the system will generate an alert notification at the end of the time limit.

The Time option can be used without the Count option, but the Count option must always be associated with a time limit (Time).

- **Count.** Must also use Time option when you select this option. Enter a number (n). This is the number of alerts that must occur during the selected time period (Time) before the system will send an alert notification to the alert's contact.

Here's an example of how these two options work together:

In our example, Batch Alerts By options are set to 10 for Count (10 alerts) and 2 for Time (2 hour period). The system retains all notifications for this alert until 10 occur in a two hour period or until the end of the time period is reached.

When the alert count reaches 10 in a 2 hour period, the system sends all alert notifications for this alert to the contact.

If an alert occurs but 10 alerts do not occur during the time limit (two hours), the system will send an alert notification to the alert's contact at the end of the time limit.

- **Time.** Select number of hours (n). The system retains alert notification for n hours. Every n hours, the system sends all retained alert notifications to the contact.

For example, if you enter 2, the system retains all notifications for this alert that occur in each two hour interval. When the two hour interval expires, the system sends all alert notifications for this alert to the contact.

10. Click **Save** to save the contact. Click **Save and Subscribe** to save the contact and add the contact to the list of contacts for this alert.

11. Click **Save** to save the alert.

Creating a new contact

To create a new contact:

1. Click **Account Admin** on the main menu.
2. Click **Profiles** on the horizontal navigation bar.
3. Click **Contacts**. The system displays a list of current contacts.
4. Click **Create** on the sub-menu. The system displays the Contact Detail screen.

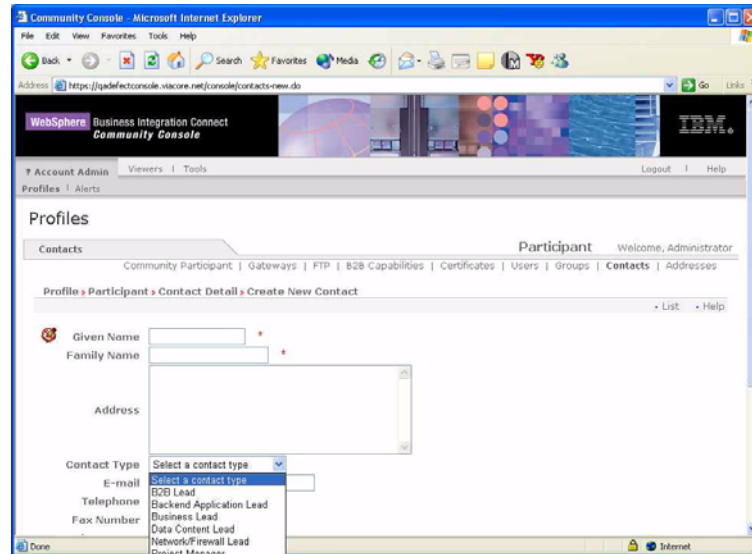


Figure 2-19. Contacts Detail screen (Create)

5. Enter the contact's name in the name text boxes.
6. Enter the contact's address in the address text box.
7. Select the Contact type from the drop-down list (for example, B2B Lead or Business Lead).
8. Enter the contact's e-mail address.
9. Enter the contact's telephone and fax number.
10. Select the contact's alert status. When enabled, this contact receives all subscribed alerts.
11. Subscribed is system populated.
12. Select the contact's visibility level. If you select Local, the contact is only visible to your organization. If you select Global, the contact is visible to the Community Operator and Community Manager. Both of these parties can subscribe the contact to alerts.

13. Click **Save**. There are several ways that you can add the contact to an alert:


To add a contact to an existing alert, see [“Adding a contact to an alert” on page 58](#).

To create a volume-based alert and add contacts to the alert, see [“Creating a volume-based alert and adding contacts” on page 73](#).

To create an event-based alert and add contacts to the alert, see [“Creating an event-based alert and adding contacts” on page 76](#).

Removing a contact

To remove a contact:

1. Click **Account Admin** on the main menu.
2. Click **Profiles** on the horizontal navigation bar.
3. Click **Contacts**. The system displays a list of current contacts.
4. Click  to delete appropriate contact.

Managing addresses

Use this feature to manage the addresses in your Participant profile. The system is configured to support multiple address types for Corporate, Billing, and Technical locations.


Performing address tasks

Table 2-19. Address tasks

| What do you want to do? | See |
|-------------------------|-------------------------|
| Edit an address. | page 64 |
| Create a new address. | page 65 |
| Delete an address. | page 66 |

Editing an address

To edit an address:

1. Click **Account Admin** on the main menu.
2. Click **Profiles** on the horizontal navigation bar.
3. Click **Addresses**. The system displays the Addresses screen.
4. Locate the address that you want to edit, and click .

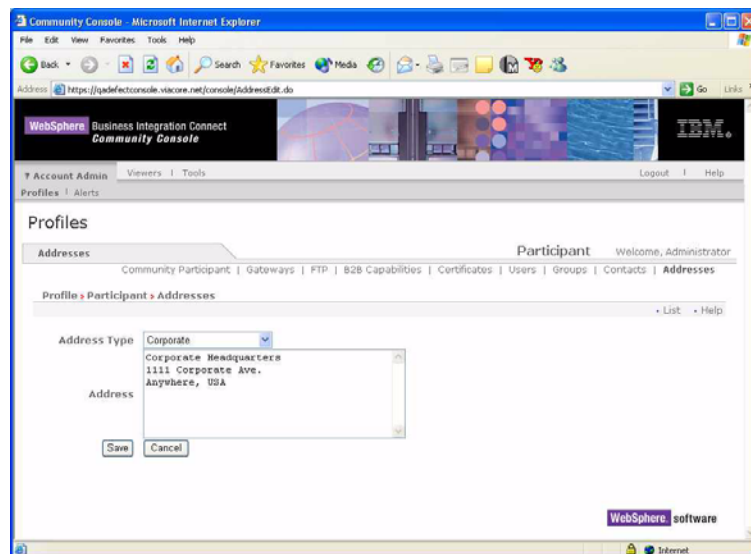


Figure 2-20. Addresses (Edit)

5. Make the required changes. The following table describes the address values.

Table 2-20. Address values

| Value | Description |
|--------------|--|
| Address Type | Corporate, Billing, and Technical |
| Address | Address, including street, city, state, and postal code. |

6. Click **Save**.

Creating a new address

To create a new address:

1. Click **Account Admin** on the main menu.
2. Click **Profiles** on the horizontal navigation bar.
3. Click **Addresses**. The system displays the Addresses screen.
4. Click **Create New Address** on the sub-menu. The system displays the Addresses screen.

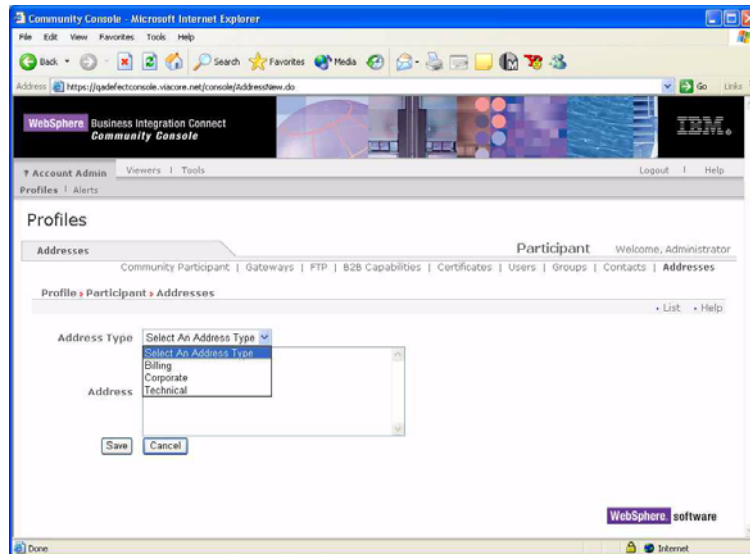


Figure 2-21. Addresses (Create)

5. Select the Address Type from the drop-down list (Billing, Corporate, or Technical).
6. Enter the address in the appropriate text boxes.
7. Click **Save**.

Deleting an address

To delete an address:

1. Click **Account Admin** on the main menu.
2. Click **Profiles** on the horizontal navigation bar.
3. Click **Addresses**. The system displays the Addresses screen.
4. Locate the address that you want to delete and click **X**.
5. Verify that you want to delete the address.

Managing alerts

Delivering information about system problems to the right people at the right time is the key to rapid problem resolution.

Business Integration Connect's alerts are used to notify key personnel of unusual fluctuations in the volume of transmissions you receive, or when business document processing errors occur.

A companion option in the Viewer module, Event Viewer, helps you further identify, troubleshoot, and resolve processing errors.

An alert consists of a text-based e-mail message sent to subscribed contacts or a distribution list of key personnel. Alerts are based on the occurrence of a system event (event-based alert) or expected document flow volume (volume-based alert).

- Use a volume-based alert to receive notification of an increase or decrease in the volume of transmissions.

For example, if you are a Participant, you can create a volume-based alert that notifies you if you do not receive any transmissions from the Community Manager on any business day (set Volume to Zero Volume, set frequency to Daily, and select Mon through Fri in the Days of Week option). This alert can highlight Community Manager network transmission difficulties.

If you are a Participant, you can also create a volume-based alert that warns you when the number of transmissions from the Community Manager exceeds the normal rate. For example, if you normally receive approximately 1000 transmissions a day, you can set the Expected Volume at 1000 and the Percent Deviation at 25%. The alert will notify you when you receive more than 1250 transmissions a day (it will also notify you when the volume of transmissions falls below 750). This alert can identify increased demand on the part of the Community Manager, which might, over time, require you to add more servers to your environment.

Note that volume-based alerts monitor volume with respect to the document flow that you select when you create the alert. Business Integration Connect only looks at documents that contain the document flow selected in your alert, and generates alerts only when all of the alert criteria are met.

- Use an event-based alert to receive notification when errors in document processing occur. For example, you might want to create an alert that notifies you if your documents fail processing due to validation errors or because duplicate documents were received. You can also create alerts that let you know when a certificate is about to expire.

You will use Business Integration Connect predefined event codes to create event-based alerts. There are five event types: Debug, Information, Warning, Error, Critical. Within each event type, there are many events. You can view and select predefined events on the Alert: Events screen. For example, 240601 AS Retry Failure, or 108000 Not a Certificate.

TIP:

- Use a volume-based alert to receive notification if expected Participant or Community Manager transmission volume falls below operating limits. This alert can highlight Participant or Community Manager network transmission difficulties.
 - Use an event-based alert to receive notification of errors in document processing. For example, you can create an event-based alert that notifies you if your documents have failed processing due to validation errors.
-

Performing alert tasks

Table 2-21. Alert tasks

| What do you want to do? | See |
|---|-------------------------|
| View or edit alert details and contacts. | page 68 |
| Searching for alerts. | page 71 |
| Add a new contact to an existing alert. | page 71 |
| Create a volume-based alert and add contacts. | page 73 |
| Create an event-based alert and add contacts. | page 76 |
| Disable or enable an alert. | page 80 |
| Remove an alert. | page 80 |

Viewing or editing alert details and contacts

The Community Manager can view all alerts, regardless of the Alert Owner (the creator of the alert).

To view or edit alert details and contact information:

1. Click **Account Admin** on the main menu.
2. Click **Alerts** on the horizontal navigation bar. The system displays the Alert Search screen.

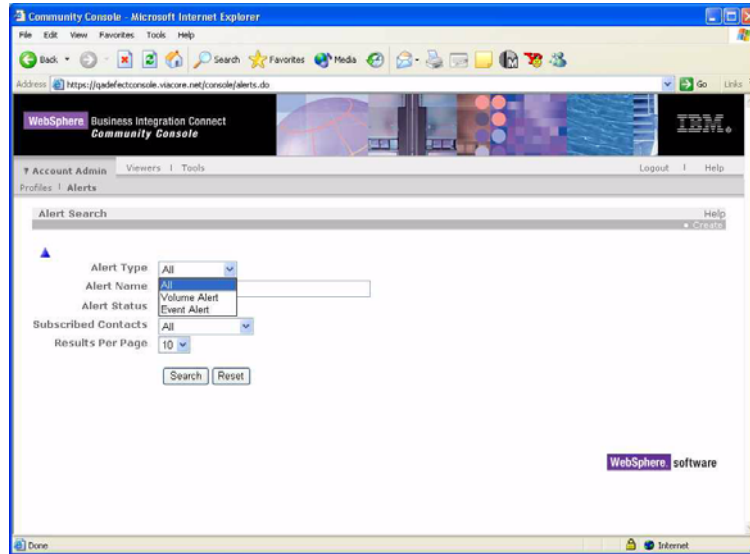


Figure 2-22. Alert Search

3. Select the search criteria from the drop-down lists; enter the Alert Name. You can also click **Search** without selecting any search criteria (the system displays all alerts).
4. Click **Search**. The system displays the Alert Search Results screen.

