IBM WebSphere Partner Gateway - Express

User Guide

Version 6.0

IBM WebSphere Partner Gateway - Express

User Guide

Version 6.0

Note:
Before using this information and the product it supports, read the information in "Notices" on page 87.

28June2005

This edition of this document applies to WebSphere Partner Gateway - Express (5724-L70), Version 6.0, and to all subsequent releases and modifications until otherwise indicated in the new editions.

To send us your comments about IBM WebSphere Business Integration documentation, 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.

Contents

Preface

About this book

This document describes how to install, configure, and use IBM(R) WebSphere(R) Partner Gateway - Express.

WebSphere Partner Gateway - Express is a lightweight, easy-to-use, cost-effective business-to-business (B2B) connectivity tool that leverages the Hypertext Transfer Protocol (HTTP) and Applicability Statement 2 (AS2) standards for transmitting documents securely over the Internet. It provides the same core capabilities as the Advanced and Enterprise editions of WebSphere Partner Gateway - Express, without the extensive scalability and features required by community managers.

WebSphere Partner Gateway - Express is easy to deploy, install, and administer. Working directories are automatically created during installation and a Web-based console allows tasks to be performed remotely 24/7 in a browser environment.

With a simple, browser-based gateway and a very small footprint, WebSphere Partner Gateway - Express is easy to use and maintain, making it ideal for companies who need to provide trading partners with B2B capabilities, but have little or no in-house IT expertise. Through its simplicity, WebSphere Partner Gateway - Express offers unparalleled flexibility in deployment and implementation.

Audience

This document is intended for organizations that use WebSphere Partner Gateway - Express to conduct B2B activities with their trading partners.

Related documents

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

You can download, install, and view the documentation at the following site: http://www.ibm.com/software/integration/wspartnergateway/express/library/infocenter

Note: Important information about this product may be available in Technical Support Technotes and Flashes issued after this document was published. These can be found on the WebSphere Business Integration Support Web site, http://www.ibm.com/software/integration/websphere/support/. Select the component area of interest and browse the Technotes and Flashes sections.

Typographic conventions

This document uses the following conventions.

`courier font`	Indicates a literal value, such as a command name, filename, information that you type, or information that the system prints on the screen.
bold	Indicates a new term the first time that it appears and screen elements such as button names.
italic	Indicates a variable name or a cross-reference.
blue outline	A blue outline, which is visible only when you view the manual online, indicates a cross-reference hyperlink. Click inside the outline to jump to the object of the reference.
{ }	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 an optional parameter.
`...`	In a syntax line, ellipses indicate a repetition of the previous parameter. For example, `option[,...]` means that you can enter multiple, comma-separated options.
`< >`	In a naming convention, angle brackets surround individual elements of a name to distinguish them from each other, as in `<server_name><`*`connector_name`*`>tmp.log`.
/, \	In this document, backslashes (\) are used as the convention for directory paths. For UNIX installations, substitute slashes (/) for backslashes. All IBM WebSphere InterChange Server product pathnames are relative to the directory where the IBM WebSphere InterChange Server product is installed on your system.
%text% and *$text*	Text within percent (%) signs indicates the value of the Windows `text` system variable or user variable. The equivalent notation in a UNIX environment is *$text*, indicating the value of the *text* UNIX environment variable.
ProductDir	Represents the directory where the product is installed.

New in this release

New in release 6.0

In the June 2005 release of the 6.0 of the WebSphere Partner Gateway - Express product, this guide has been updated with the following changes:

- Added the procedure for upgrading WebSphere Business Integration Connect - Express version 4.2.1 to WebSphere Partner Gateway - Express version 6.0
- Added support for WebSphere Application Server 6.0
- Added instructions for installing WebSphere Partner Gateway - Express on systems running i5/OS or OS/400
- Added First Steps application information for Linux and i5/OS and OS/400 installations
- Added Getting Started HTML information for i5/OS and OS/400
- Added instructions for configuring timeout and polling intervals
- Made minor editorial improvements

New in release 4.2.1

June 2004

In the June 2004 release of the 4.2.1 version of the WebSphere Business Integration Connect - Express product, this guide has been updated with the following changes:

- Added support for systems running OS/400
- Revised the information in Chapter 5, "Configuring Security," on page 41
- Added Appendix E, "Security configuration examples," on page 81
- Made editorial improvements

February 2004

In the February 2004 release of the 4.2.1 version of the WebSphere Business Integration Connect - Express product, this guide has been updated with the following changes:

- Added Appendix D, "WebSphere Partner Gateway - Express Messaging Integration," on page 79
- Made minor editorial improvements

December 2003

In the December 2003 release of the 4.2.1 version of the WebSphere Business Integration Connect - Express product, this guide has been updated with the following change:

- Added support for Linux

Chapter 1. Introduction

Critical transactions involving purchase orders, invoices, shipping notices, and other documents drive your business. The ability to exchange this information with trading partners efficiently and securely is key to success. Automating interactions with trading partners is one of the easiest ways to simultaneously lower costs, improve customer satisfaction, and increase revenues. The challenge lies in managing these relationships as the number of trading partners increases and as these relationships incorporate a variety of formats. To track these transactions, you need a solution that lets you manage the exchange of electronic information with your partners in a quick, secure, and cost-effective way. IBM WebSphere Partner Gateway - Express is that solution.

WebSphere Partner Gateway - Express is a Web-based trading partner management system that accelerates the creation and maintenance of business-partner relationships through extensive B2B (business-to-business) protocol support and secure data transport. As an AS2 (Applicability Statement 2)-certified, B2B connectivity solution, it manages the routing of documents between companies and their business contacts. It includes a set of dynamic analysis and reporting tools that provide 24x7 visibility into your document directories, so you can manage, analyze, track, and troubleshoot the flow of your business processes.

Features

The following sections describe key features of WebSphere Partner Gateway - Express.

Console-based trading partner management

Creating and managing relationships with hundreds to thousands of trading partners is complex and error prone. WebSphere Partner Gateway - Express provides an easy-to-use Web-based graphical interface for managing trading partners. The interface is similar in look-and-feel to the Community Console in the Advanced and Enterprise editions of WebSphere Partner Gateway. It is browser-based to allow for remote access and provides 24x7 at-a-glance visibility into the operation of the gateway.

The Console interface is used to enable configuration of the partner profile data, as well as review the tracking and logging data. Key features provided by the Console-based interface include the ability to:

- Send and resend Hypertext Transfer Protocol (HTTP)- and AS2-based documents to one or more participants.
- Monitor HTTP- and AS2-based documents that have been sent, received, and are pending transmission and acknowledgement.
- View historical information about successfully sent or failed documents.
- View, add, and update public certificates and private keys.
- Analyze, track, and investigate all aspects of your B2B exchange.

Support for HTTP- and AS2-based documents

To ensure the security of documents sent through the Internet, WebSphere Partner Gateway - Express supports HTTP- and AS2-based documents. Moreover,

WebSphere Partner Gateway - Express is certified by the Drummond Group for AS2 interoperability. AS2 is the Internet draft for transmitting EDI documents securely over the Internet. AS2 focuses on data privacy, data integrity, authenticity, and non-repudiation of origin and receipt. It also enables synchronized message disposition notifications (MDNs) or receipts. It also enables asynchronous MDNs.

WebSphere Partner Gateway - Express acts as an AS2-compliant system for sending and receiving data and receipts with external trading partners. AS2 capability allows EDI, XML, and binary documents to be exchanged over the Internet using standart HTTP while providing authentication, privacy, and non-repudiation of document receipt.

Secure message routing

WebSphere Partner Gateway - Express provides the security tools necessary to validate digital communications and transactions with trading partners. These tools, which are described in the following sections, deliver premium levels of security by ensuring that business transactions are conducted with known and trusted parties.

Inbound documents

WebSphere Partner Gateway - Express incorporates the following four levels of security available for documents received from trading partners.

- Secure Sockets Layer (SSL) Server authentication — Enables WebSphere Partner Gateway - Express to authenticate a partner's identity and provides transport-level security.
- Secure Sockets Layer (SSL) client authentication — Allows clients to authenticate themselves to WebSphere Partner Gateway - Express by providing their own digital certificates.
- Decryption — Transforms encrypted text into a plain-text format that can be understood.
- Verification of digital signature — Applied to electronic documents to validate that the document contents have not been tampered with.

Outbound documents

WebSphere Partner Gateway - Express incorporates the following three levels of security for documents being sent to trading partners.

- Secure Socket Layer (SSL) client authentication — Allows WebSphere Partner Gateway - Express to authenticate clients prior to sending document to them.
- Encryption — Transforms plain text into an unreadable form (ciphertext) so that the original data cannot be recovered without decrypting the data.
- Digital signature — Applied to electronic documents to validate that the document contents have not been tampered with.

Console-based transaction auditing

When you want to know if a business partner has received a document and acknowledged or responded to that document, you can use the WebSphere Partner Gateway - Express Console to view document and participant summary reports. An activity log is retained for recent transactions. The console provides access to this log so you can search for transactions that meet specified criteria.

Getting Started Checklist

The following checklist describes the steps you perform to get WebSphere Partner Gateway - Express up and running. The steps are shown in the order they should be performed. For more information about a step, go to the topics referenced in the step.

1. Install WebSphere Partner Gateway - Express. SeeChapter 2, “Installing WebSphere Partner Gateway - Express,” on page 5.
2. Start WebSphere Partner Gateway - Express. See “Starting WebSphere Partner Gateway - Express server” on page 23.
3. Use your Web browser to access the WebSphere Partner Gateway - Express Console. See “Accessing the Console” on page 24.
4. The first time you log in, you must change the default login passwords and create your first participant. See “First-time login procedure - setting the login passwords” on page 26.

   Thereafter, you can log in using the procedure described under “Subsequent login procedures” on page 28.
5. Configure and test WebSphere Partner Gateway - Express. If necessary, fine-tune your WebSphere Partner Gateway - Express configuration to suit your requirements. See Chapter 4, “Configuring and Testing,” on page 31.

   Note: If you want to test WebSphere Partner Gateway - Express with your security configuration in place, skip to the next step, then test WebSphere Partner Gateway - Express.
6. Implement security for your inbound and outbound documents. See Chapter 5, “Configuring Security,” on page 41.
7. After you have tested WebSphere Partner Gateway - Express and verified that it is working according to your requirements, you are ready to conduct transactions with your participants.
   - If you will be exchanging AS2-based documents with participants, see “Managing AS2 documents” on page 57.
   - If you will be exchanging HTTP-based documents with participants, see “Managing HTTP documents” on page 62.
8. Access reports as necessary to view a summary of the document, participant, and system activities that have occurred. SeeChapter 7, “Viewing Reports,” on page 67.

Chapter 2. Installing WebSphere Partner Gateway - Express

This chapter describes how to install IBM WebSphere Partner Gateway - Express version 6.0, either as an upgrade to version 4.2.1 or as brand new installation of WebSphere Partner Gateway - Express. You can install WebSphere Partner Gateway - Express on a personal computer (PC) running Microsoft Windows 2000 or Linux, or on a system running i5/OS and OS/400.

This chapter contains the following sections:

Minimum requirements

The following sections describe the minimum hardware and software requirements for installing Websphere Partner Gateway:

Minimum requirements for Windows

To install WebSphere Partner Gateway - Express on a Windows PC, the PC must meet the following hardware and software requirements.

Hardware

The Windows PC on which you install WebSphere Partner Gateway - Express must meet the following hardware requirements:

- 1.4 GHz or faster Intel (R) Xeon processor
- At least 512 MB of Random Access Memory (RAM)

  Note: Memory errors may occur on inbound and outbound transactions if WebSphere Partner Gateway - Express is running on a memory constrained system.
- At least 150 MB of available hard disk space

Software

The Windows PC on which you install WebSphere Partner Gateway - Express must meet the following software requirements:

- Microsoft Windows 2000 Server with Service Packs 3 and 4 installed
- Microsoft Windows 2000 Advanced with Service Packs 3 and 4 installed
- Microsoft Windows 2003 Standard and Enterprise

- A Simple Mail Transport Protocol (SMTP)-based e-mail relay server for delivering e-mail alerts and SMTP messages
- Microsoft Internet Explorer, Version 6.0 with Service Pack 1, or Mozilla, Version 1.4 or 1.7

  Note: The browser must have cookie support turned on to maintain session information. No personal information is stored in the cookie, and it expires when the browser is closed.

Minimum requirements for Linux

To install WebSphere Partner Gateway - Express on a Linux environment, the PC must have the following hardware and software requirements.

Hardware

The Linux PC on which you install WebSphere Partner Gateway - Express must meet the following hardware requirements:

- 1.4 GHz or faster Intel Xeon processor
- At least 512 MB of Random Access Memory (RAM)

  Note: Memory errors may occur on inbound and outbound transactions if WebSphere Partner Gateway - Express is running on a memory constrained system.
- At least 150 MB of available hard disk space

Software

The Linux PC on which you install WebSphere Partner Gateway - Express must meet the following software requirements:

- RedHat Advanced Server, Version 3, update 3, or SuSe Linux Enterprise Server, Version 8 with SuSE Service Pack 3 or Version 9
- A Simple Mail Transport Protocol (SMTP)-based e-mail relay server for delivering e-mail alerts and SMTP messages
- The X Windows system DISPLAY environment variable must be correctly set to enable display of the WebSphere Partner Gateway - Express installer GUI. See "Setting the DISPLAY environment variable."
- Mozilla, Version 1.4 or 1.7

  Note: The browser must have cookie support turned on to maintain session information. No personal information is stored in the cookie, and it expires when the browser is closed.

Setting the DISPLAY environment variable

The WebSphere Partner Gateway - Express installation wizard uses the X Windows system on UNIX to display the graphical user interface. The X Windows system requires that the DISPLAY environment variable be exported to the system environment. The following lines set the DISPLAY environment variable to the IP_Address from a Bourne shell:

```
DISPLAY=IP_Address:0.0

export DISPLAY
```

Use the syntax appropriate to your shell to set the DISPLAY environment variable.

Note: Test that the DISPLAY system environment variable and X Windows system are properly configured by running an X client program, such as xclock, from the command line. If the xclock client displays on the X Server window (local or remote), then the installation wizard GUI should also display properly.

