

IBM WebSphere Partner Gateway Enterprise and
Advanced Editions



Participant Guide

Version 6.0

IBM WebSphere Partner Gateway Enterprise and
Advanced Editions



Participant Guide

Version 6.0

Note!

Before using this information and the product it supports, read the information in "Notices" on page 67.

28June2005

This edition applies to Version 6, Release 0, Modification 0, of IBM^(TM)® WebSphere^(TM)® Partner Gateway Advanced Edition (5724-L68) and Enterprise Edition (5724-L69), and to all subsequent releases and modifications until otherwise indicated in new editions.

To send us your comments about this document, 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.

© Copyright International Business Machines Corporation 2004, 2005. All rights reserved.

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

Contents

About this book.	vii
Audience	vii
Typographic conventions	vii
Related documents	viii
New in this release.	ix
New in release 6.0	ix
New in release 4.2.2.	ix
Chapter 1. Introduction	1
Hub community	1
Community Operator	1
Community Manager	1
Participants	1
Community Console icons	1
Using the Community Console	3
Chapter 2. Setting up your WebSphere Partner Gateway environment	5
Logging in to the Community Console	5
Verifying your participant profile	6
Viewing and editing your participant profile.	6
Creating a gateway	7
Reviewing B2B capabilities	7
Uploading digital certificates	8
Certificate terms	9
Certificate types and supported formats	10
SSL server and client authentication	11
Loading and defining a digital certificate	11
Creating console groups	12
Creating users	12
Creating a new user	12
Adding users to groups	13
Creating contact information	13
Creating alerts and adding contacts	14
Creating a volume-based alert	15
Creating an event-based alert	17
Adding a new contact to an existing alert	19
Creating a new address	20
Chapter 3. Creating gateways	21
Overview	21
Setting up an HTTP gateway	21
Gateway Details	22
Gateway configuration	22
Setting up an HTTPS gateway	23
Gateway Details	23
Gateway Configuration	23
Setting up an FTP gateway	24
Gateway Details	24
Gateway Configuration	24
Setting up an SMTP gateway	25
Gateway Details	25
Gateway Configuration	25
Setting up a JMS gateway	26

Gateway Details	26
Gateway Configuration	26
Setting up a file-directory gateway	27
Gateway Details	27
Gateway Configuration	27
Setting up an FTPS gateway	28
Gateway Details	28
Gateway Configuration	28
Setting up an FTP Scripting gateway	29
Creating the FTP script	29
FTP script commands	29
FTP Scripting gateways	30
Gateway Details	30
Gateway Configuration	30
User-defined Attributes	31
Schedule	31
Configuring handlers	32
Specifying a default gateway	32

Chapter 4. Managing community connections and users: Account Admin 33

Managing gateways	33
Viewing a list of gateways	33
Viewing or editing gateway details	33
View, select, or edit your default gateways	34
Managing Certificates	34
Viewing and editing digital certificate details	34
Disabling a digital certificate	34
Managing groups	35
Viewing group memberships and assigning users to groups	35
Viewing, editing, or assigning group permissions.	35
Viewing or editing group details	35
Deleting a group	35
Managing users	36
Managing contacts	37
Viewing or editing contact details	37
Removing a contact.	38
Managing alerts	38
Viewing or editing alert details and contacts	38
Searching for alerts	39
Disabling or enabling an alert	39
Removing an alert	39
Managing addresses	39
Editing an address	40
Deleting an address	40

Chapter 5. Viewing events and documents: Viewers 41

Event Viewer	41
Event types	42
Performing Event Viewer tasks	42
Searching for events	42
Viewing event details	43
AS1/AS2 Viewer	43
Performing AS1/AS2 Viewer tasks	44
Searching for messages	44
Viewing message details	45
RosettaNet Viewer	46
Performing RosettaNet Viewer tasks	46
Searching for RosettaNet processes	47
Viewing RosettaNet process details	47
Viewing raw documents	48

Document Viewer	48
Searching for documents	48
Viewing document details, events, and raw document	49
Viewing data validation errors	50
Using the Stop Process feature	52
Gateway Queue	52
Viewing the gateway list	52
Viewing queued documents	53
Removing documents from the delivery queue	54
Viewing gateway details	54
Changing gateway status	54
Chapter 6. Analyzing document flow: Tools	55
Document Analysis	55
Document States	56
Viewing documents in the system	56
Viewing process and event details	57
Document Volume Report	57
Create a Document Volume Report	57
Exporting the Document Volume Report	58
Printing reports	58
Test Participant Connection	58
Web Server result codes	59
Glossary	63
Notices	67
Programming interface information	69
Trademarks and service marks	69
Index	71

About this book

IBM WebSphere Partner Gateway 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.

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.

Audience

The parties involved in an IBM WebSphere Partner Gateway trading or hub community are the Community Manager, Community Operator (also referred to as Hub Admin), 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.

Typographic conventions

This document uses the following typographic conventions:

Convention	Description
Monospace font	Text in this font indicates text that you type, values for arguments or command options, examples and code examples, or information that the system prints on the screen (message text or prompts).
bold	Boldface text indicates graphical user interface controls (for example, online button names, menu names, or menu options) and column headings in tables and text.
<i>Italics</i>	Text in italics indicates emphasis, book titles, new terms and terms that are defined in the text, variable names, or letters of the alphabet used as letters.
<i>Italic monospace font</i>	Text in italic monospace font indicates variable names within monospace-font text.
Underlined colored text	Underlined colored text indicates a cross-reference. Click the text to go to the object of the reference.
Text in a blue outline	(In PDF files only) A blue outline around text indicates a cross-reference. Click the outlined text to go to the object of the reference. This convention is the equivalent for PDF files of the "Underlined colored text" convention included in this table.
{INSTALL DIR}	Represents the directory where the product is installed.
UNIX:/Windows:	Paragraphs beginning with either of these indicate notes listing operating system differences.
“ ”(quotation marks)	(In PDF files only) Quotation marks surround cross-references to other sections of the document.
{ }	In a syntax line, curly braces surround a set of options from which you must choose one and only one.
[]	In a syntax line, square brackets surround optional parameters.

...	In a syntax line, ellipses indicate a repetition of the previous parameter. For example, <code>option[,...]</code> means that you can enter multiple, comma-separated options.
< >	Angle brackets surround variable elements of a name to distinguish them from one another. For example, <code><server_name><connector_name>tmp.log</code> .
\, /	Backslashes (\) are used as component separators in directory paths in Windows installations. For UNIX installations, substitute slashes (/) for backslashes.

Related documents

The complete set of documentation available with this product includes comprehensive information about installing, configuring, administering, and using WebSphere Partner Gateway Enterprise and Advanced Editions.

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

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

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

New in this release

New in release 6.0

This section highlights the changes to WebSphere Partner Gateway for version 6.0.

- Product name has changed from WebSphere Business Integration Connect to WebSphere Partner Gateway.
- Added a new chapter for creating gateways. See, Chapter 3, “Creating gateways,” on page 21.
- File names and directories have been updated to reflect new naming convention.
- FTP Scripting transport support has been added. See, “Setting up an FTP Scripting gateway” on page 29.
- Multiple certificate support has been added. See, “Uploading digital certificates” on page 8.

