

IBM WebSphere Partner Gateway Enterprise and
Advanced Editions



Partner Guide

Version 6.1.1

IBM WebSphere Partner Gateway Enterprise and
Advanced Editions



Partner Guide

Version 6.1.1

Note!

Before using this information and the product it supports, read the information in "Notices" on page 95.

27March2008

This edition applies to Version 6.1.1, Release 1, Modification 1, 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, e-mail 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, 2008. 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 6.1.1.	ix
New in release 6.1	ix
Chapter 1. Introduction	1
Hub community	1
Hub administrator	1
Internal partner	1
External partners	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 partner profile.	6
Viewing and editing your partner profile	6
Creating a destination	7
Reviewing B2B capabilities	7
Uploading digital certificates	9
Certificate terms.	10
Certificate types and supported formats	11
SSL server and client authentication	11
Using certificates to enable encryption	18
Using certificates to enable digital signing	23
Creating console groups	27
Creating users	27
Creating a new user	27
Configuring FTP user	28
Adding users to groups	28
Creating contact information	29
Creating alerts and adding contacts	29
Creating a volume-based alert	31
Creating an event-based alert	33
Adding a new contact to an existing alert	34
Creating a new address	35
Chapter 3. Creating destinations.	37
Overview	37
Setting up an HTTP destination	37
Destination Details	38
Destination configuration.	38
Setting up an HTTPS destination	39
Destination Details	39
Destination Configuration	39
Setting up an FTP destination	40
Destination Details	40
Destination Configuration	40
Setting up an SMTP destination	41
Destination Details	41

Destination Configuration	41
Setting up a JMS destination.	42
Destination Details	42
Destination Configuration	42
Setting up a file-directory destination.	43
Destination Details	43
Destination Configuration	43
Setting up an FTPS destination	44
Destination Details	44
Destination Configuration	44
Setting up an FTP Scripting destination	45
Creating the FTP script	45
FTP script commands	46
FTP Scripting destinations	46
Destination Details	46
Destination Configuration	47
User-defined Attributes	47
Schedule	47
Configuring handlers	48
Specifying a default destination	48

Chapter 4. Managing community connections and users: Account Admin 51

Managing destinations.	51
Viewing a list of destinations	51
Viewing or editing destination details	51
View, select, or edit your default destinations	52
Viewing destination Whereused	52
Deleting destination	52
Managing Certificates	53
Viewing and editing digital certificate details	53
Disabling a digital certificate	53
Managing groups	53
Viewing group memberships and assigning users to groups	53
Viewing, editing, or assigning group permissions.	53
Viewing or editing group details	54
Deleting a group	54
Managing users	54
Deleting users	56
Managing contacts	56
Viewing or editing contact details	56
Removing a contact.	57
Managing alerts	57
Viewing or editing alert details and contacts	57
Searching for alerts	58
Disabling or enabling an alert	58
Removing an alert	58
Event Notification	59
Managing addresses	59
Editing an address	59
Deleting an address	59

Chapter 5. Viewing events and documents: Viewers 61

Event Viewer	61
Event types	62
Performing Event Viewer tasks	62
Searching for events	62
Viewing event details	63
AS Viewer.	63
Performing AS Viewer tasks	64
Searching for messages	64

Viewing message details	65
ebMS Viewer	66
Performing ebMS Viewer tasks	66
Searching for ebMS processes	66
View ebMS process details	67
View raw documents	67
Viewing the Document Status	68
RosettaNet Viewer	68
Performing RosettaNet Viewer tasks	68
Searching for RosettaNet processes	68
Viewing RosettaNet process details	69
Viewing raw documents	70
Document Viewer	70
Searching for documents	71
Viewing document details, events, and raw document	72
Viewing data validation errors	72
Using the Stop Process feature	74
Destination Queue	74
Viewing the destination list	74
Viewing queued documents	75
Removing documents from the delivery queue	76
Viewing destination details	76
Changing destination status	77
Chapter 6. Analyzing Document Type: Tools	79
Document Analysis	79
Document States	80
Viewing documents in the system	80
Viewing process and event details	80
Custom XML File Processing	81
Document Volume Report	81
Create a Document Volume Report	82
Exporting the Document Volume Report	82
Printing reports	83
Test Partner Connection	83
Web Server result codes	83
EDI Reports	85
EDI FA Overdue Search	85
EDI Rejected Transaction Search	87
FTP Reports	89
FTP Statistics	89
FTP Connections	89
Glossary	91
Notices	95
Programming interface information	97
Trademarks and service marks	97
Index	99

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 partners 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 internal partner, hub administrator, and external partners. 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 Partner Gateway 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

This section describes the new features of IBM WebSphere Partner Gateway.

New in release 6.1.1

WebSphere Partner Gateway 6.1.1 supports the following new features:

- In the earlier releases, basic authentication support was available only for webservicess messages. This feature is now extended to all protocols. The recommendation for basic authentication is the usage of secure HTTP connection, that is, HTTPS instead of HTTP.
- Apart from signing and encryption, support for compression and decompression is provided for RNIF messages.
- Support is provided for validating the SOAP Body and SOAP Envelope. In addition, you can de-envelope a SOAP Envelope.
- The synchronous maximum time out and synchronous maximum connections can be locally controlled for every HTTP receiver.
- The FTP Server is integrated with WebSphere Partner Gateway to support AS3 protocol, FTP Scripting Destination, FTP Scripting Receiver, FTP / FTPS receiver and destination.
- Error document can be sent to initiating partner, receiving partner, or both. The error document flow can be configured in WebSphere Partner Gateway console and can be sent in either WebSphere Partner Gateway format or Web services format.
- Performance of the archiver has been improved.
- Support is provided for multiple internal partners.
- You can resend multiple Inbound or Outbound documents simultaneously.
- Support for FIPS mode is provided. The product can be configured to run on FIPS mode or default mode.
- Delete and Whereused functionality is provided for Destination, Validation Maps, Document Definitions, Interactions, and Users.
- Large file compression support is provided for AS2 and AS3 documents.
- Support is provided for encryption and signing.
- The configuration type dependencies for migration also includes Event codes and Alert Notifications. Also, the partner migration functionality has been enhanced to provide support for import / export definitions of alertable events.
- Support is provided to upload multiple certificates. New wizard is included in the console to upload and configure certificates.
- The product now supports AIX 6.1, RHEL 5 (32 and 64 bit), SLES 10 (64 bit) and Windows Server 2003 64 bit.

New in release 6.1

WebSphere Partner Gateway V6.1 supports the following new features:

- New business protocols: AS3, SOAP with attachments, CIDX, and ebXML Message Service (ebMS) 2.0 support

- Improved support for Custom XML documents includes better organization, full XPath expression support, search fields, user defined attributes, and synchronous support
- New IPv6 support and enhanced FTP Scripting for supporting AS3
- Reorganization of Document Definition attributes
- New Document Definition attributes for use with User Exits.
- Non-repudiation configurable by document type and trading partner level
- Document viewer has additional user-defined search fields.
- Improved AS Viewer support based on MDN return status
- EDI Configuration Wizard and EIF Import Wizard (previously delivered in the GA02 Support pack)
- New Alert notification mode to send notifications to all related parties (source and target partners or all subscribed contacts, which reduces alert configuration)
- Resend and Gateway permissions now available to users other than the hubadmin administrator
- New user group for allowing multiple users to have the ability to be hub administrators
- LDAP support for log-on authentication
- Use of WebSphere Application Server logging and tracing for WebSphere Partner Gateway components
- Property file configuration data now centrally located and managed by the WebSphere Partner Gateway Console
- WebSphere MQ is no longer a prerequisite product; the WebSphere Platform Messaging support is now used for internal communications
- Selective archive based on partner and/or document type
- Migration of WebSphere Partner Gateway configuration by exporting and importing definitions from one WebSphere Partner Gateway instance to another instance
- A simplified single machine (simple mode) installation option
- WebSphere Application Server Network Deployment now used for multiple machine deployments enabling clustering and central infrastructure management
- Support for using WebSphere Process Server, Version 6.1 as a backend integration system

Notes:

1. The XML-based administrative API is deprecated in version 6.1.
2. WebSphere Partner Gateway, Version 6.1 does not support the RC5 algorithm.

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: hub administrator, internal partner, and external partners.

Hub administrator

The hub administrator is a company responsible for managing the day-to-day operation of the hub community. The hub administrator 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 external partners.
- Assisting in the configuration of new external partners to the hub community.
- Strategic planning for future growth to ensure the hub community operates at peak efficiency.

The role of the hub administrator can be contracted to a third party company within the hub community, or the internal partner who purchased WebSphere Partner Gateway can elect to perform the function of the hub administrator.

Internal partner

The internal partner 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 external partners.

The internal partner can also choose to be the hub administrator.

External partners

External partners are the companies that do business with the internal partner via the hub community. External partners must complete a configuration process to connect to the hub community. Once connected, external partners can exchange electronic business documents with the internal partner.

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
	Collapse
	Copy

Table 1. Community Console icons (continued)







































Icon	Icon name
	Create role. Role is not active
	Data is contained
	Activate
	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
	Destination disabled
	Hide search criteria
	Modify
	No data contained
	Open calendar
	Enable/disable document ordering
	Pause
	Print
	Required input
	Start
	Stop processing; document is in progress, user option to request the server stop processing document

Table 1. Community Console icons (continued)

Icon	Icon name
	Synchronous data flow; no icon is displayed for asynchronous transactions
	Upload map
	View details
	View Document 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 name, and event location. The hub admin can also search by partner, 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 external partner must perform to prepare WebSphere Partner Gateway for the external partner'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 partner profile" on page 6
3. "Creating a destination" on page 7
4. "Reviewing B2B capabilities" on page 7
5. "Uploading digital certificates" on page 9
6. "Creating console groups" on page 27
7. "Creating users" on page 27
8. "Configuring FTP user" on page 28
9. "Creating contact information" on page 29
10. "Creating alerts and adding contacts" on page 29
11. "Creating a new address" on page 35

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 hub administrator 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 hub administrator.

To log in to the Community Console (these instructions are for the internal partners as well as external partners):

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.

Note: If WebSphere Partner Gateway is configured using LDAP, then you have to enter the LDAP User Name and Password. The Company Login Name is not relevant in this scenario, hence you will not be prompted to enter this information. Also, the system will not prompt you to change your password.

Verifying your partner profile

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

Partners can edit all attributes in their profile except the Company Login Name. Partners can also add and remove Business IDs, Email ID related to every Business ID, and IP addresses. IP addresses or host names can be entered for the following Operation Modes: Production, Test, CPS Manager, and CPS Partner.

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 partner profile

1. Click **Account Admin > Profiles > Partner**.
2. Click the My Profile icon to edit. The system displays the Partner Detail screen.
3. Edit your profile, as required (some values cannot be edited). For an explanation of the values, see Table 2 on page 7.

Table 2. Values on Partners screens

Value	Description
Company Login Name	Identifies the partner to the system. Maximum of 15 characters. Cannot include the following special characters: , . ! # ; : \ / & ?. Partners cannot edit this value.
Partner Display Name	The name the partner wants displayed to the hub community. Maximum of 30 characters.
Partner Type	Partner Type - external partner or internal partner. Partners can edit this value only if the property <code>bcg.allow.partner.type.edit</code> is set to True. By default, this value is set to False.
Status	Enabled or Disabled. If disabled, Partner is not visible in search criteria and drop-down lists.
Vendor Type	Identifies the partner's role, for example, Contract Manufacturer or Distributor.
Web Site	Identifies the partner'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>
Email ID	Valid Email ID of each Business ID. You can add additional Email IDs for every Business ID. This field is not visible if there are no Business IDs.
IP Address or Host Name	<ul style="list-style-type: none"> Operation Mode, for example, CPS Partner. IP Address or host name of partner.

4. Click **Save**.

Creating a destination

You must create and maintain a default destination. If you do not, you cannot create connections. Refer to Chapter 3, "Creating destinations," on page 37 for details on how to create destinations.

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 type definitions. A document type 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 type definitions:

Package. Identify document packaging formats used to transmit documents over the internet. For example, RNIF, AS1, AS2 and AS3.