Minimum requirements for Systems running i5/OS or OS/400

To install WebSphere Partner Gateway - Express on a system running i5/OS or OS/400, two sets of minimum requirements are necessary: those for the PC that will remotely install the product, and those for the system running i5/OS or OS/400. The following sections describe these two sets of minimum requirements.

Minimum requirements for PC that remotely installs the product

The PC that remotely installs WebSphere Partner Gateway - Express on a system running i5/OS or OS/400 must meet the following hardware and software requirements.

Note: You must have Administrative privileges on the Windows PC.

Hardware:

- Pentium III-class PC (500 MHz or higher recommended)
- 256 megabytes of Random Access Memory (RAM) or greater
- 500 megabytes disk space (including redistributable code)
- Designed for an XGA monitor with 1024 x 768 resolution or greater

Software:

- Windows 98, Windows Me, Windows NT 4.0 with Service Pack 6 installed, Windows 2000, Windows XP, or Windows Server 2003
- Microsoft Internet Explorer 6.0 with SP1 or Mozilla 1.4 or 1.7

  Note: The browser must have cookie support turned on to maintain session information. No personal information is stored in the cookie, and it expires when the browser is closed.

Minimum requirements for the system running i5/OS or OS/400

The system running i5/OS or OS/400 on which WebSphere Partner Gateway - Express is being installed must meet the following hardware and software requirements.

Hardware:

- A minimum processor Commercial Processing Workload (CPW) rating of 300
- At least 640MB of Random Access Memory (RAM)

  Note: Memory errors may occur on inbound and outbound transactions if WebSphere Partner Gateway - Express is running on a memory constrained system.
- At least 150MB of available hard disk space

Software:

- IBM OS/400 V5R2M0 (5722-SS1) or IBM OS/400 V5R3MO (5722-SS1)
- -5722AC3 - Crypto Access Provider 128-bit for AS/400 (if using SSL)
- QShell Interpreter (5722-SS1, Option 30)

- IBM Java Developer Kit, Version 1.4 (5722JV1, Option 6) with PTF SIXXXXX on V5R2M0 or PTF SI17535 on V5R3M0
- IBM Toolbox for Java (5722JC1)
- A Simple Mail Transport Protocol (SMPT)-based e-mail relay server for delivering e-mail alerts and SMTP messages
- WebSphere Application Server for OS/400 V6 (5733W60 Base) with Fix Pack 6.0.0.2, and either of the following:
  - WebSphere Application Server V6 Express (option 1)
  - WebSphere Application Server V6 (“Base”) (option 2)

  Note: A WebSphere Application Server for OS/400 V6 installation CD is included with the WebSphere Partner Gateway - Express installation package.

Upgrading from WebSphere Business Integration Connect - Express Version 4.2.1 to WebSphere Partner Gateway - Express Version 6.0 — all platforms

This section describes how to upgrade from Business Integration Connect - Express version 4.2.1 to WebSphere Partner Gateway - Express version 6.0. The upgrade procedure uses a graphical user interface (GUI) and applies to all platforms on which Business Integration Connect - Express version 4.2.1 is installed.

Note: If you are installing WebSphere Partner Gateway - Express for the first time, refer to the installation instructions in one of the following sections, depending on the type of installation you are performing:

- **Windows:** See “Installing WebSphere Partner Gateway - Express on a Windows system” on page 12
- **Linux:** See “Installing WebSphere Partner Gateway - Express on a Linux system” on page 15
- **i5/OS or OS/400** “Installing WebSphere Partner Gateway - Express on a system running i5/OS or OS/400” on page 18

The following steps describe how to perform the upgrade:

1. Shut down version 4.2.1 of Business Integration Connect - Express.
   a. If your existing version of Business Integration Connect - Express is running, ensure that any documents that are in progress have finished processing.
   b. Close all open Web browser sessions that are connected to the WebSphere Partner Gateway - Express console.
   c. Stop the WebSphere Partner Gateway - Express server.
2. Install the WebSphere Partner Gateway - Express version 6.0 using the installer.

   Note: The installer detects version 4.2.1 of Business Integration Connect - Express and backs up its data.

   a. Launch the installer, using Launchpad.

      On a Windows platform: Insert the WebSphere Partner Gateway - Express 6.0 CD-ROM into the CD-ROM drive on your computer. The Launchpad window opens.

Note: If the Launchpad does not start automatically, you can start it manually by executing `LaunchPad.bat`, located in the root directory of the CD.

On a Linux platform: Insert the WebSphere Partner Gateway - Express 6.0 CD-ROM into the CD-ROM drive on your computer. Open the Launchpad by executing `LaunchPad.sh`, located in the root directory of the CD.

Note: Alternatively, you can bypass the Launchpad and run the installer by changing directories to the WebSphere Partner Gateway - Express directory and executing `setupLinux`. If you do this, the installation wizard window opens, followed by a message panel telling you that an older version of Business Integration Connect - Express was detected. Proceed to 2c.

On a system running i5/OS or OS/400: Insert the WebSphere Partner Gateway - Express 6.0 CD-ROM into the CD-ROM drive on the Windows PC that is connected to the system running i5/OS or OS/400. The Launchpad window opens.

Note 1: If the Launchpad does not start automatically, you can start it manually by navigating to the **express** folder and double-clicking `Launchpad.bat`.

Note 2: Alternatively, if you want to bypass the Launchpad, you can start the installer by executing the `setup.exe -os400` command. If you do this, the Sign on to the Server window appears. Proceed to 2c.

Caution: If you omit the -os400 parameter in the `setup.exe -os400` command, the installation will occur on the Windows machine.

The Launchpad window offers five options:

- **Product Overview**, which utilizes your Web browser to take you to the IBM Web site containing product information about WebSphere Partner Gateway - Express.
- **ReadMe File**, which opens the ReadMe file on the installation disk.
- **InfoCenter Documentation**, which utilizes your Web browser to take you to the IBM WebSphere Partner Gateway - Express library Web site where you can download documentation for any edition of WebSphere Partner Gateway - Express.
- **Install the product**, which starts the installation wizard.
- **Exit**, which closes the Launchpad window.

b. Click **Install the product**.

The installation wizard window opens, followed by a message panel telling you that an older version of Business Integration Connect - Express was detected.

c. Click **Next** on the "older version detected" panel.

The Automated Backup window opens, asking whether you want to copy Business Integration Connect - Express version 4.2.1 data to a backup directory.

d. Click the **Yes** button and ensure that the displayed path to the current Business Integration Connect - Express version 4.2.1 installation location is correct.

e. Click **Next**.

The data from Business Integration Connect - Express version 4.2.1 begins copying to the 421_backup subdirectory under the WebSphere Partner Gateway - Express version 6.0 installation directory. A status box opens to show the progress of the backup operation. When data copying has finished, the status box closes.

f. Click **Next**. The HTTP Port window appears. The installation wizard detects ports that are currently in use, then assigns default unused ports for use by WebSphere Partner Gateway - Express.

   The following types of ports are displayed:

   - HTTP Port — The default communications port for normal communications
   - HTTPS1 Port — The communications port used for secure (encrypted) communications.
   - HTTP2 Port — A duplicate of the default communications port for normal communications
   - HTTPS2 Port — A duplicate of the communications port used for secure (encrypted) communications.
   - Bootstrap Port — A port that is used internally by WebSphere Partner Gateway to start the embedded version of WebSphere Application Server
   - SOAP Address Port — A port that is used internally by WebSphere Partner Gateway to start the embedded version of WebSphere Application Server

g. Make sure that the HTTP port number is the same port number used in the 4.2.1 installation. If the other default ports shown (HTTPS1, HTTP2, HTTPS2, Bootstrap, and SOAP) do not conflict with other resources on the computer, accept them.

   Note: If you specify an HTTP port that is already in use, the system generates a warning and an Exception when you start the server. If this occurs, re-install WebSphere Partner Gateway - Express and choose a different HTTP port.

h. Click **Next**. The Default Folder Name window appears.

i. The Default Folder Name window shows the name of the shortcut menu folder that WebSphere Partner Gateway - Express will install on your Start > Programs menu. Either accept the default name or change it.

j. Click **Next**. The Service Settings window appears.

k. Click **Next**. The Windows Service Installation window appears. If you would like to register WebSphere Partner Gateway - Express as a Windows service, select the Install as a Windows Service check box.

   Note: You must have administrator privileges in order to configure WebSphere Partner Gateway - Express to run as a service. If you do not have administrator privileges, you will see the Administrator check window. You must click **Back** and clear the **Install WebSphere as a service** check box.

l. Click **Next**. The Summary window appears.

m. Review your selections in the Summary window. If you need to change any of them, click the **Back** button to return to the appropriate window, make your changes, and click **Next** until you return to the Summary window.

n. Click **Next**. The Installer installs the WebSphere Partner Gateway - Express software (this can take several minutes).

Note: WebSphere Application Server 6.0 is automatically installed with the WebSphere Partner Gateway - Express product.

o. When the installation process is complete, the First Steps application options window appears, asking whether or not you want to launch the First Steps application. To learn how to get started with WebSphere Partner Gateway - Express, select **Yes**. Otherwise, click **No**.

Note: If you have installed WebSphere Partner Gateway - Express version 6.0 as an upgrade from a previous version, select **No** to avoid starting the First Steps application.

p. Click **Next**. The Installation Confirmation window appears.

q. Click **Finish** on the installation confirmation window to complete the installation process. If **Yes** was selected in the First Steps Application launch window, the First Steps application window opens. See "Using the First Steps application" on page 23 for information on using this feature.

Note: On particularly fast PCs, the First Steps window may open on top of the installation confirmation window before you have clicked **Finish**. If this happens, make the installation confirmation window the current window and click **Finish** to close it before proceeding to First Steps.

3. Start the WebSphere Partner Gateway - Express server, using the desktop shortcut provided during the installation of WebSphere Partner Gateway - Express 6.0.

Note: It can take several minutes for the WebSphere Partner Gateway - Express server to become fully operational.

4. Run the pre- data migration tool to convert the version 4.2.1 security data to data that is compatible with the 6.0 environment. Security data can include:
   - keystores for inbound data
   - truststores for inbound data
   - any PKCS12 type of files uploaded in 4.2.1

   The following steps describe how to run the pre- data migration tool.

   a. Open a command prompt window.

   b. Change the directory to WebSpere_Partner_Gateway_Express_Install_Dir.

   c. Run the shell script `bcgMigrateConvertor.bat` or `bcgMigrateConvertor.sh`, depending on your operating system.

   Note: If the 421_backup directory is not a subdirectory of the WebSpere_Partner_Gateway_Express_Install_Dir directory, you must specify the full path to the 421_backup directory as the first parameter `d`.

   d. When the migration tool has finished, close the command prompt window.

5. Run the data migration tool to migrate the Business Integration Connect - Express version 4.2.1 data saved earlier to your new WebSphere Partner Gateway - Express version 6.0 installation. To run the tool:

   a. Open a command window.

   b. Change the current directory to:
   WebSpere_Partner_Gateway_Express_Install_Dir/bin

   c. Run shell script **bcgMigrate.bat** or **bcgMigrate.sh**, depending on your operating system.

Note: If the 421_backup directory is not a subdirectory of the *WebSpere_Partner_Gateway_Express_Install_Dir* directory, you must specify the full path to the 421_backup directory as the first parameter

d. When the migration tool has finished running, close the command window.

6. Run WebSphere Partner Gateway - Express version 6.0 to confirm that it is installed and configured properly.
   a. Start the console.
      If the login screen opens in a Web browser session, the server is operational. (If the login window does not open, wait a few minutes and then try starting the console again.) **Do not** log in.
   b. Close the Web browser to exit the login screen.
   c. Stop the WebSphere Partner Gateway - Express server, using the desktop shortcut provided during the installation of WebSphere Partner Gateway - Express 6.0.
   d. Start the WebSphere Partner Gateway - Express server, using the desktop shortcut provided during the installation.
   e. Start the WebSphere Partner Gateway - Express console, using the desktop shortcut provided during the installation.

      WebSphere Partner Gateway - Express version 6.0 is now ready for use.
7. Uninstall Business Integration Connect - Express version 4.2.1. Refer to Appendix C, "Uninstalling WebSphere Partner Gateway - Express," on page 75 for instructions.

Installing WebSphere Partner Gateway - Express on a Windows system

There are three ways to install WebSphere Partner Gateway - Express on a Windows system:

- Using an installation wizard graphical user interface (GUI) — see "Using the graphical installer for Windows," below.
- Silently, using a command line interface — see "Performing a silent installation" on page 14.
- Console mode, using a command line interface — see "Installing with console mode" on page 15.

Using the graphical installer for Windows

To install WebSphere Partner Gateway - Express using the graphical installer:

1. Insert the WebSphere Partner Gateway - Express 6.0 CD-ROM into the CD-ROM drive on your computer. The Launchpad window opens.

   Note: If the Launchpad does not start automatically, you can start it manually by executing `LaunchPad.bat`, located in the root directory of the CD.

   The Launchpad window offers five options:

   - **Product Overview**, which utilizes your Web browser to take you to the IBM Web site containing product information about WebSphere Partner Gateway - Express.
   - **ReadMe File**, which opens the ReadMe file on the installation disk.

- **InfoCenter Documentation**, which utilizes your Web browser to take you to the IBM WebSphere Partner Gateway - Express library Web site where you can download documentation for any edition of WebSphere Partner Gateway - Express.
- **Install the product**, which starts the installation wizard.
- **Exit**, which closes the Launchpad window.

2. From the Launchpad, click **Install the product**. A Windows InstallShield window opens and shows the status of pre-install preparation; this can take several minutes. When pre-install preparation is completed, the InstallShield window closes and the WebSphere Partner Gateway - Express Welcome window appears.
3. Click **Next**. The Software License Agreement window appears.
4. Click **I accept the terms in the license agreement.**

   Note: You must accept the terms of the license agreement to proceed with the installation.

   Click **Next**. The Installation Directory window appears.
5. The path under **Directory Name** shows where the WebSphere Partner Gateway - Express software will be installed. You can change this path if desired by either entering a new path or clicking the **Browse** button and specifying a different path.

   Note: If you change the installation directory, make a note of the location; you will need that information in a later step.
6. Click **Next**. The HTTP Port window appears. The installation wizard detects ports that are currently in use, then assigns default unused ports for use by WebSphere Partner Gateway - Express.

