IBM WebSphere Business Integration Connect Enterprise
and
Advanced Editions

Participant Guide

IBM WebSphere Business Integration Connect Enterprise
and
Advanced Editions

Participant Guide

Notices:

Before using this information and the product it supports, be sure to read the general information under "Notices" on page 61.

29June2004

This edition applies to Version 4, Release 2, Modification 2, 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.

To send us your comments about IBM CrossWorlds documentation, email doc-comments@us.ibm.com. We look forward to hearing from you.

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

Contents

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 provides community participants with all of the information that is necessary to set up the console and to perform day-to-day tasks.

New in this release

This section describes changes made to this guide since its last release (4.2.1).

- This guide has been modified to contain only information that is necessary to administer and maintain the WebSphere Business Integration Connect environment.
- New accessibility features have been added to the Community Console to support screen readers.

Related documents

The complete set of documentation available with this product describes the features and components of WebSphere Business Integration Connect Enterprise and Advanced Editions.

You can download the documentation or read it directly online at the following site:

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

Note: Important information about this product may be available in Technical Support Technotes and Flashes issued after this document was published. These can be found on the WebSphere Business Integration Support Web site:

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

Select the component area of interest and browse the Technotes and Flashes section.

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.
italics	Indicates a variable.
/	In this document, forwardslashes (/) are used as the convention for directory paths. For Windows installations, substitute backslashes (\) for forwardslashes. All WebSphere Business Integration Connect pathnames are relative to the directory where the product is installed on your system.

Terms

The following terms are unique to this product and document processing. Additional terms appear in this guide's "Glossary" on page 53.

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.

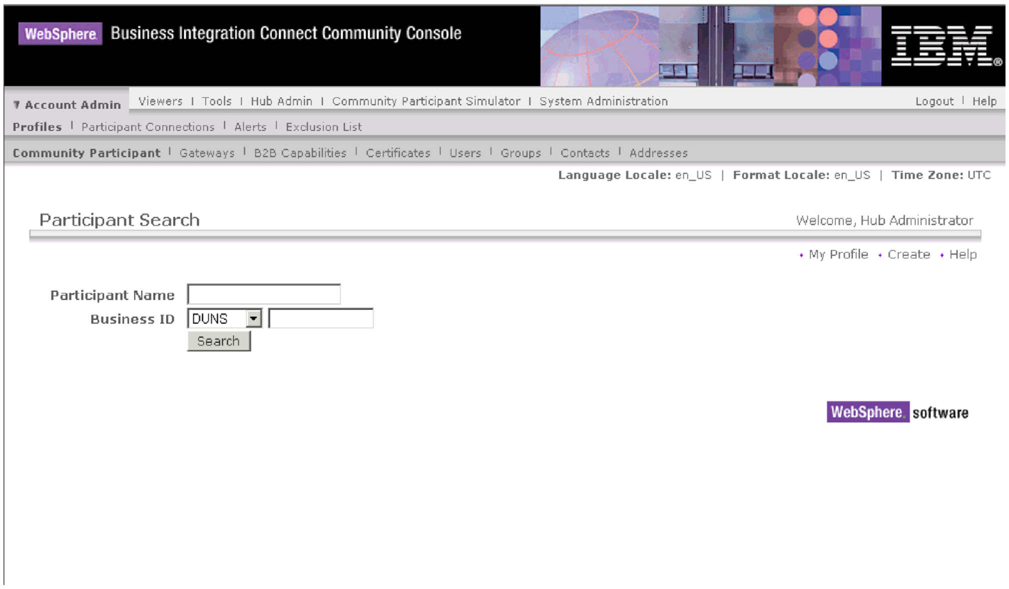
Process: A process is a series of documents or messages executed between Community Managers and participants. Taken as a whole, the documents make up a complete business process.

Getting help

Online Help

Online Help is available on the right side of each screen. See Figure 1.

Note: If you do not see a help window after clicking help, check to make sure you are not running a popup blocker.


WebSphere Business Integration Connect Community Console
IBM
Account Admin | Viewers | Tools | Hub Admin | Community Participant Simulator | System Administration
Logout | Help
Profiles | Participant Connections | Alerts | Exclusion List
Community Participant | Gateways | B2B Capabilities | Certificates | Users | Groups | Contacts | Addresses
My Profile
Create
Help
Search
WebSphere software

Language Locale: en_US | Format Locale: en_US | Time Zone: UTC

Participant Search

Welcome, Hub Administrator

Participant Name

Business ID DUNS

Figure 1. The Community Console

Customer service

Software support:

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

Passport Advantage:

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

Product documentation

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

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.

Participants

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 icons

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

Table 1. Community Console Icons

Icon	Description
Clickable icons	
🔍	Click to view detailed information.
✏	Click to modify a selected item.

Table 1. Community Console Icons (continued)

Icon	Description
✗	Click to delete one or more selected items or to activate the associated inactive item.
📄	Click to display a raw document.
	Click to view validation errors.
▶	Click to continue.
⏸	Click to pause.
🖨	Click to print a document or report.
	Click to export a report.
📅	Click to select calendar dates.
👥	Click to view the groups to which a user belongs.
👤	Click to view users in a group.
	Click to create a new action based on the selected action.
	Click to export information from the system.
✓	Click to deactivate the associated active item.
✎	Click to edit a Document Flow Definition.
	Click to see where an item is used.
	Click to view Document Flow Definition attribute setup.
	Click to upload a new map.
	Click to download a map.
	Click to edit attribute values.
	Click to edit RosettaNet attribute values.
	Click to view a previously sent original document when there is a duplicate document event.
▲	Click to hide search criteria.
🔑	Click to view permissions.
	Roll is not active; click to create role.
Help	Click to view the Help system.
Icons that show information	
*	Indicates that the field requires input from the user.