New in release 4.2.2

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 Partner Gateway environment.
- New accessibility features have been added to the Community Console to support screen readers.

Chapter 1. Introduction

Hub community

IBM WebSphere Partner Gateway'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 WebSphere Partner Gateway 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 Partner Gateway Community Console

Table 1. Community Console Icons



Icon	Icon name
	A Trade Participant Agreement (TPA) has been entered
	Collapse

Table 1. Community Console Icons (continued)






































Icon	Icon name
	Copy
	Create role. Role is not active
	Data is contained
	Deactivate
	Delete
	Display raw document
	Document in progress
	Document processing failed
	Document processing successful
	Download map
	Edit
	Edit attribute values
	Edit off
	Edit RosettaNet attribute values
	Expand
	Export information
	Export report
	Gateway disabled
	Hide search criteria
	Modify
	No data contained
	Open calendar
	Pause
	Print
	Required input
	Start
	Synchronous data flow. No icon is displayed for asynchronous transactions

Table 1. Community Console Icons (continued)

Icon	Icon name
	Upload map
	View details
	View Document Flow Definition attribute setup
	View Help system
	View members
	View original document
	View permissions
	View the group memberships
	View validation errors
	Where used

Using the Community Console

After you configure WebSphere Partner Gateway, 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 WebSphere Partner Gateway and thereafter for maintenance.

Chapter 2. Setting up your WebSphere Partner Gateway environment

This section describes the tasks that the community participant must perform to prepare WebSphere Partner Gateway for the participant's users and environment.

To configure WebSphere Partner Gateway for your company, you 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 7
5. "Uploading digital certificates" on page 8
6. "Creating console groups" on page 12
7. "Creating users" on page 12
8. "Creating contact information" on page 13
9. "Creating alerts and adding contacts" on page 14
10. "Creating a new address" on page 20

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: The WebSphere Partner Gateway 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.

In most cases, your Community Operator has sent you the user name, initial password, and company login 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 Login 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 Company 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 the Edit icon 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 Table 2.

Table 2. Values on Participants screens

Value	Description
Company Login Name	Identifies the participant to the system. Maximum of 15 characters. Cannot include the following special characters; , . ! # ; : \ / & ?. Participants cannot edit this value.
Participant Display 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. <ul style="list-style-type: none"> • DUNS numbers must equal nine digits. • DUNS+4 numbers must equal thirteen digits. • Freeform ID numbers accept up to 60 alpha, numeric, and special characters. <p>Note: EDI business IDs need to be prefixed with any qualifiers used in the EDI document. The format is EDI Qualifier plus "-" and the ID. For example, an EDI X12 using DUNS will be 01-123456789.</p>
IP Address or Host Name	<ul style="list-style-type: none"> • 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. Refer to Chapter 3, “Creating gateways,” on page 21 for details on how to create gateways.

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 Create roll icon below Set Source or Set Target tells you 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 the Edit icon 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

A digital certificate is an online identification credential, similar to a driver's license or passport. A digital certificate can be used to identify an individual or an organization.

Digital signatures are calculations based on an electronic document using public-key cryptography. Through this process, the digital signature is tied to the document being signed, as well as to the signer, and cannot be reproduced. With the passage of the federal digital signature bill, digitally signed electronic transactions have the same legal weight as transactions signed in ink.

WebSphere Partner Gateway uses digital certificates to verify the authenticity of business document transactions between the Community Manager and participants. They are also used for encryption and decryption.

You can specify a primary and a secondary certificate for outbound documents to ensure that the document exchange is not interrupted. The primary is used for all transactions. The secondary is used if the primary is expired or revoked.

Digital certificates are uploaded and identified during the configuration process.

If a certificate is found to be expired or revoked, it is disabled and is reflected as such in the console. If the primary certificate is expired or revoked, it is disabled and the secondary certificate will be set as the primary. An event is generated when a certificate is found to be expired or revoked.

The Certificate Usage option is available based on the certificate type selected. In the Hub Operator profile, Certificate Usage can be set for Digital Signature or SSL

Client certificate. In the participant profile, Certificate Usage can be set for Encryption certificate. If the same certificate is to be used for different purposes, for example, for Digital Signature and Encryption in Hub Operator profile, it needs to be loaded twice, once for the Digital Signature, and again for the Encryption certificate. However, if the certificate is used for Digital Signature and for SSL Client, then the corresponding checkboxes can be set in the same certificate entry.

Such certificates can also be loaded twice, once for Digital Signature and again for SSL Client. If so, the same pattern must be followed for the secondary certificates. For example, if the primary certificates were loaded as different certificates for Digital Signature and for SSL Client, secondary certificates should also be loaded as different certificate entries (even though the certificate may be the same).

For complete certpath building and validation, you are required to upload all of the certificates in the certificate chain. For example, if the certificate chain contains certificates A -> B -> C -> D, where A -> B means A is the issuer of B, then certificates A, B, and C should be uploaded as root certificates. If one of the certificates is not available, the certpath would not be built and the transaction would not succeed. The CA certificates can be obtained from the Certificate Repositories maintained by the Certificate Authorities or from the partner who provided the certificate. Root and intermediate certificates can only be uploaded in the Hub Operator profile.

Note: Before you can use the procedures in the following sections, the certificates must be loaded into the system. For more information on loading the certificates, refer to the *Hub Configuration Guide*.

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 14. Expired certificates are saved in the IBM WebSphere Partner Gateway 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.

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 WebSphere Partner Gateway 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 encryption 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 public part of the participant's certificate to WebSphere Partner Gateway 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 manager'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 WebSphere Partner Gateway'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 and intermediate 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 and intermediate 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 in the **Description** field for the certificate in the **Certificate** 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. Select **Certificate Usage** type:
 - Primary — used for all transactions.
 - Secondary — used if the primary is expired or revoked.
9. 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 the Community participant.

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 the View details icon to view the target user's group membership details.
3. Click the Edit icon 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 the Edit off icon 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 19.
 - To create a volume-based alert and add contacts to the alert, see "Creating a volume-based alert" on page 15.
 - To create an event-based alert and add contacts to the alert, see "Creating an event-based alert" on page 17.

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.

WebSphere Partner Gateway'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. WebSphere Partner Gateway 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 WebSphere Partner Gateway 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 16:
 - **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 than 22 will trigger an alert.
 - If Volume = 20 and Percent Deviation = 0, any document flow volume other than 20 will trigger an alert.
 - **Range.** Select Range to generate an alert if document flow volume falls outside a minimum-maximum range. Use the following steps to create an alert based on a range of values:
 - a. In the Min text box, enter the minimum number of document flows you expect to receive within a time frame selected in 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 the Edit icon.
 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 the Edit icon.
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 the View details icon to view alert details.
5. Click the Edit icon 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. Creating gateways

Gateways define entry points into the system. This chapter provides the steps for creating gateways and contains the following topics:

- “Overview”
- “Setting up an HTTP gateway”
- “Setting up an HTTPS gateway” on page 23
- “Setting up an FTP gateway” on page 24
- “Setting up an SMTP gateway” on page 25
- “Setting up a JMS gateway” on page 26
- “Setting up a file-directory gateway” on page 27
- “Setting up an FTPS gateway” on page 28
- “Setting up an FTP Scripting gateway” on page 29
- “Configuring handlers” on page 32
- “Specifying a default gateway” on page 32

Overview

WebSphere Partner Gateway uses gateways to route documents to their proper destination. The recipient can be a community participant or the Community Manager. The outbound transport protocol determines which information is used during gateway configuration.