   The following types of ports are displayed:
   - HTTP Port — The default communications port for normal communications
   - HTTPS1 Port — The communications port used for secure (encrypted) communications.
   - HTTP2 Port — A duplicate of the default communications port for normal communications
   - HTTPS2 Port — A duplicate of the communications port used for secure (encrypted) communications.
   - Bootstrap Port — A port that is used internally by WebSphere Partner Gateway to start the embedded version of WebSphere Application Server
   - SOAP Address Port — A port that is used internally by WebSphere Partner Gateway to start the embedded version of WebSphere Application Server
7. If the default ports shown will not conflict with other resources on the computer, accept them. Otherwise, change any default HTTP ports that might cause a conflict.

   Note: If you specify an HTTP port that is already in use, the system generates a warning and an Exception when you start the server. If this occurs, re-install WebSphere Partner Gateway - Express and choose a different HTTP port.
8. Click **Next**. The Default Folder Name window appears.
9. The Default Folder Name window shows the name of the shortcut menu folder that WebSphere Partner Gateway - Express will install on your Start > Programs menu. Either accept the default name or change it.

10. Click **Next**. The Windows Service Installation window appears. If you would like to register WebSphere Partner Gateway - Express as a Windows service, select the Install as a Windows Service check box.

    Note: You must have administrator privileges in order to configure WebSphere Partner Gateway - Express to run as a service. If you do not have administrator privileges, you will see the Administrator check window. You must click **Back** and clear the **Install WebSphere as a service** check box.

11. Click **Next**. The Summary window appears.
12. Review your selections in the Summary window. If you need to change any of them, click the **Back** button to return to the appropriate window, make your changes, and click **Next** until you return to the Summary window.
13. Click **Next**. The Installer installs the WebSphere Partner Gateway - Express software (this can take several minutes).

    Note: WebSphere Application Server 6.0 is automatically installed with the WebSphere Partner Gateway - Express product.

14. When the installation process is complete, the First Steps application options window appears, asking whether or not you want to launch the First Steps application. To learn how to get started with WebSphere Partner Gateway - Express, select **Yes**. Otherwise, click **No**.

    Note: If you have installed WebSphere Partner Gateway - Express version 6.0 as an upgrade from a previous version, select **No** to avoid starting the First Steps application.

15. Click **Next**. The Installation Confirmation window appears.
16. Click **Finish** on the installation confirmation window to complete the installation process. If **Yes** was selected in the First Steps Application launch window, the First Steps application window opens. See "Using the First Steps application" on page 23 for information on using this feature.

    Note: On particularly fast PCs, the First Steps window may open on top of the installation confirmation window before you have clicked **Finish**. If this happens, make the installation confirmation window the current window and click **Finish** to close it before proceeding to First Steps.

Performing a silent installation

WebSphere Partner Gateway - Express provides a way to install the code "silently" using the command line and is often used as part of a software distribution tool. A silent installation installs the program without using a GUI (graphical user interface).

This feature requires an options file that provides values for all of the installation options and must have the -silent option enabled. Each option in the file appears on a separate line.

WebSphere Partner Gateway - Express includes a sample file called BCGExpressWindowsInstall.iss. The sample file is in the **express** directory on the CD or archive file. Note that the sample file includes the -silent option enabled, which means WebSphere Partner Gateway - Express installs without a GUI if you use the file unmodified. You can either modify the provided sample file or perform an install using the GUI and record your choices to create a custom options file. For information, see "Generating an options file" on page 15.

To install WebSphere Partner Gateway - Express silently:

1. Open a command line on the machine on which you want to install the code.
2. Navigate to the location of the installation executable.
3. Enter the following command:

   setup -options *"<options file name>"*

   where *<options file name>* identifies the file that contains the option values the installer will use. This can be a full-path name.

Generating an options file

To generate an options file with settings specific to your installation:

1. Open a command line on the machine on which you want to install the code.
2. Navigate to the location of the installation executable.
3. Enter the following command:

   setup -options-record *"<options file name>"*

   where *<options file name>* identifies the file to contain the options used in the installation.

The installer runs using the GUI. It installs WebSphere Partner Gateway - Express and places the given options file in the command in the install directory. You can then edit this file with any text editor, or use it without changes to reinstall the product or create duplicate installs on other machines

Installing with console mode

IBM also provides a command line (console mode) install program that you can use to install WebSphere WebSphere Partner Gateway - Express on your computer.

To install WebSphere Partner Gateway - Express:

1. Open a command prompt window.
2. Navigate to the location of the installation executable.
3. Enter the following command at the prompt:

   ```
   setup -console
   ```

Installing WebSphere Partner Gateway - Express on a Linux system

There are three ways to install WebSphere Partner Gateway - Express:

- Using an installation wizard graphical user interface (GUI) — see “Using the graphical installer for Windows” on page 12, below.
- Silently, using a command line interface — see “Performing a silent installation” on page 14.
- Console mode, using a command line interface — see “Installing with console mode” on page 18.

Using the graphical installer for Linux

To install WebSphere Partner Gateway - Express using the graphical installer:

1. Insert the WebSphere Partner Gateway - Express 6.0 CD-ROM into the CD-ROM drive on your computer.
2. Open the Launchpad by executing `LaunchPad.sh`, located in the root directory of the CD.
   The Launchpad window opens.

Note: Alternatively, you can bypass the Launchpad and run the installer by changing directories to the WebSphere Partner Gateway - Express directory and executing `setupLinux`. If you do this, the Welcome page appears. Proceed to 4.

The Launchpad window offers five options:

- **Product Overview**, which utilizes your Web browser to take you to the IBM Web site containing product information about WebSphere Partner Gateway - Express.
- **ReadMe File**, which opens the ReadMe file on the installation disk.
- **InfoCenter Documentation**, which utilizes your Web browser to take you to the IBM WebSphere Partner Gateway - Express library Web site where you can download documentation for any edition of WebSphere Partner Gateway - Express.
- **Install the product**, which starts the installation wizard.
- **Exit**, which closes the Launchpad window.

3. From the Launchpad, click **Install the product**. The Welcome window appears.
4. Click **Next**. The Software License Agreement window appears.
5. Click **I accept the terms in the license agreement**.

   Note: You must accept the terms of the license agreement to proceed with the installation.

   Click **Next**. The Directory Name window appears.
6. The path under **Directory Name** shows where the WebSphere Partner Gateway - Express software will be installed. You can change this path if desired by either entering a new path or clicking the **Browse** button and specifying a different path.

   Note: If you change the installation directory, make a note of the location; you will need that information in a later step.
7. Click **Next**. The HTTP Port window appears. The installation wizard detects ports that are currently in use, then assigns default unused ports for use by WebSphere Partner Gateway - Express.

   The following types of ports are displayed:

   - HTTP Port — The default communications port for normal communications
   - HTTPS1 Port — The communications port used for secure (encrypted) communications.
   - HTTP2 Port — A duplicate of the default communications port for normal communications
   - HTTPS2 Port — A duplicate of the communications port used for secure (encrypted) communications.
   - Bootstrap Port — A port that is used internally by WebSphere Partner Gateway to start the embedded version of WebSphere Application Server
   - SOAP Address Port — A port that is used internally by WebSphere Partner Gateway to start the embedded version of WebSphere Application Server
8. If the default ports shown will not conflict with other resources on the computer, accept them. Otherwise, change any default HTTP ports that might cause a conflict.

Note: If you specify an HTTP port that is already in use, the system generates a warning and an Exception when you start the server. If this occurs, re-install WebSphere Partner Gateway - Express and choose a different HTTP port.

9. Click **Next**. The Default Folder window appears.
10. The Default Folder Name window shows the name of the Start Application shortcuts folder that WebSphere Partner Gateway - Express will install on your computer. Either accept the default name or change it.
11. Click **Next**. The Runlevel Service Daemon Settings window appears.
12. If you want to run WebSphere Partner Gateway - Express as a runlevel service daemon, select the ″Run WebSphere Partner Gateway - Express as a service″ check box.

    Note: You must have administrative privileges in order to configure WebSphere Partner Gateway - Express to run as a service daemon. If you do not have administrator privileges, you will see the Administrator check window. You must click **Back**, and clear the ″Run WebSphere Partner Gateway - Express as a service″ check box.
13. Click **Next**. The Summary window appears.
14. Review your selections in the Summary window. If you need to change any of them, click the **Back** button to return to the appropriate window, make your changes, and click **Next** until you return to the Summary window.
15. Click **Next**. The Installer installs the WebSphere Partner Gateway - Express software (this can take several minutes).

    Note: WebSphere Application Server 6.0 is automatically installed with the WebSphere Partner Gateway - Express product.
16. When the installation process is complete, the First Steps application options window appears, asking whether or not you want to launch the First Steps application. To learn how to get started with WebSphere Partner Gateway - Express, select **Yes**. Otherwise, click **No**.
17. Click **Next**. The Installation Confirmation window appears.
18. Click **Finish** on the installation confirmation window to complete the installation process. If **Yes** was selected in the First Steps Application launch window, the First Steps application window opens. See “Using the First Steps application” on page 23 for information on using this feature.

    Note: On particularly fast PCs, the First Steps window may open on top of the installation confirmation window before you have clicked **Finish**. If this happens, make the installation confirmation window the current window and click **Finish** to close it before proceeding to First Steps.
19. Is this installation part of a upgrade from WebSphere Partner Gateway - Express version 4.2.1 to WebSphere Partner Gateway - Express version 6.0?

    If **Yes**, go to step 5 on page 11 to complete the upgrade process.

    If **No**, the installation process is complete.

Performing a silent installation

WebSphere Partner Gateway - Express provides a way to install the code “silently” using the command line. A silent installation installs the program without using a GUI. This feature requires an options file that provides values for all of the installation options and must have the -silent option enabled. Each option in the file appears on a separate line.

WebSphere Partner Gateway - Express includes a sample file called `BCGLinuxExpressInstall.iss`. The sample file is in the `disk1` directory on the CD or archive file. Note that the sample file includes the `-silent` option enabled, which means WebSphere Partner Gateway - Express installs without a GUI if you use the file unmodified. You can either modify the provided sample file or perform an install using the GUI and record your choices to create a custom options file. For information, see "Generating an options file" on page 15.

To install WebSphere Partner Gateway - Express silently:

1. Open a command line on the machine on which you want to install the code.
2. Navigate to the location of the installation executable.
3. Enter the following command:

   `setupLinux -options "<options file name>"`

   where *<options file name>* identifies the file that contains the option values the installer will use.

Generating a response file

To generate a response file with settings specific to your installation:

1. Open a command line on the machine on which you want to install the code.
2. Navigate to the location of the installation executable.
3. Enter the following command:

   `./setupLinux -options-record "<response file name>"`

   where *<response file name>* identifies the file to contain the options used in the installation.

The installer runs using the GUI. It installs WebSphere Partner Gateway - Express and places the given response file in the command in the install directory. You can then edit this file with any text editor, or use it without changes to reinstall the product or create duplicate installs on other machines.

Installing with console mode

IBM also provides a command line (console mode) install program that you can use to install WebSphere Partner Gateway - Express on your computer. An example of when you might use console mode is when the X Windows system is not installed or is not correctly configured, thus preventing use of the installation wizard GUI.

To install WebSphere Partner Gateway - Express:

1. Open a command prompt window.
2. Navigate to the location of the installation executable.
3. Enter the following command at the prompt:

   `./setupLinux -console`

Installing WebSphere Partner Gateway - Express on a system running i5/OS or OS/400

Prior to installing WebSphere Partner Gateway - Express on a system running i5/OS or OS/400, you must confirm that you have the necessary prerequisite software installed. See "Confirming prerequisites" on page 19.

There are three ways to install WebSphere Partner Gateway - Express on a system running i5/OS or OS/400:

- Remotely from a Windows PC, using an installation wizard graphical user interface (GUI) — see "Using the graphical installer for systems running i5/OS or OS/400,".
- Silently, from a remote Windows PC, using a command line interface — see "Performing a silent installation" on page 21.
- Console mode, from a remote Windows PC, using a command line interface — see "Installing with console mode" on page 22.

Confirming prerequisites

The following steps describe how to confirm that you have the necessary prerequisite software installed on your system running i5/OS or OS/400.

1. Insert the WebSphere Partner Gateway - Express 6.0 CD-ROM into the CD-ROM drive on the Windows PC that is connected to the system running i5/OS or OS/400. The Launchpad window opens.

   Note: If the Launchpad does not start automatically, you can start it manually by navigating to the ″express″ folder and double-clicking `Launchpad.bat`.

   The Launchpad window offers the following six options:
   - **Product Overview**, which utilizes your Web browser to take you to the IBM Web site containing product information about WebSphere Partner Gateway - Express.
   - **ReadMe File**, which opens the ReadMe file on the installation disk.
   - **InfoCenter Documentation**, which utilizes your Web browser to take you to the IBM WebSphere Partner Gateway - Express library Web site where you can download documentation for any edition of WebSphere Partner Gateway - Express.
   - **Check prerequisites**, which starts the prerequisite checking wizard.
   - **Install the product**, which starts the installation wizard.
   - **Exit**, which closes the Launchpad window.
2. From the Launchpad, click Check Prerequisites. The ″Sign on to the Server″ window appears.
3. In the System field, enter a host name of the system running i5/OS or OS/400 on which you are installing WebSphere Partner Gateway - Express. In the User ID and Password fields, enter the i5/OS or OS/400 User ID and password that has ALLOBJ (All Object) authority on the system running i5/OS or OS/400, then click OK.
4. The Check Prerequisites wizard verifies that you have the required prerequisites and informs you if you are missing any software prerequisites.

   Note: If you are missing WebSphere Application Server for OS/400 V6, the wizard offers to perform a silent installation using the WebSphere Application Server for OS/400 V6 installation CD included in the installation package.

Using the graphical installer for systems running i5/OS or OS/400

To install WebSphere Partner Gateway - Express using the graphical installer:

1. Insert the WebSphere Partner Gateway - Express 6.0 CD-ROM into the CD-ROM drive on the Windows PC that is connected to the system running i5/OS or OS/400. The Launchpad window opens.

Note 1: If the Launchpad does not start automatically, you can start it manually by navigating to the **express** folder and double-clicking `Launchpad.bat` .