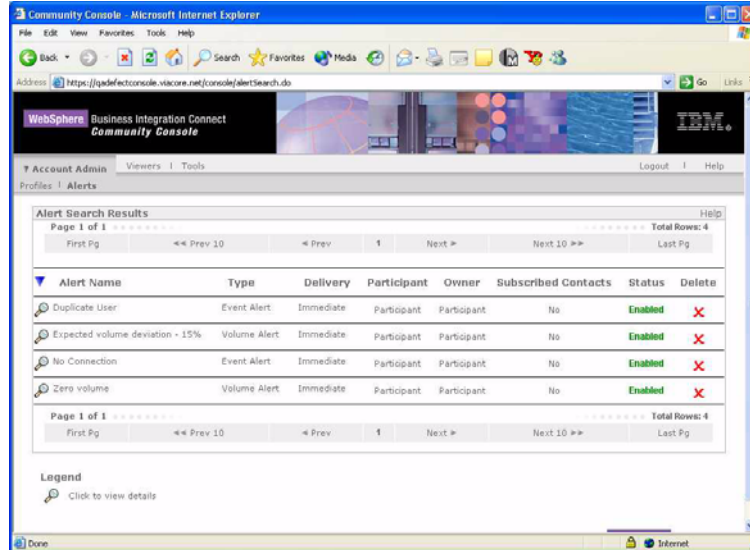




Figure 2-23. Alert Search Results

5. Click  to view an alert's details.
6. Click  to edit alert details.

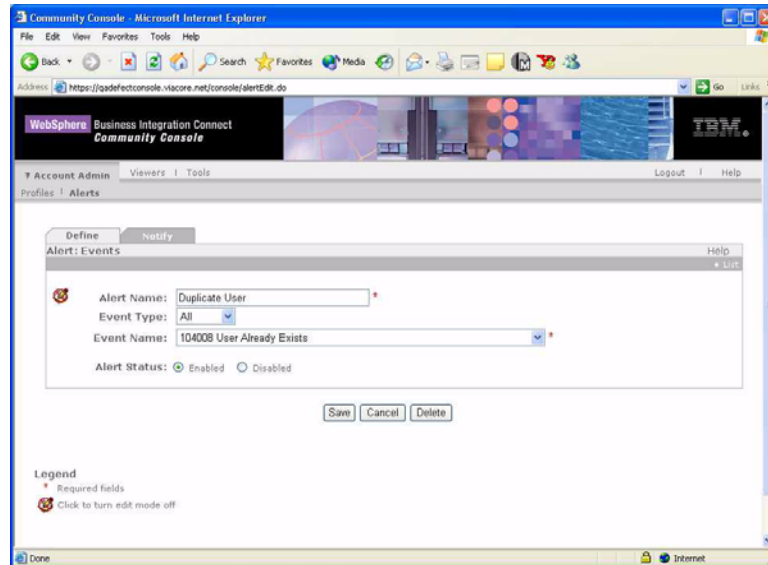


Figure 2-24. Alert: Events (Edit)

7. Edit information as required.
8. Click the **Notify** tab.

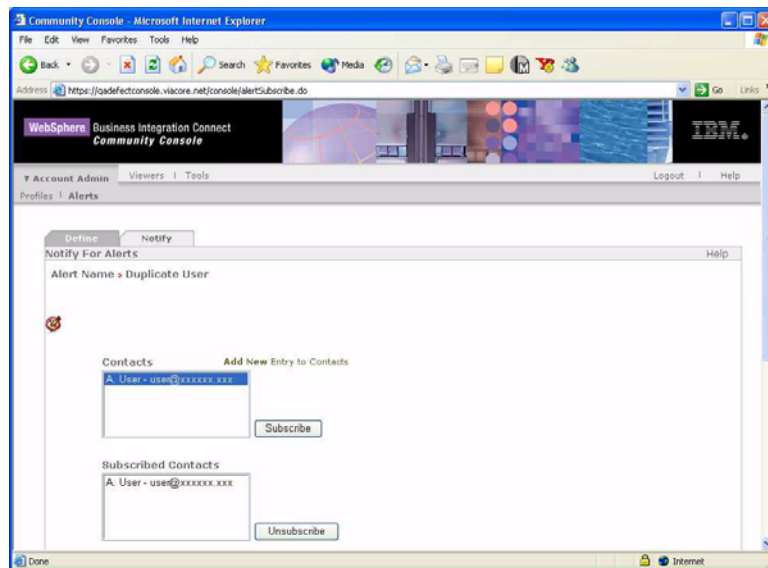


Figure 2-25. Notify tab

9. Select a Participant (Community Manager or Community Operator only). The Community Manager can view all alerts regardless of the Alert Owner.
10. Edit contacts for this alert, if desired.
11. Click **Save**.

Searching for alerts

To search for an alert:

1. Click **Account Admin** on the main menu.
2. Click **Alerts** on the horizontal navigation bar. The system displays the Alert Search screen.
3. Select the search criteria from the drop-down lists; enter the Alert Name. You can also click **Search** without selecting any search criteria (the system displays all alerts).

Table 2-22. Alert search criteria for Participants

| Value | Description |
|---------------------|--|
| Alert Type | Volume, event, or all alert types. |
| Alert Name | Name of alert. |
| Alert Status | Alerts that are enabled, disabled, or all. |
| Subscribed Contacts | Alert's assigned contacts. Selections are Has Subscribers, No Subscribers, or All. |
| Results Per Page | Controls how search results are displayed. |

Table 2-23. Alert search criteria for Community Manager and Community Operator



| Value | Description |
|---------------------|--|
| Alert Owner | Creator of the alert. |
| Alert Participant | Participant that the alert applies to. |
| Alert Type | Volume, event, or all alert types. |
| Alert Name | Name of alert. |
| Alert Status | Alerts that are enabled, disabled, or all. |
| Subscribed Contacts | Alert's assigned contacts. Selections are Has Subscribers, No Subscribers, or All. |
| Results Per Page | Controls how search results are displayed. |

4. Click **Search**. The system displays a list of alerts that meet your search criteria, if any.

Adding a new contact to an existing alert

To add a new contact to an existing alert:

1. Click **Account Admin** on the main menu.
2. Click **Alerts** on the horizontal navigation bar. The system displays the Alert Search screen.
3. Enter the search criteria from the drop-down lists; enter the Alert Name.

4. Click **Search**. The system displays a list of alerts that meet your search criteria, if any.
5. Click  to view alert details.
6. Click  to edit alert details.
7. Click the **Notify** tab.
8. Select a Participant (Community Manager and Community Operator only).
9. If the contact that you want to add is listed in the Contacts text box, select the contact and click **Subscribe**. Go to [Step 14](#).

If the contact that you want to add is not listed in the Contacts text box, click **Add New Entry to Contacts**. The system displays the Create New Contact pop-up window.

Note that the Add New Entry to Contacts option is only presented to the Alert Owner to create contacts associated with the Alert Owner. This feature does not allow the Alert Owner to add contacts for Alert Participants.

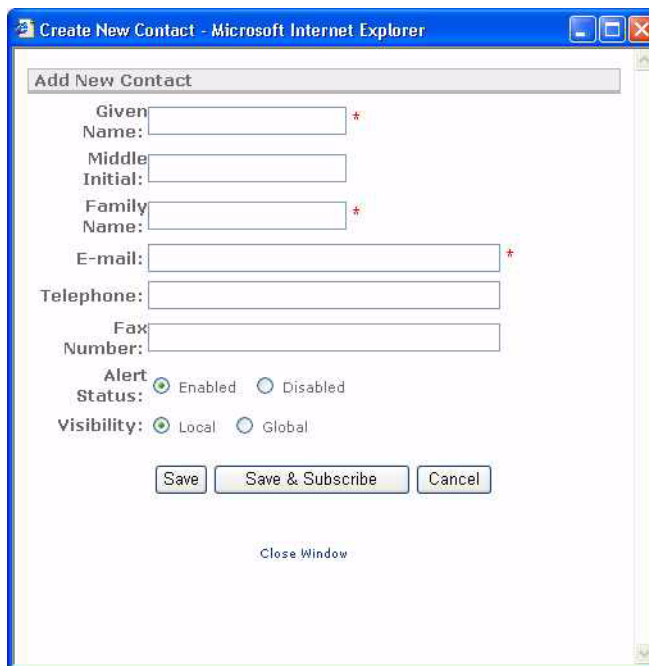


Figure 2-26. Add New Contact

10. Enter the contact's name, e-mail address, telephone and fax numbers.
11. Select the contact's Alert Status.
 - Select **Enabled** to begin sending e-mail messages to this contact when the system generates this alert.
 - Select **Disabled** if you do not want to send e-mail messages to this contact when the system generates this alert.

12. Select the contact's visibility.
 - Select **Local** to make the contact only visible to your organization.
 - Select **Global** to make the contact visible to the Community Operator and Community Manager. Both of these parties can subscribe the contact to alerts.
13. Click **Save** to save the contact. Click **Save and Subscribe** to save the contact and add the contact to the list of contacts for this alert.
14. Click **Save**.

Creating a volume-based alert and adding contacts

To create a volume-based alert and add contacts to the alert:

1. Click **Account Admin** on the main menu.
2. Click **Alerts** on the horizontal navigation bar. The system displays the Alert Search screen.
3. Click **Create** from the sub-menu. The system displays the Alerts Define tab.
4. Select **Volume Alert** for Alert Type (this is the default setting). The system displays the appropriate text boxes for a volume alert.

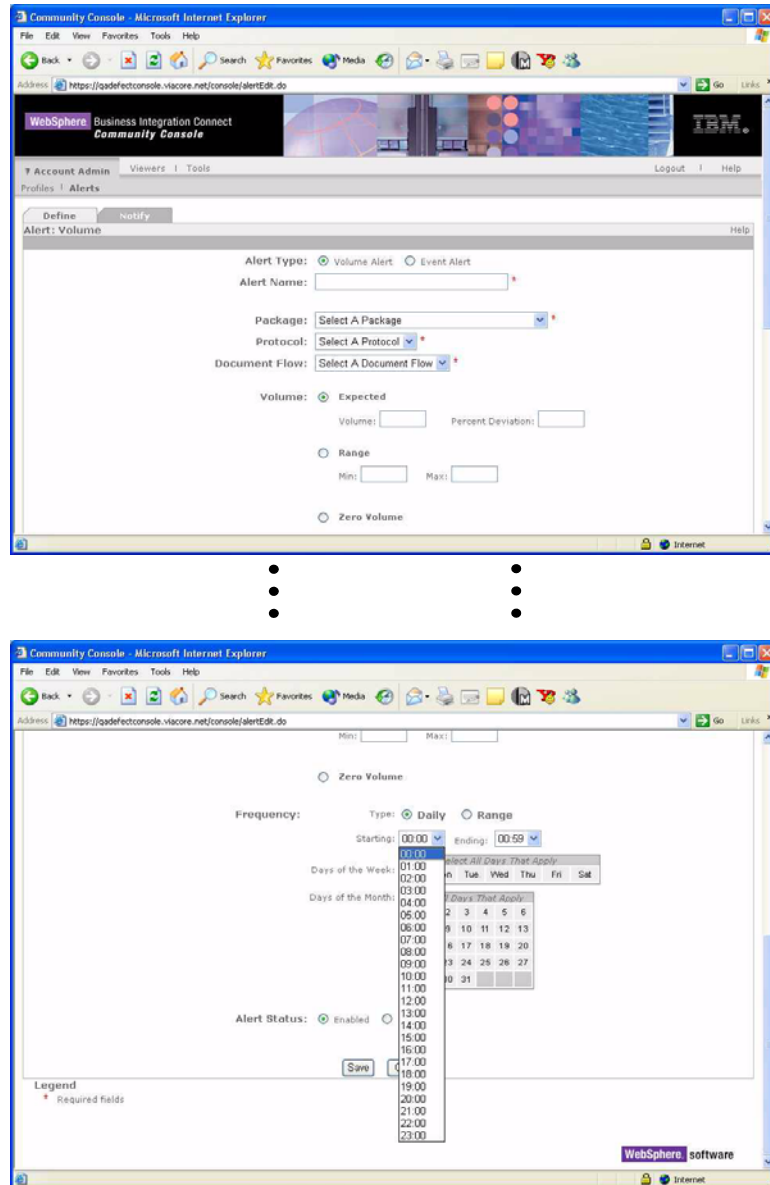


Figure 2-27. Alerts Define tab (Create Volume-Based Alert)


5. Enter a name for the alert in the text box.
6. Select a Participant with rights to create a volume-based alert (Community Manager and Community Operator only).
7. Select **Package**, **Protocol**, and **Document Flow** from the drop-down lists.

The selected Package, Protocol, and Document Flow must match the Package, Protocol, and Document Flow of the source Community Participant.

8. Select one of three volume options (Expected, Range, or Zero Volume), then proceed to [Step 9 on page 75](#):
- **Expected** - Select Expected if you want an alert generated when document flow volume deviates from an exact quantity. Use the following steps to create an alert on expected document flow volume:
 - a. In the Volume text box, enter the number of document flows you expect to receive within a time frame selected in [Step 9](#). Enter a positive number only; the alert will not function if you enter a negative number.
 - b. In the Percent Deviation text box, enter a number that defines the limit the document flow volume can deviate from before the alert is activated. For example:
 - If Volume = 20 and Percent Deviation = 10, a document flow volume less than 18 or greater than 22 will trigger an alert.
 - If Volume = 20 and Percent Deviation = 0, any document flow volume other than 20 will trigger an alert.
 - **Range**. Select Range to generate an alert if document flow volume falls outside a minimum-maximum range. Use the following steps to create an alert based on a range of values:
 - a. In the Min text box, enter the minimum number of document flows you expect to receive within a time frame selected in [Step 9](#). An alert is triggered only if document flow volume falls below this amount.
 - b. In the Max text box, enter the maximum number of document flows you expect to receive within a time frame selected in [Step 9](#).

NOTE: Both Min and Max text boxes must be filled in when creating an alert based on volume range.

- **Zero Volume**. Select Zero Volume to trigger an alert if no document flows occur within a time frame selected in [Step 9](#).
9. Select either Daily or Range for the time frame (Frequency) that the system will use to monitor document flow volume for alert generation.
- **Daily**. Select Daily to monitor document flow volume on one or more actual days of the week or month. For example, select Daily if you are going to monitor document flow volume only on one or more specific days of the week (for example, Mondays, or Mondays and Thursdays), or month (for example, the 1st and the 15th).
 - **Range**. Select Range to monitor document flow volume between two days of the week or month. For example, select Range to monitor document flow volume on all days between Monday and Friday, or all days between the 5th and 20th of each month.
10. Select the Starting and Ending time (24-hour day) that the system will monitor document flow volume for the days selected in the next step. Note that when a Range frequency is selected, the document flow volume is monitored from the Starting time of the first day of the range through the Ending time on the last day of the range.

11. Select the appropriate days during the week or month that alert monitoring will occur. If you selected Daily as a frequency, select either the actual days of the week or days of the month for alert monitoring. If you selected Range as a frequency, select two days during the week, or two days during the month that alert monitoring will fall between.
12. Select the status of this alert: Enabled or Disabled.
13. Click **Save**.
14. Click the **Notify** tab.
15. Click .
16. Select a Participant (Community Manager and Community Operator only).
17. If the contact that you want to add is listed in the Contacts text box, select the contact and click **Subscribe**. Go to [Step 22](#).

If the contact that you want to add is not listed in the Contacts text box, click **Add New Entry to Contacts**. The system displays the Create New Contact pop-up window.