Table 1. Community Console Icons (continued)

Icon	Description
TPA	Indicates that a Trade Participant Agreement (TPA) has been entered.
⚠	Indicates that a participant or gateway is disabled.
➡	Indicates that document currently in progress.
✓	Indicates that document processing was successful.
✗	Indicates that document processing failed.
🎥	View the transformation maps and connections currently using the action
⇄	Indicates synchronous data flow. No icon is displayed for asynchronous transactions.
📂	Indicates that data is contained.
📁	Indicates that no data is contained.
▢	Indicates that a hierarchical tree is in the "collapsed" view.
📂	Indicates that a hierarchical tree is in the "expanded" view.

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.

Chapter 2. Setting up your Business Integration Connect environment

This section describes the tasks that a Business Integration Connect participant's administrative user, the participant administrator, performs to prepare Business Integration Connect for the participant's users and environment.

To configure Business Integration Connect for your company, the participant administrator must perform the following activities from the Community Console in the order shown below.

1. "Logging in to the Community Console"
2. "Verifying your participant profile" on page 6
3. "Creating a gateway" on page 7
4. "Reviewing B2B capabilities" on page 9
5. "Uploading digital certificates" on page 10
6. "Creating console groups" on page 13
7. "Creating users" on page 14
8. "Creating contact information" on page 15
9. "Creating alerts and adding contacts" on page 16
10. "Creating a new address" on page 21

Logging in to the Community Console

This section provides the steps for displaying and logging into the Community Console. The recommended screen resolution is 1024x768.

Note: WBI Connect Community Console requires cookie support to be turned on to maintain session information. No personal information is stored in the cookie and it expires when the browser is closed.

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

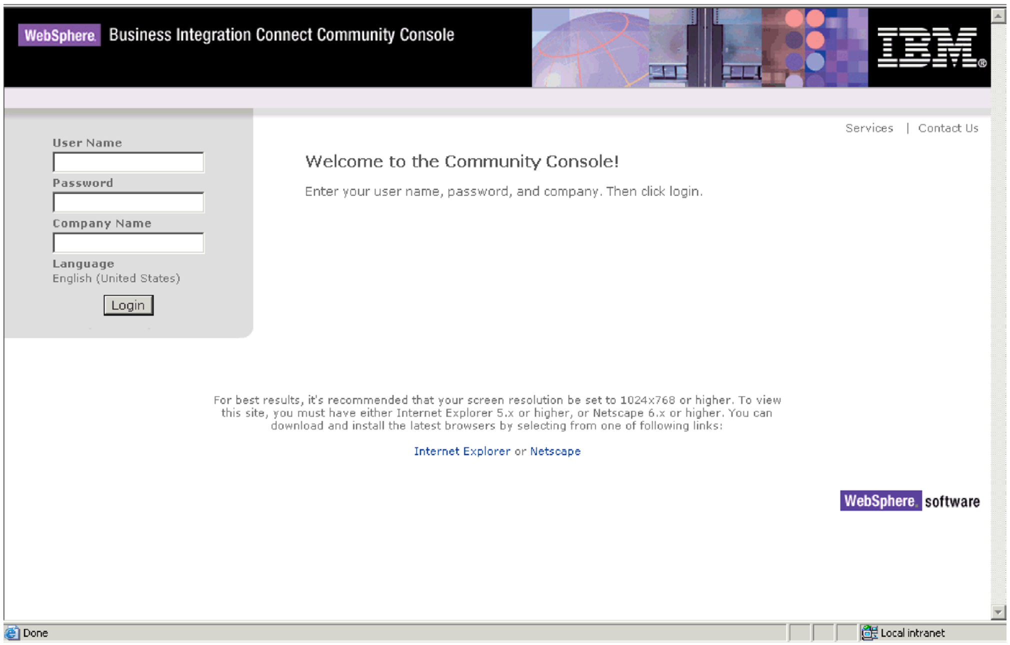
   http://<*hostname*>.<*domain*>:58080/console (unsecure)

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

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

   Note: These URLs assume the default port numbers are used. If you changed the default port numbers, replace the default numbers with the values you specified.

The browser displays the console's login screen. See Figure 2 on page 6.



Welcome to the Community Console!

Enter your user name, password, and company. Then click login.

For best results, it's recommended that your screen resolution be set to 1024x768 or higher. To view this site, you must have either Internet Explorer 5.x or higher, or Netscape 6.x or higher. You can download and install the latest browsers by selecting from one of following links:

Internet Explorer or Netscape

Figure 2. 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.

Verifying 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. Participants can also add and remove Business IDs and IP addresses. IP addresses or host names can be entered for the following Gateway types: Production, Test, CPS Manager, and CPS Participant.

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** > **Profiles** > **Community Participant**.
2. Click ✎ to edit. The system displays the Participant Detail screen.