Note 2: Alternatively, if you want to bypass the Launchpad, you can start the installer by navigating to the **express** folder and double-clicking `setup.exe -os400`. If you do this, the Sign on to the Server window appears. Proceed to 3.

Caution: If you omit the -os400 parameter in the `setup.exe -os400` command, the installation will occur on the Windows machine.

The Launchpad window offers six options:

- **Product Overview**, which utilizes your Web browser to take you to the IBM Web site containing product information about WebSphere Partner Gateway - Express.
- **ReadMe File**, which opens the ReadMe file on the installation disk.
- **InfoCenter Documentation**, which utilizes your Web browser to take you to the IBM WebSphere Partner Gateway - Express library Web site where you can download documentation for any edition of WebSphere Partner Gateway - Express.
- **Check prerequisites**, which starts the prerequisite checking wizard.
- **Install the product**, which starts the installation wizard.
- **Exit**, which closes the Launchpad window.

2. From the Launchpad, click **Install the product**.

   The Sign on to the Server window appears.
3. In the System field, enter the host name of the system running i5/OS or OS/400 on which you are installing WebSphere Partner Gateway - Express. In the User ID and Password fields, enter the i5/OS or OS/400 User ID and password that has ALLOBJ (All Object) authority on the system running i5/OS or OS/400, then click **OK**.

   The Welcome window appears.
4. Click **Next**. The Software License Agreement window appears.
5. Select **I accept the terms in the license agreement**.

   Note: You must accept the terms of the license agreement to proceed with the installation.
6. Click **Next**. The HTTP Port window appears. The installation wizard detects ports that are currently in use, then assigns default unused ports for use by WebSphere Partner Gateway - Express.

   The following types of ports are displayed:

   - HTTP Port — The default communications port for normal communications
   - HTTPS1 Port — The communications port used for secure (encrypted) communications.
   - HTTP2 Port — A duplicate of the default communications port for normal communications
   - HTTPS2 Port — A duplicate of the communications port used for secure (encrypted) communications.
   - Bootstrap Port — A port that is used internally by WebSphere Partner Gateway
   - SOAP Address Port — A port that is used internally by WebSphere Partner Gateway

7. If the default ports shown will not conflict with other resources on the computer, accept them. Otherwise, change any default HTTP ports that might cause a conflict.

   Note: If you specify an HTTP port that is already in use, the system generates a warning and an Exception when you start the server. If this occurs, re-install WebSphere Partner Gateway - Express and choose a different HTTP port.
8. Click **Next**. The Installer installs the WebSphere Partner Gateway - Express software (this can take several minutes).
9. When the installation process is complete, the First Steps application options window appears, asking whether or not you want to launch the First Steps application. To learn how to get started with WebSphere Partner Gateway - Express, select **Yes**. Otherwise, click **No**.

   Note: If you have installed WebSphere Partner Gateway - Express version 6.0 as an upgrade from a previous version, select **No** to avoid starting the First Steps application.
10. Click **Next**. The Installation Confirmation window appears.
11. Click **Finish** on the installation confirmation window to complete the installation process. If **Yes** was selected in the First Steps Application launch window, the First Steps application window opens. See "Using the First Steps application" on page 23 for information on using this feature.

    Note: On particularly fast PCs, the First Steps window may open on top of the installation confirmation window before you have clicked **Finish**. If this happens, make the installation confirmation window the current window and click **Finish** to close it before proceeding to First Steps.
12. Is this installation part of an upgrade from WebSphere Business Integration Connect - Express version 4.2.1 to WebSphere Partner Gateway - Express version 6.0?

    If **Yes**, go to step 5 on page 11 to complete the upgrade process.

    If **No**, the installation process is complete.

Performing a silent installation

WebSphere Partner Gateway - Express provides a way to install the code "silently" from a PC using the command line. A silent installation installs the program without using a GUI. This feature requires an options file that provides values for all of the installation options. Each option in the file appears on a separate line.

WebSphere Partner Gateway - Express includes a sample file called `BCGExpressInstall.iss`. The sample file is in the **express** directory on the CD or archive file. Note that the sample file includes the -silent option enabled, which means WebSphere Partner Gateway - Express installs without a GUI if you use the file unmodified. You can either modify the provided sample file or perform an install using the GUI and record your choices to create a custom options file. For information on generating an options file, see "Generating an options file" on page 22.

To install WebSphere Partner Gateway - Express silently:

1. Edit the `BCGExpressInstall.iss` options file to specify the required port numbers.
2. Open a command line on the PC from which you want to install the code.

3. Navigate to the location of the installation executable.
4. Enter the following command:
   `setup <System> <User_ID> <Password> -options <options file name> -silent`

   where *<System>* is the host name of the system running i5/OS or OS/400, *<User_ID>* is an i5/OS or OS/400 User ID with ALLOBJ (All Object) authority, *<Password>* is the password for the User ID, and *<options file name>* identifies the file that contains the option values the installer will use.

Generating an options file

To generate an options file with settings specific to your installation:

1. Open a command line on the PC from which you want to install the code.
2. Navigate to the location of the installation executable.
3. Enter the following command:
   `setup.exe <System> <User_ID> <Password> -options-record <options file name>`

   where *<options file name>* identifies the file to contain the options used in the installation.

The installer runs using the GUI. It installs WebSphere Partner Gateway - Express and places the given options file in the command in the install directory. You can then edit this file with any text editor, or use it without changes to reinstall the product or create duplicate installs on other machines

Installing with console mode

IBM also provides a command line (console mode) install program that you can use to install WebSphere Partner Gateway - Express from a PC on your computer.

To install WebSphere Partner Gateway - Express:

1. Open a command prompt window on your PC.
2. Navigate to the location of the installation executable.
3. Enter the following command at the prompt:
   `Setup -console`

Chapter 3. Getting Started

This chapter describes how to start WebSphere Partner Gateway - Express and access its Web-based console. Topics in this chapter include:

Using the First Steps application

The First Steps application provides new WebSphere Partner Gateway - Express users with an easy-to-use interface for becoming acquainted with the WebSphere Partner Gateway - Express program. First Steps can be accessed automatically, at the end of the WebSphere Partner Gateway - Express installation process, or manually at any time.

The First Steps application window appears automatically if, toward the end of installing WebSphere Partner Gateway - Express, you selected **Yes** when asked if you wanted to launch the First Steps application. You can also start First Steps manually at any time from the Start menu (Windows) or the Start Application shortcuts folder (Linux) by selecting **IBM WebSphere Partner Gateway - Express** > **First Steps**, which opens the First Steps application window.

The First Steps application window offers the following options:

- **InfoCenter Documentation**, which utilizes your Web browser to take you to the IBM WebSphere Partner Gateway - Express library Web site where you can find and download documentation for any edition of WebSphere Partner Gateway - Express, including release notes and installation guides.
- **Getting Started**, which utilizes your Web browser to open a page that provides a link to the installation ReadMe file and directs you to the places within this book where you can find starting, configuring, testing and using WebSphere Partner Gateway - Express.
- **Start Server**, which starts the WebSphere Partner Gateway - Express server. (You must start the server before you can launch the console to log on.)
- **Launch Console**, which starts the WebSphere Partner Gateway - Express console within your Web browser and enables you to log on to WebSphere Partner Gateway - Express.
- **Exit**, which closes the First Steps window.

Starting WebSphere Partner Gateway - Express server

Before you can start the WebSphere Partner Gateway - Express console and log in, you must first start the embedded WebSphere Application Server. The following instructions describe how to start the server for each operating system:

Windows or Linux:

To start WebSphere Partner Gateway - Express server on a Windows or Linux system:

Click **Start** > **Programs** > **IBM WebSphere Partner Gateway - Express** > **Start Server**. A Command Prompt window opens, a series of progress messages display in the window and WebSphere Application Server is launched.

When the Command Prompt window closes, the server is ready for use and you can start the console and log on to WebSphere Partner Gateway - Express. See "Accessing the Console" for instructions on starting the WebSphere Partner Gateway - Express console and logging on to the program.

Note: If the server fails to start, read the messages issued in the command prompt and take corrective action. If a port conflict cannot be resolved, you may need to re-install WebSphere Partner Gateway - Express using different port numbers.

i5/OS or OS/400:

To start WebSphere Partner Gateway - Express server on a system running i5/OS or OS/400:

1. Open a command line interface to the system with a user profile that has QBCGX60 as a group profile or has *ALLOBJ (All Object) authority.
2. Start the WebSphere Application Server for i5/OS or OS/400 V6 subsystem with the following command: `STRSBS QWAS6/QWAS6`.
3. Start the qsh shell interpreter with the following command: `STRQSH`.
4. In the qsh shell interpreter, enter the following command:
   ```
   cd/QIBM/UserData/WSPGExpress60
   bin/bcgStartServer
   ```

Accessing the Console

WebSphere Partner Gateway - Express provides a Web-browser-based Console for managing documents. To access the Console, use one of the following browsers, depending on your operating system:

- **Windows** : Microsoft Internet Explorer, Version 6.0 with Service Pack 1, or Mozilla, Version 1.4 or 1.7
- **Linux** : Mozilla, Version 1.4 or 1.7
- **Systems running i5/OS or OS/400**: Microsoft Internet Explorer, Version 6.0 with Service Pack 1, or Mozilla, Version 1.4 or 1.7

Note: The browser must have cookie support turned on to maintain session information. No personal information is stored in the cookie, and it expires when the browser is closed.

Tip: For best results, set your monitor resolution to 1024 x 768 or higher.

After you start the WebSphere Partner Gateway - Express server, use the First Steps application (see "Using the First Steps application" on page 23) or one of the following procedures to log into the program, depending on your preference and operating system:

Windows:

1. Click **Start** > **Programs** > **IBM WebSphere Partner Gateway - Express** > **Console**.

   Alternatively, you can type the URL of the Console into a browser, as follows: `http://<Systemname><Domainname>:<Portnumber>>/qc/index.jsp`, where *Systemname* is the host name of the Windows system, *Domainname* is the name of the domain to which the Windows system belongs, and *Portname* is the HTTP port you specified when you installed WebSphere Partner Gateway - Express.

   Note: Be sure to type the full URL, including the domain name, even if WebSphere Partner Gateway - Express is installed on your local machine. Leaving the domain name out of the URL can cause navigation problems when using the product.

   WebSphere Partner Gateway - Express displays the Welcome page in your Web browser, with a blinking cursor in the **User Name** field.
2. If this is the first time you are logging in, proceed to "First-time login procedure - setting the login passwords" on page 26. Otherwise, proceed to "Subsequent login procedures" on page 28.

Linux:

1. Open your Start Applications shortcuts folder, then select **IBM WebSphere Partner Gateway - Express** > **Console**.

   Alternatively, you can type the URL of the Console into a browser, as follows: `http://<Systemname><Domainname>:<Portnumber>>/qc/index.jsp`, where *Systemname* is the host name of the Linux system, *Domainname* is the name of the domain to which the Linux system belongs, and *Portname* is the HTTP port you specified when you installed WebSphere Partner Gateway - Express.

   Note: Be sure to type the full URL, including the domain name, even if WebSphere Partner Gateway - Express is installed on your local machine. Leaving the domain name out of the URL can cause navigation problems when using the product.

   WebSphere Partner Gateway - Express displays the Welcome page in your Web browser, with a blinking cursor in the **User Name** field.
2. If this is the first time you are logging in, proceed to "First-time login procedure - setting the login passwords" on page 26. Otherwise, proceed to "Subsequent login procedures" on page 28.

i5/OS or OS/400:

1. Open a Web browser window.
2. Direct the browser to the following URL: `http://<Systemname><Domainname>:<Portnumber>>/qc/index.jsp`, where *Systemname* is the host name of the system running i5/OS or OS/400, *Domainname* is the name of the domain to which the system running i5/OS or OS/400 belongs, and *Portname* is the HTTP port you specified when you installed WebSphere Partner Gateway - Express.

   WebSphere Partner Gateway - Express displays the Welcome page in your Web browser, with a blinking cursor in the **User Name** field.
3. If this is the first time you are logging in, proceed to "First-time login procedure - setting the login passwords" on page 26. Otherwise, proceed to "Subsequent login procedures" on page 28.

First-time login procedure - setting the login passwords

When you log into WebSphere Partner Gateway - Express for the first time, the program prompts you to change the default login passwords and create a participant. The following sections describe these procedures.

Logging in for the first time

With the Welcome page displayed, use the following procedure to log into WebSphere Partner Gateway - Express.

1. In the **User Name** field, enter the default user name: **admin**.
2. In the **Password** field, enter the default login password: **admin**.
3. Click the **Login** button. The Initialize Passwords page appears. This page enables you to change login passwords.
4. Proceed to "Changing the default login passwords."

Changing the default login passwords

The system supports two types of users: Admin and Guest. Users with Admin access have full control to all WebSphere Partner Gateway - Express features. Users with Guest access have the following limitations:

- Read-only permission to Configuration and Certificates modules.
- Pause and Stop functionality is disabled.
- Document Send and Resend functionality is disabled for both AS2 and HTTP transports.

Admin and Guest users have separate passwords for their login. Following a successful first-time login with the admin/admin user name and password, new passwords are requested. This task is performed from the Initialize Passwords page. When valid Admin and Guest passwords are supplied, they will be encrypted and stored for use in validating all future logins of both Admin and Guest users. No system functionality can be accessed until valid encrypted passwords exist for both Admin and Guest users.

1. Place the cursor in the **New Password** field under **Admin** and type a new admin login password in the field. Then, tab to the corresponding **Retype New Password** field and retype the new Admin password there.

   Note: Login passwords must be at least six characters long. They can consist of alphanumeric values and are case sensitive.
2. Place the cursor in the **New Password** field under **Guest** and type a new guest login password in the field. Then, tab to the corresponding **Retype New Password** field and retype the new Guest password there.
3. Click the **Save** button. The Login Welcome page appears.

   Note: After you change the default login password, you can update it if necessary (see "Updating your login passwords" on page 29).
4. In the User Name and Password fields, enter admin as the user name and the new admin login password you defined earlier in this procedure. (It is advisable to login as the admin user as admin privileges are required to create partners, modify configuration files, and upload certificates). The Create Participants page appears. This page lets you create and edit WebSphere Partner Gateway - Express participants.
5. Proceed to "Creating the first participant" on page 27.