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

Document type. Identifies the business process that will be processed between the internal partner and its external partners.

Activity. The business function the process performs.

Action. The individual documents that make up a complete business process. The documents are processed between the internal partner and external partner.

Each document type 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 type. 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 type 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 partner 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 type definition.
4. Click the Edit icon to view and, if desired, change lower level document type definitions (for example Protocol or Document Type). You can also change a document type 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.
- Non-repudiation required
- AS Business Id

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 internal partner and external partners. 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 partner 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 check boxes 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 29. 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 (external partners and internal partner).** 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 partners.
- **Encryption certificate (external partners and internal partner).** 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 partner's certificate to WebSphere Partner Gateway through the console and send a copy of the certificate to the Hub Operator.
- **Digital signature certificate (external partners and internal partner).** If hub community members sign the documents, the public part of the signing certificate must be uploaded to the hub at the partner 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 (internal partner).** This certificate is used by WebSphere Partner Gateway's Document Manager for the external partner 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 partners created through the console. They are used to validate signed documents received from the external partner 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, partners must have a copy of that certificate.
- If the hub community web server's certificate is from a Certificate Authority, the partners 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, partners must have a copy of that certificate.
- If the hub community web server's certificate is from a Certificate Authority, the partners must have a copy of the CA root and intermediate certificate.
- The target server must have a copy of the partner'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.

Note: Previous versions of WebSphere Partner Gateway did not support the IPv6 address format. WebSphere Partner Gateway 6.1 does support this format. Make sure at least one of your servers is configured to support the IPv6 address format. The IPv6 format configuration is only necessary on the server.

Configuring inbound SSL certificates

This section describes how to configure server authentication and client authentication for inbound connection requests from partners.

An inbound request is when the partner is sending a document to WebSphere Partner Gateway. If your community is not using SSL, you do not need an inbound or outbound SSL certificate.

Note: For inbound FTPS WebSphere Partner Gateway uses an FTP Server that is provided by the customer, so any inbound SSL configuration is per that specific FTP Server product that the customer is using.

Step 1: Obtain an SSL certificate: WebSphere Application Server uses the SSL certificate when it receives connection requests from partners through SSL. It is the certificate that the Receiver presents to identify the hub to the partner. This server certificate can be self-signed, or it can be signed by a CA. In most cases you will use a CA certificate to increase security. You might use a self-signed certificate in a test environment. Use iKeyman or the WebSphere Application Server administrative console to generate a certificate and key pair. Refer to documentation available from IBM for more information about using iKeyman or the WebSphere Application Server administrative console.

After you generate the certificate and key pair, use the certificate for inbound SSL traffic for all partners. If you have multiple Receivers or Consoles, copy the resultant key store to each instance. If the certificate is generated using the WebSphere Application Server administrative console, the key and the certificate can be imported in another key store in another server using the WebSphere Application Server administrative console. If the certificate is self-signed, provide this certificate to the partners. To obtain this certificate, use iKeyman to extract the public certificate to a file.

Generating a self-signed certificate: If you are going to use self-signed server certificates, use the following procedure.

1. Start the iKeyman utility, which is located in `/<WAS_Installation_dir>/bin`. If this is your first time using iKeyman, delete the “dummy” certificate that resides in the key store.
2. Open the Receiver or Console key store using iKeyman, and use iKeyman to generate a self-signed certificate and a key pair for the Receiver or Console key store.
3. Use iKeyman to extract to a file the certificate that will contain your public key. Save the key store to a JKS, PKCS12, or JCEKS file.
4. Distribute the certificate to your partners. The preferred method for distribution is to send the certificate in a zipped file that is password-protected, by e-mail. Your partners must call you and request the password for the zipped file.
5. Using the WebSphere Application Server administrative console, set the new certificate in the SSL Configuration and in the settings for receiver and console. You can do this by selecting the alias of the new certificate in the key store in the Configuration for each node or server.

Obtaining a CA-generated certificate: If you are going to use a certificate signed by a CA, use the following procedure.

1. Start the iKeyman utility, which is located in the `/<WAS_Installation_dir>/bin` directory.
2. Use iKeyman to generate a certificate request and a key pair for the Receiver.
3. Submit a Certificate Signing Request (CSR) to a CA.
4. When you receive the signed certificate from the CA, use iKeyman to place the signed certificate into the key store.
5. Distribute the CA certificate to all partners if required.
6. Using the WebSphere Application Server administrative console, set the new certificate in the SSL Configuration and in the settings for receiver and console. You can do this by selecting the alias of the new certificate in the key store in the Configuration for each node or server.

Note: The WebSphere Application Server administrative console can also be used to complete the previous steps.

Step 2: Authenticate clients: If you want to authenticate partners who send documents, perform the steps in this section.

Installing the client certificate: For client authentication, use the following procedure:

1. Obtain your partner’s certificate.
2. If the certificate is self-signed, install the certificate into the trust store using iKeyman or the WebSphere Application Server administrative console.
3. If the certificate is CA-issued, add the related CA certificates in the related trust store using iKeyman or the WebSphere Application Server administrative console.

Note: When you add more partners to your hub community, you can use iKeyman or the WebSphere Application Server administrative console to add their certificates to the trust store. If a partner leaves the community, you can use iKeyman or the WebSphere Application Server administrative console to remove the partner’s certificates from the trust store.

Setting up client authentication: After installing the certificate or certificates, configure WebSphere Application Server to use client authentication by running the utility script `bcgClientAuth.jacl`.

1. Navigate to the following directory: `/<ProductDir>/bin`
2. To turn on client authentication, call the script as follows:

```
./bcgwsadmin.sh -f /<ProductDir>/scripts/bcgClientAuth.jacl  
-conntype NONE set
```

Note: To turn off client authentication, call the script as follows:

```
./bcgwsadmin.sh -f /<ProductDir>/receiver/scripts/bcgClientAuth.jacl  
-conntype NONE clear
```

You must restart the `bcgreceiver` server for these changes to take effect. Client Authentication can also be enabled using the WebSphere Application Server administrative console. A value of "Supported" means that server will ask for client certificate, but, if client certificate is not available, the SSL handshake may still be established. A value of "Required" means that client certificate must be sent. Otherwise, the SSL handshake will fail.

Validating the client's certificate: There is an additional feature that can be used with SSL client authentication. This feature is enabled through the Community Console. For HTTPS, WebSphere Partner Gateway checks certificates against the Business IDs in the inbound documents. To use this feature, create the partner's profile, import the client certificate, and flag it as SSL.

1. Import the client certificate.
 - a. Click **Account Admin > Profiles > Partner** and search for the partner's profile.
 - b. Click **Certificates**.
 - c. Click **Load Certificate**.
 - d. Click **Browse** and navigate to the directory in which you have saved the certificate.
 - e. Select **SSL Client** as the type of certificate.
 - f. Type a description of the certificate (which is required).
 - g. Change the status to **Enabled**.
 - h. If you want to select a operation mode other than **Production** (the default), select it from the list.
 - i. Click **Finish**.
2. Update the client destination.
 - a. Click **Account Admin > Profiles > Partner** and search for the partner's profile.
 - b. Click **Destinations**.
 - c. Select the HTTPS destination you previously created. If you have not yet created the HTTPS destination, see "Setting up an HTTPS destination" on page 39.
 - d. Click the **Edit** icon to edit the destination.
 - e. Select **Yes** for **Validate SSL Client Certificate**.
 - f. Click **Save**.

Configuring separate keystore and truststore for receiver and console: By default, WebSphere Partner Gateway version 6.1 uses common keystore and

truststore for the Receiver and Console. However, you can configure separate keystore and truststore for receiver and console in the distributed mode installation.

To configure the keystore and truststore, create and set a separate keystore and truststore for the Receiver and Console. Also, create separate SSL configurations. The SSL configurations can be set either at Cluster level or Server level. Setting SSL configuration at cluster level is easier since the configuration is then applicable to all the servers in that cluster, and you need not configure each server separately.

Setting SSL configuration at the cluster level: While setting the SSL configuration with new keystore and truststore at cluster level, there must not be any SSL configuration set at the server level. If there is a SSL configuration set at the server level, then the SSL configuration at the cluster level will not be used; instead the one set for the server will be used.

Follow these steps to set the SSL configuration for bcgconsoleCluster:

1. Create a keystore for the Console cluster. The keystore must be created in the bcgconsole cluster scope by navigating to **Security > SSL certificate and key management > Key stores and certificates**.
2. Create a truststore for the Console cluster. The truststore must be created in the bcgconsole cluster scope by navigating to **Security > SSL certificate and key management > Key stores and certificates**.
3. Create an SSL configuration for console cluster at the Console cluster scope by navigating to **Security > SSL certificate and key management > SSL configurations**. Set the keystore and truststore that were created in the previous steps. Update the certificate aliases in the certificate aliases list by clicking **Get certificate aliases**, and select the required alias to be used for server authentication. Set the trust manager to **IbmPKIX**.
4. Set this SSL configuration in bcgconsoleCluster by overriding the inherited SSL configuration. Update the certificate aliases by clicking **Update the certificate aliases** and set the alias to be used for server authentication.
5. Restart bcgconsoleCluster.

Follow these steps to set the SSL configuration for bcgreceiverCluster:

1. Create a keystore for the Receiver cluster. The keystore must be created in the bcgreceiver cluster scope by navigating to **Security > SSL certificate and key management > Key stores and certificates**.
2. Create a truststore for the Receiver cluster. The truststore must be created in the bcgconsole cluster scope by navigating to **Security > SSL certificate and key management > Key stores and certificates**.
3. Create an SSL configuration for receiver cluster at the Receiver cluster scope by navigating to **Security > SSL certificate and key management > SSL configurations**, and set the keystore and truststore that were created in the previous steps. Get the certificate aliases by clicking **Get certificate aliases**, and select the required alias to be used for server authentication. Set the trust manager to **IbmPKIX**.
4. Set this SSL configuration in bcgreceiverCluster by overriding the inherited SSL configuration. Update the certificate aliases by clicking **Update the certificate aliases** and set the alias to be used for server authentication.
5. Restart the bcgreceiverCluster.

For more information on working with keystores, truststores, SSL configuration, and endpoint configurations, refer to the section *Securing applications and their environment of WebSphere Application Server Documentation*.

Note:

Setting NodeDefaultTrustStore in NodeDefaultSSLSetting in distributed mode: This setting must be done for simple distributed mode. But, this is also applicable for the fully distributed mode if common keystore and truststore are to be used for the Receiver and Console. If a node is federated in a cell, the signer certificates from the node are added to the CellDefaultTrustStore. By default, NodeDefaultSSLSetting refers to CellDefaultTrustStore as the truststore. For the WebSphere Partner Gateway Receiver and Console, using Signer certificates from other nodes might not be desirable. To use a dedicated truststore for the nodes in which WebSphere Partner Gateway is installed, NodeDefaultTrustStore can be set in NodeDefaultSSLSettings as the truststore.

The steps for making this change are as follows:

1. In the WebSphere Application Server administrative console, navigate to **Security > SSL certificate and key management > Manage endpoint security configurations > <node_name> > SSL configurations > NodeDefaultSSLSettings**.
2. In the field Trust store name, select **NodeDefaultTrustStore**.

Note: Ensure that NodeDefaultTrustStore is configured for the truststore that you want to use; for example, bcgSecurityTrust.jks.

3. Click **Apply**.
4. On the following page of the Console, click **Save** to update the changes to the master configuration.
5. Restart the servers in that node.

Note: For the fully distributed mode, the above changes must be made for all nodes containing bcgreceiver and bcgconsole servers. For simple distributed mode, these changes must be made for all nodes containing bcgservers.

Adding Signer certificates to trust.p12 if NodeDefaultTrustStore is set for node containing WebSphere Partner Gateway servers: Currently, NodeDefaultTrustStore refers to trust.p12. If NodeDefaultTrustStore is set for the node containing WebSphere Partner Gateway servers, bcgSecurityTrust.jks will not be used. Signer certificates from bcgSecurityTrust.jks needs to be added to trust.p12 as required.