Note that the Add New Entry to Contacts option is only presented to the Alert Owner to create contacts associated with the Alert Owner. This feature does not allow the Alert Owner to add contacts for Alert Participants.
18. Enter the contact's name, e-mail address, telephone and fax numbers.
19. Select the contact's Alert Status.
 - Select **Enabled** to begin sending e-mail messages to this contact when the system generates this alert.
 - Select **Disabled** if you do not want to send e-mail messages to this contact when the system generates this alert.
20. Select the contact's visibility.
 - Select **Local** to make the contact only visible to your organization.
 - Select **Global** to make the contact visible to the Community Operator and Community Manager. Both of these parties can subscribe the contact to alerts.
21. Click **Save** to save the contact; click **Save & Subscribe** to add the contact to the list of contacts for this alert.
22. Click **Save**.

Creating an event-based alert and adding contacts

To create an event-based alert and add contacts to the alert:

1. Click **Account Admin** on the main menu.
2. Click **Alerts** on the horizontal navigation bar.
3. Click **Create** on the sub-menu. The system displays the Define tab.

4. Select **Event Alert** for Alert Type. The system displays the appropriate text boxes for an event-based alert.

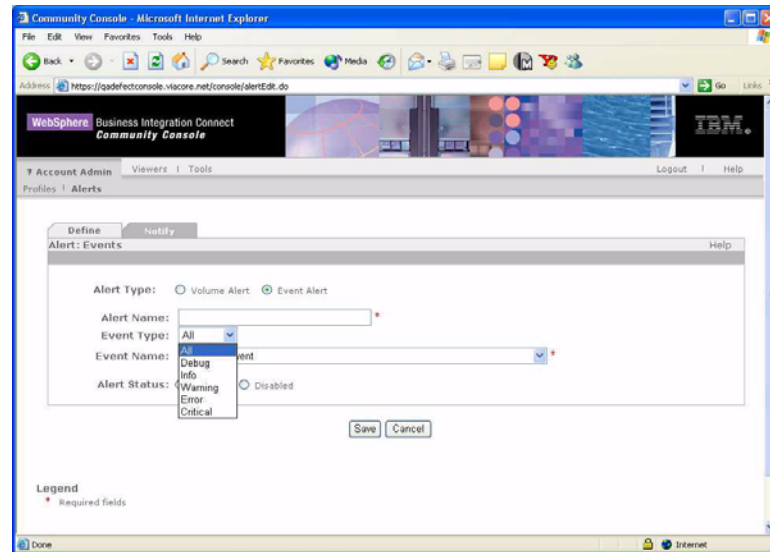



Figure 2-28. Alerts Define tab (Create Event-Based Alert)

5. Enter a name for the alert in the text box.
6. Select a Participant that will trigger the alert (this option is only available to the Community Manager and Community Operator).

Select the Any Participant option to associate the alert with all the Participants in the system. When you perform an alert search and select Any Participant as the Alert Participant, the system displays all alerts that are not associated with a specific Participant.
7. Select the event type: Debug, Information, Warning, Error, Critical, or All.
8. Select the event that will activate the alert, for example, 240601 AS Retry Failure or 108000 Not a Certificate. To create an alert that notifies you when a certificate is about to expire, select one of the following:
 - 108005 Certificate Expiration in 60 Days
 - 108006 Certificate Expiration in 30 Days
 - 108007 Certificate Expiration in 15 Days
 - 108008 Certificate Expiration in 7 Days
 - 108009 Certificate Expiration in 2 Days
9. Select the status of this alert: Enabled or Disabled.
10. Click **Save**.
11. Click the **Notify** tab.
12. Click .

13. Select a Participant (Community Manager and Community Operator only).
14. If the contact that you want to add is listed in the Contacts text box, select the contact and click **Subscribe**. Go to [Step 19](#).

If the contact that you want to add is not listed in the Contacts text box, click **Add New Entry to Contacts**. The system displays the Create New Contact pop-up window.

Note that the Add New Entry to Contacts option is only presented to the Alert Owner to create contacts associated with the Alert Owner. This feature does not allow the Alert Owner to add contacts for Alert Participants.

15. Enter the contact's name, e-mail address, telephone and fax numbers.
16. Select the contact's Alert Status.
 - Select **Enabled** to begin sending e-mail messages to this contact when the system generates this alert.
 - Select **Disabled** if you do not want to send e-mail messages to this contact when the system generates this alert.
17. Select the contact's visibility.
 - Select **Local** to make the contact only visible to your organization.
 - Select **Global** to make the contact visible to the Community Operator and Community Manager. Both of these parties can subscribe the contact to alerts.
18. Click **Save** to save the contact. Click **Save and Subscribe** to save the contact and add the contact to the list of contacts for this alert.
19. Select the Mode of Delivery:
 - **Send alerts immediately**. When you select this option, the system sends alert notifications to the contact when the alert occurs. Use this option for critical alerts.
 - **Batch Alerts By**. When you select this option, you can specify when you want the contact to receive alert notifications. Use this option for non-critical alerts.

The two options in this section, Count and Time, are not mutually exclusive.

If you select the Count option, you must always select the Time option.

- If the number of alerts (Count) is reached during the time limit that you have selected (Time), the system generates an alert notification.
- If an alert occurs but the number of alerts (Count) is not reached during the time limit that you have selected (Time), the system will generate an alert notification at the end of the time limit.

The Time option can be used without the Count option, but the Count option must always be associated with a time limit (Time).

- **Count.** Must also use Time option when you select this option. Enter a number (n). This is the number of alerts that must occur during the selected time period (Time) before the system will send an alert notification to the alert's contact.

Here's an example of how these two options work together:

In our example, Batch Alerts By options are set to 10 for Count (10 alerts) and 2 for Time (2 hour period). The system retains all notifications for this alert until 10 occur in a two hour period or until the end of the time period is reached.

When the alert count reaches 10 in a 2 hour period, the system sends all alert notifications for this alert to the contact.

If an alert occurs but 10 alerts do not occur during the time limit (two hours), the system will send an alert notification to the alert's contact at the end of the time limit.

- **Time.** Select number of hours (n). The system retains alert notification for n hours. Every n hours, the system sends all retained alert notifications to the contact.

For example, if you enter 2, the system retains all notifications for this alert that occur in each two hour interval. When the two hour interval expires, the system sends all alert notifications for this alert to the contact.

20. Click **Save**.

Disabling or enabling an alert

To disable or enable an existing alert:

1. Click **Account Admin** on the main menu.
2. Click **Alerts** on the horizontal navigation bar. The system displays the Alert Search screen.
3. Select the search criteria from the drop-down lists; enter the Alert Name.
4. Click **Search**. The system displays a list of alerts that meet your search criteria, if any.
5. Locate the alert and click **Disabled** or **Enabled** under Status. Only the Community Operator and Alert Owner (creator of the alert) has permission to edit alert Status.

Removing an alert

To remove an alert:

1. Click **Account Admin** on the main menu.
2. Click **Alerts** on the horizontal navigation bar. The system displays the Alert Search screen.
3. Select the search criteria from the drop-down lists; enter the Alert Name.
4. Click **Search**. The system displays a list of alerts that meet your search criteria, if any.
5. Locate the alert and click **X** to delete. Only the Community Operator and Alert Owner (the creator of the alert) can remove an alert.

Chapter 3. Viewing events and documents: Viewers

The Viewers module includes the following features:

- Event Viewer
- RosettaNet Viewer
- AS1/AS2 Viewer
- Document Viewer

These features give you a view into overall system health. They are also troubleshooting tools for event resolution.

You can locate a specific event and then research why it occurred. The Event Viewer allows you to search for events by time, date, event type, event code, and event location. The Hub Admin can also search by Participant, Source IP, and Event IP.

The data that the Event Viewer generates identifies, among other things, the Event Code, TimeStamp, and Source IP, and allows you to view the event and document details to diagnose the problem. You can also view the raw document, which identifies the field, value, and reason for the error.

Use the RosettaNet Viewer to locate a specific process that generated an event. When you identify the target process, you can view process details and the raw document.

Use the AS1/AS2 Viewer to search for and view transport information for documents using the AS1 or AS2 communication protocol. You can view message IDs, Message Disposition Notification (MDN) destination URI and status, and document details (the document and wrapper).

The Document Viewer is used to locate and view a specific document that you want to research. You can search for documents based on date, time, type of process, (From Process or To Process), Participant connection, gateway type, document status, protocol, document flow, and process version. The search results display all documents that meet your search criteria, and identify time stamps, process, participant connection, and gateway types. Locate the target document and use the viewer's features to view the raw document.

NOTE: The term Participants is used on the Viewer screens to identify a hub-community member, including the Community Manager.

The RosettaNet and AS1/AS2 Viewers include additional search criteria for the Hub Admin. For more information, see the [WebSphere Business Integration Connect Administrator Guide](#).

Table 3-1. Viewers

| What feature do you want to use? | See |
|----------------------------------|-------------------------|
| Event Viewer | page 82 |
| RosettaNet Viewer | page 92 |
| AS1/AS2 Viewer | page 87 |
| Document Viewer | page 96 |

Event Viewer

Use the Event Viewer to view and research events.

An event tells you know that something unusual has happened in the system. An event can let you know that a system operation or function was successful (for example, a Participant was successfully added to the system, or a Participant connection was successfully created between Community Manager and Participant). An event can also identify a problem (for example, the system could not process a document or the system detected a non-critical error in a document). Most types of documents are resent multiple times, so when a document fails and generates an alert, it is something that you should investigate and correct to prevent similar failures in the future.

WebSphere Business Integration Connect includes predefined events. Use the product's Alerts feature, Account Admin module, to create event-based alerts. This process identifies the events that are of concern to you. Then use the Contacts feature, also in the Account Admin module, to identify the staff members that the system will notify if those events occur.

The Event Viewer displays events based on specific search criteria. You can locate a specific event and then research why it occurred. The Event Viewer allows you to search for events by time, date, event type (debug, information, warning, error, and critical), event code (for example, 210031), and event location.

Data available through the Event Viewer includes event name, time stamp, user, and Participant information. This data helps you identify the document or process that created the event. If the event is related to a document, you can also view the raw document, which identifies the field, value, and reason for the error.

Event types

WebSphere Business Integration Connect includes the following event types.

Table 3-2. Event types

| Event type | Description |
|-------------|--|
| Debug | Debug events are used for low-level system operations and support. Their visibility and use is subject to the permission level of the user. Not all users have access to Debug events. |
| Information | Informational events are generated at the successful completion of a system operation. These events are also used to provide the status of documents currently being processed. Informational events require no user action. |
| Warning | Warning events occur due to non-critical anomalies in document processing or system functions that allow the operation to continue. |
| Error | Error events occur due to anomalies in document processing that cause the process to terminate. |
| Critical | Critical events are generated when services are terminated due to system failure. Critical events require intervention by support personnel. |

Performing Event Viewer tasks

Table 3-3. Event Viewer tasks

| What do you want to do? | See |
|-------------------------|-------------------------|
| Search for events. | page 83 |
| View event details. | page 85 |

Searching for events

To search for specific events:

1. Click **Viewers** on the main menu.
2. Click **Event Viewer** on the horizontal navigation bar.

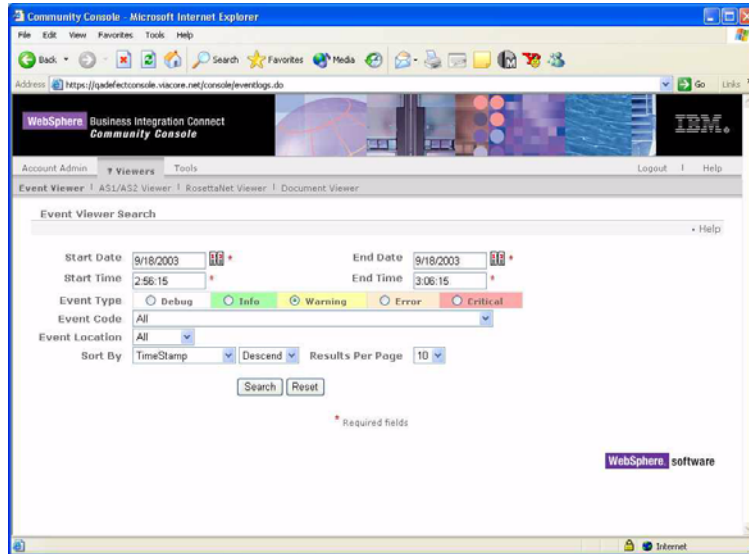


Figure 3-1. Event Viewer Search


Events are organized by severity from left to right in the Event Viewer Search screen. Information on the left is the least severe event type; Critical on the right is the most severe. (Debug events cannot be viewed by all users.) For any selected event, that event and all events with greater severity are displayed in the Event Viewer. For example, if the Warning event type is selected in the search criteria, Warning, Error, and Critical events are displayed. If Informational events are selected, all event types are displayed

3. Select the search criteria from the drop-down lists.

Table 3-4. Event Search criteria

| Value | Description |
|---------------------|---|
| Start date and time | Date and time the first event occurred. Default is ten minutes prior. |
| End date and time | Date and time the last event occurred. |
| Participants | Select all Participants or a specific Participant (Community Manager only). |
| Event type | Type of event: Debug, Info, Warning, Error, or Critical. |
| Event code | Search on available event codes based on selected event type. |
| Event location | Location where event was generated: all, unknown, source (from), target (to). |
| Sort by | Value used to sort results. |
| Descend | Sort in descending or ascending order. |
| Results per page | Number of records displayed per page. |

Table 3-4. Event Search criteria

| Value | Description |
|--------------|--|
| Refresh | Default setting is Off. Click  to turn on (Community Manager only). When Refresh is On, the Event Viewer will first perform a new query, then remain in refresh mode. |
| Refresh Rate | Controls how often search results are refreshed (Community Manager only). |

- Click **Search**. The system displays a list of events.