Creating the first participant

When you log into WebSphere Partner Gateway - Express for the first time, the program automatically opens the Create Participant page, enabling you to create the first participant with whom WebSphere Partner Gateway - Express can communicate. (If this is not your first time logging in, you must manually access the Create Participants page. To do that, see "Configuring participants" on page 31..)

To create the first participant:

1. Complete the entries in the Create Participant page (see Table 1 on page 27).
2. Click the **Save** button. The Manage Participants page appears. This page enables you to create additional participants, edit the participants you have already created, and delete participants you no longer need. For more information, see "Configuring participants" on page 31.

Table 1. Create Participant page

Parameter	Description
Participant Name	Enter the name of this participant without any spaces.
Document Receipt Protocol	
HTTP	Check if you will be using the HTTP protocol (non-secure).
HTTPS	Check if you will be using the HTTPS protocol (secure using SSL).
User Alerts	
Enabled	Click whether you want to enable (**Yes**) or disable (**No**) user alerts. If you click **Yes**, the system uses the remaining parameters to route alerts to the users you specify.
E-Mail Host	Enter the e-mail host or server that will be used. You must enter a value here if **User Alerts** is enabled. Example: mail.mycompany.com
Authentication Name	Enter the user name required to connect to the mail server on the e-mail host. If authentication is not required to relay mail, leave this field blank.
Authentication Password	Enter the password corresponding to the user name specified for the mail server on the e-mail host.
E-Mail Recipients	Enter the e-mail addresses of all recipients who will be receiving e-mail from WebSphere Partner Gateway - Express. Separate each e-mail address with a comma. At least one e-mail recipient is required if User Alerts is enabled. Example: johndoe@mycompany.com,maryf@mycompany.com
Capabilities	
Protocol HTTP	Indicates whether ″raw″ documents (i.e. non-AS2 packaged content) can be sent (**Can Send**) or received (**Can Receive**). If you do not select **Can Send**, all documents dropped in the Send directory will be moved to the Error directory when transmitting the document. If **Can Receive** is not selected, documents which are received without AS2 packaging are placed in the rec_err directory for the participant.

Table 1. Create Participant page (continued)

Parameter	Description
Protocol - AS2	Indicates whether AS2-packaged documents can be sent (**Can Send**) or received (**Can Receive**). If you do not select **Can Send**, all documents dropped in the send directory will be moved to the appropriate error directory when transmitting the document. If you do not select **Can Receive**, documents which are received without AS2 packaging are placed in the appropriate rec_err directory for the participant.
AS2 Participant ID	The AS2 ID, which is required by the AS2 packaging standard. If any documents are to be AS2 packaged for transmission, then this value must be supplied. In other words, an AS2 Participant ID is required if any AS2 capabilities are enabled.
Content Type	If Can Send and/or Can Receive is selected, then the Content Type must be specified. Check the content type that is to be sent (**Can Send**) and received (**Can Receive**). If **Binary** is checked, enter a binary content type. For example, octet-stream.

Where to go from here

After you create your first participant, you can perform WebSphere Partner Gateway - Express activities. The remaining sections in this guide describe how to perform these tasks. When you finish, click the **Logout** link at the top-right area of the current window (see "Understanding the user interface" on page 29).

Note: The Console automatically times-out after 30 minutes of inactivity.

Subsequent login procedures

After you log in to WebSphere Partner Gateway - Express for the first time, subsequent logins are performed using the following procedure.

1. With the Welcome page displayed, enter your user name in the **User Name** field and your login password in the **Password** field.
2. Click the **Login** button. The Document Summary page appears (see "Viewing the Document Summary report" on page 67).
3. Perform the desired WebSphere Partner Gateway - Express activities. The remaining sections in this guide describe how to perform these tasks.

   Note: The system supports two types of users: Guest and Admin. Users with Guest access have the following limitations:
   - Read-only permission to Configuration and Certificates modules.
   - Pause and stop functionality is disabled.
4. When you finish your session, click the **Logout** link at the top-right area of the current page (see "Understanding the user interface" on page 29).

   Note: The Console automatically times-out after 5 minutes of inactivity.

Understanding the user interface

The WebSphere Partner Gateway - Express user interface is displayed by your Web browser. After the Welcome page, the user interface consists of tabs to access functional categories and, within each selected tab, a horizontal navigation bar provides access to specific functional pages that are displayed in a work area below the navigation bar.

When you click a category tab:

- The horizontal navigation bar shows the associated functions available within the tab you selected.
- In the navigation bar, the first functional page associated with the current tab appears in the work area and the page name is highlighted on the navigation bar.

After you log onto WebSphere Partner Gateway - Express, the default displayed tab is **Reports**, with the **Document Summary** function highlighted on the navigation bar and the Document Summary page displayed in the work area. Other functions available on the Reports tab are Participant Summary and Activity Logs. To access those functions, simply click a desired function name on the navigation bar to display that function's page in the work area.

To change the displayed functional category, simply click its tab. For example, if you click the **AS2** tab, Pending Transmission, Pending MDN, Sent, Received, Send, and Resend appear in the horizontal navigation bar. **Pending Transmission** is highlighted on the navigation bar and the work area shows the Pending Transmission page. To display a different AS2 function page, click the function name in the navigation bar.

Note: You can use your browser's Forward and Backward controls to navigate through the WebSphere Partner Gateway - Express pages and tabs that you have accessed in your current session.

Below the IBM logo at the top-right corner of user interface window is the **Logout** link, which enables you log out from the current WebSphere Partner Gateway - Express session. The application continues to run in the background. To log in again, use the procedure under "Subsequent login procedures" on page 28.

Below the Logout link are the following two buttons:

- **Pause/Play** — A round green button initially containing two vertical bars that lets you temporarily stop sending documents. Click this button once to pause document transmission. The button toggles to a Play button, with the vertical bars replaced by a right-pointing arrowhead; click it again to resume document transmission and toggle the button's function back to Pause.
- **Stop** — A red button containing an X that shuts down WebSphere Partner Gateway - Express. If you click this button, a cautionary message appears and gives you the option of continuing or canceling the shutdown.

Updating your login passwords

There may be times when you want to change your login passwords. WebSphere Partner Gateway - Express simplifies this task by providing an **Update Password** link on the Login Welcome page. To change your login password, use the following procedure.

Note: If you have started a WebSphere Partner Gateway - Express session, click **Logout** to end the session.

1. From the Login Welcome page. click **Update Password**. The Welcome page appears with the following four fields:
   - User Name
   - Current Password
   - New Password
   - Retype New Password
2. Type your WebSphere Partner Gateway - Express user name in the **User Name** field.
3. Type your current password in the **Current Password** field.
4. Type your new password in the **New Password** field.

   Note: Login passwords must be at least six characters long. They can consist of alphanumeric values and are case sensitive.
5. Retype your new password in the **Retype New Password** field.
6. Click the **Save & Login** button. Your password is changed and the Document Summary page appears.

Chapter 4. Configuring and Testing

When you install WebSphere Partner Gateway - Express, the program uses various default settings. You can use the **Configuration** tab to adjust these settings to suit your requirements. After you configure WebSphere Partner Gateway - Express, you can test it to make sure it is operating as desired.

This chapter describes how to configure and test WebSphere Partner Gateway - Express. Topics in this chapter include:

Accessing Configuration functions

All configuration activities are performed using the function pages accessed by clicking the **Configuration** tab. The Participants page displays by default in the work area. Use the navigation bar to access other configuration pages.

When you click the Configuration tab, the horizontal navigation bar contains the following:

- **Participants** lets you create, edit, and delete participants. See "Configuring participants" on page 31.
- **AS2** lets you select AS2 parameters for your participants. See "Configuring AS2 parameters" on page 35.
- **HTTP** lets you select HTTP parameters for your participants. See "Configuring HTTP parameters" on page 37.
- **My Profile** lets you create a profile for your company. See "Configuring your profile" on page 33.

Configuring participants

Participants configuration is performed using the Manage Participants page, accessed from the Configuration tab. The Manage Participants page shows all participants you have created. Initially, this page shows only the participant you created when you logged into the system for the first time. However, you can display this page whenever necessary to add, edit, or delete participants.

Adding participants

To add participants from the Manage Participants page:

1. Click the **Configuration** tab. The Manage Participants page should display by default. If it does not, click **Manage Participants** in the navigation bar.
2. Click the **Create Participant** button. The Create Participant page appears.
3. Complete the entries in the Create Participant page (see Table 2 on page 32).

4. Click the **Save** button.
5. To add more participants, repeat steps 2 through 4.

Table 2. Create Participant page

Parameter	Description
Participant Name	Enter the name of this participant without any spaces.
Document Receipt Protocol	
HTTP	Check if you will be using the HTTP protocol (non-secure).
HTTPS	Check if you will be using the HTTPS protocol (secure).
User Alerts	
Enabled	Click whether you want to enable (**Yes**) or disable (**No**) user alerts. If you click **Yes**, the system uses the remaining parameters to route alerts to the users you specify.
E-Mail Host	Enter the e-mail host or server that will be used. You must enter a value here if **User Alerts** is enabled. Example: mail.mycompany.com
Authentication Name	Enter the user name required to connect to the mail server on the e-mail host. If authentication is not required to relay mail, leave this field blank.
Authentication Password	Enter the password corresponding to the user name specified for the mail server on the e-mail host.
E-Mail Recipients	Enter the e-mail addresses of all recipients who will be receiving e-mail from WebSphere Partner Gateway - Express. Separate each e-mail address with a comma. Example: johndoe@mycompany.com,maryf@mycompany.com
Capabilities	
Protocol HTTP	Indicates whether ″raw″ documents (i.e. non-AS2 packaged content) can be sent (**Can Send**) or received (**Can Receive**). If you do not select **Can Send**, all documents dropped in the Send directory will be moved to the error directory without transmitting the document. If **Can Receive** is selected, documents that are received without AS2 packaging are placed in the rec_err directory for the participant.
Protocol - AS2	Indicates whether AS2-packaged documents can be sent (**Can Send**) or received (**Can Receive**). If you do not select **Can Send**, all documents dropped in the Send directory will be moved to the appropriate error directory when transmitting the document. If you select **Can Receive**, documents that are received without AS2 packaging are placed in the appropriate rec_err directory for the participant.
AS2 Participant ID	The AS2 ID that is required by the AS2 packaging standard. If any documents are to be AS2 packaged for transmission, then this value must be supplied.

Table 2. Create Participant page (continued)

Parameter	Description
Content Type	If transmission or receipt of AS2 Binary packaged documents is to be supported, then the Content Type field must be supplied. Check the content type that is to be sent (**Can Send**) and received (**Can Receive**). If **Binary** is checked, enter a binary content type. Note that the if **Binary** is selected, the content type that you enter must match the content type specified in the AS2 capabilities configuration of that participant. For example, if your participant is configured to receive octet-stream, you would enter octet-stream as the content type.

Editing participants

There may be times when you need to edit the information entered for a participant. To edit a participant:

1. Click the **Configuration** tab. The Manage Participants page should display by default. If it does not, click **Manage Participants** in the navigation bar.
2. Click the Edit icon next to the participant you want to edit. An Edit Participant page opens, showing the information previously specified for the participant.
3. Change the information as required. If you need assistance, refer to Table 2.
4. When you finish editing the participant, click the **Save** button. The changes are saved and you are returned to the Manage Participants page.
5. To edit information for additional participants, repeat steps 2 through 4.

Deleting participants

If you no longer need a participant, use the following procedure to delete the participant.

1. Click the **Configuration** tab. The Manage Participants page should display by default. If it does not, click **Manage Participants** in the navigation bar.
2. In the **Delete** column, click the Delete icon for the participant you want to delete. A cautionary message displays, giving you the option of continuing or canceling the deletion.
3. Click **OK** to delete the participant or **Cancel** to retain the participant.

Configuring your profile

Using the My Profile page accessed from the Configuration tab, you can create a company profile that includes:

- Your receipt address
- Your company's AS2 ID
- Details about your company, such as the company name and address

The following procedure describes how to configure the My Profile parameters. You must complete the Receipt Address information before receiving any documents and the Company AS2 ID information before posting any AS2 documents.

1. Click the **Configuration** tab, then click **My Profile** in the navigation bar. The Manage My Profile page appears.
2. Click the **Edit** button. The Manage My Profile editing page appears.

3. Complete the entries in the Manage My Profile editing page (see Table 3).

   Important: If you change the port numbers, you must also change Console the shortcut. See "Creating a new Console shortcut" on page 35 for instructions.

4. Click the **Save** button.

Table 3. Manage My Profile page parameters

Parameter	Description
Receipt Address	At least one receipt address domain name (either unsecure or secure) is required. The receipt address entered here also appears in the Manage AS2 and Manage HTTP pages (see "Configuring AS2 parameters" on page 35 and "Configuring HTTP parameters" on page 37). If you change the port number, you must specify the new port number the next time you want to access the console (see "Accessing the Console" on page 24). **Important:** If you change the port number, you must also changes the Console shortcut. See "Creating a new Console shortcut" on page 35 for instructions.
Unsecure	Enter the domain and port number that will be used to handle unsecure transactions. **Note:** Do not include the "http://" prefix. The receipt address entered here also appears in the Manage AS2 and Manage HTTP pages (see "Configuring AS2 parameters" on page 35 and "Configuring HTTP parameters" on page 37). If you change the port number, you must specify the new port number the next time you want to access the console (see "Accessing the Console" on page 24). **Important:** If you change the port number, you must also change the Console shortcut. See "Creating a new Console shortcut" on page 35 for instructions.
Secure	Enter the domain and port number that will be used to handle secure transactions. **Note:** Do not include the "https://" prefix. **Important:** If you change the port number, you must also change the Console shortcut. See "Creating a new Console shortcut" on page 35 for instructions.
Company AS2 ID	
Sender ID	If you will be sending AS2-based documents, enter your AS2 ID. The ID entered here also appears in the Manage AS2 page (see "Configuring AS2 parameters" on page 35).
Company Details	
Company Name	Enter the name of your company.
Address	Enter your company's full mailing address.
Business ID Type	Select a business ID type (**DUNS**, **DUNS+4**, or **Freeform**).
Identifier	Enter the identifier corresponding to the business type you selected.