Configuring outbound SSL certificates

An outbound request is when WebSphere Partner Gateway is sending a document to a partner. If your community is not using SSL, you do not need an inbound or outbound SSL certificate.

Step 1: Authenticate the server: When SSL is being used to send outbound documents to your partners, WebSphere Partner Gateway requests a server-side certificate from the partners. The same CA certificate can be used for multiple partners. The certificate must be in X.509 DER format.

Note: You can convert the format with the iKeyman utility. Follow these steps to use iKeyman to convert the format:

1. Start iKeyman.
2. Create a new blank key store or open an existing key store.

3. In the Key Database Content, select **Signer Certificates**.
4. Add the ARM certificate using the **Add** option.
5. Extract the same certificate as a Binary DER data using the **Extract** option.
6. Close iKeyman.

Install the partner's self-signed certificate into the Hub Operator profile. If the certificate was signed by a CA and the CA root certificate and any other certificates that are part of the certificate chain are not already installed in the Hub Operator profile, install the certificates in the Hub Operator profile.

1. Click **Account Admin > Profiles > Certificates** to display the Certificate List page.

Make sure you are logged in to the Community Console as the Hub Operator or Internal Partner.

2. Click **Load PKCS12**.

Note: The PKCS12 file being uploaded should contain only one private key and the associated certificate. You can also upload the certificate and the PKCS#8-formatted private key separately.

3. Select **SSL Client** as the type of certificate.
4. Type a description of the certificate (which is required).
5. Change the status to **Enabled**.
6. Click **Browse** and navigate to the directory in which you have saved the certificate.
7. Select the certificate and click **Open**.
8. Enter the password.
9. If you want to select a operation mode other than **Production** (the default), select it from the list.
10. If you have two SSL certificates, indicate whether this is the primary or secondary certificate by selecting **Primary** or **Secondary** from the **Certificate Usage** list.
11. Click **Upload** and then click **Save**.

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

Step 2: Authenticate clients: If SSL client authentication is required, the partner will, in turn, request a certificate from the hub. Use the Community Console to import your certificate into WebSphere Partner Gateway. You can generate the certificate using iKeyman. If the certificate is a self-signed certificate, it must be provided to the partner. If it is a CA-signed certificate, the CA root certificate must be given to the partners, so that they can add it to their trusted certificates.

You can have more than one SSL certificate. One is the primary certificate, which is the one used by default. The other is a secondary certificate, which is used if the primary certificate expires.

Using a self-signed certificate: If you are going to use a self-signed certificate, use the following procedure.

1. Start the iKeyman utility.
2. Use iKeyman to generate a self-signed certificate and a key pair.
3. Use iKeyman to extract to a file the certificate that will contain your public key.

4. Distribute the certificate to your partners. The preferred method for distribution is to send the certificate in a zipped file that is password-protected, by e-mail. Your partners must call you and request the password for the zipped file.
5. Use iKeyman to export the self-signed certificate and private key pair in the form of a PKCS12 file.
6. Install the self-signed certificate and key through the Community Console.
 - a. Click **Account Admin > Profiles > Certificates** to display the Certificate List page.
Make sure you are logged in to the Community Console as the Hub Operator.
 - b. Click **Load PKCS12**.

Note: The PKCS12 file being uploaded should contain only one private key and the associated certificate. You can also upload the certificate and the PKCS#8-formatted private key separately.
 - c. Select **SSL Client** as the type of certificate.
 - d. Type a description of the certificate (which is required).
 - e. Change the status to **Enabled**.
 - f. Click **Browse** and navigate to the directory in which you have saved the certificate.
 - g. Select the certificate and click **Open**.
 - h. Enter the password.
 - i. If you want to select a operation mode other than **Production** (the default), select it from the list.
 - j. If you have two SSL certificates, indicate whether this is the primary or secondary certificate by selecting **Primary** or **Secondary** from the **Certificate Usage** list.
 - k. Click **Upload** and then click **Save**.

If you are uploading primary and secondary certificates for both SSL client authentication and digital signature and you are uploading the primary certificates as two separate entries, make sure that the corresponding secondary certificates are uploaded as two different entries.

Using a CA-signed certificate: If you are going to use a certificate signed by a CA, use the following procedure:

1. Use iKeyman to generate a certificate request and a key pair for the Receiver.
2. Submit a Certificate Signing Request (CSR) to a CA.
3. When you receive the signed certificate from the CA, use iKeyman to place the signed certificate into the key store.
4. Distribute the signing CA certificate to all partners.

Using certificates to enable encryption

This section describes encryption certificates.

Creating and installing inbound encryption certificates

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

Note the following important restriction about receiving encrypted AS2 messages from partners. If a partner sends an encrypted AS2 message but uses the wrong certificate, the decryption fails. No MDN is returned to the partner to indicate the failure, however. In order for your partner to receive MDNs in this situation, create a connection to the partner with the following document definition:

- Package: **AS** to Package: **None**
- Protocol: **Binary** to Protocol: **Binary**
- Document Type: **Binary** to Document Type: **Binary**

The connection created must be AS to None connection, that is, creating a connection by activating the AS B2B capability on one partner and None B2B capability on the other. Please ensure that the source gateway on the AS side is a SMTP gateway (in case of AS1), HTTP gateway (in case of AS2) or FTP gateway (in case of AS3), which is configured to MDN address. Thus, the decryption failure MDN is sent back over this AS to None Binary connection.

Step 1: Obtain a certificate:

Generating a self-signed certificate: If you are going to use a self-signed certificate, use the following procedure.

1. Start the iKeyman utility.
2. Use iKeyman to generate a self-signed certificate and a key pair.
3. Use iKeyman to extract to a file the certificate that will contain your public key.
4. Distribute the certificate to your partners. They are required to import the file into their B2B product for use as an encryption certificate. Advise them to use it when they want to send encrypted files to the internal partner. If your certificate is CA-signed, provide the CA certificate as well.
5. Use iKeyman to save the self-signed certificate and private key pair in the form of a PKCS12 file.
6. Navigate to **Profile > {Hub Operator/internal partner} > certificates > create new certificate**.
7. In the **Which Partner does this Certificate(s) belong to** drop-down, select the partner to associate the newly uploaded Certificate.
8. Click **Search** to find specific or sub-set of partners.
9. Click **Browse** next to **Certificate Location** to upload the Certificate.
10. Click **Next**.
11. In the Provide certificate details, enter the following certificate information: **Leaf certificate, Root CA certificate Or intermediate CA certificate**.
12. Associate this certificate to **Encryption**.
13. In the **Certificate usage**, select **Primary** or **Secondary**.
14. Select **enabled** or **disabled** in the **Status** based on whether you want to enable or disable the Certificate after uploading
15. Select the **Operation mode**.
16. Click **Finish** to save the changes and close the wizard.

Using a CA-signed certificate: If you are going to use a certificate signed by a CA, use the following procedure:

1. Start the iKeyman utility.
2. Use iKeyman to generate a certificate request and a key pair for the Receiver.
3. Submit a Certificate Signing Request (CSR) to a CA.

4. When you receive the signed certificate from the CA, use iKeyman to place the signed certificate into the key store.

Step 2: Distribute the certificate: Distribute the signing CA certificate to all partners.

Installing outbound encryption certificates

The outbound encryption certificate is used when the hub sends encrypted documents to partners. WebSphere Partner Gateway encrypts documents with the public keys of the partners, and the partners decrypt the documents with their private keys.

The partner can have more than one encryption certificate. One is the primary certificate, which is the one used by default. The other is a secondary certificate, which is used if the primary certificate expires.

Step 1: Obtain a partner's certificate: Obtain the partner's encryption certificate. The certificate must be in X.509 DER format. Note that WebSphere Partner Gateway supports only X5.09 certificates.

Step 2: Install the partner's certificate: Install the certificate through the Community Console under the partner's profile by completing the following procedure:

1. Navigate to **Profile > External partner > certificates > Load Certificate**.
2. In the **Select Partner, File Location, Password** page of the wizard, enter the following values:
 - **Which partner does this certificate(s) belongs to:** Select the partner to associate the newly uploaded certificate. Click Search to find a specific partner or subset of a partners. If the partner is a Hub Operator or Internal Partner, enter the certificate location, private key location, and password (OR) Provide the truststore or keystore with password. For External Partner, enter the certificate location (OR) provide the trust store location containing the certificate chain.
 - **Certificate Location:** Click **Browse** to select the location of the certificate public.
3. Click **Next** to go to the **Certificate Details** page of the wizard.
4. In the **Certificate Details** page of the wizard, enter the following details of the certificate:
 - **Leaf Certificate Name** - The name of the Leaf Certificate. The field name depends on whether the certificate is a Leaf certificate, Root CA certificate or an intermediate CA certificate.
 - **Description** - The description of the Leaf Certificate.
 - **Certificate Type** - Associate this certificate to Encryption.
 - **Certificate Usage** - Associate an usage for the certificate. The values are Primary and Secondary.
 - **Operation Mode** - Enter the mode of operation.
 - **Status** - Select enabled or disabled based on whether you want to enable or disable a certificate after upload. The Next button is enabled only if the certificate is enabled.
 - **Set Management** - You can either associate a certificate to an existing set or create a new set. If the certificate is a secondary certificate, it can only be associated to an existing set. You can associate the certificate to any set for

an internal partner with type encrypt or for a external partner with type SSL (Incoming client auth) or Signing (Verify).

5. Click **Next** to go to Set page of the wizard. If the certificate is primary, you do not have to create sets and associate the certificate to a set and participant connection. If you have selected **Create new set** check box, then **Create New Set** page of the wizard will open. Otherwise, the **Add to Existing** page of the wizard will open. If the file contains a private key of the internal partner or the public certificate of the external partner used for SSL / Digital Signature, then you can click **Finish**.
6. In the **Create New Set** page of the wizard, enter the details of the new set. For Primary certificates, you do not have to create sets and associate a certificate to it. Enter the following values:
 - **Set Name** - The name of the Set.
 - **Description** - The description of the Set.
 - **Status** - Select enabled or disabled. If it is disabled the **Next** button will not be enabled.
 - **Make default settings** - Select this check box if you want this set to be the default.
7. In the **Add to Existing Set** page of the wizard, select set(s) to add the certificate. Enter the following values:
 - **Select from the list of Sets available for the selected Certificate type** - From the list, select set(s) to add the certificate.
 - **Make default settings** - Select this check box if you want this set to be the default.
8. From the **Create New Set** or **Add to Existing Set**, click **Next** to go to the **Default Settings** page of the wizard. The **Next** button will be enabled only if the status of the set is enabled.
9. Select **enabled** or **disabled** in the **Status** based on whether you want to enable or disable the Certificate after upload.

Note: If you have selected the **Make default set** check box in the earlier page (Create new set or Add to existing set), then you need to associate the set to an operation mode. This will display certificate usages against operation modes. The encryption will be disabled for internal partners. SSL Client and Digital Signature will be disabled for external partners.

10. Click **Next** to go to the Configuration page of the wizard. In case you click **Finish** and there are some missing roots or intermediate CA certificates, you will be prompted to upload. If you click "Yes" in the prompt window, the first page of the wizard will open. Click **Cancel** if you want to upload at a later stage.
11. In the Configuration page of the wizard, enter the following values:

Note: The Configuration page displays a list of certificate(set) usage against operation modes. The current set name is pre-populated for all, but you can reset it.

- **From Partner** - This field will be pre-populated with the value of the internal partner.
- **To Partner** - This drop-down is pre-populated with the list of all external partners. You can also select the value "All" to include all external partners.
- **From Package** - From the drop-down, select the package Document Flow Definitions objects of the internal partner.

- **To Package** - From the list, select the package Document Flow Definitions objects of the external partner.
12. Click **Add more connections** if you want to associate the set to other participant connections.
 13. Click **Add Secondary Certificate** to add a secondary certificate to the current set.
 14. Click **Finish** to upload the Certificate. In case there are some missing roots or intermediate CA certificates, you will be prompted to upload. If you click "Yes" in the prompt window, the first page of the wizard will open. Click **Cancel** in the prompt window if you want to upload at a later stage.