The following transports are supported (by default) for participant gateways:

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

Note: You can define an SMTP gateway for participants only (not for the Community Manager).

- File directory
- FTP Scripting

You can also specify a user-defined transport, which you upload during the creation of the gateway.

Setting up an HTTP gateway

You set up an HTTP gateway so that documents can be sent from the hub to your participant’s IP address. When you set up an HTTP gateway, you can also specify that documents be sent through a configured proxy server.

To begin the process of creating an HTTP gateway, use the following procedure.

1. Click **Account Admin > Profiles > Gateways**.
2. Click **Create**.

Gateway Details

From the **Gateway List** page, perform the following steps:

1. Type a name to identify the gateway. This is a required field. This is the name that will appear on the list of gateways.
2. Optionally indicate the status of the gateway. **Enabled** is the default. A gateway that is enabled is ready to send documents. A gateway that is disabled cannot send documents.
3. Optionally indicate whether the gateway is Online or Offline. The default is **Online**.
4. Optionally enter a description of the gateway.

Gateway configuration

In the **Gateway Configuration** section of the page, perform the following steps:

1. Select **HTTP/1.1** from the **Transport** list.
2. In the **Address** field, enter the URI where the document will be delivered. This field is required.
The format is: `http://<server name>:<optional port>/<path>`
An example of this format is:
`http://anotherserver.ibm.com:57080/bcgreceiver/Receiver`
When you are setting up a gateway to be used for a Web service, specify the private URL supplied by the Web service provider. This is where WebSphere Partner Gateway will invoke the Web service when it acts as a proxy for the Web service provider.
3. Optionally enter a user name and password, if a user name and password are required to access the HTTP server.
4. In the **Retry Count** field, enter the number of times you want the gateway to attempt to send a document before it fails. The default is 3.
5. In the **Retry Interval** field, enter the amount of time the gateway should wait before attempting to send the document again. The default is 300 seconds.
6. In the **Number of Threads** field, enter the number of documents that can be processed simultaneously. The default is 3.
7. In the **Validate Client IP** field, select **Yes** if you want the IP address of the sender to be validated before the document is processed. Select **No** otherwise. The default is **No**.
8. In the **Auto Queue** field, select **Yes** if you want the gateway to be placed offline (automatically) if a delivery failure is about to occur because the number of retries has been exhausted. Select **No** otherwise. The default is **No**.
When you select **Auto Queue**, all documents remain queued until the gateway is placed online manually.
9. In the **Connection Timeout** field, enter the number of seconds a socket will remain open with no traffic. The default is 120 seconds.
10. If you want to configure the Preprocess or Postprocess step for the gateway, go to “Configuring handlers” on page 32. Otherwise, click **Save**.

Setting up an HTTPS gateway

You set up an HTTPS gateway so that documents can be sent from the hub to your participant's IP address. When you set up an HTTPS gateway, you can also specify that documents be sent through a configured proxy server.

To create HTTPS gateways, use the following procedure.

1. Click **Account Admin > Profiles > Gateways**.
2. Click **Create**.

Gateway Details

From the Gateway List page, perform the following steps:

1. Type a name to identify the gateway. This is a required field.
2. Optionally indicate the status of the gateway. **Enabled** is the default. A gateway that is enabled is ready to send documents. A gateway that is disabled cannot send documents.
3. Optionally indicate whether the gateway is Online or Offline. The default is **Online**.
4. Optionally enter a description of the gateway.

Gateway Configuration

In the **Gateway Configuration** section of the page, perform the following steps:

1. Select **HTTPS/1.0** or **HTTPS/1.1** from the **Transport** list.
2. In the **Address** field, enter the URI where the document will be delivered. This field is required.
The format is: `https://<server name>:<optional port>/<path>`
For example:
`https://anotherserver.ibm.com:57443/bcgreceiver/Receiver`
3. Optionally enter a user name and password, if a user name and password are required to access the secure HTTP server.
4. In the **Retry Count** field, enter the number of times you want the gateway to attempt to send a document before it fails. The default is 3.
5. In the **Retry Interval** field, enter the amount of time the gateway should wait before attempting to send the document again. The default is 300 seconds.
6. In the **Number of Threads** field, enter the number of documents that can be processed simultaneously. The default is 3.
7. In the **Validate Client IP** field, select **Yes** if you want the IP address of the sender to be validated before the document is processed. Select **No** otherwise. The default is **No**.
8. In the **Validate Client SSL Cert** field, select **Yes** if you want the digital certificate of the sending partner to be validated against the business id associated with the document. The default is **No**.
9. In the **Auto Queue** field, select **Yes** if you want the gateway to be placed offline (automatically) if a delivery failure is about to occur because the number of retries has been exhausted. Select **No** otherwise. The default is **No**.
When you select **Auto Queue**, all documents remain queued until the gateway is placed online manually.
10. In the **Connection Timeout** field, enter the number of seconds a socket will remain open with no traffic. The default is 120 seconds.

11. If you want to configure the Preprocess or Postprocess step for the gateway, go to “Configuring handlers” on page 32. Otherwise, click **Save**.

Setting up an FTP gateway

To create an FTP gateway, use the following procedure.

1. Click **Account Admin > Profiles > Gateways**.
2. Click **Create**.

Gateway Details

From the Gateway Details page, perform the following steps:

1. Type a name to identify the gateway. This is a required field.
2. Optionally indicate the status of the gateway. **Enabled** is the default. A gateway that is enabled is ready to send documents. A gateway that is disabled cannot send documents.
3. Optionally indicate whether the gateway is Online or Offline. The default is **Online**.
4. Optionally enter a description of the gateway.

Gateway Configuration

In the **Gateway Configuration** section of the page, perform the following steps:

1. Select **FTP** from the **Transport** list.
2. In the **Address** field, enter the URI where the document will be delivered. This field is required.

The format is: `ftp://<ftp server name>:<portno>`

For example:

`ftp://ftpserver1.ibm.com:2115`

If you do not enter a port number, the standard FTP port is used.

3. Optionally enter a user name and password, if a user name and password are required to access the FTP server.
4. In the **Retry Count** field, enter the number of times you want the gateway to attempt to send a document before it fails. The default is 3.
5. In the **Retry Interval** field, enter the amount of time the gateway should wait before attempting to send the document again. The default is 300 seconds.
6. In the **Number of Threads** field, enter the number of documents that can be processed simultaneously. The default is 3.
7. In the **Validate Client IP** field, select **Yes** if you want the IP address of the sender to be validated before the document is processed. Select **No** otherwise. The default is **No**.
8. In the **Auto Queue** field, select **Yes** if you want the gateway to be placed offline (automatically) if a delivery failure is about to occur because the number of retries has been exhausted. Select **No** otherwise. The default is **No**.
When you select **Auto Queue**, all documents remain queued until the gateway is placed online manually.
9. In the **Connection Timeout** field, enter the number of seconds a socket will remain open with no traffic. The default is 120 seconds.
10. In the **Use Unique File Name** field, leave the box checked if you want. Otherwise, click the box to remove the check. If you select **Use Unique File Name**, the original file name will be stored in the database.