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

Table 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	Participant Type - Community Participant or Community Manager. Participants can edit this value.
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. • 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 or Host Name	• Gateway Type, for example, CPS Participant. • IP Address or host name of participant.

4. Click **Save**.

Creating a gateway

You must create and maintain a default gateway. If you do not, you cannot create connections. You cannot disable the 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.

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

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.

To create a gateway:

1. Click **Account Admin** > **Profiles** > **Gateways**.
2. Click **Create** in the upper right corner of the screen.
3. Enter a unique name for the gateway.

4. 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.
5. Select Online or Offline. If offline, documents are queued until the gateway is placed online.
6. Enter a description of the gateway.
7. Select the gateway transport method (for example, HTTP 1.1 or SMTP). See Table 3 for transport information examples.

   Note: Users can create their own transport for use during the creation of a user exit gateway.

Table 3. Required information for transport methods

Transport	**HTTP**	**HTTPS**	**FTP**	**FTPS**	**File Directory**	**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 ftp://...	Must match file://...	Must match file://...	Must match mailto:...
User Name for URI	Required if authen.. is required.	Required if authen.. is required.	Required if authent.. is required.	Required if authent.. is required.		Required if authen.. is required.	Required if authen.. is required.
Password for URI	Required if authen.. is required.	Required if authen.. is required.	Required if authen.. is required.	Required if authent.. is required.		Required if authen.. is required.	Required if authen.. is required.
Authen.. Required						Optional	Optional

8. 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.

   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.
9. Enter the Password for the URI (not required for JMS). This is required whenever authentication is required.
10. Select **Yes** or **No** to require authentication. This is often required by JMS or SMTP, If it is required, then username and password will also have to be configured.
11. If you did not select JMS as the transport method, click **Save** now. If JMS is the selected transport, continue to the next step.
12. Enter the other required information for the gateway types choosen.
13. Click **Save**. To add additional gateways, repeat these steps.

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

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.

Reviewing and editing B2B capabilities:

1. Click **Account Admin** > **Profiles** > **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 below Set Source or Set Target tells you that that the capability is not enabled in that role (that is, as the source, target, or both).
   - The Enabled column displays the status of the package: Enabled or Disabled.

   Note: The target, source, or both capability must be set before you can enable it.
2. Set the 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.

3. Set the capability to initiate (**Set Source**), receive (**Set Target**), or initiate and receive for each lower level document flow definition.

4. 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.
   - 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.

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

Uploading digital 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 "Creating alerts and adding contacts" on page 16. 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 can 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. 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 or 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.
- **SSL Server certificate.** Enables SSL server authentication. The CA of the SSL server certificate has to be exchanged among the participants.
- **Encryption certificate (Participants and Community Manager)**. If hub community members encrypt files, the public key portion of encrytion certificate has to be sent to the hub community members. The corresponding private key part of the encryption certificate must be uploaded to the hub operator level through the console. You must upload the the public part of the participant's 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 hub community members sign the documents, the public part of the signing certificate must be uploaded to the hub at the participant level as a signature certificate. If the hub-manager has to sign the documents it is sending to hub community members, you must send the public part of the hub mamanger's certificate to the hub community members. The hub's signature certificate has to be uploaded through console for the Hub Operator.
- **VTP certificate (Community Manager)**. This certificate is used by Business Integration Connect's Document Manager for the Community Participant Simulator feature. 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.

SSL server and 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.

Loading and defining a digital certificate

1. Click **Account Admin** > **Profiles** > **Certificates**. The system displays the Certificate List screen.
2. Click **Load Certificate** in the upper right corner of the screen. The system displays the Create New Certificate screen.
3. 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.
4. Enter a unique name (Description) for the certificate in the Certificate Name text box.
5. Select Enabled or Disabled.
6. Click **Browse** and navigate to the digital certificate.
7. Select the Gateway Type, for example, CPS Participant (SSL certificates only). This feature allows you to select a certificate based on destination.
8. Click **Upload**.

Creating console groups

Use the Group 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 system automatically creates the Administrator and Default groups with default permission settings. Default permission settings can be overridden by the Hub Admin and participant Admin.

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

To create groups:

1. Click **Account Admin** > **Profiles** > **Groups**. The system displays the Group List screen.

2. Click **Create** in the upper right corner of the screen. The system displays the Group Detail screen.
3. Enter the new group's **Name** and **Description.**
4. Click **Save**. To add additional groups, repeat these steps.

Creating users

Use this feature to create 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.

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.

1. Click **Account Admin** > **Profiles** > **Users**. The system displays the User List screen.
2. Click **Create** in upper right corner of the screen. The system displays the User Detail screen.
3. Enter the user name (login name for the user).
4. Select if you want to Enable or Disable console access for this user.
5. Enter the user's name (Given Name and Family Name.)
6. Enter the e-mail address that the system will use to send alert notifications to the user.
7. Enter the user's telephone and fax numbers.
8. 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.
9. Select if the user is only visible to your organization (Local), or visible to the entire hub community (Global).
10. 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.
11. Click **Save**. Repeat these steps to add additional users.

Adding users to groups

1. Click **Account Admin** > **Profiles** > **Users**. The system displays the User List screen.

2. Click 🔍 to view the target user’s group membership details.
3. Click ✏ to edit the user’s group memberships.
4. Select a group and click the **Add to Group** or **Remove from Group** button to add or remove a user from a group.
5. Click ✔ when you finish editing.