Repeat this step if the partner has a second encryption certificate.

Step 3: Install any CA-issued certificates: If the certificate was signed by a CA and the CA root certificate and any other certificates that are part of the certificate chain are not already installed in the Hub Operator profile, install the certificates now by following this procedure:

Note: You do not have to perform this step if the CA-issued certificate is already installed.

1. Navigate to **Profile > Hub Operator > certificates > create new certificate**.
2. In the **Which Partner does this Certificate(s) belong to** drop-down, select the partner to associate the newly uploaded Certificate.
3. Click **Search** to find specific or sub-set of partners.
4. Click **Browse** next to **Trust store (or) Keystore location**.
5. For both Certificate and Trust store, enter **Password**.
6. If Trust store, enter the **Keystore type** click **Next**.
7. In the **Select end entity certificate to upload** page of the wizard, select a certificate to be loaded.

Note: When you load certificates using a trust store that has more than one certificate, the **Select the list of root and intermediate CA Certificates to be uploaded** is populated with all the certificates. You can also upload multiple certificates.

8. Click **Finish**.

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

For example, to alter the attributes of a partner connection, click **Account Admin > Connections** and then select the partners. Click **Attributes** and then edit the attribute (for example, **AS Encrypted**).

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, the corresponding event (Certificate revoked or expired) can also be seen in the Event Viewer. Note that these two events might be separated by other events.

To display the Event Viewer complete the following:

1. Click **Viewers > Event Viewer**.
2. Select the appropriate search criteria.
3. Click **Search**.

See the *WebSphere Partner Gateway Administrator Guide* for information on using the Event Viewer.

Using certificates to enable digital signing

Creating an outbound signature certificate

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

You can have more than one digital signature certificate. One is the primary certificate, which is the one used by default. The other is a secondary certificate, which is used if the primary certificate expires.

Generating a self-signed certificate: If you are going to use a self-signed certificate, use the following procedure.

1. Start the iKeyman utility.
2. Use iKeyman to generate a self-signed certificate and a key pair.
3. Use iKeyman to extract to a file the certificate that will contain your public key.
4. Distribute the certificate to your partners. The preferred method for distribution is to send the certificate in a zipped file that is password protected, by e-mail. Your partners must call you and request the password for the zipped file.
5. Use iKeyman to export the self-signed certificate and private key pair in the form of a PKCS12 file.

Installing outbound self-signed certificate:

1. Navigate to **Profile > {Hub Operator/Internal partner} > certificates > Load Certificate**.
2. In the **Select Partner, File Location, Password** page of the wizard, enter the following values:
 - **Which partner does this certificate(s) belongs to:** Select the partner to associate the newly uploaded certificate. Click **Search** to find a specific partner or subset of a partners. If the partner is a Hub Operator or Internal Partner, enter the certificate location, private key location, and password (OR) Provide the truststore or keystore with password. For External Partner, enter the certificate location (OR) provide the trust store location containing the certificate chain.
 - **Private Key:** Click **Browse** to select the Private Key of the certificate.
 - **Password:** If the certificate has a password, enter the value.
 - **Trust Store (or) Keystore Location:** Click **Browse** to select the Keystore Location. Key store is a collection of private keys along with trusted root and CA certificates.
 - **Password:** Enter the password for Keystore Location.
 - **Type:** Select the type of Trust store (or) Keystore. The available values in the drop-down are: JKS, JCEKS, and PKCS12.
3. Click **Next** to go to **Certificate Details** page of the wizard. The **Select end entity and CA certificates** page of the wizard will open when you load

certificates via a trust store that has more than one certificate. The list of certificates available in the trust store is displayed.

4. In the **Select end entity certificate and CA Certificate** page of the wizard, enter the following values:
 - **The keystore contains more than one End Entity certificate. Select the certificate to be uploaded?** - The drop-down has a list of all the End Entity certificates. Select the certificate to upload.
 - **Password** - If the keystore has a password, select this check box and enter the password in the text box.
 - **Select the List of Root and Intermediate CA certificates to be uploaded** - From the list box, select the Root and Intermediate CA certificates to upload.
5. Click **Next** to go to the **Certificate Details** page of the wizard.
6. In the **Certificate Details** page of the wizard, enter the following details of the certificate:
 - **Leaf Certificate Name** - The name of the Leaf Certificate. The field name depends on whether the certificate is a Leaf certificate, Root CA certificate or an intermediate CA certificate.
 - **Description** - The description of the Leaf Certificate.
 - **Certificate Type** - Associate this certificate to Encryption.
 - **Certificate Usage** - Associate an usage for the certificate. The values are Primary and Secondary.
 - **Operation Mode** - Enter the mode of operation.
 - **Status** - Select enabled or disabled based on whether you want to enable or disable a certificate after upload. The Next button is enabled only if the certificate is enabled.
 - **Set Management** - You can either associate a certificate to an existing set or create a new set. If the certificate is a secondary certificate, it can only be associated to an existing set. You can associate the certificate to any set for an internal partner with type encrypt or for an external partner with type SSL (Incoming client auth) or Signing (Verify).

Note: For hub operator, there will not be any set management. The certificates will be associated to the default set created.
7. Click **Next** to go to Set page of the wizard. If the certificate is primary, you do not have to create sets and associate the certificate to a set and participant connection. If you have selected **Create new set** check box, then **Create New Set** page of the wizard will open. Otherwise, the **Add to Existing** page of the wizard will open. If the file contains a private key of the internal partner or the public certificate of the external partner used for SSL / Digital Signature, then you can click **Finish**.
8. In the **Create New Set** page of the wizard, enter the details of the new set. For Primary certificates, you do not have to create sets and associate a certificate to it. Enter the following values:
 - **Set Name** - The name of the Set.
 - **Description** - The description of the Set.
 - **Status** - Select enabled or disabled. If it is disabled the **Next** button will not be enabled.
 - **Make default settings** - Select this check box if you want this set to be the default.

9. In the **Add to Existing Set** page of the wizard, select set(s) to add the certificate. Enter the following values:
 - **Select from the list of Sets available for the selected Certificate type** - From the list, select set(s) to add the certificate.
 - **Make default settings** - Select this check box if you want this set to be the default.
10. From the **Create New Set** or **Add to Existing Set**, click **Next** to go to the **Default Settings** page of the wizard. The **Next** button will be enabled only if the status of the set is enabled.
11. Select **enabled** or **disabled** in the **Status** based on whether you want to enable or disable the Certificate after upload.

Note: If you have selected the **Make default set** check box in the earlier page (Create new set or Add to existing set), then you need to associate the set to an operation mode. This will display certificate usages against operation modes. The encryption will be disabled for internal partners. SSL Client and Digital Signature will be disabled for external partners.

12. Click **Next** to go to the Configuration page of the wizard. In case you click **Finish** and there are some missing roots or intermediate CA certificates, you will be prompted to upload. If you click "Yes" in the prompt window, the first page of the wizard will open. Click **Cancel** if you want to upload at a later stage.
13. In the Configuration page of the wizard, enter the following values:

Note: The Configuration page displays a list of certificate(set) usage against operation modes. The current set name is pre-populated for all, but you can reset it.

- **From Partner** - This field will be pre-populated with the value of the internal partner.
 - **To Partner** - This drop-down is pre-populated with the list of all external partners. You can also select the value "All" to include all external partners.
 - **From Package** - From the drop-down, select the package Document Flow Definitions objects of the internal partner.
 - **To Package** - From the list, select the package Document Flow Definitions objects of the external partner.
14. Click **Add more connections** if you want to associate the set to other participant connections.
 15. Click **Add Secondary Certificate** to add a secondary certificate to the current set.
 16. Click **Finish** to upload the Certificate. In case there are some missing roots or intermediate CA certificates, you will be prompted to upload. If you click "Yes" in the prompt window, the first page of the wizard will open. Click **Cancel** in the prompt window if you want to upload at a later stage.

If you are uploading primary and secondary certificates for both SSL client authentication and digital signature and you are uploading the primary certificates as two separate entries, make sure that the corresponding secondary certificates are uploaded as two different entries.

Obtaining a CA-signed certificate: If you are going to use a certificate signed by a CA, use the following procedure:

1. Start the iKeyman utility.

2. Use iKeyman to generate a certificate request and a key pair for the Receiver.
3. Submit a Certificate Signing Request (CSR) to a CA.
4. When you receive the signed certificate from the CA, use iKeyman to place the signed certificate into the key store.
5. Distribute the signing CA certificate to all partners.

Installing an inbound signature certificate

The Document Manager uses the partner's signed certificate to verify the sender's signature when you receive documents. The partners send their self-signed signature certificates in X.509 DER format to you. You, in turn, install the partners' certificates through the Community Console under the respective partner's profile.

To install the certificate, use the following procedure.

1. Receive the partner's X.509 signature certificate in DER format.
2. Navigate to **Profile > External partner > certificates > Load certificate**.
3. Click **Search** to find specific or sub-set of partners.
4. Click **Browse** next to **Certificate Location** to upload the Certificate.
5. Click **Next** to go to **Certificate Details** page of the wizard.
6. Associate this certificate to **Digital Signature**.
7. Select **enabled** or **disabled** in the **Status** based on whether you want to enable or disable the Certificate after uploading.
8. Select the **Operation mode**. If you are a hub operator, you do not have the option to select the **Operation mode**.
9. Click **Finish** to save the changes and close the wizard.
10. If the certificate is signed by a CA and the CA root certificate and any other certificates that are part of the certificate chain are not already installed in the Hub Operator profile, install the certificates now. This is only applicable for Trust Store/Keystore.
 - a. Click **Account Admin > Profiles > Certificates** to display the Certificate List page.
Make sure you are logged in to the Community Console as the Hub Operator, and install the certificate in your own profile.
 - b. Click **Load Certificate**.
 - c. Select **Root and Intermediate**.
 - d. Type a description of the certificate (which is required).
 - e. Change the status to **Enabled**.
 - f. Click **Browse** and navigate to the directory in which you have saved the certificate.
 - g. Select the certificate and click **Open**.
 - h. Click **Upload** and then click **Save**.

Note: You do not have to perform the previous step if the CA certificate is already installed.
11. Enable signing at the package (highest level), partner, or connection level (lowest level). Your setting can override other settings at the connection level. The connection summary will inform you if any required attribute is missing. For example, to alter the attributes of a partner connection, click **Account Admin > Connections** and then select the partners. Click **Attributes** and then edit the attribute (for example, **AS Signed**).

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 changed by any user of hub administrator groups or the administrator group of the partner.

Warning: Administrator and Default groups are system generated and cannot be edited or deleted. The Hub Administrator group 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 partner 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). The user name is unique.

- 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 the **Status** as to whether 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 the **Language Locale**, **Format Locale**, and **Time Zone**.
9. Select the **Alert Status** as to whether 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.

10. Select the user's **Subscribed Visibility** as to whether the user is only visible to your organization (Local), or visible to the entire hub community (Global).
11. 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.
12. Click **Save**. Repeat these steps to add additional users.

Configuring FTP user

To enable current user as a FTP user, do the following:

1. Click **Account Admin > Profiles > Users**. The system displays the User List screen.
2. Select the required user and click **Edit** icon.
3. Click **FTP Configuration**.
4. Enter the **Home directory**, which is the relative path from the value specified for the `bcg.ftp.config.rootdirectory`. This is a required field.
5. Enable or disable **Write Permission** to the home directory.
6. Enable or disable permission to **Create/Remove Directory**.
7. Select **Max Login Number**, which is the maximum concurrent login allowed. If you select Custom Limit, enter the customized value in the text box.
8. Select **Max Login from Same IP**, which is the maximum concurrent login allowed from the same IP address. If you select Custom Limit from the list, enter the customized value in the text box.
9. Select **Max Idle Time**, which is the maximum idle time in seconds after which the user connection is discarded. If you select Custom Limit from the list, enter the customized value in the text box.
10. Select **Max. upload**, which is the maximum rate of upload in bytes/sec. If you select Custom Limit from the list, enter the customized value in the text box.
11. Select **Max. Download**, which is the maximum rate of download in bytes/sec. If you select Custom Limit from the list, enter the customized value in the text box.
12. Click **Save**.