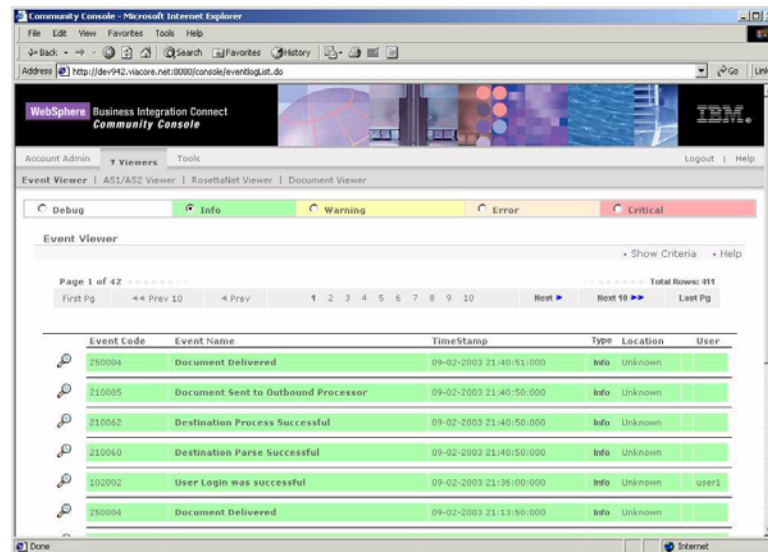






Figure 3-2. Event Viewer search results

TIP: The event list can be re-filtered based on the event type selected at the top of the Event Viewer screen. The next screen refresh reflects the new selected event type.

Viewing event details

To view event details:

- Click **Viewers** on the main menu.
- Click **Event Viewer** on the horizontal navigation bar if not displayed.
- Select the search criteria from the drop-down lists.
- Click **Search**. The system displays a list of events.
- Click  next to the event you want to view. The system displays event details and associated documents.

6. Click  next to the document that you want to view, if one exists.
7. Click  to view the raw document, if one exists.
8. Click  to view validation errors.

TIP: If a duplicate document event is displayed in the Event Viewer Detail, view the previously sent original document by selecting  in Document Details.

AS1/AS2 Viewer

Use the AS1/AS2 Viewer to view packaged B2B transactions and B2B process details that use the AS1 or AS2 (Applicability Statement 1 or 2) communication protocol. You can view the choreography of the B2B process and associated business documents, acknowledgment signals, process state, HTTP headers, and contents of the transmitted documents.

Like its predecessor AS1, which defines a standard for data transmissions using SMTP, AS2 defines a standard for data transmissions using HTTP.

AS2 identifies how to connect, deliver, validate, and reply to data; it does not concern itself with the content of the document, only the transport. AS2 creates a wrapper around a document so that it can be transported over the Internet using HTTP or HTTPS. The document and wrapper together is called a message. AS2 provides security and encryption around the HTTP packets. Another bonus with AS2 is that it provides a measure of security not found in FTP. AS2 provides an encryption base with guaranteed delivery.

An important component of AS2 is the receipt mechanism, which is referred to as an MDN (Message Disposition Notification). This ensures the sender of the document that the recipient has successfully received the document. The sender specifies how the MDN is to be sent back (synchronously or asynchronously; signed or unsigned).

You can use the AS1/AS2 Viewer to view the message ID, Time Stamps, Document Flow, Gateway Type, Synchronous status, as well as document details. Additional document processing information is displayed when viewing document details.

Performing AS1/AS2 Viewer tasks

Table 3-5. AS1/AS2 Viewer tasks

| What do you want to do? | See |
|-------------------------|-------------------------|
| Search for messages | page 87 |
| Viewing message details | page 89 |

Searching for messages

To search for specific AS1/AS2 messages:

1. Click **Viewers** on the main menu.
2. Select **AS1/AS2 Viewer** from the horizontal navigation bar. The system displays the AS1/AS2 Viewer screen.

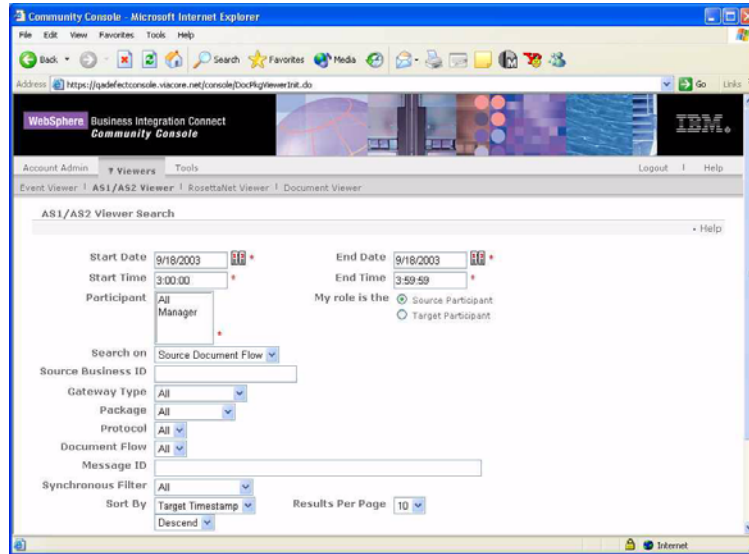


Figure 3-3. AS1/AS2 Viewer

3. Select the search criteria from the drop-down lists.

Table 3-6. AS1/AS2 Viewer search criteria

| Value | Description |
|-------------------------------|--|
| Start Date and Time | Date and time the process was initiated. |
| End Date and Time | Date and time the process was completed. |
| Source and Target Participant | Identifies the source (initiating) and the target (receiving) Participants (Community Manager only). |
| Participant | Identifies if the search applies to all Participants or the Community Manager (Participant only). |
| My role is the | Identifies if the search looks for documents in which the Participant is the Target or Source (Participant only). |
| Initiating Business ID | Business identification number of the source Participant, for example, Duns. |
| Gateway Type | Production or test. Test is only available on systems that support the test gateway type. |
| Package | Describes the document format, packaging, encryption, and content-type identification. |
| Protocol | Document format available to the Participants, for example, RosettaNet or XML. |
| Document Flow | The specific business process. |
| Message ID | ID number assigned to the AS1 or AS2 packaged document. Search criteria can include the asterisk (*) wildcard. Maximum length, 255 characters. |

Table 3-6. AS1/AS2 Viewer search criteria

| Value | Description |
|--------------------|--|
| Synchronous Filter | Search for documents received in synchronous mode. This means that the connection between the initiator and the Document Manager stays open until the transaction is complete, including request, acknowledgement, response, and acknowledgement (Community Manager only). |
| Sort by | Sort results by this value. |
| Descend or Ascend | Ascend. Displays the oldest time stamp first or the end of the alphabet. Descend. Displays the most recent time stamp or the beginning of the alphabet. |
| Results per page | Use to select the number of records displayed per page. |

- Click **Search**. The system displays a list of messages.

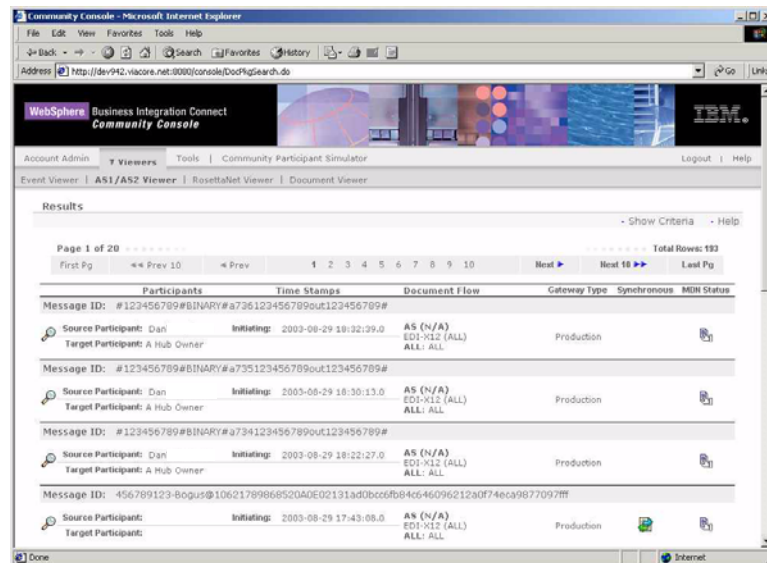



Figure 3-4. AS1/AS2 search results

Viewing message details

To view message details:

- Click **Viewers** on the main menu.
- Select **AS1/AS2 Viewer** from the horizontal navigation bar.
- Select the search criteria from the drop-down lists.
- Click **Search**. The system displays a list of messages.

- Click  next to the message that you want to view. The system displays the message and the associated document details.

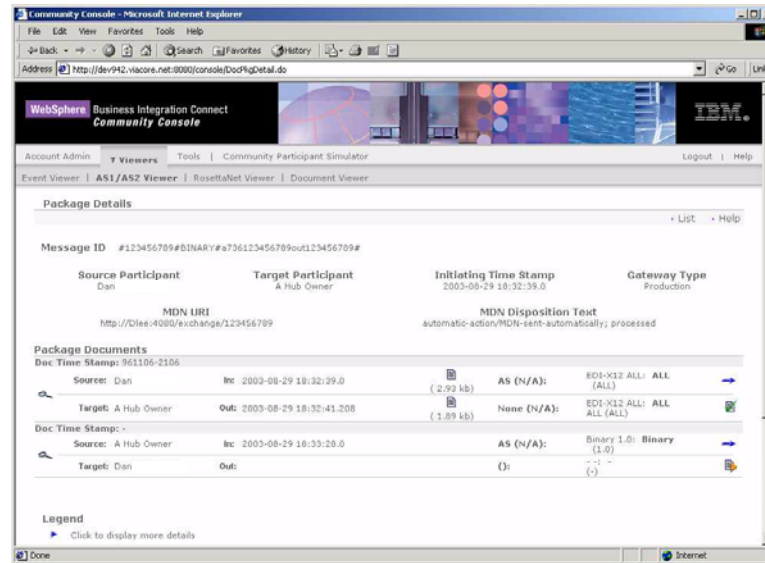



Figure 3-5. View AS1/AS2 message

Table 3-7. AS1/AS2 Viewer: Package Details

| Value | Description |
|-----------------------|---|
| Message ID | ID number assigned to the AS1 or AS2 packaged document. This number identifies the package only. The document itself has a separate Document ID number that is displayed when viewing the document details. Maximum length, 255 characters. |
| Source Participant | Participant initiating a business process. |
| Target Participant | Participant receiving the business process. |
| Initiating Time Stamp | Date and time the document begins processing. |
| Gateway Type | Test or production. Test is only available on systems that support the test gateway type. |

Table 3-7. AS1/AS2 Viewer: Package Details

| Value | Description |
|----------------------|---|
| MDN URI | The destination address for the MDN. The address can be specified as a HTTP URI, or an e-mail address. |
| MDN Disposition Text | <p>This text provides the status of the originating message that was received (either successful or failed). Examples include the following:</p> <ul style="list-style-type: none">• Automatic-action/MDN-sent-automatically; processed.• Automatic-action/MDN-sent-automatically;processed/Warning;duplicate-document.• Automatic-action/MDN-sent-automatically;processed/Error;description-failed.• Automatic-action/MDN-sent-automatically;failed:unsupported MIC-algorithms. |

6. (Optional) Click  to view the raw document.

RosettaNet Viewer

RosettaNet is a group of companies that created an industry standard for e-business transactions. Participant Interface Processes (PIPs) define business processes between members of the hub-community. Each PIP identifies a specific business document and how it is processed between the Community Manager and Participants.

The RosettaNet Viewer displays the choreography of documents that make up a business process. Values that are viewable using the RosettaNet Viewer include process state, details, raw documents, and associated process events.

The RosettaNet Viewer displays processes based on specific search criteria.

Performing RosettaNet Viewer tasks

Table 3-8. RosettaNet Viewer tasks

| What do you want to do? | See |
|----------------------------------|-------------------------|
| Search for RosettaNet processes. | page 92 |
| View RosettaNet process details. | page 94 |
| View raw documents. | page 95 |

Searching for RosettaNet processes

To search for RosettaNet processes:

1. Click **Viewers** on the main menu.
2. Click **RosettaNet Viewer** on the horizontal navigation bar. The system displays the RosettaNet Viewer Search screen.

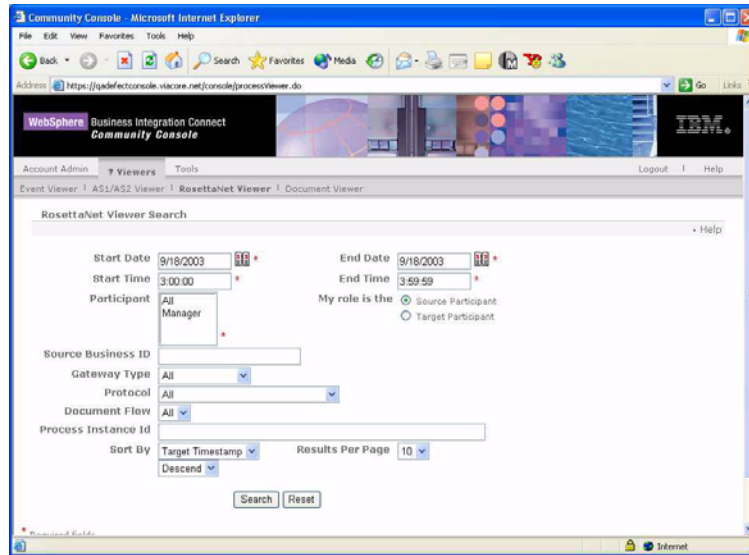


Figure 3-6. RosettaNet Viewer Search

3. Select the search criteria from the drop-down lists.

Table 3-9. RosettaNet search criteria

| Value | Description |
|-------------------------------|--|
| Start Date and Time | The date and time that the process was initiated. |
| End Date and Time | The date and time that the process was completed. |
| Source and Target Participant | Identifies the source (initiating) and the target (receiving) Participants (Community Manager only). |
| Participant | Identifies if the search applies to all Participants or the Community Manager (Participant only). |
| My role is the | Identifies if the search looks for documents in which the Participant is the Target or Source (Participant only). |
| Initiating Business ID | Business identification number of initiating Participant, for example, DUNS. |
| Gateway Type | Production or test. Test is only available on systems that support the test gateway type. |
| Protocol | Protocols available to the Participants. |
| Document Flow | The specific business process. |
| Process Instance ID | Unique identification number assigned to the process. Criteria can include asterisk (*) wildcard. |
| Synchronous Filter | Search for documents received in synchronous mode. This means that the connection between the initiator and the Document Manager stays open until the transaction is complete, including request, acknowledgement, response, and acknowledgement (Community Manager only). |