11. If you want to configure the Preprocess or Postprocess step for the gateway, go to “Configuring handlers” on page 32. Otherwise, click **Save**.

Setting up an SMTP gateway

To create an SMTP gateway, use the following procedure.

1. Click **Account Admin > Profiles > Gateways**.
2. Click **Create**.

Gateway Details

From the Gateway List page, perform the following steps:

1. Type a name to identify the gateway. This is a required field.
2. Optionally indicate the status of the gateway. **Enabled** is the default. A gateway that is enabled is ready to send documents. A gateway that is disabled cannot send documents.
3. Optionally indicate whether the gateway is Online or Offline. The default is **Online**.
4. Optionally enter a description of the gateway.

Gateway Configuration

In the **Gateway Configuration** section of the page, perform the following steps:

1. Select **SMTP** from the **Transport** list.
2. In the **Address** field, enter the URI where the document will be delivered. This field is required.
The format is: `mailto:<user@server name>`
For example:
`mailto:admin@anotherserver.ibm.com`
3. Optionally enter a user name and password, if a user name and password are required to access the SMTP server.
4. In the **Retry Count** field, enter the number of times you want the gateway to attempt to send a document before it fails. The default is 3.
5. In the **Retry Interval** field, enter the amount of time the gateway should wait before attempting to send the document again. The default is 300 seconds.
6. In the **Number of Threads** field, enter the number of documents that can be processed simultaneously. The default is 3.
7. In the **Validate Client IP** field, select **Yes** if you want the IP address of the sender to be validated before the document is processed. Select **No** otherwise. The default is **No**.
8. In the **Auto Queue** field, select **Yes** if you want the gateway to be placed offline (automatically) if a delivery failure is about to occur because the number of retries has been exhausted. Select **No** otherwise. The default is **No**.
When you select **Auto Queue**, all documents remain queued until the gateway is placed online manually.
9. In the **Authentication Required** field, indicate whether a user name and password are supplied with the document. The default is **No**.
10. If you want to configure the Preprocess or Postprocess step for the gateway, go to “Configuring handlers” on page 32. Otherwise, click **Save**.

Setting up a JMS gateway

To create JMS gateways, use the following procedure.

1. Click **Account Admin > Profiles > Gateways**.
2. Click **Create**.

Gateway Details

From the Gateway List page, perform the following steps:

1. Type a name to identify the gateway. This is a required field.
2. Optionally indicate the status of the gateway. **Enabled** is the default. A gateway that is enabled is ready to send documents. A gateway that is disabled cannot send documents.
3. Optionally indicate whether the gateway is Online or Offline. The default is **Online**.
4. Optionally enter a description of the gateway.

Gateway Configuration

In the **Gateway Configuration** section of the page, perform the following steps:

1. Select **JMS** from the **Transport** list.
2. In the **Address** field, enter the URI where the document will be delivered. This field is required.

For WebSphere MQ JMS, the format of the target URI is as follows:

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

For example:

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

The directory contains the “.bindings” file for the file-based JNDI. This file indicates to WebSphere Partner Gateway how to route the document to its intended destination. This field is required.

3. Optionally enter a user name and password, if a user name and password are required to access the JMS queue.
4. In the **Retry Count** field, enter the number of times you want the gateway to attempt to send a document before it fails. The default is 3.
5. In the **Retry Interval** field, enter the amount of time the gateway should wait before attempting to send the document again. The default is 300 seconds.
6. In the **Number of Threads** field, enter the number of documents that can be processed simultaneously. The default is 3.
7. In the **Validate Client IP** field, select **Yes** if you want the IP address of the sender to be validated before the document is processed. Select **No** otherwise. The default is **No**.
8. In the **Auto Queue** field, select **Yes** if you want the gateway to be placed offline (automatically) if a delivery failure is about to occur because the number of retries has been exhausted. Select **No** otherwise. The default is **No**.
When you select **Auto Queue**, all documents remain queued until the gateway is placed online manually.
9. In the **Authentication Required** field, indicate whether a user name and password are supplied with the document. The default is **No**.
10. In the **JMS Factory Name** field, enter the name of the Java class the JMS provider uses to connect to the JMS queue. This field is required.

11. In the **JMS Message Class** field, enter the message class. The choices are any valid JMS Message class, such as `TextMessage` or `BytesMessage`. This field is required.
12. In the **JMS Message Type** field, enter the type of message. This is an optional field.
13. In the **Provider URL Packages** field, enter the name of the classes (or JAR file) that Java uses to understand the JMS context URL. This field is optional. If you do not specify a value, the file system path to the bindings file is used.
14. In the **JMS Queue Name** field, enter the name of the JMS queue where documents are to be sent. This field is required.
15. In the **JMS JNDI Factory Name** field, enter the factory name used to connect to the name service. This field is required.
16. If you want to configure the Preprocess or Postprocess step for the gateway, go to “Configuring handlers” on page 32. Otherwise, click **Save**.

Setting up a file-directory gateway

To create file-directory gateways, use the following procedure.

1. Click **Account Admin > Profiles > Gateways**.
2. Click **Create**.

Gateway Details

From the Gateway List page, perform the following steps:

1. Type a name to identify the gateway. This is a required field.
2. Optionally indicate the status of the gateway. **Enabled** is the default. A gateway that is enabled is ready to send documents. A gateway that is disabled cannot send documents.
3. Optionally indicate whether the gateway is Online or Offline. The default is **Online**.
4. Optionally enter a description of the gateway.

Gateway Configuration

In the **Gateway Configuration** section of the page, perform the following steps:

1. Select **File Directory** from the **Transport** list.
2. In the **Address** field, enter the URI where the document will be delivered. This field is required.

The format for UNIX systems and for Windows systems in which the file directory is on the same drive on which WebSphere Partner Gateway is installed is: `file:///<path to target directory>`

For example:

```
file:///localfiledir
```

where *localfiledir* is a directory off the root directory.

For Windows systems in which the file directory is on a separate drive from WebSphere Partner Gateway, the format is: `file:///<drive letter>:/<path>`

3. In the **Retry Count** field, enter the number of times you want the gateway to attempt to send a document before it fails. The default is 3.
4. In the **Retry Interval** field, enter the amount of time the gateway should wait before attempting to send the document again. The default is 300 seconds.
5. In the **Number of Threads** field, enter the number of documents that should be processed simultaneously. The default is 3.

6. In the **Validate Client IP** field, select **Yes** if you want the IP address of the sender to be validated before the document is processed. Select **No** otherwise. The default is **No**.
7. In the **Auto Queue** field, select **Yes** if you want the gateway to be placed offline (automatically) if a delivery failure is about to occur because the number of retries has been exhausted. Select **No** otherwise. The default is **No**.
When you select **Auto Queue**, all documents remain queued until the gateway is placed online manually.
8. In the **Use Unique File Name** field, leave the box checked if you want. Otherwise, click the box to remove the check. If you select **Use Unique File Name**, the original file name will be stored in the database.
9. If you want to configure the Preprocess or Postprocess step for the gateway, go to “Configuring handlers” on page 32. Otherwise, click **Save**.