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 **Add to Group** or **Remove from Group** 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 internal partner'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 **Given Name** and **Family Name**.
4. Enter the contact's **Address**.
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 **Language Locale**, **Format Locale**, and **Time Zone**.
9. Select the **Alert Status** as to whether you want to Enable or Disable alert notification for this contact. When enabled, the contact receives all subscribed alerts. When disabled, the contact does not receive alerts.

Note: The Subscribed value is system populated.

10. Select the contact's **Subscribed Visibility**. If you select Local, the contact is only visible to your organization. If you select Global, the contact is visible to the hub administrator and internal partner. 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 34.
 - To create a volume-based alert and add contacts to the alert, see "Creating a volume-based alert" on page 31.
 - To create an event-based alert and add contacts to the alert, see "Creating an event-based alert" on page 33.

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 an external partner, you can create a volume-based alert that notifies you if you do not receive any transmissions from the internal partner 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 internal partner network transmission difficulties.

If you are an external partner, you can also create a volume-based alert that warns you when the number of transmissions from the internal partner 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 internal partner, 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 type that you select when you create the alert. WebSphere Partner Gateway only looks at documents that contain the document type 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 external partner can only create a volume-based alert on the volume of documents sent to the internal partner. For the external partner to set up a volume-based alert on the volume of documents sent from the internal partner to the external partner, the external partner would request the hub administrator to set up a volume-based alert on the external partner's behalf, specifying the external partner as the alert owner.

Tip:

- Use a volume-based alert to receive notification if expected
- External partner or internal partner transmission volume falls below operating limits. This alert can highlight external partner or internal partner 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 an **Alert Name** for the alert.
5. Select a **Partner** with rights to create a volume-based alert (internal partner and hub administrator only).
6. Select **Package**, **Protocol**, and **Document Type** from the drop-down lists. The selected Package, Protocol, and Document Type must match the Package, Protocol, and Document Type of the source external partner.
7. Select one of three volume options (Expected, Range, or Zero Volume), then proceed to 8 on page 31:
 - **Expected** - Select Expected if you want an alert generated when document type volume deviates from an exact quantity. Use the following steps to create an alert on expected document type volume:
 - a. In the Volume text box, enter the number of document types 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 types 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 types 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 types 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 **Alert Status** of this alert as Enabled or Disabled.
 12. Click **Save**.
 13. Click the **Notify** tab.
 14. Click the Edit icon.
 15. Select a partner (internal partner and hub administrator 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 partners.
 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 hub administrator and internal partner. 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

Note: The Alert e-mail server needs to be configured. See the *Administration Guide* for configuring the alert e-mail server

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 an **Alert Name** for the alert. This will be your identifier for this alert.
5. Select a **Partner** that will trigger the alert (this option is only available to the internal partner and hub administrator).

Select the Any Partner option to associate the alert with all the partners in the system. When you perform an alert search and select Any partner as the Alert Partner, the system displays all alerts that are not associated with a specific partner.

6. Select **Package**, **Protocol**, and **Document Type** from the drop-down lists.
7. Select the event type: Debug, Information, Warning, Error, Critical, or All. This acts as a filter to limit the events that appear in Event Name list.
8. 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
9. Select the status of this alert: Enabled or Disabled.

10. Click **Save**.

11. Click the **Notify** tab.

12. Click the Edit icon.

13. Select a partner (internal partner and hub administrator only).

14. If the contact that you want to add is listed in the Contacts text box, select the contact and click **Subscribe**. Go to 19.

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

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

15. Enter the contact's name, e-mail address, telephone and fax numbers. Only the e-mail address is used for sending out alerts. The rest of the entries is for additional informational purposes.
16. Select the contact's Alert Status.
 - Select **Enabled** to begin sending e-mail messages to this contact when the system generates this alert.
 - Select **Disabled** if you do not want to send e-mail messages to this contact when the system generates this alert.
17. Select the contact's visibility.

- Select **Local** to make the contact only visible to your organization.
 - Select **Global** to make the contact visible to the hub administrator and internal partner. Both of these parties can subscribe the contact to alerts.
18. Click **Save** to save the contact. Click **Save and Subscribe** to save the contact and add the contact to the list of contacts for this alert.
19. Select the Mode of Delivery:

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

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

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

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

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

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

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

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

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

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

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

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

20. Click **Save**.

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 partner (internal partner and hub administrator 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 Partners.
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 hub administrator and internal partner. 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 partner 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 destinations

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

- “Overview”
- “Setting up an HTTP destination”
- “Setting up an HTTPS destination” on page 39
- “Setting up an FTP destination” on page 40
- “Setting up an SMTP destination” on page 41
- “Setting up a JMS destination” on page 42
- “Setting up a file-directory destination” on page 43
- “Setting up an FTPS destination” on page 44
- “Setting up an FTP Scripting destination” on page 45
- “Configuring handlers” on page 48
- “Specifying a default destination” on page 48

Overview

WebSphere Partner Gateway uses destinations to route documents to their proper destination. The recipient can be an external partner or the internal partner. The outbound transport protocol determines which information is used during destination configuration.

The following transports are supported (by default) for partner destinations:

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

Note: You can define an SMTP destination for external partners only (not for the internal partner).

- File directory
- FTP Scripting

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

Setting up an HTTP destination

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

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

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

Destination Details

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

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

Destination configuration

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

1. Optionally, select a proxy server to be used. The **Forward Proxy List** includes any proxy servers that you have created, including the default proxy server. The default value for this field is **Use default forward proxy**. If you want the selected partner to use a different proxy server, select that server from the list. If you do not want to use this feature for the selected partner, select **Use no forward proxy**.
2. Select **HTTP/1.1** from the **Transport** list.
3. 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 destination 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.
4. Optionally enter a user name and password, if a user name and password are required to access the HTTP server.
5. In the **Retry Count** field, enter the number of times you want the destination to attempt to send a document before it fails. The default is 3.
6. In the **Retry Interval** field, enter the amount of time the destination should wait before attempting to send the document again. The default is 300 seconds.
7. In the **Number of Threads** field, enter the number of documents that can be processed simultaneously. The default is 3.
8. 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**.
9. In the **Auto Queue** field, select **Yes** if you want the destination 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 destination 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 destination, go to “Configuring handlers” on page 48. Otherwise, click **Save**.

Setting up an HTTPS destination

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

To create HTTPS destinations, use the following procedure.

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

Destination Details

From the Destination List page, perform the following steps:

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

Destination Configuration

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

1. Select **HTTPS/1.0** or **HTTPS/1.1** from the **Transport** list. HTTP/S destination configuration does not contain forward proxy configuration.
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 destination 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 destination 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 destination 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 destination 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 destination, go to “Configuring handlers” on page 48. Otherwise, click **Save**.

Setting up an FTP destination

To create an FTP destination, use the following procedure.

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

Destination Details

From the Destination Details page, perform the following steps:

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

Destination Configuration

In the **Destination 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 destination 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 destination 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 destination 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 destination 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 destination, go to “Configuring handlers” on page 48. Otherwise, click **Save**.

Setting up an SMTP destination

To create an SMTP destination, use the following procedure.

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

Destination Details

From the Destination List page, perform the following steps:

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

Destination Configuration

In the **Destination 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 destination 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 destination 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 destination 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 destination 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 destination, go to “Configuring handlers” on page 48. Otherwise, click **Save**.

Setting up a JMS destination

To create JMS destinations, use the following procedure.

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

Destination Details

From the Destination List page, perform the following steps:

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

Destination Configuration

In the **Destination 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 JMS 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 destination 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 destination 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 destination 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 destination 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 destination, go to “Configuring handlers” on page 48. Otherwise, click **Save**.

Setting up a file-directory destination

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

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

Destination Details

From the Destination List page, perform the following steps:

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

Destination Configuration

In the **Destination 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 destination 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 destination 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 destination 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 destination 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 destination, go to “Configuring handlers” on page 48. Otherwise, click **Save**.

Setting up an FTPS destination

To create FTPS destinations, use the following procedure.

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

Destination Details

From the Destination List page, perform the following steps:

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

Destination Configuration

In the **Destination 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 destination 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 destination 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 destination 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 destination 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 destination, go to “Configuring handlers” on page 48. Otherwise, click **Save**.

Setting up an FTP Scripting destination

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

Creating the FTP script

To use an FTP Scripting destination, 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 destinations, 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 destination is put in service by the values you enter when you create a specific instance of an FTP scripting destination, as shown in the following table:

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

Script parameter	FTP Scripting destination 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 destinations

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

To create FTP Scripting destinations, use the following procedure.

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

Destination Details

From the Destination List page, perform the following steps:

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

Destination Configuration

In the **Destination 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 destination 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 destination 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 destination will request a lock, so that no other instances of an FTP Scripting destination 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 %BCGOPTION x % 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 destination 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 destination 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 destination, go to “Configuring handlers.” Otherwise, click **Save**.

Configuring handlers

You can modify two processing points for a destination--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 destination

After you create destinations for the internal partner or external partner, select one of the destinations as the default destination.

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

A list of destinations defined for the partner is displayed.

4. From the **Production** list, select the destination that will be the default for this partner. You can also set default destinations for other types of destinations, 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 Partner Connection Not Found, RosettaNet Validation Error, and Document Delivery Failed.

You will also use this module to maintain your partner profile, certificates, destinations, 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 destinations”

“Managing Certificates” on page 53

“Managing groups” on page 53

“Managing users” on page 54

“Managing contacts” on page 56

“Managing alerts” on page 57

“Managing addresses” on page 59

Managing destinations

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

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

Viewing a list of destinations

Click **Account Admin > Profiles > Destinations** to view a list of destinations in the system.

Viewing or editing destination details

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

1. Click **Account Admin > Profiles > Destinations**. The system displays the Destination List screen.
2. Click the View details icon to view destinations details.
3. Click the Edit icon to edit destination details.

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

Table 5. Values on the destination screen

Value	Description
Destination Name	Name of destination. Note: Destination Name is a user-defined free format field. Users should use different names for individual destinations 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 destination is placed online.
Status	Enabled or Disabled. Documents routing through a destination with a disabled status fail processing.
Default	Identifies the default destination.

5. Click **Save**.

View, select, or edit your default destinations

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

Viewing destination Whereused

To view the details of where all a particular destination is employed, use the following procedure:

1. Click **Account Admin > Profiles > Destinations**
2. From the destination list, click **Whereused** icon against the appropriate destination. The list of where all the selected destination is being used is displayed.

Note: This screen is provided with paging info as there could be many channels using the destination. Every page will hold a maximum of 10 connections.

Deleting destination

This delete destination feature is available for all the destinations except for default destination. To delete a destination, use the following procedure:

1. Click **Account Admin > Profiles > Destinations**.
2. From the list of destinations, click the **Delete** icon that is against the destination to be deleted.

Note: **Delete** icon will not be available for default destination. Also, delete operation is allowed only if the selected destination is not used at the connections. In case you need information about the usage of the destination, see "Viewing destination Whereused."

3. Click **OK** in the warning window to confirm deletion.

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. This facility is available only to the administrator group users of internal/external partners.

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 **Add to Group** to assign users to the group.
5. Click Edit off icon to save and exit.

Viewing, editing, or assigning group permissions

The group permission for users and groups cannot be set by even administrator group user. The permissions of other groups can always be lesser or equal to that

of administrator permissions. For example, if the administrator has read only permission to Address, the permission of other groups can be "no access" or "read only".

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 Hub Administrator 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 partner profiles. This facility is available only to the administrator group users of internal/external partners.

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**.

Deleting users

You must have the appropriate permissions to delete users. All users can be deleted using this functionality except HUBADMIN.

Use this feature to delete a user:

1. Click **Account Admin > Profiles > Users**
2. Click **Delete** icon against the user you want to delete.
3. In the warning window, click **OK** to confirm your deletion. Click of **Cancel** will abort the deletion.