Creating contact information

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.

To create new contacts:

1. Click **Account Admin** > **Profiles** > **Contacts**. The system displays a list of current contacts.
2. Click **Create** in the upper right corner of the screen. The system displays the Contact Detail screen.
3. Enter the contact’s name in the name text boxes.
4. Enter the contact’s address in the address text box.
5. Select the Contact type from the drop-down list (for example, B2B Lead or Business Lead).
6. Enter the contact’s e-mail address.
7. Enter the contact’s telephone and fax number.
8. Select the contact’s alert status. When enabled, this contact receives all subscribed alerts.
9. Subscribed is system populated.
10. 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.
11. 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 new contact to an existing alert” on page 20.

    To create a volume-based alert and add contacts to the alert, see “Creating a volume-based alert” on page 17.

    To create an event-based alert and add contacts to the alert, see “Creating an event-based alert” on page 19.

Creating alerts and adding contacts

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 108001 Not a Certificate.

Note: The Community participant can only create a volume-based alert on the volume of documents sent to the Community Manager. For the participant to set up a volume-based alert on the volume of documents sent from the Community Manager to the participant, the participant would request the Community Operator to set up a volume-based alert on the participant's behalf, specifying the participant as the alert owner.

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.

Creating a volume-based alert

1. Click **Account Admin** > **Alerts**. The system displays the Alert Search screen.
2. Click **Create** in the upper right corner of the screen. The system displays the Alerts Define tab.
3. Select **Volume Alert** for Alert Type (this is the default setting). The system displays the appropriate text boxes for a volume alert.
4. Enter a name for the alert in the text box.
5. Select a participant with rights to create a volume-based alert (Community Manager and Community Operator only).
6. 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.
7. Select one of three volume options (Expected, Range, or Zero Volume), then proceed to 8 on page 17:
   - **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 8. 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 then 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 8. 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 8.

        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 8.
8. 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.

9. 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.
10. 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.
11. Select the status of this alert: Enabled or Disabled.
12. Click **Save**.
13. Click the **Notify** tab.
14. Click ✎ .
15. Select a participant (Community Manager and Community Operator only).
16. If the contact that you want to add is listed in the Contacts text box, select the contact and click **Subscribe**. Go to 21.

    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.
17. Enter the contact's name, e-mail address, telephone and fax numbers.
18. 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.
19. 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.
20. Click **Save** to save the contact; click **Save & Subscribe** to add the contact to the list of contacts for this alert.
21. Click **Save**.

    Note: Changes made to volume-based alerts, after the original monitoring period, become effective on the next monitoring period day. For example, an alert monitors from 1-3 PM on Wednesdays and Thursdays. On Wednesday at 4 PM, the alert is changed to monitor from 5-7 PM. The alert will not monitor twice on Wednesday; the change will become effective on Thursday.

Creating an event-based alert

1. Click **Account Admin** > **Alerts**. The system displays the Alert Search screen.
2. Click **Create** in the upper right corner of the screen. The system displays the Alerts Define tab.
3. Select **Event Alert** for Alert Type. The system displays the appropriate text boxes for an event-based alert.
4. Enter a name for the alert in the text box.
5. 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.
6. Select the event type: Debug, Information, Warning, Error, Critical, or All.
7. Select the event that will activate the alert, for example, BCG240601 AS Retry Failure, or 108001 Not a Certificate. To create an alert that notifies you when a certificate is about to expire, select one of the following:
   - BCG108005 Certificate Expiration in 60 Days
   - BCG108006 Certificate Expiration in 30 Days
   - BCG108007 Certificate Expiration in 15 Days
   - BCG108008 Certificate Expiration in 7 Days
   - BCG108009 Certificate Expiration in 2 Days
8. Select the status of this alert: Enabled or Disabled.
9. Click **Save**.
10. Click the **Notify** tab.
11. Click ✎.
12. Select a participant (Community Manager and Community Operator only).
13. If the contact that you want to add is listed in the Contacts text box, select the contact and click **Subscribe**. Go to 18.

    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.
14. Enter the contact's name, e-mail address, telephone and fax numbers.
15. 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.
16. 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.

17. 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.
18. 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.
19. Click **Save**.

Adding a new contact to an existing alert

1. Click **Account Admin** > **Alerts**. The system displays the Alert Search screen.
2. Enter the search criteria from the drop-down lists; enter the Alert Name.
3. Click **Search**. The system displays a list of alerts that meet your search criteria, if any.
4. Click 🔍 to view alert details.
5. Click ✎ to edit alert details.

6. Click the **Notify** tab.
7. Select a participant (Community Manager and Community Operator only).
8. If the contact that you want to add is listed in the Contacts text box, select the contact and click **Subscribe**. Go to 13.

   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.
9. Enter the contact's name, e-mail address, telephone and fax numbers.
10. 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.
11. 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.
12. 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.
13. Click **Save.**

Creating a new address

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

To create a new address:

1. Click **Account Admin** > **Profiles** > **Addresses**. The system displays the Addresses screen.
2. Click **Create New Address** in the upper right corner of the screen. The system displays the Addresses screen.
3. Select the Address Type from the drop-down list (Billing, Corporate, or Technical).
4. Enter the address in the appropriate text boxes.
5. Click **Save**.