Table 3-9. RosettaNet search criteria

| Value | Description |
|-------------------|--|
| Sort By | Sort results, for example, by Received Time Stamp. |
| Descend or Ascend | Ascend - Displays oldest time stamp first or end of the alphabet. Descend - Displays most recent time stamp or beginning of the alphabet. |
| Results Per Page | Display n number of results per page. |

- Click **Search**. The system displays RosettaNet processes that match your search criteria.

| Process Instance ID | Source Participant | Target Participant | Initiating | Time Stamps | Document Flow | Gateway Type |
|-------------------------------------|--------------------|--------------------|-----------------------|-------------|--|--------------|
| PIDBC-DELLCTIEU10620276546240000005 | Your Company Name | A Hub Owner | 2003-08-27 23:40:54.0 | | RosettaNet (1.1): 3A4 Request Purchase Order | Production |
| PIDBC-DELLCTIEU10620264070150000004 | Your Company Name | A Hub Owner | 2003-08-27 23:20:06.0 | | RosettaNet (1.1): 3A4 Request Purchase Order | Production |
| PIDBC-DELLCTIEU10620234130610000003 | Your Company Name | A Hub Owner | 2003-08-27 22:30:12.0 | | RosettaNet (1.1): 3A4 Request Purchase Order | Production |
| PIDBC-DELLCTIEU10620230420460000002 | Your Company Name | A Hub Owner | 2003-08-27 22:24:15.0 | | RosettaNet (1.1): 3A4 Request Purchase Order | Production |
| PIDBC-DELLCTIEU10620081169680000001 | Your Company Name | A Hub Owner | 2003-08-27 18:15:25.0 | | RosettaNet (1.1): 3A4 Request Purchase Order | Production |
| PIDBC-DELLCTIEU10619194823600000003 | Your Company Name | A Hub Owner | 2003-08-26 17:30:02.0 | | RosettaNet (1.1): 3A4 Request Purchase Order | Production |
| PIDBC-DELLCTIEU10619190851410000002 | Your Company Name | A Hub Owner | 2003-08-26 17:31:24.0 | | RosettaNet (1.1): 3A7 | |

Figure 3-7. RosettaNet search results



Viewing RosettaNet process details

To view RosettaNet process details:

- Click **Viewers** on the main menu.
- Click **RosettaNet Viewer** on the horizontal navigation bar. The system displays the RosettaNet Viewer.
- Select the search criteria from the drop-down lists.
- Click **Search**. The system displays the results of your search.



Table 3-10. Document processing details

| Value | Description |
|---------------------|--|
| Participants | Participants involved in the business process. |
| Time Stamps | Date and time the first document begins processing. |
| Document Flow | The specific business process, for example RosettaNet (1.1): 3A7. |
| Gateway Type | For example, Production. |
| Process Instance ID | Unique number assigned to the process by the initiating community member. |
| Document ID | Proprietary document identifier assigned by the sending Participant. The field is not in a fixed location and varies by document type. |
| Source Participant | Initiating Participant. |
| Target Participant | Receiving Participant. |

5. Click  next to the RosettaNet process you want to view. The system displays details and associated documents for the selected process.
6. Click  next to the document you want to view. The system displays the document and associated event details.

Viewing raw documents

To view a raw document associated with a RosettaNet process:

1. Click **Viewers** on the main menu.
2. Click **RosettaNet Viewer** on the horizontal navigation bar.
3. Select the search criteria from the drop-down lists.
4. Click **Search**. The system displays a list of processes.
5. Click  next to the process that you want to view. The system displays process details and associated documents for the selected process.
6. Click  adjacent to the Document Flow to display the raw document.

RESTRICTIONS: Raw documents greater than 100K are truncated.

TIP:

- To troubleshoot documents that have failed processing, see [“Viewing data validation errors” on page 100](#).
 - The raw document viewer displays the HTTP header with the raw document.
-

Document Viewer

Use the Document Viewer to view individual documents that make up a process. You can use search criteria to display raw documents and associated document processing details and events.

Performing Document Viewer tasks

Table 3-11. Document Viewer tasks

| What do you want to do? | See |
|--|--------------------------|
| Search for documents | page 96 |
| Viewing document details, events, and raw document | page 99 |
| Viewing data validation errors | page 100 |

Searching for documents

To search for documents in the system:

1. Click **Viewers** on the main menu.
2. Click **Document Viewer** on the horizontal navigation bar. The system displays the Document Viewer Search screen.

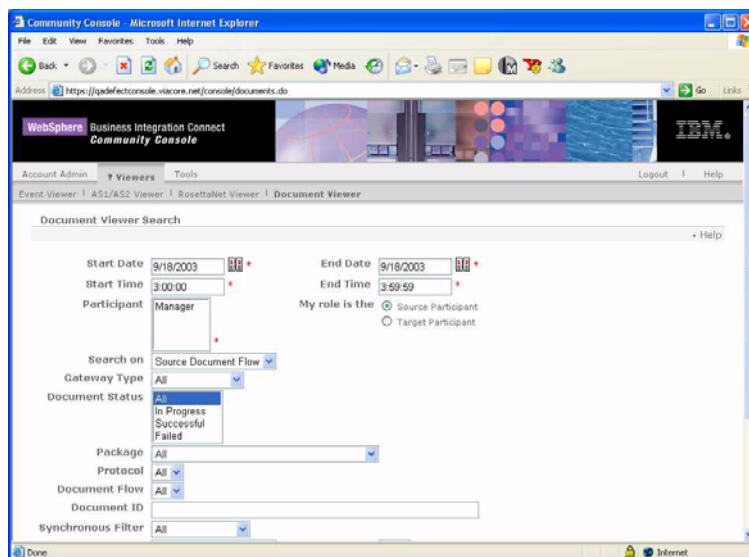


Figure 3-8. Document Viewer

3. Select the search criteria from the drop-down lists.

Table 3-12. Document Viewer search criteria

| Value | Description |
|-------------------------------|--|
| Start date and time | Date and time the process was initiated. |
| End date and time | Date and time the process was completed. |
| Source and Target Participant | Identifies the source (initiating) and the target (receiving) Participants (Community Manager only). |
| Participant | Identifies if the search applies to all Participants or the Community Manager (Participant only). |
| My role is the | Identifies if the search looks for documents in which the Participant is the Target or Source (Participant only). |
| Search on | Search on From or To document flow. |
| Gateway Type | Production or test. Test is only available on systems that support the test gateway type. |
| Document status | Current document status in system: failed, successful, in-progress, or all. |
| Package | Describes the document format, packaging, encryption, and content-type identification |
| Protocol | Type of process protocol available to the Participants. |
| Document Flow | The specific business process. |
| Document ID | Created by the source Participant. Criteria can include asterisk (*) wildcard. |
| Synchronous Filter | Search for documents received in synchronous mode. This means that the connection between the initiator and the Document Manager stays open until the transaction is complete, including request, acknowledgement, response, and acknowledgement (Community Manager only). |
| Sort By | Value used to sort results. |
| Results per page | Number of records displayed per page. |
| Descend | Sort results in descending or ascending order. |

NOTE: Warning events are displayed by default. To see all events, select Debug.

4. Click **Search**. The system displays a list of documents that meet your search criteria.

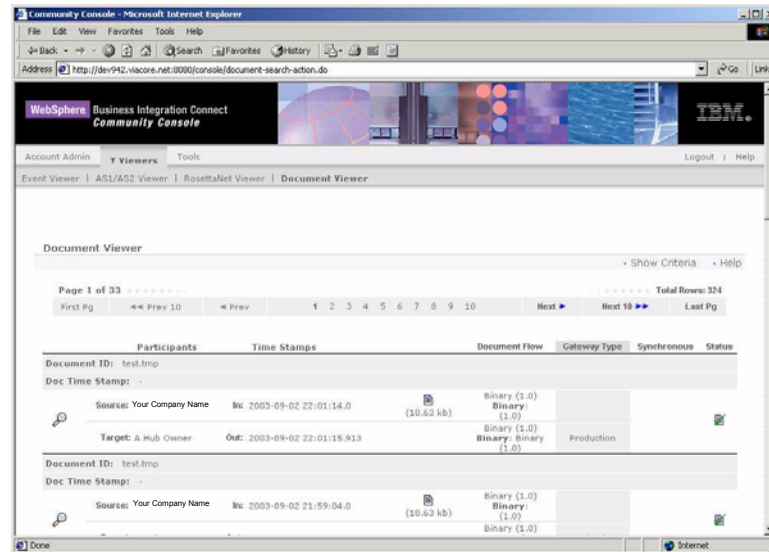








Figure 3-9. Document Viewer search results

Table 3-13. Document information available using the Document Viewer

| Value | Description |
|---------------|---|
| Participants | Source (From) and target (To) Participants involved in the business process. |
| Time Stamps | Date and time the document begins and ends processing. |
| Document Flow | Business process that is being transacted. |
| Gateway Type | Test or production. Test is only available on systems that support the test gateway type. |
| Synchronous | Identifies that the document was received in synchronous mode. This means that the connection between the initiator and the Document Manager stays open until the transaction is complete, including request, acknowledgement, response, and acknowledgement. |
| Status |  Document currently in progress.  Document processing was successful.  Document failed processing. |




Viewing document details, events, and raw document

To view process details for a document:

1. Click **Viewers** on the main menu.
2. Click **Document Viewer** on the horizontal navigation bar. The system displays the Document Viewer Search screen.
3. Select the search criteria from the drop-down lists.
4. Click **Search**. The system displays a list of documents.
 - To view a document's details and events, click  next to the document. The system displays process details and events for the selected document. Click  in the events screen to view event details.
 - To view the raw document with HTTP header, click  next to the document. The system displays the raw document's content.

The following document processing information is displayed when you view document details:

Table 3-14. Document processing values available using the Document Viewer

| Value | Description |
|---------------------------------|---|
| Reference ID | Unique identification number assigned to the document by the system. |
| Document ID | Unique identification number assigned to the document by the source Participant. |
| Doc Time Stamp | Date and time document was created by Participant. |
| Gateway | Gateway the document passed through. |
| Connection Document Flow | Actions performed on a document by the system to ensure its compatibility with business requirements between Participants. |
| Status |  Document currently in progress.  Document processing was successful.  Document failed processing. |
| Source and Target | Source and target Participants involved in business process. |
| In Time Stamp | Date and time the document was received by the system from the Participant. |
| End State Time Stamp | Date and time the document was successfully routed by the system to the target Participant. |
| Source and Target Business ID | Business identification number of Source and Target Participants, for example, DUNS. |
| Source and Target Document Flow | The specific business process transacted between source and target Participants. |

RESTRICTIONS: Raw documents larger than 100K are truncated.

TIP: If the system displays a Duplicate Document event, view the previously sent original document by selecting ► next to the Duplicate Document event, then selecting 📄.

TIP: To troubleshoot documents that have failed processing, see “[Viewing data validation errors](#)” on page 100.

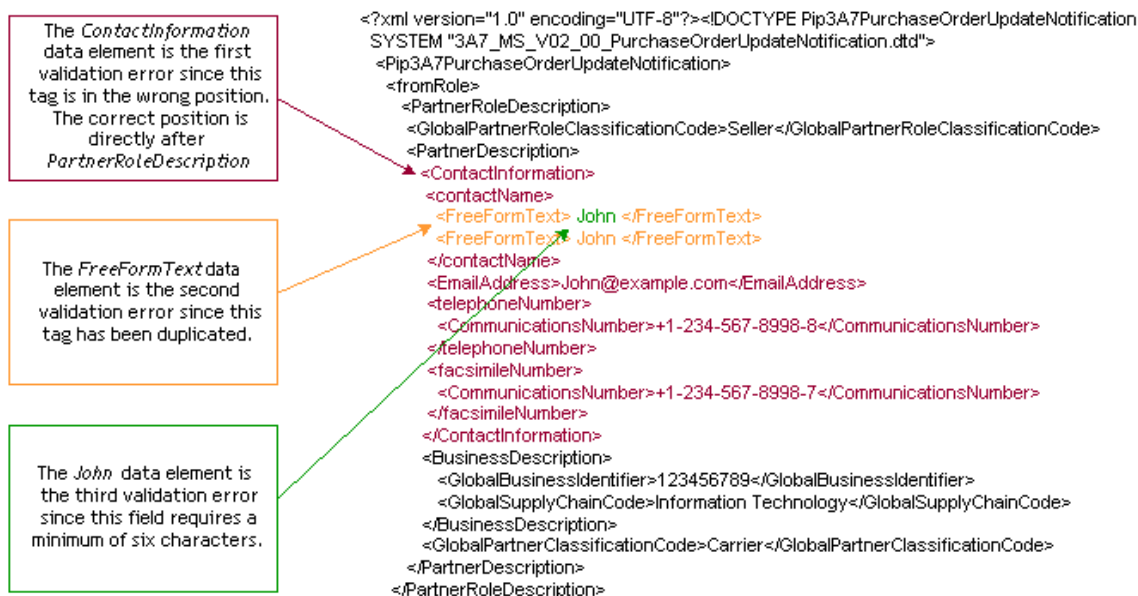
Viewing data validation errors

You can quickly search for documents that have failed processing using the color-coded text in the XML fields that contain validation errors. Fields that contain validation errors are displayed in **red**. If up to three separate validation errors occur within nested XML fields, the following colors are used to distinguish between the error fields:

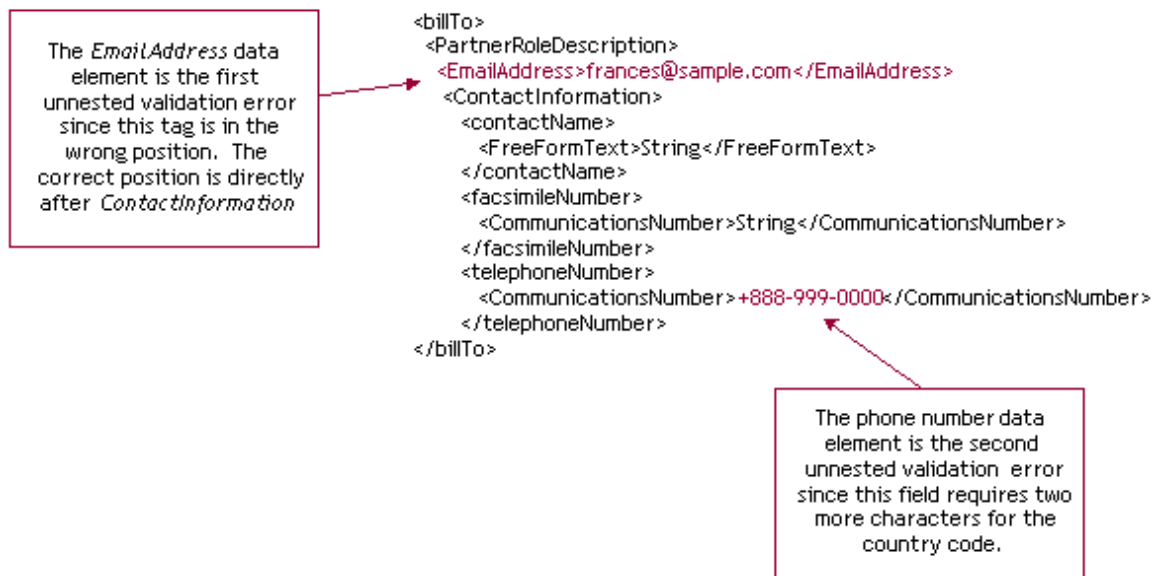
Table 3-15. Color-coded document validation errors

| Value | Description |
|--------|-------------------------|
| Red | First validation error |
| Orange | Second validation error |
| Green | Third validation error |

The following is an example of nested XML validation errors:



Example of non-nested XML validation errors:



To view validation errors in a raw document, see [“Viewing raw documents” on page 95](#).