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 internal partner'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 hub administrator and internal partner. 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 hub administrator and internal partner. 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 internal partner 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 partner (internal partner or hub administrator only). The internal partner 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 Partners

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 internal partner and hub administrator

Value	Description
Alert Owner	Creator of the alert.
Alert Partner	Partner 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 hub administrator 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 hub administrator and Alert Owner (the creator of the alert) can remove an alert.

Event Notification

WebSphere Partner Gateway allows you to configure an Event Alert, so that when the Event occurs, both the Source Partner and the Target Partner of the event will be notified. There are now two options available for Alert Notification. They are:

- Notify all Related Parties
- Notify Subscribed Contacts Only

When the Notify all Related Parties option is selected, the alert will automatically notify the Source Partner contacts and the Target Partner contacts of the Event, as well as the Alert Owner's contacts. The user does not need to (and is not allowed) to specify "Subscribed Contacts" when this mode is selected. When the Notify Subscribed Contacts Only mode is selected, the alert alerts only the subscribed contacts.

After determining the parties to be notified, you are able to choose if you will:

- Send the alerts immediately
- Batch the alerts (by count or time)

Note: The Alert e-mail server must be configured to use this additional functionality. See the, *System Administrator Guide* for instructions on configuring this server.

Managing addresses

Use this feature to manage the addresses in your partner 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”
- “AS Viewer” on page 63
- “ebMS Viewer” on page 66
- “RosettaNet Viewer” on page 68
- “Document Viewer” on page 70
- “Destination Queue” on page 74

The RosettaNet and AS Viewers include additional search criteria for the hub admin. For more information, see the *Administrator Guide*.

Note: The term partners is used on the Viewer screens to identify a hub community member, including the internal partner.

Event Viewer

The Event Viewer allows you to search for events by time, date, event type, event name, and event location. The hub admin can also search by partner, Source IP, and Event ID.

The data that the Event Viewer generates identifies, among other things, the Event Name, 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 partner was successfully added to the system, or a partner connection was successfully created between internal partner and external partner). 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 Partner Gateway 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 Name (for example, 210031), and event location.

Data available through the Event Viewer includes event name, time stamp, user, and partner 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 Partner Gateway 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 62
View event details.	page 63

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.
partners	Select all partners or a specific partner (internal partner only).
Event type	Type of event: Debug, Info, Warning, Error, or Critical.
Event name	Search on available event names 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 (internal partner 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.

AS Viewer

Use the AS Viewer to search for and view transport information for documents using the AS1, AS2 or AS3 communication protocols. You can view message IDs, Message Disposition Notification (MDN) destination URI and status, and document details (the document and wrapper).

The AS Viewer can also be used to view packaged B2B transactions and B2B process details that use the AS1, AS2 or AS3 (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. AS2 provides an encryption base with guaranteed delivery. AS3 provides a new standard for securely transmitting documents over FTP or FTPS.

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 AS Viewer to view the message ID, Time Stamps, DocumentType, Destination Type, Synchronous status, as well as document details. Additional document processing information is displayed when viewing document details.

Performing AS Viewer tasks

Table 17. AS1/AS2 Viewer tasks

What do you want to do?	See
Search for AS messages	page "Searching for messages"
Viewing raw documents	page "Viewing message details" on page 65

Searching for messages

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

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

Table 18. AS Viewer search criteria

Value	Description
Start Date and Time	Date and time the process was initiated.
End Date and Time	Date and time the process was completed.
Source Partner	Identifies the transmitting partner (internal partner only).
Target Partner	Identifies the receiving partner.
Search on	Specifies if the document to be searched is the source or the target document type.
AS Source Business ID	Business identification number of the source partner, for example, Duns.
Payload Source Business ID	Payload source identification number.
Operation Mode	Production, Test, RN Simulator External Partner, or RN Simulator Internal Partner. Test is only available on systems that support the test destination type.
Package	Describes the document format, packaging, encryption, and content-type identification.
Protocol	Document format available to the partners, for example, RosettaNet or XML.
Document Type	The specific business process.
Message ID	ID number assigned to the AS1, AS2 or AS3 packaged document. Search criteria can include the asterisk (*) wildcard. Maximum length, 255 characters.
Document ID	Unique identification number assigned to the document.
Synch / Async	Search for documents received in synchronous or asynchronous mode. The synchronous mode 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).
MDN Status	This field allow you to select the status of the MDN on this message.
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 > AS Viewer**. The system displays the AS 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. AS Viewer: Package Details

Value	Description
Message ID	ID number assigned to the AS1, AS2 or AS3 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 Partner	Partner initiating a business process.
Target Partner	Partner receiving the business process.
Initiating Time Stamp	Date and time the document begins processing.
Destination Type	Test or production. Test is only available on systems that support the test destination 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.

ebMS Viewer

The ebXML Message Service (ebMS) mechanism provides a standard way to exchange business Messages among ebXML Trading Partners. It provides a reliable means to exchange business messages without relying on proprietary technologies and solutions. An ebXML message contains structures for a message header (necessary for routing and delivery) and a payload section. ebMS provides a standard way to exchange business Messages among ebXML Trading Partners. An ebXML message is a communication protocol independent MIME/Multipart message envelope.

Performing ebMS Viewer tasks

Table 20. ebMS Viewer tasks

What do you want to do?	See
Search for ebMS Processes	"Searching for ebMS processes"
View ebMS Processes	"View ebMS process details" on page 67
View Raw Documents	"View raw documents" on page 67
Viewing Document Status	"Viewing the Document Status" on page 68

Searching for ebMS processes

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

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

Value	Description
Start Date and Time	The date and time that the process was initiated.
End Date and Time	The date and time that the process was completed.
Source Partner	Identifies the sending partner.
Target Partner	Identifies the receiving partner.
Source Business ID	Business identification number of initiating partner, for example, DUNS.
Operation Mode	Production, test, RN Simulator External Partner or RN Simulator Internal Partner. Test is only available on systems that support the test destination type.
Protocol	Protocols available to the partners.
Document Type	Type of document to be processed.
Conversation ID	Unique identification information 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 ebMS processes that match your search criteria.

View ebMS process details

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

Table 21. ebMS Viewer search criteria values

Value	Description
Partners	Partners involved in the business process.
Source Time Stamp	Date and time the first document begins processing.
Document Type	The specific business process, for example: ebMS 2.0 : ALMSERVICE Production
Operation Mode	Mode of Operation, for example: Production
Conversation Id	Unique identification number assigned to this event

View raw documents

To view the raw document:

1. Click **Viewers > ebMS Viewer**.
2. Select the search criteria from the drop down lists see, "Searching for ebMS processes" on page 66
3. Click **Search**.
4. Click the "Click to view raw document" icon under the **Legend** section .

- To troubleshoot documents that have failed processing, see “Viewing data validation errors” on page 72.
- The raw document viewer displays the HTTP header with the raw document.

Viewing the Document Status

1. Click **Viewers > ebMS Viewer**.
2. Select the search criteria from the drop down lists see, “Searching for ebMS processes” on page 66
3. Click **Search**.
4. Click **Request Status** .
5. Click **View Status**.

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. Partner 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 internal partner and external partners.

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 22. RosettaNet Viewer tasks

What do you want to do?	See
Search for RosettaNet processes.	page 68
View RosettaNet process details.	page 69
View raw documents.	page 70

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. **START HERE**

Table 23. RosettaNet search criteria

Value	Description
Start Date and Time	The date and time that the process was initiated.
End Date and Time	The date and time that the process was completed.
Source Partner	Identifies the sending partner.
Target Partner	Identifies the receiving partner.
Source Business ID	Business identification number of initiating partner, for example, DUNS.
Operation Mode	Production, test, RN Simulator External Partner or RN Simulator Internal Partner. Test is only available on systems that support the test destination type.
Protocol	Protocols available to the partners.
Document Type	Type of document to be processed.
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.
4. Click the View details icon next to the ebMS 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 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 24. Document processing details

Value	Description
Partners	Partners involved in the business process.
Time Stamps	Date and time the first document begins processing.
DocumentType	The specific business process, for example RosettaNet (1.1): 3A7.
Destination 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 partner. The field is not in a fixed location and varies by document type.
Source Partner	Initiating partner.
Target Partner	Receiving partner.

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 DocumentType 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 72.
- 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), partner connection, destination type, document status, protocol, document type, and process version.

Some protocols, such as custom Extensible Markup Language (XML) protocol using XML formats, can extract information from documents and save it so you search for it using the Document Viewer. That is the purpose of the user search field attributes in an XML format definition. In the case of document routed using an XML format that includes search fields, the document information obtained using the search fields can be the target of a search. An example is a custom XML document that is a purchase order. Using your knowledge of the document structure, you can define an XML format with a search field that extracts the purchase order number. When documents are routed using this XML format, you can search for them using the purchase order number by entering the number in the appropriate User Defined search field in the Document Viewer search screen.

Routing for Electronic Data Interchange (EDI) documents that extracts information from the document can also be defined. This is done by coding a DIS map so that it will populate the values for the User Defined search fields.

You can also write a user exit that will extract information from the document so that it can be the target of a search. Use the user exit method `BusinessDocumentInterface.setAttribute()` to populate the values for the User Defined search fields.

The search results display all documents that meet your search criteria, and identify time stamps, process, partner connection, and destination types. Locate the target document and use the viewer’s features to view the raw document. You can also use the Document Viewer to re-send 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 25. Document Viewer search criteria

Value	Description
Start date and time	Date and time the process was initiated.
End date and time	Date and time the process was completed.
Source Partner	Identifies the sending partner.
Target Partner	Identifies the receiving partner. .
Search on	Search on From or To document type.
Operation Mode	Production, test, RN Simulator External Partner or RN Simulator Internal Partner. Test is only available on systems that support the test destination 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 partners.
Document Type	The specific business process.
Document ID	Created by the source partner. 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 partner.
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.
User Defined Search Fields	Perform search based on user-defined criteria.

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

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

Table 26. Document information available using the Document Viewer

Value	Description
Partners	Source (From) and target (To) partners involved in the business process.
Time Stamps	Date and time the document begins and ends processing.
Document Type	Business process that is being transacted.
Destination Type	Test or production. Test is only available on systems that support the test destination 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 27. Document processing values available using the Document Viewer

Value	Description
Reference ID	Unique identification number assigned to the document by the system.
Document ID	Unique identification number assigned to the document by the source partner.
Doc Time Stamp	Date and time document was created by partner.
Destination	Destination the document passed through.
Connection Document Type	Actions performed on a document by the system to ensure its compatibility with business requirements between partners.
Source and Target	Source and target partners involved in business process.
In Time Stamp	Date and time the document was received by the system from the partner.
End State Time Stamp	Date and time the document was successfully routed by the system to the target partner.
Source and Target Business ID	Business identification number of Source and Target partners, for example, DUNS.
Source and Target Document Type	The specific business process transacted between source and target partners.

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 72.

Viewing data validation errors

You can quickly search for documents that have failed processing using the color-coded text in the XML fields that contain validation errors. Fields that contain validation errors are displayed in red. If up to three separate validation errors

occur within nested XML fields, the following colors are used to distinguish between the error fields:

Table 28. Color-coded document validation errors

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

The following is an example of nested XML validation errors:

```

<?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>
            </BusinessDescription>
          </PartnerDescription>
        </PartnerRoleDescription>
      </fromRole>
    </Pip3A7PurchaseOrderUpdateNotification>
  </SYSTEM>
</?xml>

```

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.

Example of non-nested XML validation errors:

```

<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>
    </ContactInformation>
  </PartnerRoleDescription>
</billTo>

```

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

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

To view validation errors in a raw document, see “Viewing raw documents” on page 70.

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 not restricted to hubadmin user. The permissions of the group needs to be configured to avail this facility.

Note: It can 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.

Destination Queue

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

The Destination 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 Destination Queue, you can:

- See a list of all destinations containing documents queued for delivery
- View a document that has been in a destination 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 documents from the queue.

Note: If you are implementing an FTP Scripting Destination with an interval or calendar schedule, documents may stay in this queue for an extended period until that interval or date and time is reached. This is expected operation, and the documents should not be removed from the queue.