Chapter 3. 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, 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 4. Account Admin features

What feature do you want to use?
“Managing gateways”
“Managing Certificates” on page 24
“Managing groups” on page 25
“Managing users” on page 26
“Managing contacts” on page 27
“Managing alerts” on page 28
“Managing addresses” on page 30

Managing gateways

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

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

Viewing a list of gateways

Click **Account Admin** > **Profiles** > **Gateways** to view a list of gateways in the system.

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** > **Profiles** >**Gateways**. The system displays the Gateway List screen.
2. Click 🔍 to view gateways details.

3. Click ✎ to edit gateway details.
4. Edit information as required. The following table describes gateway values.

Table 5. Values on the gateway screen

Value	Description
Gateway Name	Name of gateway. Note: Gateway Name is a user-defined free format field. While uniqueness is not required, users should use different names for individual gateways to avoid potential confusion.
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.

5. Click **Save**.

View, select, or edit your default gateways

1. Click **Account Admin** > **Profiles** > **Gateways**. The system displays the Gateway List screen.
2. Click **View Default Gateways** in the upper right corner of the screen. The system displays the Default Gateway List screen.
3. Use the drop-down lists to select or change one or more default gateways.
4. Click **Save**.

Managing Certificates

This section provides the steps for viewing , editing, and deleting digital certicates using the Community Console.

Viewing and editing digital certificate details

1. Click **Account Admin** > **Profiles** > **Certificates**. The system displays a list of existing digital certificates.
2. Click 🔍 to view certificate details. The system displays the Certificate Details screen.
3. Click ✎ to edit the certificate.
4. Edit as required.
5. Click **Save**.

Disabling a digital certificate

1. Click **Account Admin** > **Profiles** > **Certificates**. The system displays the Certificate List screen.
2. Click 🔍 to view certificate details. The system displays the Certificate Details screen.
3. Click ✎ to edit the certificate.
4. Click **Disabled**.

5. Click **Save**.

Managing groups

You can view, edit, and delete groups using the Community Console.

Viewing group memberships and assigning users to groups

1. Click **Account Admin** > **Profiles** > **Groups**. The system displays the Group List screen.

Table 6. Values on the Group List screen

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

2. 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.
3. Click ✎ to edit users in a group.
4. Click the **Add to Group** button to assign users to the group.
5. Click ⊘ to save and exit.

Viewing, editing, or assigning group permissions

1. Click **Account Admin** > **Profiles** > **Groups**. The system displays the Group List screen.
2. Click 🔑 to view a group's permissions. The system displays a list of the selected group's permissions.
3. Select **No Access**, **Read Only,** or **Read/Write** for each feature.
4. Click **Save**.

Viewing or editing group details

1. Click **Account Admin** > **Profiles** > **Groups**. The system displays the Group List screen.
2. Click 🔍 to view group details (Name and Description). The system displays the Group Detail screen.
3. Click ✎ to edit group details (you cannot edit system generated groups).
4. Edit as required.
5. 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.

Deleting a group

1. Click **Account Admin** > **Profiles** > **Groups**. The system displays the Group List screen.
2. Click 🔍 to view group details. The system displays the Group Details screen.

3. Click ✎ to edit group details.
4. Click **Delete**. Confirm that you want to delete.

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

Managing users

Use this feature to view and edit user profiles.

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

1. Click **Account Admin** > **Profiles** > **Users**. The system displays the User List screen.

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

Table 7. 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.

2. Click 🔍 to view a user's details.
3. Click ✎ to edit a user's details.
4. Edit information as required. The following table describes the values on the User Details screen.

Table 8. 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.
Language Locale	Select the geographic area of the user. Will default to the locale set by the hub administrator.
Format Locale	Select the country of the user. Will default to the locale set by the hub administrator.
Time Zone	Select the time zone of the user. Will default to the time zone set by the hub administrator.
Alert Status	When enabled, this user will receive all subscribed alerts. Select Disable to stop this user from receiving all alerts.
Subscribed	This value is system populated.
Visibility	Select Local to have user visible only within your organization. Select Global to have user visible by your organization and the manager.

Note: The default system locale and time zone after installation and startup is English (United States) at UTC. The system uses UTC for its time zone calculations the UTC default cannot be changed at the system level. However, all users can change the time zone that is displayed within the community console.

Once the *Hubadmin* user logs into the system for the first time, it will pickup the system locale and time zone (English, UTC). Since the Hubadmin user is the super-user responsible for system configuration, the community console locale and time zone selected by the Hubadmin user will become the new default for all community console users. Individual users also have the option of changing their locale and time zone as needed.

5. Click **Save**.

Managing contacts

Use the Contacts feature to view and edit contact information for key personnel.

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.

Viewing or editing contact details

1. Click **Account Admin** > **Profiles** > **Contacts**. The system displays a list of current contacts.

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

Table 9. 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.
Visibility	• 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.

2. Click 🔍 to view contact details. The system displays the Contact Detail screen.
3. Click ✎ to edit contact details.

4. Edit information as required. The following table describes contact values.

Table 10. 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	• 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.

5. Click **Save**.

Removing a contact

1. Click **Account Admin** > **Profiles** > **Contacts**. The system displays a list of current contacts.
2. Click ✗ to delete appropriate contact.