RESTRICTIONS: The console only displays the first 100KB of a raw document. Validation errors beyond 100KB are not viewable.

Chapter 4. Analyzing document flow: Tools

Use the Document Analysis tool to get a detailed overview of the number of documents in the system, by state (Received, In Progress, Failed, and Successful). Search criteria includes date, time, type of process (To or From), gateway type, protocol, document flow, and process version. Use the search results to locate and view the documents that failed, to investigate the reason for the failures.

The Document Volume Report is a valuable tool used to manage, track, and troubleshoot the flow of your business documents. The report displays the volume of documents processed by the system within a specific time period. This report can be viewed, printed, and saved (exported) to send to other staff members. You can customize this report to view information based on specific search criteria.

The Test Participant Connection tool is used to test the gateway or Web server.

Table 4-1. Tools

| What feature do you want to use? | See |
|----------------------------------|--------------------------|
| Document Analysis | page 104 |
| Document Volume Report | page 107 |
| Test Participant Connection | page 110 |

Document Analysis

Use the Document Analysis tool to get a detailed overview of the number of documents in the system, by state, within a specific time period.

Use the search criteria to locate failed documents and investigate the reason for the failures.

The Document Analysis screen includes an alarm. If a process has failed, the row containing the failed process flashes red.

Document States

The following table describes the different document states.

Table 4-2. Document States

| State | Description |
|-------------|--|
| Received | The document has been received by the system and is waiting for processing. |
| In Progress | <p>The document is currently in one of the following processing steps:</p> <ul style="list-style-type: none">• Incomplete. For example, the system is waiting for other documents.• Data Validation. For example, the system is checking document content.• Translation. For example, the system is converting the document to another protocol.• Queue. For example, the document is waiting to be routed to the Participant or Community Manager. |
| Failed | Document processing was interrupted due to errors in the system, data validation, or duplicates. |
| Successful | The final message that completes document processing has been transmitted from the system to the target Participant. |

Viewing documents in the system

To view documents currently in the system:

1. Click **Tools** on the main menu.
2. Click **Document Analysis** on the horizontal navigation bar. The system displays the Document Analysis Search screen.

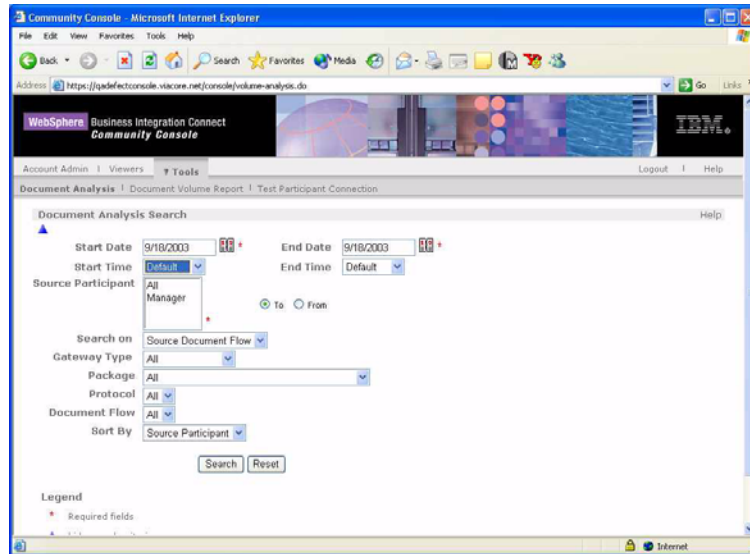


Figure 4-1. Document Analysis Search

3. Select the search criteria from the drop-down lists.

Table 4-3. Document Search Criteria

| Value | Description |
|--------------------|--|
| Start Date & Time | The date and time the process was initiated. |
| End Date & Time | The date and time the process was completed. |
| Source Participant | The Participant that initiated the business process (Community Manager only). |
| Target Participant | The Participant that received the business process (Community Manager only). |
| Participant | The initiating or receiving Participant (Participant only). |
| To or From | Designates if the Participant is the receiving (To) or initiating (From) Participant (Participant only). |
| Search On | Search on From document flow or To document flow. |
| Gateway Type | For example, Production or test. Test is only available on systems that support the test gateway type. |
| Package | Describes document format, packaging, encryption, and content-type identification. |
| Protocol | Document protocol available to the Participants. |
| Document Flow | Specific business process. |
| Sort By | Sort results by From Participant Name or To Participant Name. |

Table 4-3. Document Search Criteria

| Value | Description |
|--------------|---|
| Refresh | Controls if the search results are refreshed periodically (Community Manager only). |
| Refresh Rate | Controls how often search results are refreshed (Community Manager only). |

- Click **Search**. The system displays the Document Analysis Summary.

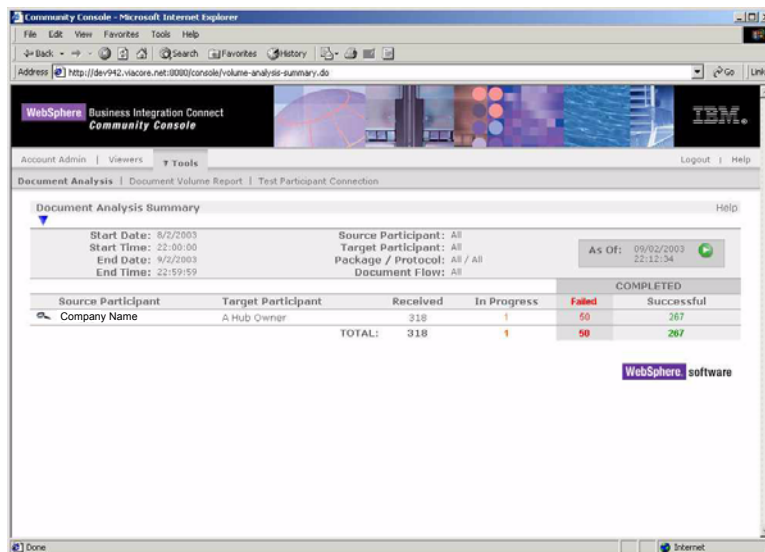



Figure 4-2. Document Analysis Summary

Viewing process and event details

To view process or event details:

- Click **Tools** on the main menu.
- Click **Document Analysis** on the horizontal navigation bar. The system displays the Document Analysis Search screen.
- Select the search criteria from the drop-down lists.
- Click **Search**. The system displays the Document Analysis Summary.
- Click  next to the Source and Target Participants that you want to view. The system displays a list of all documents for the selected Participants. Document quantity is arranged in columns by document processing state.
- Select the quantity link in the Received, In Progress, Failed, or Successful columns. The system presents document processing details in the Document Analysis Report. If you selected Failed, the report also includes a Document Event Summary.

Document Volume Report

The Document Volume Report is a valuable tool used to manage, track, and troubleshoot the flow of your business documents. The report displays the volume of documents processed by the system within a specific time period. This report can be viewed, printed, and saved (exported) to send to other staff members.

You can customize this report to view information based on specific search criteria.

The Document Volume Report shows the number of documents currently in process by their state:

Table 4-4. Document States

| Value | Description |
|----------------|---|
| Total Received | The total number of documents received by system. |
| In Progress | Documents that are In Progress are being tested and validated. No error has been detected, but the process is not yet complete. |
| Failed | Document processing was interrupted due to error. |
| Successful | The final message that completes document processing has been transmitted from the system to the target Participant. |

TIP:

Use this report to perform the following tasks:

- Determine if key business processes have completed.
 - Track trends in process volume for cost control.
 - Manage process quality - success and failure.
 - If you are the Community Manager, help Participants track process efficiency.
-

Create a Document Volume Report

To create a Document Volume Report:

1. Click **Tools** on the main menu.
2. Click **Document Volume Report** on the horizontal navigation bar. The system displays the Document Volume Report Search screen.

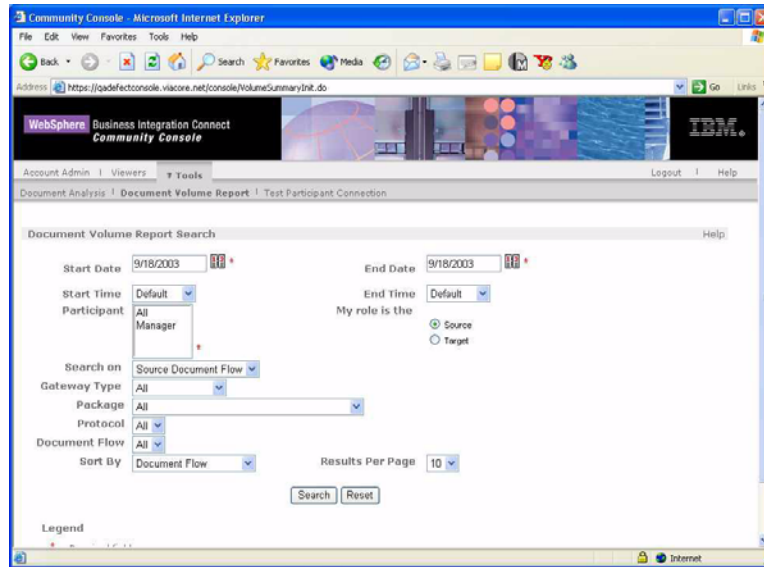


Figure 4-3. Document Volume Report Search

3. Select the search criteria from the drop-down lists.


Table 4-5. Document Volume Report Search Criteria

| Value | Description |
|--------------------|--|
| Start date & time | The date and time the process was initiated. |
| End date & time | The date and time the process was completed. |
| Source Participant | The Participant that initiated the business process (Community Manager only). |
| Target Participant | The Participant that received the business process (Community Manager only). |
| Participant | The initiating or receiving Participant (Participant only). |
| To or From | Designates if the Participant is the receiving (To) or initiating (From) Participant (Participant only). |
| Search on | Search on From document flow or To document flow. |
| Gateway Type | Production or test. Test only available on systems that support the test gateway type. |
| Package | Describes document format, packaging, encryption, and content-type identification. |
| Protocol | Type of process protocol, for example, XML, EDI, flat file. |
| Document Flow | Specific business process. |
| Sort By | Sort results by this criteria (Document Flow or Target Document flow). |
| Results Per Page | Number of records displayed per page. |

4. Click **Search**. The system displays the report.

Exporting the Document Volume Report


To create and save (export) the Document Volume Report:

1. Click **Tools** on the main menu.
2. Click **Document Volume Report** on the horizontal navigation bar. The system displays the Document Volume Report Search screen.
3. Select the search criteria from the drop-down lists.
4. Click **Search**. The system displays the report.
5. Click  to export the report. Navigate to the desired location to save the file.

NOTE: Reports are saved as comma-separated value (.CSV) files. The file name has an “.csv” suffix.

Printing reports

To print the Document Volume Reports:

1. Click **Tools** on the main menu.
2. Click **Document Volume Report** on the horizontal navigation bar. The system displays the Document volume Report Search screen.
3. Select the search criteria from the drop-down lists.
4. Click **Search**. The system displays the report.
5. Click  to print the report.

Test Participant Connection

The Test Participant Connection feature allows you to test the gateway or Web server. If you are the Community Manager, you can also select a specific Participant. The test consists of sending a blank POST request to a gateway or URL. The request is similar to entering the Yahoo's URL (www.yahoo.com) into your browser address field. Nothing is sent; it is an empty request. The response received from the gateway or Web server will indicate its status:

- If a response is returned, the server is up.
- If nothing is returned, the server is down.

IMPORTANT: The Test Participant Connection feature works with HTTP; it does not work with HTTPS.

Test Participant connection

To test a Participant connection:

1. Click **Tools** from the main menu.
2. Click **Test Participant Connection** on the horizontal navigation bar. The system displays the Test Participant Connection screen.

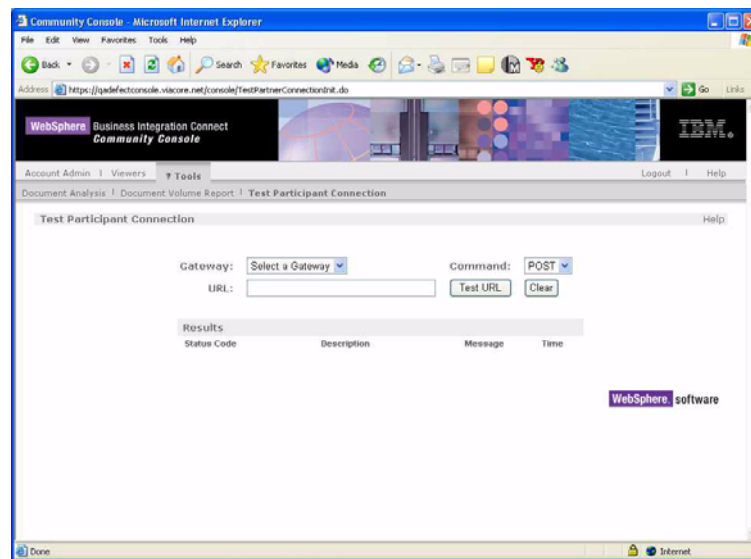


Figure 4-4. Test Participant Connection

3. Select the test criteria from the drop-down lists.

Table 4-6. Test Participant Connection Values

| Value | Description |
|-------------|--|
| Participant | Participant to be tested (Community Manager only). |
| Gateway | Displays available gateways based on the Participant selected above. |
| URL | Dynamically populated based on the Gateway selected above. |
| Command | Post or Get. |

4. Click **Test URL**. The system displays the test results. For information on the status code returned, see the following sections.