- View destination details to ensure proper operation. Documents backing up in a Destination Queue can indicate a fault in the delivery manager or destination.
- Confirm destination status. An offline destination causes documents to collect in the queue until the destination is placed online. Destination status does not affect connection functionality, and documents continue to be processed and placed in the queue for delivery.
- Limit the size of the Destination Queue list with the **Partner Name** and **Destination** fields.

Viewing the destination list

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

1. Select **Viewers > Destination Queue**. The Console displays the Destination Queue window.

2. Input the parameters shown in Table 29.

Table 29. Destination Queue window

Criteria	Description
Partner Name	To complete this field you can: <ol style="list-style-type: none"> 1. Specify the Partner name. 2. Specify part of the partner name in this field and click Show Partners. Select the partner from the partner list. 3. Specify the wildcard * and click Show Partners. Select the partner from the partner list.
Destination	Clicking Show Partners displays a Partner field on the page. The Partner field lists all the available partners in alphabetical order. The first item in this list is A11, which is selected by default. The rest of the list is an ordered list of destination transports. On this list, you can select only a single destination. The default is A11. Note: The Destination list is automatically populated with the selected partner's destinations and the list is presented in alphabetical order.
Queued at least	Minimum number of minutes a document has been waiting in the destination queue. For example, if 6 minutes is selected, all destinations containing documents that have been waiting for delivery for 6 minutes or more will be displayed. The default is 0.
Sort By	Sort search results by Partner (default) or Destination Name.
Refresh	Turn refresh on or off (default).
Minimum Queued	Minimum number of documents in a destination queue. The default is 1.
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 Rate	Number of seconds the Console waits before updating displayed data.

3. Click **Search**. The system finds all documents in the destination that match your search criteria. Table 30 shows the information returned from the search.

Table 30. Results after destination queue search

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

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

Viewing queued documents

To view documents queued for a specific Partner:

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

- From the Queue Documents Search window, specify the search criteria (see Table 31 on page 76).

Table 31. Queue Documents Search window

Criteria	Description
Partner Name	To complete this field you can: <ol style="list-style-type: none"> Specify the Partner name in the field. Specify part of the partner name in this field and click Show Partners. Select the partner from the list. Specify the wildcard * and click Show Partners. Select the partner from the partner list. <p>Note: Clicking Show Partners displays a Partner field on the page. The Partner field lists all the available partners in alphabetical order.</p>
Destination	The first item in this list is All, which is selected by default. The rest of the list is an ordered list of destination transports. On this list, you can select only a single destination. The default is All. <p>Note: The Destination list is automatically populated with the selected partner's destinations and the list is presented in alphabetical list.</p>
Sort By	Select whether the list should be sorted by Partners (the default), by Destinations, Reference ID, or Queued timestamp (the time the document was last sent).
Reference ID	Type the unique identification number assigned to the document by the system.
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.
Document ID	Type the unique identification number assigned to the document by the source partner.
Results Per Page	Specifies the number of documents displayed on a page.
Maximum Documents Allowed	Specifies the number of records to be displayed.

- Click **Search**. The results of the queues search are displayed.

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.

- Click **Viewers > Destination Queue**.
- From the Destination Queue window, click **Search**.
- Complete the parameters in the window (see Table 30 on page 75).
- Click the delete icon to delete the document.

Viewing destination details

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

- Click **Viewers > Destination Queue**.
- From the Destination Queue window, type the search criteria (see Table 29 on page 75).
- Click **Search**.

4. From the list of destinations, click the document count link in the **Queued** column. Destination details and a list of queued documents appear.

Changing destination status

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

1. Click **Viewers > Destination Queue**.
2. From the Destination Queue window, type the search criteria (see Table 29 on page 75).
3. Click **Search**.
4. From the list of destinations, click the document count link in the **Queued** column. Destination details and a list of queued documents appear.
5. Click **Online** in **Destination Info** to place a destination offline, or click **Offline** to place destination online. (You must be logged in as hub admin to change destination status.)

Chapter 6. Analyzing Document Type: 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), destination type, protocol, Document Type, 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 Partner Connection tool is used to test the destination or Web server.

Table 32. Tools

What feature do you want to use?	See
Document Analysis	page 79
Document Volume Report	page 81
Test Partner Connection	page 83
EDI Reports	page 85
FTP Reports	page 89

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 33. 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 external partner or internal partner.
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 partner.

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 34. 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 Partner	The partner that initiated the business process (internal partner only).
Target Partner	The partner that received the business process (internal partner only).
Search On	Search on From document type or To document type.
Destination Type	For example, Production or test. Test is only available on systems that support the test destination type.
Package	Describes document format, packaging, encryption, and content-type identification.
Protocol	Document protocol available to the partners.
document type	Specific business process.
Sort By	Sort results by Source Partner Name or Target Partner Name.
Refresh	Controls if the search results are refreshed periodically (internal partner only).
Refresh Rate	Controls how often search results are refreshed (internal partner 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 partners that you want to view. The system displays a list of all documents for the selected partners. 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.

Custom XML File Processing

WebSphere Partner Gateway V6.0 and earlier versions provided support for custom Extensible Markup Language (XML) processing by using XML formats. WebSphere Partner Gateway V6.0 and earlier XML formats do not allow the full use of the XPath expression language to extract processing information from documents. That is why WebSphere Partner Gateway V6.1 redesigned the way that XML formats operate. In WebSphere Partner Gateway V6.1, XPath version 1.0 expressions can be used in the formats. The added processing power of full XPath support limits the size of files that can be used with the full XPath XML formats. To allow large files to be processed an option is provided that you set when you define a document family. Formats in a family with the large file processing option have the same limited XPath processing power that was provided by WebSphere Partner Gateway V6.0 and earlier versions, but large files can be processed. When the large file option is used in a document family, then these limitations are placed on the expressions used in the XML formats that are stored in the family:

1. Only simple element paths that begin at the root of the document can be used.
2. Element paths must not include namespace prefixes even though they may appear in the documents.

The Manage XMLFormats window includes a drop-down list labeled Large file options. The list includes choices: *None*, *Use large file processor*, and *Use namespace-aware large file processor*. The user selects a large file option if they are writing XML formats that will match large documents that cannot be handled using the full XPath processor. The namespace-aware option means that element paths include namespace prefixes when they appear in a document.

Note: This option cannot be changed once the family is created. This is because the document family may already include XML formats that will be made invalid if the family type is changed. Custom XML File processing is unavailable to partners.

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 35. 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 partner.

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 internal partner, help partners 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 36. 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 Partner	The partner that initiated the business process (internal partner only).
Target Partner	The partner that received the business process (internal partner only).
Search on	Search on From document type or To document type.
Destination Type	Production or test. Test only available on systems that support the test destination type.
Package	Describes document format, packaging, encryption, and content-type identification.
Protocol	Type of process protocol, for example, XML, EDI, flat file.
document type	Specific business process.
Sort By	Sort results by this criteria (document type or Target document type).
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 Partner Connection

The Test Partner Connection feature allows you to test the destination or Web server. If you are the internal partner, you can also select a specific partner. The test consists of sending a blank POST request to a destination 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 destination 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 Partner Connection feature works with HTTP that does not require any connection parameters.

To test a partner connection:

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

Table 37. Test Partner Connection Values

Value	Description
Partner	Partner to be tested (internal partner only).
Destination	Displays available destinations based on the partner selected above.
URL	Dynamically populated based on the destination 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 does not 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 does not 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 does not 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 do not 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 could not give you a meaningful response. There is typically 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 Destination - The server received an invalid response from the destination 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 - Destination Time out - The server did not receive a timely response from the destination or upstream server it accessed in attempting to complete the request.
- 505 - HTTP Version Not Supported

EDI Reports

Use EDI Reports to search overdue electronic data interchange (EDI) functional acknowledgments (FA). You can also search for rejected electronic data interchange (EDI) transactions. The following sections detail the procedure to use EDI Reports.

EDI FA Overdue Search

The EDI FA Overdue Search page provides search criteria for performing a search for overdue electronic data interchange (EDI) functional acknowledgments (FA).

Note: Any records, returned by previous EDI FA overdue searches, that were removed from the resulting reports will be ignored by later searches. Therefore, removed records are not displayed in later reports. Records can be removed from a report by selecting **Ignore Selected Records** on the EDI FA Overdue Report page. Only the hub administrator can remove records from a report.

To search for the EDI FA Overdue records, do the following:

1. Click **Tools > EDI Reports**. The EDI FA Overdue Search screen is displayed.

2. Select one or more search criteria from the drop-down list:

Table 38. EDI FA Overdue Search Criteria

Value	Description
Start date & time	The date and time the transaction was initiated.
End date & time	The date and time the transaction was completed.
Source Partner	The partner that initiated the transaction.
Target Partner	The partner that received the transaction.
Search on	Search on Source document type or Target document type.
Package	Describes document format, packaging, encryption, and content-type identification.
Protocol	Type of process protocol, for example, XML, EDI, flat file. The protocols displayed vary depending on the value you select in the Package field.
Document type	Specific document type. The types displayed vary depending on the value you select in the Protocol field.
Reference ID	Specifies a transaction ID.
Sort By	Specifies the criteria for sorting the search results. The defaults are Overtime Due and Descend. Use Descend to display the most overdue FAs first. Select Ascend to display the least overdue FAs first.
Results Per Page	Specifies the number of transaction search results to display on each page.

3. Click **Search** to display the EDI FA Overdue Search report.

Viewing EDI FA Overdue reports

Depending on the search criteria selected on the EDI FA Overdue Search page, the search result is displayed in the EDI FA Overdue Report page.

The following data, when applicable, is displayed in the EDI FA Overdue report.

Table 39. EDI FA Overdue Report

Value	Description
Date	The Date on which the EDI was sent from the source partner to the target partner.
Time	The time (GMT) at which the EDI was sent from the source partner to the target partner.
ActivityID	The virtually unique ID (VUID) of the transaction.
Source Trading Partner	The partner that sent the transaction.
Source Package	The source package of the transaction.
Source Protocol	The source protocol of the transaction.
Source Document Type	The source document type of the transaction.
Target Trading Partner	The partner that sent the transaction.
Target Package	The target package of the transaction.
Target Protocol	The target protocol of the transaction.
Target Document Type	The target document type of the transaction.
Interchange Number	The interchange number of the transaction.
Group Number	The group number of the transaction.
Transaction Number	The identifying number of the transaction.
FA Due By	The date that the FA for the transaction was due.
Overdue By	The amount of time that the FA is overdue.
Ignore Selected Records	When you select this option for a record, that particular record is removed from the report. Once a record is removed from a report, that record is ignored by later EDI FA overdue searches, and therefore, is not displayed in the resulting reports. Only the hub administrator can remove records from a report.

EDI Rejected Transaction Search

The EDI Rejected Transaction Search page contains criteria for performing searches for electronic data interchange (EDI) transactions that have a functional acknowledgment (FA) containing an error code. Transaction records without FAs are not returned by an EDI rejected transaction search.

To search for the EDI Rejected records, do the following:

1. Click **Tools > EDI Reports > EDI Rejected Report**.

2. Select one or more search criteria from the drop-down list:

Table 40. EDI Rejected Transaction Search Criteria

Value	Description
Start date & time	The date and time the transaction was initiated.
End date & time	The date and time the transaction was completed.
Source Partner	The partner that initiated the transaction.
Target Partner	The partner that received the transaction.
Search on	Search on Source document type or Target document type.
Package	Describes document format, packaging, encryption, and content-type identification.
Protocol	Type of process protocol, for example, XML, EDI, flat file. The protocols displayed vary depending on the value you select in the Package field.
Document type	Specific document type. The types displayed vary depending on the value you select in the Protocol field.
Reference ID	Specifies a transaction ID.
Sort By	Specifies the criteria for sorting the search results. The defaults are Overtime Due and Descend. Use Descend to display the most overdue FAs first. Select Ascend to display the least overdue FAs first.
Results Per Page	Specifies the number of transaction search results to display on each page.

3. Click **Search** to view the EDI Rejected Transaction report.

Viewing EDI Rejected Transaction reports

Depending on the search criteria selected on the EDI Rejected Transaction Search page, the search result is displayed in the EDI Rejected Transaction Report page.