Managing alerts

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.

Viewing or editing alert details and contacts

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

1. Click **Account Admin** > **Alerts**. The system displays the Alert Search screen.
2. 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).
3. Click **Search**. The system displays the Alert Search Results screen.
4. Click 🔍 to view an alert’s details.
5. Click ✎ to edit alert details.
6. Edit information as required.
7. Click the **Notify** tab.
8. Select a participant (Community Manager or Community Operator only). The Community Manager can view all alerts regardless of the Alert Owner.

9. Edit contacts for this alert, if desired.
10. Click **Save**.

Searching for alerts

1. Click **Account Admin** > **Alerts**. The system displays the Alert Search screen.
2. 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 11. 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 12. 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.

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

Disabling or enabling an alert

1. Click **Account Admin** > **Alerts**. The system displays the Alert Search screen.
2. Select the search criteria from the drop-down lists; enter the Alert Name.
3. Click **Search**. The system displays a list of alerts that meet your search criteria, if any.
4. 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

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

Managing addresses

Use this feature to manage the addresses in your participant profile.

Editing an address

1. Click **Account Admin** > **Profiles** > **Addresses**. The system displays the Addresses screen.
2. Locate the address that you want to edit, and click ✎.
3. Make the required changes. The following table describes the address values.

Table 13. Address values

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

4. Click **Save**.

Deleting an address

1. Click **Account Admin** > **Profiles** > **Addresses**. The system displays the Addresses screen.
2. Locate the address that you want to delete and click ✗ .
3. Verify that you want to delete the address.

Chapter 4. Viewing events and documents: Viewers

The Viewers module includes the following features:

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

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 ID.

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 14. Viewers

What feature do you want to use?	See
Event Viewer	page 32
RosettaNet Viewer	page 37
AS1/AS2 Viewer	page 39
Document Viewer	page 39

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 15. 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 16. Event Viewer tasks

What do you want to do?	See
Search for events.	page 33
View event details.	page 34

Searching for events

1. Click **Viewers** > **Event Viewer**.

   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

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

Table 17. 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.
Ascend or Descend	Sort in ascending or descending order.
Results per page	Number of records displayed per page.
Refresh	Default setting is Off. 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).

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

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

1. Click **Viewers** > **Event Viewer**.
2. Select the search criteria from the drop-down lists.
3. Click **Search**. The system displays a list of events.
4. Click 🔍 next to the event you want to view. The system displays event details and associated documents.
5. Click 🔍 next to the document that you want to view, if one exists.
6. Click 📄 to view the raw document, if one exists.
7. 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 18. AS1/AS2 Viewer tasks

What do you want to do?	See
Search for messages	page 37
Viewing raw documents	page 39

Searching for messages

1. Click **Viewers** > **AS1/AS2 Viewer**. The system displays the AS1/AS2 Viewer screen.

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

Table 19. 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.
Participant	Identifies the participant (Community Manager only).
My role is the	Specifies if the participant is the source (initiating) or the target (receiving).
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 of 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.
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 and Message Disposition Notification (MDN).
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.

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

Viewing message details

1. Click **Viewers** > **AS1/AS2 Viewer**. The system displays the AS1/AS2 Viewer screen.
2. Select the search criteria from the drop-down lists.
3. Click **Search**. The system displays a list of messages.
4. Click 🔍 next to the message that you want to view. The system displays the message and the associated document details.

Table 20. 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.
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	This text provides the status of the originating message that was received (either successful or failed). Examples include the following: • Automatic-=action/MDN-sent-automatically; processed. • Automatic-action/MDN-sent-automatically;processed/Warning;duplicate-document. • Automatic-action/MDN-sent-automatically;processed/Error;description-failed. • Automatic-action/MDN-sent-automatically;failed:unsupported MIC-algorithms.

5. (Optional) 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 21. RosettaNet Viewer tasks

What do you want to do?	See
Search for RosettaNet processes.	page 37
View RosettaNet process details.	page 38
View raw documents.	page 39

Searching for RosettaNet processes

1. Click **Viewers** > **RosettaNet Viewer**. The system displays the RosettaNet Viewer Search screen.

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

Table 22. 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.
Participant	Identifies the participant (Community Manager only).
My role is the	Specifies if the participant is the source (initiating) or the target (receiving).
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.
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.

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

Viewing RosettaNet process details

1. Click **Viewers** > **RosettaNet Viewer**. The system displays the RosettaNet Viewer Search screen.
2. Select the search criteria from the drop-down lists.
3. Click **Search**. The system displays the results of your search.

Table 23. 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.

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

Viewing raw documents

1. Click **Viewers** > **RosettaNet Viewer**. The system displays the RosettaNet Viewer Search screen.
2. Select the search criteria from the drop-down lists.
3. Click **Search**. The system displays a list of processes.
4. Click 🔍 next to the process that you want to view. The system displays process details and associated documents for the selected process.
5. 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 41.
- 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.

When viewing cXML document details, all documents related to the selected request or response are displayed under the Associated Documents header. The magnifying glass icon will be missing from the first document. It represents the document that is currently being viewed in the details above.