Web Server result codes

200 Series:

- 200 - OK - Successful transmission. This is not an error. Here is the file that you requested.
- 201 - Created - The request has been fulfilled and resulted in the creation of a new resource. The newly created resource can be referenced by the URLs returned in the URL-header field of the response, with the most specific URL for the resource given by a Location header field.
- 202 - Accepted - The request has been accepted for processing, but the processing has not yet completed.
- 203 - Non-Authoritative Information - The returned META information in the Entity-Header is not the definitive set as available from the origin server, but is gathered from a local or third-party copy.
- 204 - No Content - The server has fulfilled the request, but there is no new information to send back.
- 206 - Partial Content - You requested a range of bytes in the file, and here they are. This is new in HTTP 1.1

300 Series:

- 301 - Moved Permanently - The requested resource has been assigned a new permanent URL and any future references to this resource should be done using one of the returned URLs.
- 302 - Moved Temporarily - The requested resource resides temporarily under a new URL. Redirection to a new URL. The original page has moved. This is not an error; most browsers invisibly fetch the new page when they see this result.

400 Series:

- 400 - Bad Request - The request could not be understood by the server because it has a malformed syntax. Bad request was made by the client.

- 401 - Unauthorized - The request requires user authentication. The response must include a WWW-Authenticate header field containing a challenge applicable to the requested source. The user asked for a document but did not provide a valid username or password.
- 402 - Payment Required - This code is not currently supported, but is reserved for future use.
- 403 - Forbidden - The server understood the request but is refusing to perform the request because of an unspecified reason. Access is explicitly denied to this document. (This might happen because the web server doesn't have read permission for the file you're requesting.) The server refuses to send you this file. Maybe permission has been explicitly turned off.
- 404 - Not Found - The server has not found anything matching the requested URL. This file doesn't exist. What you get if you give a bad URL to your browser. This can also be sent if the server has been told to protect the document by telling unauthorized people that it doesn't exist. 404 errors are the result of requests for pages which do not exist, and can come from a URL typed incorrectly, a bookmark which points to a file no longer there, search engines looking for a robots.txt (which is used to mark pages you don't want indexed by search engines), people guessing filenames, bad links from your site or other sites, etc.
- 405 - Method Not Allowed - The method specified in the request line is not allowed for the resource identified by the request URL.
- 406 - None Acceptable - The server has found a resource matching the request URL, but not one that satisfies the conditions identified by the Accept and Accept-Encoding request headers.
- 407 - Proxy Authentication Required - This code is reserved for future use. It is similar to 401 (Unauthorized) but indicates that the client must first authenticate itself with a proxy. HTTP 1.0 does not provide a means for proxy authentication.
- 408 - Request Time out - The client did not produce a request within the time the server was prepared to wait.
- 409 - Conflict - The request could not be completed due to a conflict with the current state of the resource.
- 410 - Gone - The requested resource is no longer available at the server and no forwarding address is known.
- 411 - Authorization Refused - The request credentials provided by the client were rejected by the server or insufficient to grant authorization to access the resource.
- 412 - Precondition Failed
- 413 - Request Entity Too Large
- 414 - Request URI Too Large
- 415 - Unsupported Media Type

500 Series:

- 500 - Internal Server Error - The server encountered an unexpected condition that prevented it from fulfilling the request. Something went wrong with the web server and it couldn't give you a meaningful response. There is usually nothing that can be done from the browser end to fix this error; the server administrator will probably need to check the server's error log to see what happened. This is often the error message for a CGI script which has not been properly coded.
- 501 - Method Not Implemented - The server does not support the functionality required to fulfill the request. Application method (either GET or POST) is not implemented.
- 502 - Bad Gateway - The server received an invalid response from the gateway or upstream server it accessed in attempting to fulfill the request.
- 503 - Service Temporarily Unavailable - The server is currently unable to handle the request due to a temporary overloading or maintenance of the server. Server is out of resources.
- 504 - Gateway Time out - The server did not receive a timely response from the gateway or upstream server it accessed in attempting to complete the request.
- 505 - HTTP Version Not Supported

Chapter 5. Community Participant Simulator

This feature, which can be used before and after the Hub Community goes live, simulates production traffic (requests, responses, and acknowledgements) between the Community Manager and a Participant. The Community Manager's administrative user, the Manager Admin, uses this feature to verify that documents are formatted correctly and contain valid business content.

The Community Participant Simulator (CPS) gives the Community Manager the ability to test their backend systems (Document Managers and Receivers) without initiating the test from their own backend applications, and without requiring a Participant to transmit data. As a result, they can test without engaging test systems or technical support personnel.

To initiate the test, the Manager Admin uploads a test document. This feature only accepts RNIF v2.0; it is not compatible with RNIF 1.1. The test document must be a RosettaNet Service Content file; you cannot upload a RNO (RosettaNet Object). Service Content is the primary component of the payload of a RosettaNet Business Message. It is an XML document that represents the business content specified by a particular PIP. The payload also includes any file attachments. WebSphere Business Integration Connect uses the test document to identify routing and processing information.

The CPS does not generate receipt acknowledgements. If a 3A4 confirmation is sent to CPS, the Document Manager closes the exchange with an 0A1.

Note that the installation process creates a sink gateway (that is, a bit bucket), to receive acknowledgements during the testing process:

`http://<hostname>:<port#>/console/sink`

or

`https://<hostname>:<port#>/console/sink`

The following instructions are for the Manager Admin, the Community Manager's administrative user.

Preparing for the test process

Before you start the test process, you must perform the following tasks, which are dependent on the role that you are simulating, a request or response from the Community Manager, or a request or response from a Participant. For more information, see [“Setting up test scenarios” on page 116](#):

- Copy your VTP digital certificate to the file system:
`/opt/data/vcrouter/vms/security/vtp`

You can obtain this certificate from a CA, or it can be self-signed.

Edit the `vtp` values that appear in the `bcg_console.properties` file.

Edit the `bcg.certs.vtp.CertificateDir` location in the `bcg_router.properties` file.

Business Integration Connect automatically loads the VTP digital certificate for every Participant in the database, allowing you to post to any Participant. These certificates are not visible on the console.

- Verify that your gateways and connections are configured and that they are working properly.
- Verify that your targets are enabled and configured with the appropriate URL for incoming messages. Different traffic occurs on different targets. If the target's URLs are not correct, documents will not be processed.

This requirement only applies when you are testing a document that requires a response.

For more information about targets, see the IBM WebSphere Business Integration Connect [Administrator Guide](#).

- Verify the Business IDs that appear in the header of your test document. The Business IDs drive the routing process. They control where the document is sent.

For example, if you are sending your document to yourself, the Community Manager, the "to" Business ID in the document header must be your own Business ID. The system uses the "to" Business ID to find the correct connection.

The following is an example of the "from" and "to" Business IDs in a test document (lines that are not relevant have been removed):

```
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE Preamble SYSTEM "3A4_MS_V02_02_PurchaseOrderRequest.dtd">
<Pip3A4PurchaseOrderRequest>
  <fromRole>
    <GlobalBusinessIdentifier>987654321</GlobalBusinessIdentifier>
  <toRole>
    <GlobalBusinessIdentifier>567890123</GlobalBusinessIdentifier>
```

Setting up test scenarios

You can use the Community Participant Simulator to test the following scenarios between you and your Participants:

Table 5-1. Test scenarios

| Scenario | Destination for Connection | URL |
|---|----------------------------|----------------------------------|
| 1. One way outbound from Community Manager to Participant. Simulating Community Manager. | VTP_Owner | VTP_OWNER |
| 2. One way inbound from Participant to Community Manager. Simulating Participant. | VTP_TP | Not applicable in this scenario. |

Table 5-1. Test scenarios

| Scenario | Destination for Connection | URL |
|--|----------------------------|-----------|
| 3. Two way outbound from Community Manager to Participant (Upload Request). Simulating Community Manager. | VTP_Owner | VTP_OWNER |
| 4. Two way inbound from Participant to Community Manager (Upload Request). Simulating Participant. | VTP_TP | VTP_TP |
| 5. Two way outbound from Community Manager to Participant (Upload Response). Simulating Participant. | VTP_TP | VTP_TP |
| 6. Two way inbound from Participant to Community Manager (Upload Response). Simulating Owner. | VTP_Owner | VTP_Owner |

Uploading and viewing your requests and responses

You must test your system's ability to send requests and responses. You use the same screen, Upload Document, to upload both types of documents.

When you send a request, use the feature's second screen, View Document Flows, to examine the document to verify that it was processed correctly (it is an open document pending response). Examine your internal application to verify that the document was received and processed correctly. Use a text editor to edit the "to" and destination sections of the request to create a response. Then upload the response.

When you send a response, you can also use the View Document Flows screen to examine the document. It is not necessary to edit a response.

The View Document Flows does not show documents that are pending acknowledgment.

Initiate and view document flow

To initiate and view a document flow:

1. Click **Community Participant Simulator** on the main menu. The system displays the Initiate Document Flow, Upload Document screen.

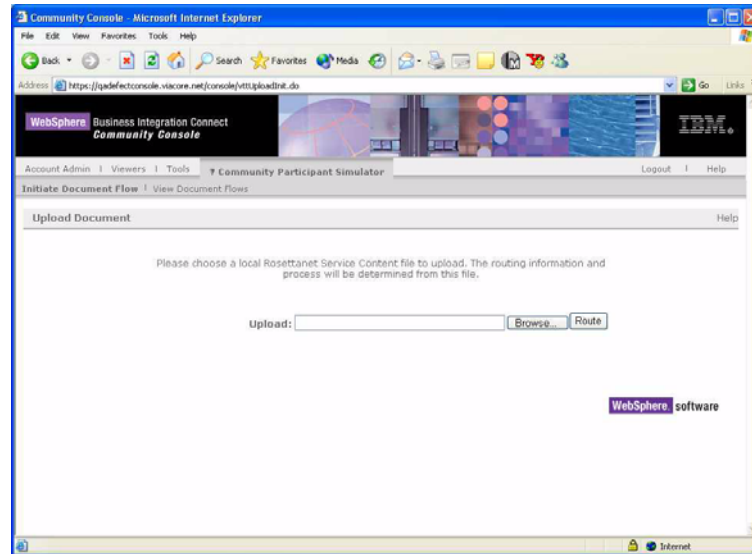




Figure 5-1. Initiate document flow

2. Click **Browse** to locate the RosettaNet Service Content document that you want to upload. The document must be signed with a digital signature.
3. Click **Route** to start the test process. The document is routed through the system to the appropriate destination based on routing information in the document.
 - If the document is successfully routed, the system displays a message with links to the RosettaNet and Document Viewers. Use these links to track the routing progress of the document.
 - If an error occurs during document routing, the system displays an error message that includes a list of system generated events. Use this information to correct errors in the document, then resubmit the document through the CPS.
4. If you are simulating a one-way scenario, the test is complete.

Searching for an open document

To locate an open document:

1. Click **Community Participant Simulator** on the main menu. The system displays the Initiate Document Flow screen.
2. Click **View Document Flows** to view open test message document flows.
3. Click  to view an open document flow. The system displays the Open CPS Document Flow screen.
4. Click  to view the raw document.

Responding to an open document

To respond to an open document:

1. Use a text editor to edit the to and destination sections of the process requiring a response document (change VTP_OWNER to VTP_TP, or change VTP_TP to VTP_OWNER), and make the appropriate changes to the target's URL.

Table 5-2. Test scenarios

| Scenario | Destination for Connection | URL |
|--|----------------------------|-----------|
| 1. Two way outbound from Community Manager to Participant (Upload Request). Simulating Community Manager. | VTP_TP | VTP_TP |
| 2. Two way inbound from Participant to Community Manager (Upload Request). Simulating Participant. | VTP_OWNER | VTP_OWNER |
| 3. Two way outbound from Community Manager to Participant (Upload Response). Simulating Participant. | VTP_OWNER | VTP_OWNER |
| 4. Two way inbound from Participant to Community Manager (Upload Response). Simulating Community Manager. | VTP_TP | VTP_TP |

2. Click **Community Participant Simulator** on the main menu. The system displays the Initiate Document Flow screen.
3. Click **View Document Flows** from the horizontal navigation bar. The system displays a list of documents.
4. Click **Respond** adjacent to the document requiring a response document.
5. Click **Browse** and select the edited document.
6. Click **Route**. The document is routed through the system to the appropriate destination based on routing information in the document.
7. Click **View Document Flows** to view the document.

Removing an open document

To remove an open document:

1. Click **Community Participant Simulator** on the main menu. The system displays the Initiate Document Flow screen.
2. Click **View Document Flows** from the horizontal navigation bar. The system displays a list of documents.
3. Click **Remove** next to the displayed document. The document is deleted from the system.

Glossary

A

Account Admin: The Account Admin module allows you to view and edit the information that identifies your company to the network. This screen is also used to manage console access privileges to other personnel in your organization.

Action: Actions performed on a document by the system to ensure its compatibility with business requirements between Participants.

Action Instance ID: Identifies documents with content that is of a business nature, such as a purchase order or RFQ.

Activation: Connecting a Participant to the system.

Alert: Alerts provide for rapid notification and resolution when pre-established operating limits have been breached. An alert consists of a text based e-mail message sent to individuals or a distribution list of key personnel either within or outside the Network. Alerts can be based on the occurrence of a system event or expected process volume.

Attempt Count: Indicates whether transaction is a first attempt or a retry. 1 is a first attempt. 2 or greater are number of retries.

B

Business Process: A predefined set of transactions that represent the method of performing the work needed to achieve a business objective.

Business Rules Testing: The process of testing and repairing document content errors between Participants.