Table 3. Manage My Profile page parameters (continued)

Parameter	Description
Vendor Type	Select the vendor type category appropriate for your company.
Web Site	Enter your company's Web site.

Creating a new Console shortcut

If you changed either of the port numbers in the Manage My Profile page, you must also create a new Console shortcut. The following steps describe how to do this.

Windows

1. In Windows Explorer, navigate to the Start menu shortcuts directory for WebSphere Partner Gateway:
   `C:\Documents and Settings\All Users\Start Menu\Programs\IBM WebSphere Partner Gateway - Express`
2. With the cursor in the right-hand pane, right-click then select New > Shortcut. The Create Shortcut window appears.
3. Type the URL for the Console. The URL contains the machine name and the port number. For example, type
   `http://<MachineName>:<PortNumber>/qc/index.jsp`
4. Click Next.
5. Type a name for the shortcut. For example, type `Console`.
6. Click Finish.
7. Right-click the shortcut, then select Properties.
8. In the Web Document Tab, click the Change Icon, then select the Internet Explorer icon, if it is not already selected.
9. Click OK.

Linux

1. Navigate to Product Install Home.
2. Navigate to the directory scripts within Product Install Home.
3. Open the `Console.sh` file in any text editor.
4. Edit the last line which contains the port number in the URL. For example, edit the URL as follows:
   From:
   `$BROWSER "http://testmachine.in.ibm.com:59080/qc/index.jsp`
   To:
   `$BROWSER "http://testmachine.in.ibm.com:80/qc/index.jsp`

Configuring AS2 parameters

WebSphere Partner Gateway - Express enables you to define AS2 parameters for each participant. You define AS2 configuration parameters using the Manage AS2 page, accessed by selecting **AS2** from the Configuration tab navigation bar. The page shows you at a glance which parameters have (a check icon) and have not (an X icon) been set.

To configure AS2 parameters:

1. Click the **Configuration** tab, then click **AS2** in the navigation bar. The Manage AS2 page appears.

2. From the **Selected Participants** drop-down list, select the participant whose AS2 configuration you want to configure.
3. Scroll down to and click the **Edit** button. The Manage AS2 editing page appears. This page shows the parameters for inbound AS2 documents coming into the system and outbound AS2 documents leaving the system. The Inbound parameters are read-only on this page, but can be changed using the **My Profile** page, accessed from the Configuration tab navigation bar.
4. Complete the entries in the Manage AS2 page (see Table 4 for assistance).
5. Click the **Save** button.
6. To specify AS2 configuration parameters for other participants, repeat steps 2 through 5.

Table 4. Manage AS2 page parameters

Parameter	Description
Inbound	
Unsecure Receipt Address	Read-only field showing the HTTP document receipt URL (if previously defined). This parameter is set using the Configuration tab's My Profile page (see "Configuring your profile" on page 33).
Secure Receipt Address	Read-only file showing the HTTPS document receipt URL (if previously defined). This parameter is set using the Configuration tab's My Profile page (see "Configuring your profile" on page 33).
Participant ID	Read-only field that shows the AS2 ID associated with this participant. This parameter is set on the Configuration tab's Manage Participants page (see "Configuring participants" on page 31).
Basic Authentication Required	If basic authentication of senders is desired, click within the **Basic Authentication Required** checkbox to add a check mark in the box.
User Name	If Basic Authentication Required is checked, enter the authorized sender's user name.
Password	If an authorized sender's user name is defined, enter the senders password.
Identify the Partner	Depending on how you wish to identify the partner, select either **Using Basic Authentication** or **Using AS2 ID**.
Outbound	
Participant	Read-only field that shows the name of the participant.
Destination Address	Enter the address where outbound AS2 documents for this participant are sent.
Basic Authentication Required	If basic authentication of participants is desired, click within the **Basic Authentication Required** checkbox to add a check mark in the box.
User Name	If Basic Authentication Required is checked, enter the authorized participant's user name.
Password	If an authorized participant's user name is defined, enter the participant's password.
Request MDN	Check if a Message Disposition Notification (MDN) is required as proof of receipt for outbound AS2 documents from this participant.

Table 4. Manage AS2 page parameters (continued)

Parameter	Description
Synchronous or Asynchronous	Select whether outbound AS2 documents will be sent synchronously or asynchronously.
HTTP or HTTPS	Select whether the HTTPS or HTTP protocol is to be used with outbound AS2 documents.
Request Signed MDN	Check if a digitally signed MDN is required as proof of receipt for outbound AS2 documents.
Sign Documents	Check to digitally sign outbound AS2 documents. It is the user's responsibility to ensure that the appropriate digital certificate is loaded prior to sending Signed/Encrypted documents. If the appropriate certificate is not loaded, document transmission will fail.
Encrypt Documents	Check to encrypt outbound AS2 documents. It is the user's responsibility to ensure the appropriate digital certificate is loaded prior to sending Signed/Encrypted documents. Should the appropriate certificate not be loaded, document transmission will fail.
Compress Documents	Check to compress outbound AS2 documents.

Configuring HTTP parameters

WebSphere Partner Gateway - Express enables you to define HTTP parameters for each participant. You define HTTP configuration parameters using the Manage HTTP page accessed from the Configuration tab navigation bar.

To configure HTTP parameters:

1. Click the **Configuration** tab, then click **HTTP** in the navigation bar. The Manage HTTP page appears.
2. From the **Selected Participants** drop-down list, select the participant whose HTTP configuration you want to configure.
3. Click the **Edit** button. The Manage HTTP page appears. This page shows the parameters for inbound HTTP documents coming into the system and outbound HTTP documents leaving the system. The Inbound parameters are read-only and can be changed using **My Profile** on the **Configuration** tab's navigation bar.
4. Complete the entries in the Manage HTTP page (see Table 5).
5. Click the **Save** button.
6. To specify HTTP configuration parameters for other participants, repeat steps 2 through 5.

Table 5. Manage HTTP page parameters

Parameter	Description
Inbound	
Unsecure Receipt Address	Read-only field showing the HTTP document receipt URL.
Participant Mapping Method	Basic authentication is mandatory for the receipt of plain HTTP documents. The basic authentication name is used to determine the originating partner rather.

Table 5. Manage HTTP page parameters (continued)

Parameter	Description
User Name	Enter the user name that the participant will use as part of the basic authentication to authenticate himself to WebSphere Partner Gateway - Express. This name must be unique between participants as it is used to uniquely identify the origin of documents.
Password	Enter the password that the participant will use as part of the basic authentication to authenticate himself to WebSphere Partner Gateway - Express.
Outbound	
Destination Address	Enter the address where outbound documents are sent.
Basic Authentication Required	Check if basic authentication is required by the remote system.
User Name	Enter the user name that the remote system expects to authenticate this participant.
Password	Enter the password that the remote system expects to authenticate this participant.

Manually configuring the properties files

Although most configuration tasks can be performed by using the WebSphere Partner Gateway - Express GUI, you may find it useful to perform manual configuration for the following tasks:

- Configuring timeout property values
- Using the JACL scripts for various configuration tasks

The following sections describe how to configure timeout property values and how and when to use JACL scripts for manual configuration.

Configuring timeout values

If a trading partner takes a long time to process a message and send the MDN back, WebSphere Partner Gateway - Express may fail with a timeout message. To fix this problem or prevent it from happening, you can configure the following timeout property values: the synchronous/socket connection timeout value and the asynchronous MDN timeout value. The following steps describe how to configure timeout property values.

Configuring synchronous/socket connection timeout value

The following steps describe how to configure the synchronous/socket connection timeout value.

1. Open the `bcg.properties` file. This file is located in the following directory.
   `<ProductDir>/config`
2. Find the following property:
   `bcg.connector.sender.as2parm.SyncMDNtimeout=60000`
3. Change the number `60000` to represent a new number of milliseconds.
4. Save and close the file.

Configuring asynchronous MDN timeout value

The following steps describe how to configure the asynchronous MDN timeout value.

1. Open the `partner.properties` file for the trading partner whose MDN timeout value you want to configure. This file is located in the following directory: `<ProductDir>/config/partners/<name_of_parner>`
2. Find the following property: `bcg.connector.sender.as2.parm.MDNTimeout=10`
3. Change the number `10` to represent a new number of minutes.
4. Save and close the file.

Using JACL scripts for manual configuration

Although most of the configuration tasks can be done in the WebSphere Partner Gateway - Express GUI, the following JACL scripts are provided for manual configuration. You can invoke the scripts by following the instructions provided inside each script. The JACL scripts are located at *<ProductDir>*/jaclScripts.

Note: For detailed instructions on running the bcgSetCRLDP.jacl script, see "Running the bcgSetCRLDP.jacl script" on page 55.

Important: Any WAS configuration changes made manually or through the WebSphere Partner Gateway - Express GUI require the WAS server to be restarted.

Table 6. JACL scripts

JACL script	Description
bcgApplication.jacl	This script is used for installing, uninstalling, or updating the application. It also sets the WAS extended class path (ws_ext_dirs). **Caution:** This JACL file works on the existing application deployment, so you must supply the appropriate arguments to the scripts.
bcgClientAuth.jacl	This script sets the client authentication required flag.
bcgCustomService.jacl	This script sets up the custom service.
bcgSetCRLDP.jacl	This script enables or disables CRL distribution point checking when the revocation check is performed. See "Running the bcgSetCRLDP.jacl script" on page 55 for instructions on using this script.
bcgJavaWorkingDirectory.jacl	This script sets the current working directory for JVM.
bcgSetJVMHeapAttrs.jacl	This script changes the initial heap size and maximum heap size of the JVM for WAS.
bcgSsl.jacl	This script configures the WAS server for inbound SSL server authentication. It configures the WAS server's keystore and truststore. **Caution:** This JACL file modifies the SSL inbound keystore and truststore file entries in the security.xml file. If you give incorrect entries to the script's arguments, the WebSphere Partner Gateway - Express server will fail to start.

Testing WebSphere Partner Gateway - Express

After you use the instructions in the previous sections of this chapter to configure WebSphere Partner Gateway - Express as desired, use the following procedure to be sure that WebSphere Partner Gateway - Express is operating as desired.

1. Install and run two instances of WebSphere Partner Gateway - Express on different systems.
2. Send a document from one instance of WebSphere Partner Gateway - Express to the other.
   - If you sent an AS2-based document, see “Sending AS2 documents” on page 57.
   - If you sent an HTTP-based document, see “Sending HTTP documents” on page 62.
3. After you send the document, go to the Sent page of the instance that sent the document and verify that the document was sent.
   - If you sent an AS2-based document, see “Viewing sent AS2 documents” on page 59.
   - If you sent an HTTP-based document, see “Viewing sent HTTP documents” on page 64.
4. Go to the instance that received the document and verify that the document was received.
   - If you received an AS2-based document, see “Viewing received AS2 documents” on page 61.
   - If you received an HTTP-based document, see “Viewing received HTTP documents” on page 65.

   Note: WebSphere Partner Gateway - Express does not save the original file name on all received documents. Instead, a unique identification number is generated and used as the file name on incoming documents.
5. If the document was received, skip to step 6. Otherwise, go to the Pending Transmission page and see whether the document is waiting to be transmitted.
   - For AS2-based documents, see “Viewing pending AS2 documents” on page 60. If you requested a Message Disposition Notification for your document, also see “Viewing AS2 documents pending MDNs” on page 61.
   - If you sent an HTTP-based document, see “Viewing pending HTTP documents” on page 65.

   If the document is not sent or received, check your configuration, then resend the document and see whether the problem is corrected.
6. If the document was sent and received successfully, send a document from the instance that received the document. Then check that the document was sent and received successfully.

Chapter 5. Configuring Security

Security means that the contents of transactions cannot be accessed by unauthorized individuals while the documents are in transit. WebSphere Partner Gateway - Express supports a number of security features to safeguard documents, such as encryption and decryption, digital signing, a multi-level authentication process that incorporates Secure Sockets Layer (SSL), and client authentication.

This chapter describes how to configure the security features of WebSphere Partner Gateway - Express. Topics in this chapter include:

Displaying the Security menu

All security activities are performed using the Security tab. When you click the **Security** tab, the Inbound page appears by default. However, you can use the horizontal navigation bar to access other security pages. The navigation bar contains the following:

- **Inbound** enables you to configure security for documents received by WebSphere Partner Gateway - Express.
- **Outbound** enables you to configure security for documents sent by WebSphere Partner Gateway - Express.
- **Certifying Authority** enables you to add and delete CA (certifying authorities) certificates. See "Adding certificates from certifying authorities" on page 53.
- **Certificate Revocation List** enables you to add and delete CRLs. See "Working with certification revocation lists" on page 54.

Configuring encryption and decryption

WebSphere Partner Gateway - Express uses a cryptographic system known as public key encryption to ensure secure communication between trading partners. Public key encryption uses a pair of mathematically related keys. A document encrypted with the first key must be decrypted with the second, and a document encrypted with the second must be decrypted with the first. Each participant in a public key system has a pair of keys. One of these keys is kept secret; this is the private key. The other key is distributed to anyone who wants it; this is the public key. WebSphere Partner Gateway - Express uses a partner's public key to encrypt a document; the private key is used for decryption.

This section describes how to configure encryption with WebSphere Partner Gateway - Express, and includes the following topics:

Configuring encryption for outbound documents

To configure encryption for outbound documents, you must first upload the trading partner's public certificate, which contains the public key, then enable encryption for outbound documents to that partner. These configuration steps will automatically encrypt any outbound documents sent to that partner using the partner's public key. Upon receiving the encrypted document, the trading partner must then use their private key to decrypt the document. The following sections describe how to configure encryption for outbound documents.

"Uploading the trading partner's public certificate"

"Enabling encryption for outbound documents"

Uploading the trading partner's public certificate

To upload the trading partner's public certificate, which contains the public key, use the following procedure.

1. Click the **Security** tab, then click **Outbound** in the navigation bar. The Outbound page appears.
2. From the **Selected Participant** drop-down menu, select the participant for whom you want to upload the public certificate.
3. Locate the Encryption row, then, in the **Upload** column, click the **Add/Update Certificate/Key** icon. The Upload Encryption Public Certificate page appears.
4. In the Public Certificate field, enter the path and name of the public certificate file you want to upload. Alternatively, click the **Browse** button to select the public certificate file you want to upload, then click **Open**.