Setting up an FTPS gateway

To create FTPS gateways, use the following procedure.

1. Click **Account Admin > Profiles > Gateways**.
2. Click **Create**.

Gateway Details

From the Gateway List page, perform the following steps:

1. Type a name to identify the gateway. This is a required field.
2. Optionally indicate the status of the gateway. **Enabled** is the default. A gateway that is enabled is ready to send documents. A gateway that is disabled cannot send documents.
3. Optionally indicate whether the gateway is Online or Offline. The default is **Online**.
4. Optionally enter a description of the gateway.

Gateway Configuration

In the **Gateway Configuration** section of the page, perform the following steps:

1. Select **FTPS** from the **Transport** list.
2. In the **Address** field, enter the URI where the document will be delivered. This field is required.
The format is: `ftp://<ftp server name>:<portno>`
For example:
`ftp://ftpserver1.ibm.com:2115`
If you do not enter a port number, the standard FTP port is used.
3. Optionally enter a user name and password, if a user name and password are required to access the secure FTP server.
4. In the **Retry Count** field, enter the number of times you want the gateway to attempt to send a document before it fails. The default is 3.
5. In the **Retry Interval** field, enter the amount of time the gateway should wait before attempting to send the document again. The default is 300 seconds.
6. In the **Number of Threads** field, enter the number of documents that should be processed simultaneously. The default is 3.
7. In the **Validate Client IP** field, select **Yes** if you want the IP address of the sender to be validated before the document is processed. Select **No** otherwise. The default is **No**.

8. In the **Auto Queue** field, select **Yes** if you want the gateway to be placed offline (automatically) if a delivery failure is about to occur because the number of retries has been exhausted. Select **No** otherwise. The default is **No**.
When you select **Auto Queue**, all documents remain queued until the gateway is placed online manually.
9. In the **Connection Timeout** field, enter the number of seconds a socket will remain open with no traffic. The default is 120 seconds.
10. In the **Use Unique File Name** field, leave the box checked if you want. Otherwise, click the box to remove the check. If you select **Use Unique File Name**, the original file name will be stored in the database.
11. If you want to configure the Preprocess or Postprocess step for the gateway, go to “Configuring handlers” on page 32. Otherwise, click **Save**.

Setting up an FTP Scripting gateway

An FTP Scripting gateway runs according to the schedule you set. The behavior of an FTP Scripting gateway is governed by an FTP command script.

Creating the FTP script

To use an FTP Scripting gateway, you create a file that includes all the FTP commands required that can be accepted by your FTP server.

1. Create a script for the gateways, to indicate the actions you want performed. The following script is an example of connecting to the specified FTP server (with the name and password specified), changing to the specified directory on the FTP server, and sending all the files to the specified directory on the server.

```
open %BCGSERVERIP% %BCGUSERID% %BCGPASSWORD% %BCGOPTIONx%
cd %BCGOPTIONx%
mput *
quit
```

The placeholders (for example, %BCGSERVERIP%) are replaced when the gateway is put in service by the values you enter when you create a specific instance of an FTP scripting gateway, as shown in the following table:

Table 3. How script parameters map to FTP Scripting gateway field entries

Script parameter	FTP Scripting gateway field entry
%BCGSERVERIP%	Server IP
%BCGUSERID%	User ID
%BCGPASSWORD%	Password
%BCGOPTIONx%	Optionx, under User Defined Attributes

You can have up to 10 user-defined options.

2. Save the file.

FTP script commands

You can use the following commands when creating the script:

- `ascii`, `binary`, `passive`

These commands are not sent to the FTP Server. They modify the mode of transfer (`ascii`, `binary`, or `passive`) to the FTP Server.

- `cd`

This command changes to the specified directory.

- `delete`

This command removes a file from the FTP server.

- **mkdir**

This command creates a directory on the FTP server.

- **mput**

This command takes a single argument, which specifies one or more files to be transferred to the remote system. This argument can contain the standard wild card characters to identify multiple files ('*' and '?').

- **open**

This command takes 3 parameters; ftp server ip address, username and password. These map to the %BCGSERVERIP% %BCGUSERID% and %BCGPASSWORD% variables respectively. The first line of your FTP Scripting Target script should be: open %BCGSERVERIP% %BCGUSERID% %BCGPASSWORD%.

- **quit, bye**

This command ends an existing connection to an FTP Server.

- **quote**

This command indicates that everything after the QUOTE should be sent to the remote system as a command. This allows you to send commands to a remote FTP server that might not be defined in the standard FTP protocol.

- **rmdir**

This command removes a directory from the FTP server.

- **site**

This command can be used to issue site-specific commands to the remote system. The remote system determines if the contents of this command are valid.

FTP Scripting gateways

If you will be using FTP Scripting gateways, perform the following tasks:

To create FTP Scripting gateways, use the following procedure.

1. Click **Account Admin > Profiles > Gateways**.
2. Click **Create**.

Gateway Details

From the Gateway List page, perform the following steps:

1. Type a name to identify the gateway. This is a required field.
2. Optionally indicate the status of the gateway. **Enabled** is the default. A gateway that is enabled is ready to send documents. A gateway that is disabled cannot send documents.
3. Optionally indicate whether the gateway is Online or Offline. The default is **Online**.
4. Optionally enter a description of the gateway.

Gateway Configuration

In the **Gateway Configuration** section of the page, perform the following steps:

1. Select **FTP Scripting** from the **Transport** list.
2. Enter the IP address of the FTP server to which you are sending documents. The value you enter here will replace %BCGSERVERIP% when the FTP script is run.

3. Enter the user ID and password required to access the FTP server. The values you enter here will replace %BCGUSERID% and %BCGPASSWORD% when the FTP script is run.
4. If the target is in secure mode, use the default of **Yes** for **FTPS Mode**. Otherwise, click **No**.
5. Upload the script file by following these steps:
 - a. Click **Upload Script File**.
 - b. Type the name of the file that contains the script for processing documents, or click **Browse** to navigate to the file.
 - c. Click **Load File** to load the script file into the **Currently loaded script** file text box.
 - d. If the script file is the one you want to use, click **Save**.
 - e. Click **Close Window**.
6. In the **Retry Count** field, enter the number of times you want the gateway to attempt to send a document before it fails. The default is 3.
7. In the **Retry Interval** field, enter the amount of time the gateway should wait before attempting to send the document again. The default is 300 seconds.
8. For **Connection Timeout**, enter the number of seconds a socket will remain open with no traffic. The default is 120 seconds.
9. In the **Lock User** field, indicate whether the gateway will request a lock, so that no other instances of an FTP Scripting gateway can gain access to the same FTP server directory at the same time.

User-defined Attributes

If you want to specify additional attributes, perform the following steps. The value you enter for the option will replace %BCGOPTIONx% when the FTP script is run (where x corresponds to the number of the option.)

1. Click **New**.
2. Type a value next to **Option 1**
3. If you have additional attributes to specify, click **New** again and type a value.
4. Repeat step 3 as often as necessary to define all the attributes.