Business Signal Code: Identifies type of signal (document) sent in response to an action. Examples include receipt or acceptance acknowledgment, or general exception.

C

Participant connection: A participant connection defines the connection between two specific community member's environments by which one unique process is executed.

Choreography: The required order of documents needed to successfully complete a business process.

Classification: Identifies role of Participant in a business process.

Closed: Date and time last document in a process is transacted or a process has been cancelled.

Community Console: The Community Console is a Web based tool used to monitor the flow of your company's business documents to and from your Community Manager or Participants.

Community Manager Child: Community Manager Child is a special Participant type that acts like a Participant in the console but like a Community Manager when routing.

Community Participant: A Hub-community member that exchanges business transactions with the Community Manager.

D

Data Mitigation: The process of testing and repairing errors in document structure and format based on business process standards.

Digital Signature: A digital signature is an electronic signature that is used to authenticate the identity of Participants, and to ensure that the original content of a document that has been sent is unchanged.

Document: A collection of information adhering to an organizational convention. Information can be text, pictures, and sound.

Document Flow Definition: Gives the system all of the necessary information to receive, process, and route documents between community members. Document flow definition types include package, protocol, document flow, activity and action.

Document Protocol: A set of rules and instructions (protocol) for the formatting and transmission of information across a computer network. Examples include RosettaNet, XML, flat file, and EDI.

DUNS: The D&B D-U-N-S Number is a unique nine-digit identification sequence, which provides unique identifiers of single business entities, while linking corporate family structures together. D&B links the D&B D-U-N-S Numbers of parents, subsidiaries, headquarters and branches on more than 64 million corporate family members around the world. Used by the world's most influential standards-setting organizations, it is recognized, recommended and often required by more than 50 global, industry and trade associations, including the United Nations, the U.S. Federal Government, the Australian Government and the European Commission. In today's global economy, the D&B D-U-N-S Number has become the standard for keeping track of the world's businesses.

E

EDI: The computer-to-computer transfer of information in a structured, pre-determined format. Traditionally, the focus of EDI activity has been on the replacement of pre-defined business forms, such as purchase orders and invoices, with similarly defined electronic forms.

Event: A message generated by the system associated with the processing of documents.

F

Filter: To remove data within a sub-transaction based on predefined parameters.

FTP: File Transfer Protocol (FTP), a standard Internet protocol, is the simplest way to exchange files between computers on the Internet.

G

Gateway: A B2B network point that acts as the entrance to another network. Data translation and compatibility issues can be resolved by a gateway to ensure data transfer.

Gateway Type: Identifies documents that are routed to a particular gateway during testing or for live production.

Global: Contact person can be assigned alerts by Participant and Community Manager.

Group: A collection of users given access privilege to the console for performing selected functions.

H

HTTP: The Hypertext Transfer Protocol (HTTP) is the set of rules (protocol) for exchanging files (text, graphic images, sound, video, and other multimedia files) on the Web.

HTTPS: HTTPS (Hypertext Transfer Protocol over Secure Socket Layer) is a Web protocol that encrypts and decrypts user page requests as well as the pages that are returned by the Web server.

I

In Response Business Action: Identifies type of business document sent in response to an action in the same process.

In Response to ID: ID number of In Response Business Action.

Inbound Manager: Retrieves documents from the NAS and prepares them for the appropriate action task by the business process engine.

L

Live: The state at which a Participant has successfully completed business rules testing, and the Community Manager issued a service request to move them to a live status.

P

Packages: Identify document packaging formats that can be received by the system's server. For example, AS1 and AS2.

PIP (Partner Interface Process): Define business processes between Community Managers and Partners (in WebSphere Business Integration Connect, Partners are Participants). Each PIP identifies a specific business document and how it is processed.

Process Instance ID: Unique identification number for a particular business process.

Production: Destination gateway used for routing live documents.

Profile: The Profile module allows you to view and edit the information that identifies your company to the system.

Protocols: Identify specific types of document formats for a variety of business processes. For example, RosettaNet and XML.

Provisioning: Provisioning (or on-boarding) consists of completing a sequence of steps required for connecting a user's B2B gateway to the system infrastructure.

R

Reports: The Reports module allows users to create detailed reports on the volume of documents being processed as well as events generated by the system.

RNIF: The RosettaNet Implementation Framework (RNIF) is a guideline for creating a standard envelope-container for all Partner Interface Processes (PIPs).

RTF: Rich Text Format (RTF) is a file format that lets you exchange text files between different word processors in different operating systems. For example, you can create a file using Microsoft® Word in Windows 98, save it as an RTF file (it will have a .rtf file name suffix), and send it to someone who uses WordPerfect 6.0 on Windows 3.1.

S

Service: Identifies whether message is RosettaNet based.

Servlet: Small program running on the Web server that writes the incoming document to the NAS.

Signal: The document sent in response to an action.

Signal Instance ID: Identifies documents that are positive or negative acknowledgments sent in response to actions.

Signal Version: Version of business process sent as a signal.

SMTP: Simple Mail Transfer Protocol is a protocol used in sending and receiving e-mail.

SR: Service request

SSL: Secure sockets layer is a secure method of sending data using the HTTP protocol.

State: Documents being processed by the system are in one of four states: received, in progress, failed, or successful.

Subscribed contact: A subscribed contact is an individual who has been designated to receive e-mail alerts.

Substitute: To replace data within a sub-transaction with other data based on predefined parameters.

T

Test: The state at which a Participant is undergoing data mitigation or business rules testing during the provisioning process.

Tools: The Tools module allows you to troubleshoot process failure by allowing you to see faulty documents, data fields, and their associated events.

Transaction: A sequence of information exchange and related work that is treated as a unit for the purposes of conducting business between Participants.

Transaction ID: ID number of business process.

Transform: Replace the contents of a document with data from a cross reference table.

Translation: When a document is converted from one protocol to another.

Transport Protocol: A set of rules (protocol) used to send data in the form of message units between computers over the Internet. Examples include HTTP, HTTPS, SMTP, and FTP.

U

URL: A URL (Uniform Resource Locator) is the address of a document or process (resource) accessible on the Internet.

V

Validation: Validation is the act of comparing a process sub-transaction against the specified requirements to determine its validity or invalidity. Content and transaction sequence are typical parameters.

Version: The particular release of a document protocol.

Visibility: Visibility defines if a contact person can be assigned to an alert by a Participant (local) or also by the Community Manager (global).

W

Wildcard: Criteria for wildcard searches includes the asterisk (*).

Index

A

- Account Admin features 23
- Action, definition 5, 37
- Activity, definition 37
- Add contact to existing alert 71
- Addresses
 - create address 65
 - delete 66
 - description 64
 - edit 64
 - values 65
- Administrative group
 - default permissions settings 51
- Administrative users
 - description 10
 - privileges 15
- Alerts
 - add contact to existing alert 71
 - create event-based alert 76
 - create volume-based alert 73
 - description 67
 - disable alert 80
 - remove alert 80
 - search criteria 71
 - search criteria, Participants 71
 - search for alerts 71
 - view or edit alert details and contacts 68
- AS1/AS2 Viewer 96
 - description 87
 - package details 90
 - search criteria 88
 - searching for messages 87
 - viewing message details 89
- Assign
 - group membership 52
 - group permissions 53
 - users to groups 49
- Authentication Required 29

B

- B2B capabilities, description 37
- Business action, definition 5
- Business process, definition 6

C

- Certificates 40
 - description 40
 - disabling 45
 - expiration alert, create 77
 - types and supported formats 41
 - upload certificate 44
 - values 43
 - view 43
 - view certificate details 43
 - view digital certificates 43
- Community Console
 - definition 6
 - display 17
 - non-administrative users, description 12
 - users 09
 - using 21
- Community Manager
 - description 6, 9
 - user, description 12
- Community Operator
 - description 6, 9
 - user, description 12
- Community Participant
 - description 6, 9
 - user, description 12
- Community Participant Simulator
 - description 115
 - initiate and view document flows 118
 - preparing for the test process 115
 - removing an open document 120
 - responding to an open document 119
 - searching for an open document 119
 - setting up test scenarios 116
 - uploading and viewing requests and responses 117
- Company Web site 7
- configuration file
 - FTP 34

- Contacts
 - add to alert 58
 - create contact 62
 - description 56
 - details 57
 - remove contact 63
 - values 52, 56, 57
 - view or edit contact details 56
- Create
 - certificate expiration alert 77
 - Document Volume Report 107
 - event-based alert 76
 - gateways 28
 - new address 65
 - new contact 62
 - new group 54
 - new user 49
 - volume-based alert 73
- Critical event type 83
- Customer Service 7
- D
- Debug events 21, 83
- Decryption
 - definition 40
- Default gateway
 - edit 30
 - select 30
 - view 30
- Default permission settings
 - groups 51
- Delete
 - address 66
 - group 55
- Digital signature certificate, definition 42, 44
- Digital signature, definition 40
- Disable alert 80
- Display console 17
- Document
 - definition 6
 - details, Document Viewer 98
 - processing values, Document Viewer 99
 - searching for 96
- Document Analysis
 - description 104
 - search criteria 105
 - viewing documents 104
 - viewing process and event details 106
- Document flow, definition 37
- Document protocol, definition 6
- Document states
 - definitions 104
 - Document Volume Report 107
- Document Viewer
 - description 96
 - document details 98
 - document processing values 99
 - search criteria 97
 - values 88, 90, 98, 99
- Document Volume Report
 - create 107
 - description 107
 - document states 107
 - exporting 109
 - printing 109
 - search criteria 109
- DUNS numbers 25
- DUNS+4 25
- E
- Edit
 - address 64
 - alert details and contacts 68
 - contact details 56
 - gateway details 27
 - group details 53
 - user details 46
- Enable alert 80
- Encryption
 - certificate, definition 44
 - definition 40
- Error event type 83
- Error fields
 - validation errors 100
- Event types 83
 - descriptions 83

- Event Viewer
 - description 82
 - search criteria 84
 - viewing event details 85
- Events
 - search criteria 84
 - searching for 83
- Exporting
 - Document Volume Report 109
- F
- Features
 - links to 22
- Freeform ID numbers 25
- FTP 31
 - AuthUserFile parameter 34
 - binary file naming convention 32
 - changing account status (ProFTPD) 36
 - changing password (ProFTPD) 36
 - configuration 31
 - creating account 36
 - description 31
 - DirFakeGroup parameter 34
 - DirFakeUser parameter 34
 - group parameter 34
 - Include
 - \$SHARED_STORAGE/ftp/ftp.ipa
 - c1 parameter 34
 - password file, description 35
 - proftpd.conf 34
 - scripts 34, 35
 - server directory structure 32
 - ServerAdmin parameter 34
 - setting up 33
 - setting up using non-ProFTPD servers 34
 - setting up using ProFTPD server 33
 - user parameter 34
- G
- Gateways
 - create 28
 - description 26
 - values 27
 - view list 26
 - view or edit gateway details 27
- Getting Help 7
- Groups 51, 52
 - assigning users to 49
 - create 54
 - default permission settings 51
 - delete 57
 - description 51
 - permissions, view edit assign 53
 - values 52
 - view group memberships 52
 - view or edit group details 53
- H
- Help 7
- HTTP 29
- HTTPS 29
- Hub Admin
 - description 10
 - privileges 15
- Hub-community
 - configurations 10
 - configurations, description 12, 13, 14
 - description 11
- I
- Icons 18
- Information event type 83
- J
- JMS 29
- K
- Key, definition 40
- L
- Links to modules and features 22
- Log in to console 17
- Log out of console 17, 18
- Logout link 18
- M
- Manager Admin
 - description 11
 - privileges 15
- Modules
 - links to 22
- MQ JMS 29

MQ JNDI bindings 29

N

Non-repudiation, definition 40

O

Online Help 7

Operator Admin

description 11

privileges 17

P

Package Details

AS1/AS2 Viewer 90

Package, definition 6, 37

Participant

description 9

Participant Admin

description 11

privileges 15

Participant connection, definition 6

Participant Profile

description 24

editing 24

values 25

viewing 24

Passport Advantage 7

Password for URI 29

Printing reports

Document Volume Report 109

Private key, definition 40

Process, definition 6

ProFTPD 31, 33

Protocol, definition 37

Public key, definition 41

R

Raw documents

viewing 95

Remove

alert 80

contact 63

Result codes

Web Server 111

RosettaNet Viewer

description 92

document processing, details 95

search criteria 93

searching for processes 92

viewing process details 94

RosettaNet, definition 6

S

Search

for alerts 71

for documents 96

for events 83

for messages, AS1/AS2 Viewer 87

for RosettaNet processes 92

Search criteria

alerts 72

AS1/AS2 Viewer 88

Document Analysis 105

Document Viewer 97

Document Volume Report 108

Event Viewer 84

RosettaNet Viewer 93

Self-signed key, definition 41

SMTP 29

Software Support 7

SSL Client certificate, definition 41, 44

T

Target URI 29

Test Participant Connection

description 110

values 111

Web Server result codes 111

Third-party Community Operator

description 12

Tools

description 103

Document Analysis 104

Document Volume Report 107

Test Participant Connection 110

Transport method

required information 29

Transport Protocol Version 29

Typographic conventions 5

U

Upload

- certificate 44

User Name for URI 29

Users

- assign to groups 49
- create new user 49
- description 46
- values 47
- view or edit user details 46

V

Validation errors

- viewing 100

Values

- Addresses 65
- Contacts 52, 56, 57
- Document Viewer 88, 90, 98, 99
- Gateways 27
- Participant Profile 25
- Test Participant Connection 111

View

- alert details and contacts 68
- certificate details 43
- contact details 56
- digital certificates 43
- gateway details 27
- gateway list 26
- group details 53
- group permissions 53
- user details 46

Viewers

- AS1/AS2 Viewer 87
- description 81
- Document Viewer 96
- Event Viewer 82
- RosettaNet Viewer 92

Viewing

- document details 99
- document processing details, RosettaNet Viewer 95
- documents
 - Document Analysis 104
- event details, Event Viewer 85
- events 99
- message details, AS1/AS2 Viewer 89
- process and event details, Document Analysis 106
- Raw documents 95
- raw documents 99
- RosettaNet process details 94
- validation errors 100

VTP digital certificate 115

- definition 42

W

- Warning event type 83
- Web Server result codes 111

X

- X.509 certificate, definition 41

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.