   Note: The certificates must be DER encoded. DER encoded certificates typically have a `.der` or `.cer` extension.
5. Click the **Submit** button.

Enabling encryption for outbound documents

To enable encryption for documents being sent to a particular trading partner, use the following procedure.

1. Click the **Configuration** tab, then click **AS2** in the navigation bar.
2. From the **Selected Participant** drop-down menu, select the participant for whom outbound documents will be encrypted.
3. Click the **Edit** button. The Manage AS2 editing page opens, enabling you to edit both Inbound and Outbound AS2 parameters.
4. In the Outbound section of the page, select the **Encrypt Documents** check box, then click **Save**.

Configuring decryption for inbound documents

In order to receive encrypted documents from a partner, you must first create a public certificate, or public key, then send that public certificate to the partner. To create a public certificate, you must first generate or upload a self-signed document decryption keypair, then download and save the public certificate portion of that keypair and send it to the partner. The following sections describe how to create a public certificate.

"Generating a new self-signed document decryption keypair" on page 43

"Uploading an existing decryption keypair" on page 43

"Downloading a public certificate for decryption" on page 44

Generating a new self-signed document decryption keypair

The following procedure describes how to use WebSphere Partner Gateway - Express to generate a new self-signed decryption keypair for securing inbound documents.

Note: If a document decryption keypair already exists, refer to "Uploading an existing decryption keypair."

When you generate a self-signed decryption keypair, it is uploaded into WebSphere Partner Gateway - Express automatically. The generated decryption certificate is also stored in the Express Certifying Authority (CA) directory.

1. Click the **Security** tab to display the Inbound page. If the page does not appear, click **Inbound** in the navigation bar.
2. From the **Selected Participant** drop-down menu, select the participant for whom you want to generate the self-signed keypair.
3. Locate the Decryption row, then, in the **Generate** column, click the **Generate Self-Signed Certificate** icon. The Inbound page appears.
4. Complete the entries in the Inbound page (see Table 7).
5. Click the **Create** button. The self-signed keypair is uploaded and appears in the Inbound page. A new file called `decrypt.der` is added to the **Decryption** row, and the certificate is automatically added to the the **Certifying Authority** page. Also, the partner name is automatically added to the filename. For example, if the parner's name is Partner1, the filename will be `decryptPartner1.der`.

Table 7. Inbound page for Generated Self-Signed Document Decryption Keystore

Parameter	Description
Common Name	Enter the server host name.
Organization	Enter the name of the participant's company.
Organizational Unit	Enter the name of the department where the participant works.
Locality	Enter the locale or city where the participant works.
State	Enter the state or province where the participant works.
Country	Enter the country where the participant works.
E-mail Address	Enter the participant's e-mail address.
Certificate Validity	Enter the number of days for which the certificate is valid.
Private Key Password	Enter the private key password.

Uploading an existing decryption keypair

To upload an existing decryption keypair for securing inbound documents, use the following procedure.

Note: Use these instructions only if a decryption keypair already exists. Otherwise, refer to "Generating a new self-signed document decryption keypair."

1. Click the **Security** tab to display the Inbound page. If the page does not appear, click **Inbound** in the navigation bar.
2. From the **Selected Participant** drop-down menu, select the participant for whom you want to upload the keypair.

3. Locate the Decryption row, then, in the **Upload** column, click the **Add/Update Certificate Key** icon. The Inbound page appears.
4. Complete the entries in the Inbound page (see Table 7 on page 43).
5. Click the **Submit** button. The decryption pair is uploaded and appears in the Inbound page. A copy of the decryption certificate will also be uploaded to the Express Certifying Authority (CA) directory.

Table 8. Inbound page for Uploading an Existing Decryption Keypair

Parameter	Description
Private Key File	The private key file must be in PKCS#8 format. If the private key file is not present in PKCS#8 format, the private key will be extracted from PKCS12 type of file if PKCS#12 file is uploaded in the PrivateKey file upload field. Enter the full path and name of the private key file to be uploaded. Alternatively, click **Browse** to navigate to the file, then select the file and click **Open** to load the full-path name into the field.
Private Key Password	Enter the private key password for the decryption file.
Public Certificate	The public certificate must be in the DER format. Enter the full path and name of the public certificate file to be uploaded. Alternatively, click **Browse** to navigate to the file, then select the file and click **Open** to load the full-path name into the field.

Downloading a public certificate for decryption

After you generate or upload a keypair into WebSphere Partner Gateway - Express, you must download the public certificate before you can send it to the trading partner. This is the certificate that the partner will use to encrypt documents that you will decrypt with the private key upon receipt.

1. Click the **Security** tab to display the Inbound page. If the page does not appear, click **Inbound** in the navigation bar.
2. From the **Selected Participant** drop-down menu, select the participant whose certificate you want to download.
3. Locate the Decryption row, then, in the Download column, click the **Download Public Certificate** icon. A ″file-download″ dialogue box appears.

   Note: Depending on your browser version and firewall settings, the dialogue box may prompt you to select either opening the file or saving it to disk. If this occurs select the ″save″ option.
4. Click **Save** (or it's equivalent) to display the Save As dialog box.
5. In the Save As dialog box, select a location where you want to download the certificate, and rename the file to something appropriate, then click **Save**.
6. Send this file to the trading partner.

Configuring and verifying digital signatures

Digital signing is the mechanism for ensuring non-repudiation. Non-repudiation is a service that ensures that a participant cannot deny having originated and sent a message (called "Non-Repudiation of Origin and Content"). It also ensures that the participant cannot deny having received a message (called "Non-Repudiation of Receipt"). In an authentication system that uses public key encryption, digital signatures are used to sign certificates.

A digital signature allows an originator to sign a message in such a way that the message can be verified that it was signed by no one other than that entity and consequently that the message has not been modified since it was signed. WebSphere Partner Gateway - Express uses digital signatures to secure inbound and outbound documents.

The following sections describes how to configure outbound digital signatures and digital signature verification on inbound documents.

Configuring digital signatures for outbound documents

To configure digital signatures for outbound documents, you must first create or upload a document signing keypair, then download the public key portion of that keypair to be sent to the trading partner. Creating a document signing keypair can be done either by generating a new self-signed document signing keypair, or by uploading an existing document signing keypair. The following sections describe how to configure digital signing for outbound documents.

"Generating a self-signed document signing keypair"

"Uploading an existing document signing keypair" on page 46

"Downloading a document signing public certificate" on page 47

Generating a self-signed document signing keypair

The following procedure describes how to use WebSphere Partner Gateway - Express to generate a new self-signed document signing keypair.

Note: If a document signing keypair already exists, refer to "Uploading an existing document signing keypair" on page 46.

When you generate a self-signed document signing keypair, it is uploaded into WebSphere Partner Gateway - Express automatically. To generate a self-signed document signing keypair for securing outbound documents, use the following procedure.

1. Click the **Security** tab, then click **Outbound** in the navigation bar. The Outbound page appears.
2. From the **Selected Participant** drop-down menu, select the participant for whom you want to generate the self-signed keypair.
3. Locate the Verification row, then, in the Generate column, click the **Generate Self-Signed Certificate** icon. The Outbound page appears.
4. Complete the entries in the Outbound page (see Table 9 on page 46).
5. Click the **Create** button. The self-signed keypair is uploaded and appears in the Outbound page.

Note: The role changes from **Verification** to **Signing**.

Table 9. Outbound page for Generated Self-Signed Document Signing Keypair

Parameter	Description
Common Name	Enter the server host name.
Organization	Enter the name of the participant's company.
Organizational Unit	Enter the name of the department where the participant works.
Locality	Enter the locale or city where the participant works.
State	Enter the state or province where the participant works.
Country	Enter the country where the participant works.
E-mail Address	Enter the participant's e-mail address.
Certificate Validity	Enter the number of days for which the keypair is valid.
Private Key Password	Enter the private key password.

Uploading an existing document signing keypair

To upload a document signing keypair for securing outbound documents, use the following procedure.

Note: Use these instructions only if a document signing keypair already exists. Otherwise, refer to "Generating a self-signed document signing keypair" on page 45.

1. Click the **Security** tab, then click **Outbound** in the navigation bar. The Outbound page appears.
2. From the **Selected Participant** drop-down menu, select the participant for whom you want to upload the keypair.
3. Locate the **Signing** row, then in the Upload column, click the **Add/Update Certificate/Key** button. The Upload Document Signing Keypair page appears.
4. Complete the entries in the page (see Table 10).
5. Click the **Submit** button. The keypair is uploaded and appears in the Outbound page.

Table 10. Outbound page for Document Signing Keypair

Parameter	Description
Private Key File	The private kay file must be in PKCS#8 format. If the private key file is not present in PKCS#8 format, the private key will be extracted from PKCS12 type of file if PKCS#12 file is uploaded in the PrivateKey file upload field. Enter the path and name of the private key file you want to upload. Alternatively, click the **Browse** button to select the private key file you want to upload.
Private Key Password	Enter the private key password.
Public Certificate	The public certificate must be in the DER format. Enter the path and name of the public certificate file you want to upload. Alternatively, click the **Browse** button to select the public certificate file you want to upload.

Downloading a document signing public certificate

After you upload a document signing keypair into WebSphere Partner Gateway - Express, you must download the keypair's public certificate before you can send it to the partner. If the partner is using WebSphere Partner Gateway - Express, the partner is expected to load the document signing certificate into his or her list of certifying authorities (see "Adding new certificates" on page 54).

1. Click the **Security** tab, then click **Outbound** in the horizontal navigation bar. The Outbound page appears.
2. From the **Selected Participant** drop-down menu, select the participant whose document signing public certificate you want to download.
3. Locate the **Signing** row, then in the Download column, click the **Download Public Certificate** button. A ″file-download″ page appears.

   Note: Depending on your browser version and firewall settings, the dialogue box may prompt you to select either opening the file or saving it to disk. If this occurs select the ″save″ option.
4. Click **Save** (or equivalent) to display the Save As dialog box.
5. Select a location where you want to download the document signing public certificate, rename the file to an appropriate name, then click **Save**.
6. Send the saved file to the trading partner.

Configuring digital signature verification for inbound documents

If your trading partner is going to send you digitally-signed documents, you must obtain that trading partner's public signature certificate and add it to the Certifying Authority tab. The following procedure describes how to do this.

1. Click the **Security** tab, then click **Certifying Authority** in the navigation bar. The Certifying Authority page appears.
2. Click the **Add New Certificate** button.
3. Enter the path and name of the public certificate file you want to add. Alternatively, click the **Browse** button to select the public certificate file you want to add.
4. Click **Submit** to add the file to the list of Certifying Authority certificate files.

Enabling digital signature

To enable digital signature, use the following procedure.

1. Click the **Configuration** tab, then click **AS2** in the navigation bar.
2. From the **Selected Participant** drop-down menu, select the participant for whose outbound documents you want to enable encryption.
3. Click the **Edit** button. The Manage AS2 editing page appears.
4. In the Outbound section, select the **Sign Documents** check box, then click **Save**.

Using the Secure Sockets Layer (SSL) protocol

WebSphere Partner Gateway - Express uses the Secure Sockets Layer (SSL) protocol to secure inbound and outbound documents. SSL is a commonly used protocol for managing security over the Internet. SSL provides secure connections by enabling two applications linked through a network connection to authenticate the other's identity and by encrypting the data exchanged between the applications.

An SSL connection begins with a handshake. During this stage, the applications exchange digital certificates, agree on the encryption algorithms to use, and generate encryption keys used for the remainder of the session.

The SSL protocol provides the following security features:

- Server authentication — the server uses its digital certificate, issued by a trusted certificate authority, to authenticate itself to clients.
- Client authentication — optionally, clients might be required to authenticate themselves to the server by providing their own digital certificates. This type of authentication is also referred to as mutual authentication.
- Data privacy — all client requests and server responses are encrypted to maintain the confidentiality of the data exchanged over the network.
- Data integrity — data that flows between a client and server is protected from third-party tampering.

The following sections describe how to use SSL for inbound server and client authentication and outbound client authentication.

"Using keystores for inbound server authentication"

"Using truststores for inbound client authentication" on page 50

"Using keypairs for outbound client authentication" on page 51

"Enabling HTTPS" on page 53

Using keystores for inbound server authentication

A keystore for securing inbound documents over an SSL connection can be generated and uploaded automatically within WebSphere Partner Gateway - Express or uploaded from a location outside the application. The keystore can then be downloaded.

A keystore is a protected database that holds keys and certificates. If your participants have keys and certificates and use SSL, you can use the Inbound page to make the keystore available. The following topics describe how to use keystores for inbound server authentication.

"Generating a self-signed SSL keystore"

"Uploading an SSL keystore" on page 49

"Downloading an SSL keystore" on page 49

Generating a self-signed SSL keystore

The following procedure describes how to use WebSphere Partner Gateway - Express to generate a self-signed SSL keystore for securing inbound documents. When you generate a self-signed keystore, it is uploaded into WebSphere Partner Gateway - Express automatically.

1. Click the **Security** tab to display the Inbound page. If the page does not appear, click **Inbound** in the navigation bar.
2. Locate the SSL Connection row, then, in the **Generate** column, click the **Generate Self-Signed Certificate** icon. The Inbound Generate Self-Signed SSL Keystore page appears.
3. Complete the entries in the Inbound page (see Table 11 on page 49).

4. Click the **Create** button. The self-signed keystore is uploaded and appears in the Inbound page.

Table 11. Inbound page for Generated Self-Signed SSL Keystore

Parameter	Description
Common Name	Enter the server host name.
Organization	Enter the name of the participant's company.
Organizational Unit	Enter the name of the department where the participant works.
Locality	Enter the locale or city where the participant works.
State	Enter the state or province where the participant works.
Country	Enter the country where the participant works.
E-mail Address	Enter the participant's e-mail address.
Certificate Validity	Enter the number of days for which the keystore is valid.
Keystore Password	Enter the keystore password.
Private Key Password	Enter the private key password.

Uploading an SSL keystore

If you have an SSL keystore you want to upload into WebSphere Partner Gateway - Express, use the following procedure.