For example, suppose your FTP script looked like this:

```
Open %BCGSERVERIP% %BCGUSERID% %BCGPASSWORD%
    cd %BCGOPTION1%
    mput *
    quit
```

The %BCGOPTION% in this case would be a directory name.

Schedule

From the Schedule section of the page, perform the following steps:

1. Indicate whether you want interval-based scheduling or calendar-based scheduling.
 - If you select **Interval Based Scheduling**, select the number of seconds that should elapse before the gateway is polled (or accept the default value).
 - If you select **Calendar Based Scheduling**, choose the type of scheduling (**Daily Schedule**, **Weekly Schedule**, or **Custom Schedule**).
 - If you select **Daily Schedule**, enter the time of day when the gateway should be polled.

- If you select **Weekly Schedule**, select one or more days of the week in addition to the time of day.
 - If you select **Custom Schedule**, select the time of day and then choose **Range** or **Selective Days** for the week and the month. With **Range**, you indicate the start date and the end date. (For example, click **Mon** and **Fri** if you want the server polled at a certain time on weekdays only.) With **Selective Days**, you choose the specific days of the week and month.
2. If you want to configure the Preprocess or Postprocess step for the gateway, go to “Configuring handlers.” Otherwise, click **Save**.

Configuring handlers

You can modify two processing points for a gateway--Preprocess and Postprocess.

No handlers are provided by default for the Preprocess or Postprocess step, and, therefore, no handlers are listed by default in the **Available List**. If you have uploaded a handler, you can select it and move it to the **Configured List**.

To apply a user-written handler for these configuration points, you must first upload the handler. Refer to the *Hub Configuration Guide* for steps on uploading the handler. Then perform the following steps:

1. Select **preprocess** or **postprocess** from the **Configuration Point Handlers** list.
2. Select the handler from the **Available List** and click **Add**.
3. If you want to change the attributes of the handler, select it from the **Configured List** and click **Configure**. You will see a list of attributes that can be changed. Make the necessary changes and click **Set Values**.
4. Click **Save**.

You can further modify the **Configured List** as follows:

- Remove a handler by selecting the handler from the **Configured List** and clicking **Remove**. The handler is moved to the **Available List**.
- Rearrange the order in which the handler is processed by selecting the handler and clicking **Move Up** or **Move Down**.

Specifying a default gateway

After you create gateways for the Community Manager or participant, select one of the gateways as the default gateway.

1. Click **Account Admin > Profiles > Gateways**.
2. Click **Create**.
3. Click **View Default Gateways**.

A list of gateways defined for the participant is displayed.

4. From the **Production** list, select the gateway that will be the default for this participant. You can also set default gateways for other types of gateways, such as **Test**.
5. Click **Save**.

Chapter 4. Managing community connections and users: Account Admin

The features in the Account Admin module control how WebSphere Partner Gateway 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 34

"Managing groups" on page 35

"Managing users" on page 36

"Managing contacts" on page 37

"Managing alerts" on page 38

"Managing addresses" on page 39

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 the View details icon to view gateways details.
3. Click the Edit icon 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 certificate 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 the View details icon to view certificate details. The system displays the Certificate Details screen.
3. Click the Edit icon 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 the View details icon to view certificate details. The system displays the Certificate Details screen.
3. Click the Edit icon 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 the View members icon to view a list of members in a group. If this icon does not appear, there are no members in the group. Click Memberships in the sub-menu.
3. Click the Edit icon to edit users in a group.
4. Click the **Add to Group** button to assign users to the group.
5. Click Edit off icon 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 the View permissions icon 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 the View details icon to view group details (Name and Description). The system displays the Group Detail screen.
3. Click the Edit icon 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 the View details icon to view group details. The system displays the Group Details screen.
3. Click the Edit icon 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 the View details icon to view a user's details.
3. Click the Edit icon 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	<ul style="list-style-type: none">• Local - Contact is only visible to your organization.• Global - Contact is visible to the Community Operator and Community Manager. Both of these parties can subscribe the contact to alerts.
Subscribed	If this option is selected, one or more alerts are assigned to this contact. If the contact is removed from the system, all alert subscriptions to this contact are removed from the system.
Alert Status	When the Alert Status is enabled, this contact receives all subscribed alerts.

2. Click the View details icon to view contact details. The system displays the Contact Detail screen.
3. Click the Edit icon 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	<ul style="list-style-type: none">• Local - Contact is only visible to your organization.• Global - Contact is visible to the Community Operator and Community Manager. Both of these parties can subscribe the contact to alerts.

5. Click **Save**.

Removing a contact

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

Managing alerts

WebSphere Partner Gateway'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, it, 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 the View details icon to view an alert's details.
5. Click the Edit icon 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 the Delete icon 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 the Edit icon.
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 the Delete icon.
3. Verify that you want to delete the address.

Chapter 5. Viewing events and documents: Viewers

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

The Viewers module includes the following features:

- “Event Viewer”
- “AS1/AS2 Viewer” on page 43
- “RosettaNet Viewer” on page 46
- “Document Viewer” on page 48
- “Gateway Queue” on page 52

The RosettaNet and AS1/AS2 Viewers include additional search criteria for the Hub Admin. For more information, see the *Administrator Guide*.

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

Event Viewer

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.

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 14. 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 15. Event Viewer tasks

What do you want to do?	See
Search for events.	page 42
View event details.	page 43

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 16. 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 the View details icon next to the event you want to view. The system displays event details and associated documents.
5. Click the View details icon next to the document that you want to view, if one exists.
6. Click the Display raw document icon to view the raw document, if one exists.
7. Click the View validation errors icon to view validation errors.

When the error message No valid encryption certificate found is displayed, neither the primary nor the secondary certificate is valid. The certificates might be expired or they might have been revoked. If the certificates were expired or revoked, you see the corresponding event (No valid encryption certificate found) in the Event Viewer.

Tip: If a duplicate document event is displayed in the Event Viewer Detail, view the previously sent original document by clicking the View original document icon in Document Details.

AS1/AS2 Viewer

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 AS1/AS2 Viewer can also be used 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 17. AS1/AS2 Viewer tasks

What do you want to do?	See
Search for messages	page 47
Viewing raw documents	page 48

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 18. 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 or XML.
Document Flow	The specific business process.
Message ID	ID number assigned to the AS1 or AS2 packaged document. Search criteria can include the asterisk (*) wildcard. Maximum length, 255 characters.
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 the View details icon next to the message that you want to view. The system displays the message and the associated document details.

Table 19. 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: <ul style="list-style-type: none"> • Automatic=action/MDN-sent-automatically; processed. • Automatic-action/MDN-sent-automatically;processed/Warning;duplicate-document. • Automatic-action/MDN-sent-automatically;processed/Error;description-failed. • Automatic-action/MDN-sent-automatically;failed:unsupported MIC-algorithms.

5. (Optional) Click the Display raw document icon to view the raw document.

RosettaNet Viewer

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.

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 20. RosettaNet Viewer tasks

What do you want to do?	See
Search for RosettaNet processes.	page 47
View RosettaNet process details.	page 47
View raw documents.	page 48

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 21. 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 22. 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 the View details icon next to the RosettaNet process you want to view. The system displays details and associated documents for the selected process.