Table 24. Document Viewer tasks

What do you want to do?	See
Searching for documents	page 33
Viewing document details, events, and raw document	page 40
Viewing data validation errors	page 41
Using the Stop Process feature	page 42

Searching for documents

1. Click **Viewers** > **Document Viewer**. The system displays the Document Viewer Search screen.

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

Table 25. 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.
Participant	Identifies the participant (Community Manager only).
My role is the	Specifies if the participant is the source (initiating) or the target (receiving).
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. You can choose In Progress, Successful, or Failed. The default is 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.
Reference ID	ID number created by the system for tracking document status.
Source IP Address	IP address of the source participant.
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 and acknowledgement or request and response.
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.

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

Table 26. 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 and acknowledgement or request and response.

Viewing document details, events, and raw document

1. Click **Viewers** > **Document Viewer**. The system displays the Document Viewer Search screen.
2. Select the search criteria from the drop-down lists.

3. 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 the blue arrow icon 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 27. 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.
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 the blue arrow icon next to the Duplicate Document event, then selecting 📋 .

Tip: To troubleshoot documents that have failed processing, see "Viewing data validation errors" on page 41.

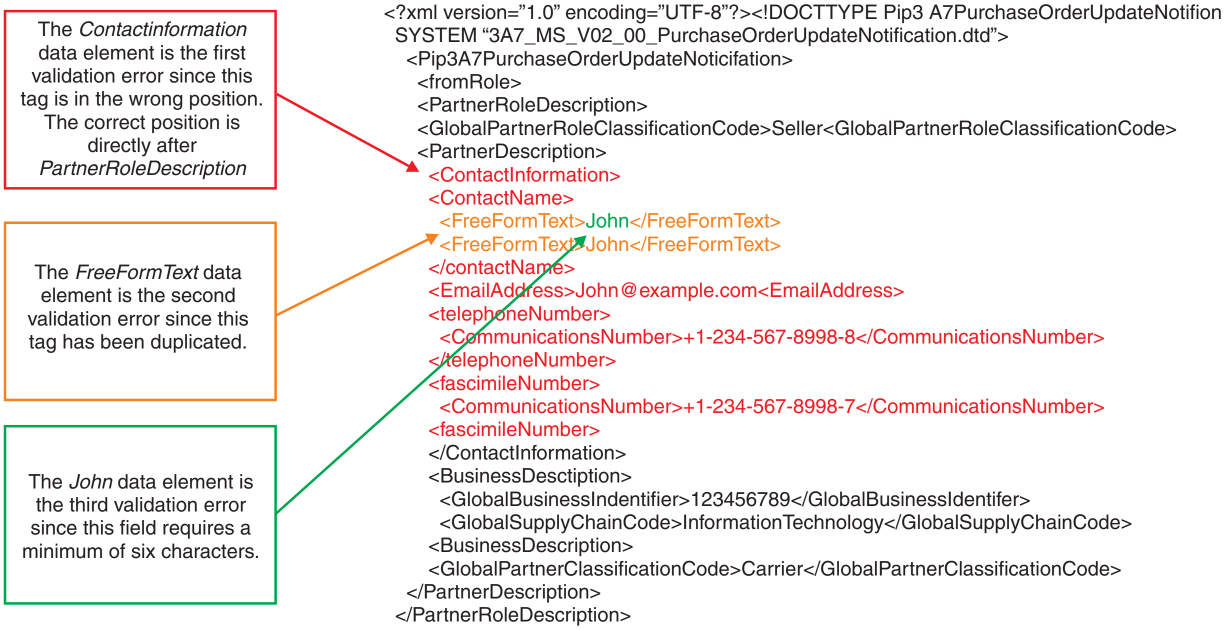
Viewing data validation errors

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 28. 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:



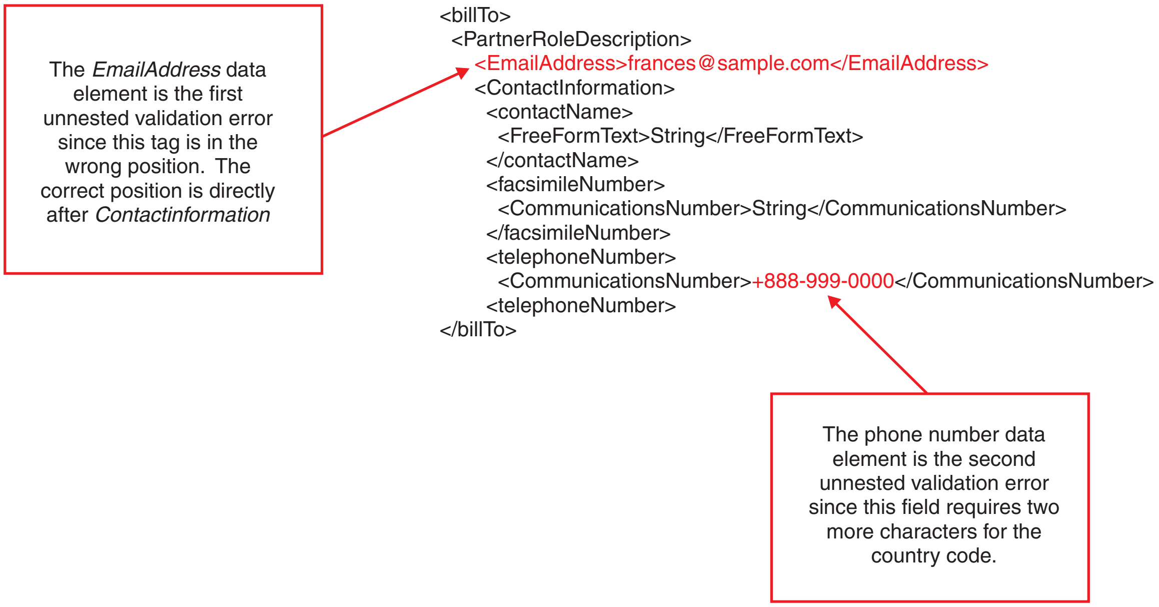
The *Contactinformation* data element is the first validation error since this tag is in the wrong position. The correct position is directly after *PartnerRoleDescription*

The *FreeFormText* data element is the second validation error since this tag has been duplicated.