The following data, when applicable, is displayed in the EDI Rejected Transaction report.

Table 41. EDI Rejected Transaction Report

Value	Description
Date	The Date on which the EDI was received.
Time	The time (GMT) at which the EDI transaction was sent from the source partner to the target partner.
ActivityID	The virtually unique ID (VUID) of the transaction.
Source Trading Partner	The partner that sent the transaction.
Source Package	The source package of the transaction.
Source Protocol	The source protocol of the transaction.
Source Document Type	The source document type of the transaction.
Target Trading Partner	The partner that received the transaction.
Target Package	The target package of the transaction.
Target Protocol	The target protocol of the transaction.
Target Document Type	The target document type of the transaction.
Interchange Number	The interchange number of the transaction.
Group Number	The group number of the transaction.
Transaction Number	The identifying number of the transaction.
Status Code	The status code of FA.
Status Text	The status text of FA.

FTP Reports

FTP Reports provides details on FTP Statistics and FTP Connections.

FTP Statistics

The FTP Statistics page will display the FTP Server Status in Read Only Mode.

Note: The statistics will not be displayed if the FTP Server or the FTP Management Server is not available.

To view the FTP server status, do the following:

1. Click **Tools > FTP Reports**. The FTP Statistics page gets displayed.
2. The following server status information is displayed:

Table 42. FTP Statistics

Value	Description
Server start time	Start time of the FTP Server.
Number of directories created	Number of directories created by users using mkdir.
Number of directories removed	Number of directories removed by users using rmdir.
Number of file uploaded	Number of files uploaded by all users.
Number of files downloaded	Number of files downloaded by all users.
Number of files deleted	Number of files deleted by all users using delete command.
Uploaded Bytes	Total number of bytes uploaded.
Downloaded Bytes	Total number of bytes downloaded.
Current logins	Displays existing logins.
Total Logins	Total logins since the last reset.
Total failed logins	Total number of logins failed.
Current Connections	Current connections since the last reset.
Total Connections	Total connections since the last reset.

3. Click **Reload** to refresh current logins.
4. Click **Reset** to reset the values.

FTP Connections

View FTP Connections by following the steps mentioned below:

1. Click **Tools > FTP Reports > FTP Connections**.
2. The following connection information is displayed in the report:

Table 43. FTP Connections

Value	Description
Login Name	The login userid for this connection. If this is blank, it means that the user has only established a connection but has not logged in.
Login Time	The time when the user logged in. If this is blank, it means that the user has only established a connection.
Last Access Time	The time when the user last accessed this connection. If this is blank, it means that the user has only logged in and not issued any command yet.
Client Address	The client IP from which the user has logged in.

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. (1) Actions performed on a document by the system to ensure its compatibility with business requirements between partners. (2) A series of processing steps, such as document validation and transformation.

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

Activation. Connecting a partner 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 partners.

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

C

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

Certificate set. A set of primary and secondary certificates that can be associated to a participant connection.

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

Classification. Identifies role of partner 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 internal partner or external partners.

Internal Partner Child. Internal Partner Child is a special partner type that acts like a partner in the console but like an internal partner when routing.

External Partner. A hub community member that exchanges business transactions with the internal partner.

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 partners, and to ensure that the original content of a document that has been sent is unchanged.

De-envelope . To extract a document from an EDI envelope.

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

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

Document Definition. Gives the system all of the necessary information to receive, process, and route documents between community members. Document Definition types include package, protocol, document type, 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

Operation Mode. Identifies documents that are routed to a particular gateway during testing or for live production.

Global. Contact person can be assigned alerts by partner and internal partner.

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 partner has successfully completed business rules testing, and the internal partner 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 internal partners 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 partner 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 partners.

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 partner (local) or also by the internal partner (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) 1995-2008 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:

IBM the IBM logo AIX CICS DB2 DB2 Universal Database IBMLink IMS MQSeries MVS OS/390 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 6.1.

Index

A

- Account Admin features 51
- Action, definition 8
- Activity, definition 8
- Add contact to existing alert 34
- Addresses
 - delete 59
 - description 35, 59
 - edit 59
 - values 59
- Alerts
 - add contact to existing alert 34
 - create event-based alert 33
 - create volume-based alert 31
 - description 29, 57
 - disable alert 58
 - remove alert 58
 - search criteria 58
 - search criteria, Partners 58
 - search for alerts 58
 - view or edit alert details and contacts 57
- AS attributes
 - AS Encrypted 22
 - AS Signed 26
- AS Encrypted attribute 22
- AS Signed attribute 26
- AS1/AS2 Viewer 70
 - description 63
 - package details 66
 - search criteria 65
 - searching for messages 64
 - viewing message details 65
- Assign
 - group membership 53
 - group permissions 53
 - users to groups 28

B

- B2B capabilities, description 7
- bcgClientAuth.jacl script
 - setting up client authentication 14

C

- calendar-based scheduling
 - FTP Scripting destination 47
- Certificate revoked or expired message 22
- certificates
 - format, converting 16
 - signature 23, 26
- Certificates
 - expiration alert, create 33
 - types and supported formats 11
- Changing
 - destination status 77
- client authentication
 - configuring 14
 - inbound SSL 13
 - outbound SSL 17

- commands
 - FTP 46
- Community Console
 - display 5
 - users 1
 - using 3
- configuration points
 - destinations 48
- Contacts
 - description 29, 56
 - details 57
 - remove contact 57
 - values 53, 56, 57
 - view or edit contact details 56
- Create
 - certificate expiration alert 33
 - Document Volume Report 82
 - event-based alert 33
 - gateways 7
 - new group 27
 - new user 27
 - volume-based alert 31
- Critical event type 62

D

- Debug events 3, 62
- Decryption
 - definition 10
- default destination
 - example of setting 48
- Default destination
 - edit 52
 - select 52
 - view 52
- Delete
 - address 59
 - group 54
- destination
 - changing status 77
 - removing documents from the queue 76
 - viewing details 76
 - viewing queued documents 75
 - viewing the list 74
- destinations
 - default 48
 - file-directory 43
 - FTP 40
 - FTP Scripting 45, 46
 - FTPS 44
 - HTTP 37
 - HTTPS 39
 - JMS 42
 - SMTP 41
 - transports supported 37
 - values 52
 - view list 51
 - view or edit destination details 51
- Details, viewing destination 76
- digital signature
 - enabling 26

- Digital signature certificate, definition 11
- Digital signature, definition 10
- Disable alert 58
- Display console 5
- Document
 - details, Document Viewer 71
 - processing values, Document Viewer 72
- Document Analysis
 - description 79
 - search criteria 80
 - viewing documents 80
 - viewing process and event details 80
- Document states
 - definitions 79
 - Document Volume Report 81, 82
- document type, definition 8
- Document Viewer
 - description 70
 - document details 71
 - document processing values 72
 - search criteria 71
 - values 65, 66, 71, 72
- Document Volume Report
 - create 82
 - description 81
 - document states 81, 82
 - exporting 82
 - printing 83
 - search criteria 82
- Documents
 - removing from the queue 76
 - viewing queued 75
- DUNS numbers 7
- DUNS+4 7

E

- EDI FA Overdue
 - report 87
 - search criteria 86
- EDI Rejected Transaction
 - report 88
 - search criteria 88
- Edit
 - address 59
 - alert details and contacts 57
 - contact details 56
 - destination details 51
 - group details 54
- Enable alert 58
- encryption
 - enabling 22
- Encryption
 - definition 10
- Error event type 62
- Error fields
 - validation errors 73
- Event types 62
 - descriptions 62
- Event Viewer 22
 - description 61
 - search criteria 63
 - viewing event details 63
- Events
 - search criteria 63
 - searching for 62

- Exporting
 - Document Volume Report 82
- external partner
 - description 1

F

- Freeform ID numbers 7
- FTP commands 46
- FTP Connections
 - report 89
- FTP destinations 40
- FTP scripts
 - commands allowed in 46
 - destinations 45
- FTP Statistics
 - report 89

G

- Gateways
 - create 7
 - description 51
- Groups 53
 - assigning users to 28
 - create 27
 - delete 54
 - description 53
 - permissions, view edit assign 53
 - values 53
 - view group memberships 53
 - view or edit group details 54

H

- hub administrator
 - description 1
- Hub-community
 - description 1

I

- Icons 1
- inbound signature certificates 26
- inbound SSL
 - client authentication 13
 - server authentication 12
- Information event type 62
- internal partner
 - description 1
- interval-based scheduling
 - FTP Scripting destination 47

J

- JMS destinations 42

K

- Key, definition 10

L

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

N

- No valid encryption certificate found message 22
- Non-repudiation, definition 10

O

- outbound signature certificates 23
- outbound SSL
 - client authentication 17
 - server authentication 16

P

- Package Details
 - AS1/AS2 Viewer 66
- Package, definition 8
- partner
 - description 1
- Partner Profile
 - description 6
 - editing 6
 - values 7
 - viewing 6
- primary certificates
 - outbound digital signature 23
 - outbound encryption 20
 - outbound SSL 17
- Printing reports
 - Document Volume Report 83
- Private key, definition 10
- Protocol, definition 8
- Public key, definition 11

Q

- Queue, removing documents from 76
- Queued documents, viewing 75

R

- Raw documents
 - viewing 70
- Remove
 - alert 58
 - contact 57
- Removing documents from the queue 76
- Report
 - EDI FA Overdue 87
 - EDI Rejected Transaction 88
 - FTP Connections 89
 - FTP Statistics 89
- Result codes
 - Web Server 83
- RosettaNet Viewer
 - description 68
 - document processing, details 69
 - search criteria 69
 - searching for processes 68
 - viewing process details 69

S

- Search
 - for alerts 58
 - for events 62
 - for messages, AS1/AS2 Viewer 64
 - for RosettaNet processes 68
- Search criteria
 - alerts 58
 - AS1/AS2 Viewer 65
 - Document Analysis 80
 - Document Viewer 71
 - Document Volume Report 82
 - EDI FA Overdue 86
 - EDI Rejected Transaction 88
 - Event Viewer 63
 - RosettaNet Viewer 69
- secondary certificates
 - outbound digital signature 23
 - outbound encryption 20
 - outbound SSL 17
- Self-signed key, definition 11
- server authentication
 - inbound SSL 12
 - outbound SSL 16
- signature certificates
 - inbound 26
 - outbound 23
- SMTP destinations 41
- SSL certificates
 - client authentication, inbound 13
 - client authentication, outbound 17
 - inbound 12
 - server authentication, inbound 12
 - server authentication, outbound 16
- SSL Client certificate, definition 11
- Status, change destination 77

T

- Test Partner Connection
 - description 83
 - values 83
 - Web Server result codes 83
- Tools
 - description 79
 - Document Analysis 79
 - Document Volume Report 81
 - Test Partner Connection 83
- transports
 - destination, system-supplied 37

U

- Users
 - assign to groups 28
 - create new user 27
 - description 27, 54
 - values 55

V

- Validate Client SSL certificate option 14
- Validation errors
 - viewing 72

- Values
 - Addresses 59
 - Contacts 53, 56, 57
 - destinations 52
 - Document Viewer 65, 66, 71, 72
 - Partner Profile 7
 - Test Partner Connection 83
- View
 - alert details and contacts 57
 - contact details 56
 - destination details 51
 - destination list 51
 - group details 54
 - group permissions 53
- Viewers
 - AS1/AS2 Viewer 63
 - description 61
 - Document Viewer 70
 - Event Viewer 61
 - RosettaNet Viewer 68
- Viewing
 - destination details 76
 - destination list 74
 - document details 72
 - document processing details, RosettaNet Viewer 69
 - documents
 - Document Analysis 80
 - event details, Event Viewer 63
 - events 72
 - message details, AS1/AS2 Viewer 65
 - process and event details, Document Analysis 80
 - queued documents 75
 - raw documents 72
 - Raw documents 70
 - RosettaNet process details 69
 - validation errors 72
- VTP digital certificate
 - definition 11

W

- Warning event type 62
- Web Server result codes 83

X

- X.509 certificate, definition 11



Printed in USA