5. Click the View details icon 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 the View details icon next to the process that you want to view. The system displays process details and associated documents for the selected process.
5. Click the Display raw document icon next 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 50.
- The raw document viewer displays the HTTP header with the raw document.

Document Viewer

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. You can also use the Document Viewer to resend failed or successful documents.

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 23. 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 24. 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 the open folder icon next to the document displayed under the Associated Documents header. The system displays process details and events for the selected document. For EDI Interchange documents, if there are child EDI transactions from either de-enveloping or enveloping, they can be shown by selecting the **Document children** source or target radio button. See the *Administrator Guide* for more information on viewing EDI documents.
 - To view the raw document with HTTP header, click the Display raw document icon 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 25. 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 click the View original document icon.

Tip: To troubleshoot documents that have failed processing, see "Viewing data validation errors" on page 50.

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 26. 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"?><!DOCTYPE Pip3 A7PurchaseOrderUpdateNotification
SYSTEM "3A7_MS_V02_00_PurchaseOrderUpdateNotification.dtd">
<Pip3A7PurchaseOrderUpdateNotification>
  <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>
  <facsimileNumber>
  <CommunicationsNumber>+1-234-567-8998-7</CommunicationsNumber>
  </facsimileNumber>
  </ContactInformation>
  <BusinessDescription>
  <GlobalBusinessIdentifier>123456789</GlobalBusinessIdentifier>
  <GlobalSupplyChainCode>InformationTechnology</GlobalSupplyChainCode>
  <BusinessDescription>
  <GlobalPartnerClassificationCode>Carrier</GlobalPartnerClassificationCode>
  </PartnerDescription>
</PartnerRoleDescription>

```

Example of non-nested XML validation errors:

The *EmailAddress* data element is the first un-nested 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 un-nested 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 48.

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.

Gateway Queue

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

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

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

Viewing the gateway list

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

1. Click **Viewers > Gateway Queue**. The Console displays the Gateway Queue window.

2. Input the parameters shown in Table 27.

Table 27. Gateway Queue window

Criteria	Description
Queued at least	Minimum number of minutes a document has been waiting in the gateway queue. For example, if 6 minutes is selected, all gateways containing documents that have been waiting for delivery for 6 minutes or more will be displayed. The default is 0.
Minimum Queued	Minimum number of documents in a gateway queue. The default is 1.
Sort By	Sort search results by Participant (default), Gateway Name, or Last Sent Timestamp.
Direction	Click Ascend to display documents starting with the oldest time stamp or end of the alphabet, or Descend to display documents starting with the most recent time stamp or the beginning of the alphabet.
Refresh	Turn refresh on or off (default).
Refresh Rate	Number of seconds the Console waits before updating displayed data.

3. Click **Search**. The system finds all documents in the gateway that match your search criteria. **Table 28** shows the information returned from the search.

Table 28. Results after gateway queue search

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

Note: For the Console to display a gateway, the gateway must meet all the requirements of the search criteria using AND logic.

Viewing queued documents

To search for queued documents that meet specific search criteria, use the following procedure:

1. Click **Viewers > Gateway Queue**.
2. From the Gateway Queue window, click **Search**.

3. Complete the following parameters in the window:

Table 29. Search criteria for the Gateway Queue

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

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

Removing documents from the delivery queue

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

1. Click **Viewers > Gateway Queue**.
2. From the Gateway Queue window, click **Search**.
3. Complete the parameters in the window (see Table 29 on page 54).
4. Click the delete icon to delete the document.

Viewing gateway details

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

1. Click **Viewers > Gateway Queue**.
2. From the Gateway Queue window, type the search criteria (see Table 27 on page 53).
3. Click **Search**.
4. From the list of gateways, click the document count link in the **Queued** column. Gateway details and a list of queued documents appear.

Changing gateway status

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

1. Click **Viewers > Gateway Queue**.
2. From the Gateway Queue window, type the search criteria (see Table 27 on page 53).
3. Click **Search**.
4. From the list of gateways, click the document count link in the **Queued** column. Gateway details and a list of queued documents appear.
5. Click **Online** in **Gateway Info** to place a gateway offline, or click **Offline** to place gateway online. (You must be logged in as Hub Admin to change gateway status.)

Chapter 6. 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 30. Tools

What feature do you want to use?	See
Document Analysis	page 55
Document Volume Report	page 57
Test Participant Connection	page 58

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 31. 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: <ul style="list-style-type: none">• Incomplete. For example, the system is waiting for other documents.• Data Validation. For example, the system is checking document content.• Translation. For example, the system is converting the document to another protocol.• Queue. For example, the document is waiting to be routed to the participant or Community Manager.
Failed	Document processing was interrupted due to errors in the system, data validation, or duplicates.
Successful	The final message that completes document processing has been transmitted from the system to the target participant.

Viewing documents in the system

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

Table 32. 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 Source Participant Name or Target 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 the View details icon 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 33. 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 34. 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 the Export report icon 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 the Print icon 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 35. 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 fulfilling the request. Something went wrong with the web server and it couldn't give you a meaningful response. There is usually nothing that can be done from the browser end to fix this error; the server administrator will probably need to check the server's error log to see what happened. This is often the error message for a CGI script which has not been properly coded.
- 501 - Method Not Implemented - The server does not support the functionality required to fulfill the request. Application method (either GET or POST) is not implemented.
- 502 - Bad Gateway - The server received an invalid response from the gateway or upstream server it accessed in attempting to fulfill the request.

- 503 - Service Temporarily Unavailable - The server is currently unable to handle the request due to a temporary overloading or maintenance of the server. Server is out of resources.
- 504 - Gateway Time out - The server did not receive a timely response from the gateway or upstream server it accessed in attempting to complete the request.