The *John* data element is the third validation error since this field requires a minimum of six characters.

```
<?xml version=”1.0” encoding=”UTF-8”?><!DOCTTYPE Pip3 A7PurchaseOrderUpdateNotifion
 SYSTEM “3A7_MS_V02_00_PurchaseOrderUpdateNotification.dtd”>
  <Pip3A7PurchaseOrderUpdateNoticifation>
   <fromRole>
   <PartnerRoleDescription>
   <GlobalPartnerRoleClassificationCode>Seller<GlobalPartnerRoleClassificationCode>
   <PartnerDescription>
    <ContactInformation>
    <ContactName>
     <FreeFormText>John</FreeFormText>
     <FreeFormText>John</FreeFormText>
    </contactName>
    <EmailAddress>John@example.com<EmailAddress>
    <telephoneNumber>
     <CommunicationsNumber>+1-234-567-8998-8</CommunicationsNumber>
    </telephoneNumber>
    <fascimileNumber>
     <CommunicationsNumber>+1-234-567-8998-7</CommunicationsNumber>
    <fascimileNumber>
    </ContactInformation>
    <BusinessDesctiption>
     <GlobalBusinessIndentifier>123456789</GlobalBusinessIdentifer>
     <GlobalSupplyChainCode>InformationTechnology</GlobalSupplyChainCode>
    <BusinessDescription>
    <GlobalPartnerClassificationCode>Carrier</GlobalPartnerClassificationCode>
  </PartnerDescription>
 </PartnerRoleDescription>
```

Example of non-nested XML validation errors:



The *EmailAddress* data element is the first unnested validation error since this tag is in the wrong position. The correct position is directly after *Contactinformation*

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

The phone number data element is the second unnested validation error since this field requires two more characters for the country code.

To view validation errors in a raw document, see “Viewing raw documents” on page 39.

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

Using the Stop Process feature

Click **Stop Process** to fail a document currently in progress. This feature is only available to hub admin users.

Note: It may take up to one hour for the system to fail the document. During this time, the Document Viewer will continue to display the document status as in progress.

Chapter 5. 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 29. Tools

What feature do you want to use?	See
Document Analysis	page 45
Document Volume Report	page 47
Test Participant Connection	page 48

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 30. Document States

State	Description
Received	The document has been received by the system and is waiting for processing.
In Progress	The document is currently in one of the following processing steps: • **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

1. Click **Tools** > **Document Analysis**. The system displays the Document Analysis Search screen.
2. Select the search criteria from the drop-down lists.

Table 31. 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).
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.
Refresh	Controls if the search results are refreshed periodically (Community Manager only).
Refresh Rate	Controls how often search results are refreshed (Community Manager only).

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

Viewing process and event details

1. Click **Tools** > **Document Analysis**. The system displays the Document Analysis Search screen.

2. Select the search criteria from the drop-down lists.
3. Click **Search**. The system displays the Document Analysis Summary.
4. 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.
5. 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 32. 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.

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

1. Click **Tools** > **Document Volume Report**. The system displays the Document Volume Report Search screen.

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

Table 33. 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).
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.

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

Exporting the Document Volume Report

1. Click **Tools** > **Document Volume Report**. The system displays the Document Volume Report Search screen.
2. Select the search criteria from the drop-down lists.
3. Click **Search**. The system displays the report.
4. 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

1. Click **Tools** > **Document Volume Report**. The system displays the Document Volume Report Search screen.
2. Select the search criteria from the drop-down lists.
3. Click **Search**. The system displays the report.
4. 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 that does not require any connection parameters.

To test a participant connection:

1. Click **Tools > Test Participant Connection**. The system displays the Test Participant Connection screen.
2. Select the test criteria from the drop-down lists.

Table 34. 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.

3. 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 filling 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

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. (1) Documents being processed by the system are in one of four states (2) 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

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 necessarily 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 may contain 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 may contain 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.

Websphere Business Integration Connect contains code named ICU4J which is licensed to you by IBM under the terms of the International Program License Agreement, subject to its Excluded Components terms. However, IBM is required to provide the following language to you as a notice:

COPYRIGHT AND PERMISSION NOTICE

Programming interface information

Programming interface information, if provided, 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 or registered trademarks of International Business Machines Corporation in the United States or other countries, or both:

IBM
the IBM logo
AIX
CrossWorlds
DB2
DB2 Universal Database
Domino
Lotus
Lotus Notes
MQIntegrator

MQSeries
Tivoli
WebSphere

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

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

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.

WebSphere Business Integration Connect Enterprise and Advanced Editions Version 4.2.2.

Printed in USA