- 505 - HTTP Version Not Supported

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 Partner Gateway, 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 (*).

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 Partner Gateway 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

Copyright (c) 1995-2003 International Business Machines Corporation and others

All rights reserved.

Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the "Software"), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, provided that the above copyright notice(s) and this permission notice appear in all copies of the Software and that both the above copyright notice(s) and this permission notice appear in supporting documentation.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OF THIRD PARTY RIGHTS. IN NO EVENT SHALL THE COPYRIGHT HOLDER OR HOLDERS INCLUDED IN THIS NOTICE BE LIABLE FOR ANY CLAIM, OR ANY SPECIAL INDIRECT OR CONSEQUENTIAL DAMAGES, OR ANY DAMAGES WHATSOEVER RESULTING FROM LOSS OF USE, DATA OR PROFITS, WHETHER IN AN ACTION OF CONTRACT, NEGLIGENCE OR OTHER TORTIOUS ACTION, ARISING OUT OF OR IN CONNECTION WITH THE USE OR PERFORMANCE OF THIS SOFTWARE.

Except as contained in this notice, the name of a copyright holder shall not be used in advertising or otherwise to promote the sale, use or other dealings in this Software without prior written authorization of the copyright holder.

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:

i5/OS
IBM
the IBM logo
AIX
CICS
CrossWorlds
DB2
DB2 Universal Database
Domino
IMS
Informix
iSeries
Lotus
Lotus Notes
MQIntegrator

MQSeries
MVS
OS/400
Passport Advantage
SupportPac
WebSphere
z/OS

Microsoft, Windows, Windows NT, 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.

Linux is a trademark of Linus Torvalds in the United States, other countries, or both.

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



WebSphere Partner Gateway Enterprise and Advanced Editions, version 6.0.

Index

A

- Account Admin features 33
- Action, definition 7
- Activity, definition 7
- Add contact to existing alert 19
- Addresses
 - delete 40
 - description 20, 39
 - edit 40
 - values 40
- Alerts
 - add contact to existing alert 19
 - create event-based alert 17
 - create volume-based alert 15
 - description 14, 38
 - disable alert 39
 - remove alert 39
 - search criteria 39
 - search criteria, Participants 39
 - search for alerts 39
 - view or edit alert details and contacts 38
- AS1/AS2 Viewer 48
 - description 43
 - package details 46
 - search criteria 45
 - searching for messages 44
 - viewing message details 45
- Assign
 - group membership 35
 - group permissions 35
 - users to groups 13

B

- B2B capabilities, description 7

C

- calendar-based scheduling
 - FTP Scripting gateway 31
- Certificates
 - expiration alert, create 17
 - types and supported formats 10
- Changing
 - gateway status 54
- commands
 - FTP 29
- Community Console
 - display 5
 - users 1
 - using 3
- Community Manager
 - description 1
- Community Operator
 - description 1
- Community Participant
 - description 1
- configuration points
 - gateways 32

- Contacts
 - description 13, 37
 - details 38
 - remove contact 38
 - values 35, 37, 38
 - view or edit contact details 37
- Create
 - certificate expiration alert 17
 - Document Volume Report 57
 - event-based alert 17
 - gateways 7
 - new group 12
 - new user 12
 - volume-based alert 15
- Critical event type 42

D

- Debug events 3, 42
- Decryption
 - definition 10
- default gateway
 - example of setting 32
- Default gateway
 - edit 34
 - select 34
 - view 34
- Delete
 - address 40
 - group 35
- Details, viewing gateway 54
- Digital signature certificate, definition 11
- Digital signature, definition 9
- Disable alert 39
- Display console 5
- Document
 - details, Document Viewer 49
 - processing values, Document Viewer 50
- Document Analysis
 - description 55
 - search criteria 56
 - viewing documents 56
 - viewing process and event details 57
- Document flow, definition 7
- Document states
 - definitions 55
 - Document Volume Report 57
- Document Viewer
 - description 48
 - document details 49
 - document processing values 50
 - search criteria 49
 - values 45, 46, 49, 50
- Document Volume Report
 - create 57
 - description 57
 - document states 57
 - exporting 58
 - printing 58
 - search criteria 58

- Documents
 - removing from the queue 54
 - viewing queued 53
- DUNS numbers 6
- DUNS+4 6

E

- Edit
 - address 40
 - alert details and contacts 38
 - contact details 37
 - gateway details 33
 - group details 35
- Enable alert 39
- Encryption
 - certificate, definition 11
 - definition 10
- Error event type 42
- Error fields
 - validation errors 51
- Event types 42
 - descriptions 42
- Event Viewer
 - description 41
 - search criteria 43
 - viewing event details 43
- Events
 - search criteria 43
 - searching for 42
- Exporting
 - Document Volume Report 58

F

- Freeform ID numbers 6
- FTP commands 29
- FTP gateways 24
- FTP scripts
 - commands allowed in 29
 - gateways 29

G

- Gateway
 - changing status 54
 - removing documents from the queue 54
 - viewing details 54
 - viewing queued documents 53
 - viewing the list 52
- gateways
 - default 32
 - file-directory 27
 - FTP 24
 - FTP Scripting 29, 30
 - FTPS 28
 - HTTP 21
 - HTTPS 23
 - JMS 26
 - SMTP 25
 - transports supported 21
- Gateways
 - create 7
 - description 33
 - values 34
 - view list 33

- Gateways (*continued*)
 - view or edit gateway details 33
- Groups 35
 - assigning users to 13
 - create 12
 - delete 35
 - description 35
 - permissions, view edit assign 35
 - values 35
 - view group memberships 35
 - view or edit group details 35

H

- Hub-community
 - description 1

I

- Icons 1
- Information event type 42
- interval-based scheduling
 - FTP Scripting gateway 31

J

- JMS gateways 26

K

- Key, definition 10

L

- Log in to console 5
- Log out of console 5

N

- Non-repudiation, definition 10

P

- Package Details
 - AS1/AS2 Viewer 46
- Package, definition 7
- Participant
 - description 1
- Participant Profile
 - description 6
 - editing 6
 - values 6
 - viewing 6
- Printing reports
 - Document Volume Report 58
- Private key, definition 10
- Protocol, definition 7
- Public key, definition 10

Q

- Queue, removing documents from 54
- Queued documents, viewing 53

R

- Raw documents
 - viewing 48
- Remove
 - alert 39
 - contact 38
- Removing documents from the queue 54
- Result codes
 - Web Server 59
- RosettaNet Viewer
 - description 46
 - document processing, details 47
 - search criteria 47
 - searching for processes 47
 - viewing process details 47

S

- Search
 - for alerts 39
 - for events 42
 - for messages, AS1/AS2 Viewer 44
 - for RosettaNet processes 47
- Search criteria
 - alerts 39
 - AS1/AS2 Viewer 45
 - Document Analysis 56
 - Document Viewer 49
 - Document Volume Report 58
 - Event Viewer 43
 - RosettaNet Viewer 47
- Self-signed key, definition 10
- SMTP gateways 25
- SSL Client certificate, definition 10, 11
- Status, change gateway 54

T

- Test Participant Connection
 - description 58
 - values 59
 - Web Server result codes 59
- Tools
 - description 55
 - Document Analysis 55
 - Document Volume Report 57
 - Test Participant Connection 58
- transports
 - gateway, system-supplied 21

U

- Users
 - assign to groups 13
 - create new user 12
 - description 12, 36
 - values 36

V

- Validation errors
 - viewing 50
- Values
 - Addresses 40
 - Contacts 35, 37, 38

Values (continued)

- Document Viewer 45, 46, 49, 50
- Gateways 34
- Participant Profile 6
- Test Participant Connection 59

View

- alert details and contacts 38
- contact details 37
- gateway details 33
- gateway list 33
- group details 35
- group permissions 35

Viewers

- AS1/AS2 Viewer 43
- description 41
- Document Viewer 48
- Event Viewer 41
- RosettaNet Viewer 46

Viewing

- document details 49
 - document processing details, RosettaNet Viewer 47
 - documents
 - Document Analysis 56
 - event details, Event Viewer 43
 - events 49
 - gateway details 54
 - gateway list 52
 - message details, AS1/AS2 Viewer 45
 - process and event details, Document Analysis 57
 - queued documents 53
 - raw documents 49
 - Raw documents 48
 - RosettaNet process details 47
 - validation errors 50
- ### VTP digital certificate
- definition 11

W

- Warning event type 42
- Web Server result codes 59

X

- X.509 certificate, definition 10



Printed in USA