1. Click the **Security** tab to display the Inbound page. If the page does not appear, click **Inbound** in the horizontal navigation bar.
2. Locate the SSL Connection row, then, in the Upload column, click the **Add/Update Certificate/Key** icon. The Inbound page appears.
3. Complete the entries in the Inbound page (see Table 12).
4. Click the **Submit** button. The keystore is uploaded and appears in the Inbound page.

Table 12. Inbound page for Uploaded SSL Keystore

Parameter	Description
Keystore File	Enter the path and name of the keystore file you want to upload. Alternatively, click the **Browse** button to select the keystore file you want to upload.
Keystore Password	Enter the keystore password for the keystore you want to upload.
Key Password	Enter the key password for the keystore you want to upload.

Downloading an SSL keystore

After you upload an SSL keystore into WebSphere Partner Gateway - Express, you can use the following procedure to download the public certificate encapsulated in the keystore database.

1. Click the **Security** tab to display the Inbound page. If the page does not appear, click **Inbound** in the horizontal navigation bar.
2. Locate the SSL Connection row, then, in the Download column, click the **Download Public Certificate** icon. A ″file-download″ page appears.

   Note: Depending on your browser version and firewall settings, the dialogue box may prompt you to select either opening the file or saving it to disk. If this occurs select the ″save″ option.

3. Click **Save** (or equivalent) to display the Save As dialog box, select a location where you want to download the certificate, and click **Save**.

Using truststores for inbound client authentication

A truststore is used for client authentication, when WebSphere Partner Gateway - Express wants to verify the certificate provided by the server. From a truststore, the system can ascertain whether to trust a client and allow the client access to the site.

Using the Inbound page, you can upload a truststore for client authentication. The truststore can then be deleted when it is no longer required.

If the truststore you want to upload has not been created, you can use keytool to create it. The following section describes this procedure.

Important: To enable client authentication, you must first run the bcgClientAuth.jacl script, located at `<ProductDir>/jaclScripts`. Instructions for invoking the script are in the script itself.

Using keytool

Keytool is a key and certificate management utility. It lets you create keys for use in self-authentication (where WebSphere Partner Gateway - Express authenticates itself to other entities and services) or data integrity and authentication services, using digital signatures. It also lets you cache the public keys (in the form of certificates) of their communicating peers.

Keytool stores the certificates in a truststore. The default truststore implementation implements the keystore as a file. Once you create the file, you can use the procedure under "Uploading a truststore for client authentication" on page 51 to upload the file into WebSphere Partner Gateway - Express.

The following procedures describe how to use keytool to create a truststore, list certificates in a truststore, add certificates to a truststore, and delete certificates from a truststore. The commands used to perform these procedures can be executed from any system that has Java installed. For convenience, keytool is provided in the `was\java\jre\bin` directory of the WebSphere Partner Gateway - Express CD.

Note: You can also use ikeyman, a GUI bundled with WebSphere Partner Gateway - Express that allows you to manage certificates in a truststore. The ikeyman executables are located in the `was\bin` directory.

Creating a truststore: To create a truststore, use the following procedure.

1. Open a command prompt window and set the current directory to the location of the `keytool.exe` file.
2. Execute the following command:

```
keytool -genkey -keystore <truststore filename> -storetype PKCS12
```

Listing certificates in a truststore: To list certificates in a truststore, use the following procedure.

1. Open a command prompt window and set the current directory to the location of the `keytool.exe` file.
2. Execute the following command:

```
keytool -list -v -keystore <truststore>
```

3. When keytool prompts you for a truststore password, enter the appropriate password to list the certificates in the truststore.

Adding a certificate to a truststore: To add a certificate to a truststore, use the following procedure.

1. Open a command prompt window and set the current directory to the location of the `keytool.exe` file.
2. Execute the following command. In this command, the alias option lets you assign a name to the certificate that is easy to remember. This will allow you to identify the truststore entries easily when you list it in the future.
   `keytool –import –keystore <truststore> –file <certificate file> -trustcacerts –alias <cert name>`
3. When keytool prompts you for a truststore password, enter the appropriate password to add the certificates to the truststore.

Removing a certificate from a truststore: To remove a certificate from a truststore, use the following procedure.

1. Open a command prompt window and set the current directory to the location of the `keytool.exe` file.
2. Execute the following command.
   `keytool –delete –alias <cert name> -keystore truststore`
3. When keytool prompts you for a truststore password, enter the appropriate password to remove the certificate from the truststore.

Uploading a truststore for client authentication: After a truststore has been created, use the following procedure to upload it for client authentication of inbound documents.

1. Click the **Security** tab to display the Inbound page. If the page does not appear, click **Inbound** in the navigation bar.
2. From the **Selected Participant** drop-down menu, select the participant for whom you want to upload the truststore.
3. Locate the Client Auth row, then, in the Upload column, click the **Add/Update Certificate/Key** icon. The Inbound Upload Truststore for Client Authentication page appears.
4. Complete the entries in the page (see Table 13).
5. Click the **Submit** button. The truststore is uploaded and appears in the Inbound page.

Table 13. Inbound page for Uploaded Truststore for Client Authentication

Parameter	Description
Truststore File	Enter the path and name of the truststore file you want to upload. Alternatively, click the **Browse** button to select the truststore file you want to upload.
Truststore Password	Enter the truststore password.

Using keypairs for outbound client authentication

For outbound documents, client authentication is where WebSphere Partner Gateway - Express identifies itself to a remote server. The following topics describe how to use keypairs for outbound client authentication.

"Generating a self-signed SSL client certificate keypair" on page 52

"Uploading a client authentication keypair"

"Downloading the client certificate for client authentication" on page 53

Generating a self-signed SSL client certificate keypair

The following procedure describes how to use WebSphere Partner Gateway - Express to generate a self-signed SSL client certificate keypair. When you generate a self-signed SSL client certification keypair, it is uploaded into WebSphere Partner Gateway - Express automatically.

1. Click the **Security** tab, then click **Outbound** in the navigation bar. The Outbound page appears.
2. From the **Selected Participant** drop-down menu, select the participant for whom you want to generate the self-signed keypair.
3. Locate the Client Auth row, then, in the Generate column, click the **Generate Self-Signed Certificate** icon. The Outbound page appears.
4. Complete the entries in the Outbound page (see Table 14).
5. Click the **Create** button. The self-signed keystore is uploaded and appears in the Outbound page.

Table 14. Outbound page for Generated Self-Signed SSL Client Certificate Keypair

Parameter	Description
Common Name	Enter the server host name.
Organization	Enter the name of the participant's company.
Organizational Unit	Enter the name of the department where the participant works.
Locality	Enter the locale or city where the participant works.
State	Enter the state or province where the participant works.
Country	Enter the country where the participant works.
E-mail Address	Enter the participant's e-mail address.
Certificate Validity	Enter the number of days for which the keypair is valid.
Private Key Password	Enter the private key password.

Uploading a client authentication keypair

To upload a client authentication keypair identifying this client to a remote SSL-enabled host, use the following procedure.

1. Click the **Security** tab, then click **Outbound** in the navigation bar. The Outbound page appears.
2. From the **Selected Participant** drop-down menu, select the participant for whom you want to upload the keypair.
3. Locate the Client Auth row, then, in the Upload column, click the **Add/Update Certificate/Key** icon. The Outbound Upload Client Certificate Keypair page appears.
4. Complete only the **Public Certificate** entry in the Outbound page (see Table 15 on page 53).
5. Click the **Submit** button. The keypair is uploaded and appears in the Outbound page.

Table 15. Outbound page for Client Authentication Keypair

Parameter	Description
Public Certificate	Enter the path and name of the public certificate file you want to upload. Alternatively, click the **Browse** button to select the public certificate file you want to upload.

Downloading the client certificate for client authentication

After you upload a keypair into WebSphere Partner Gateway - Express, you can use the following procedure to download the public certificate. This public certificate can be e-mailed to the partner for inclusion within the partner's truststore.

1. Click the **Security** tab, then click **Outbound** in the navigation bar. The Outbound page appears.
2. From the **Selected Participant** drop-down menu, select the participant whose keypair you want to download.
3. Locate the Client Auth row, then, in the Download column, click the **Download Public Certificate** icon. A ″file-download″ page appears.

   Note: Depending on your browser version and firewall settings, the dialogue box may prompt you to select either opening the file or saving it to disk. If this occurs select the ″save″ option.
4. Click **Save** (or equivalent) to display the Save As dialog box, select a location where you want to download the keypair, and click **Save**.

Enabling HTTPS

The following steps describe how to enable HTTPS.

1. Click the **Configuration** tab, then click **My Profile** in the navigation bar. The Manage My Profile page appears.
2. Click the **Edit** button to open the Manage My Profile editing page.
3. In the Secure field (under Domain) of the Receipt Address section, enter a domain name, then enter an available HTTPS port number in the corresponding Port field.
4. If appropriate or necessary, fill in fields under Company AS2 ID and Company Details, then click **Save**.
5. Click the **Configuration** tab, then click **Manage Participants** in the navigation bar. The Manage Participants page appears.
6. Click **Edit** for the participant whose HTTPS you want to enable. The Edit Participant page appears.
7. Select the HTTPS check box, then click **Save**.

Adding certificates from certifying authorities

WebSphere Partner Gateway - Express uses digital certificates to develop trust in the user's public key. A certificate is, essentially, an endorsement of the authenticity of a private key. Certificates can be digitally signed by highly trusted parties that perform background checks on the certificate owners to verify their identities. These highly trusted parties are CAs, and can confer varying levels of trust to certificates. In fact, CAs can delegate trust to other CAs by signing the secondary CA's certificate. This creates a certificate "chain." In this way, a trusted third party (the CA) vouches for the authenticity of the certificate, and the method used to vouch is a digital signature included in the certificate.

Using the Certifying Authority page, you can add and delete certificates.

Important: All CA certificates in the certification path must be added. If any CA certificate is not added, the certificate path will not be built, and document processing will fail.

Adding new certificates

To add new public certificates to the Certifying Authority, use the following procedure.

Note: When you upload a CA certificate, be sure to upload the corresponding CA certificate chain.

1. Click the **Security** tab, then click **Certifying Authority** in the navigation bar. The Certifying Authority page appears.
2. Click the **Add New Certificate** button. The Certifying Authority page appears.
3. Click the **Browse** button. The File Upload dialog box appears.
4. Navigate to the location where the certificate you want to add is located. Then click the certificate and click the **Open** button. The path where the certificate resides appears in the Certifying Authority page.
5. Click the **Submit** button. The certificate is added to WebSphere Partner Gateway - Express and its name appears in the Certifying Authority page.

   Important: If the certificate contains a noncompliant key usage, a warning message appears asking if you want to continue to upload or discard the certificate. If you choose to continue to upload the noncompliant certificate, you must replace it with a compliant certificate before using it.
6. To add more certificates, repeat steps 2 through 5.

Deleting a certificate

If you no longer need a certificate, use the following procedure to delete it from WebSphere Partner Gateway - Express.

1. Click the **Security** tab, then click **Certifying Authority** in the horizontal navigation bar. The Certifying Authority page appears.
2. In the **Delete** column, click the **Delete Certificate/Key** icon that corresponds to the certificate you want to delete. A confirmation dialogue box appears, asking you to confirm that you want to proceed with the deletion.
3. Click **OK** to delete the certificate or **Cancel** to retain it.

Working with certification revocation lists

WebSphere Partner Gateway - Express includes a Certificate Revocation List (CRL) feature. The CRL, issued by a Certificate Authority (CA), identifies community participants who have revoked certificates prior to their scheduled expiration date. Participants with revoked certificates will be denied access to WebSphere Partner Gateway - Express.

Each revoked certificate is identified in a CRL by its certificate serial number. WebSphere Partner Gateway - Express's Document Manager scans the CRL every 60 seconds and refuses connections to participants if the list contains one or more of their certificates.

CRLs are stored in the following location: `/<shared data directory>/security/crl`. WebSphere Partner Gateway - Express uses the setting bcg.http.CRLDir in the bcg.properties file to identify the location of the CRL directory.

For example, in the bcg.properties file, you would use the following setting:

```
bcg.http.CRLDir=/<shared data directory>/security/crl
```

Using the Certificate Revocation List page, you can add and delete Certificate Revocation Lists (CRLs). CRLs contain lists of keys that have been compromised and should therefore not be trusted.

Adding new CRLs

To add new CRLs, use the following procedure.

1. Click the **Security** tab, then click **Certificate Revocation List** in the navigation bar. The Certificate Revocation List page appears.
2. Click the **Add New CRL** button. The Certificate Revocation List page appears.
3. Click the **Browse** button. The File Upload dialog box appears.
4. Navigate to the location where the CRL you want to add is located. Then click the CRL and click the **Open** button. The path where the CRL resides appears in the Certificate Revocation List page.
5. Click the **Submit** button. The CRL is added to WebSphere Partner Gateway - Express and its name appears in the Certificate Revocation List page.
6. To add more CRLs, repeat steps 2 through 5.

Deleting a CRL

If you no longer need a CRL, use the following procedure to delete it from WebSphere Partner Gateway - Express.

1. Click the **Security** tab, then click **Certificate Revocation List** in the navigation bar. A Certificate Revocation List page appears.
2. In the **Delete** column, click the **Delete Certificate/Key** icon for the CRL you want to delete. A confirmation dialogue box appears, asking you to confirm that you want to proceed with the deletion.
3. Click **OK** to delete the CRL or **Cancel** to retain it.

Running the bcgSetCRLDP.jacl script

CAs maintain and update the CRLs. These CRLs are typically stored in a CRL distribution point. CRLs are used while doing revocation checks for the certificates to determine whether the certificate is revoked.

The bcgSetCRLDP.jacl script can be used to enable or disable CRL distribution point checking when the revocation check is performed. If you need the CRL distribution points to be accessed when revocation checking of a certificate is performed, enable the use of CRL distribution points. If the certificates you have installed contain a CRL DP extension, you can enable the use of CRL distribution point s so that the distribution points are accessed when the revocation check is performed. If you have downloaded all the required CRLs in the directory set in bcg.properties for the property bcg.CRLDir, you might not want to enable the use of CRL distribution points. If the current CRLs are not likely to be available in the bcg.CRLDir directory, you should enable the use of CRL distribution points.

The CRL distribution points accessible via HTTP and LDAP are supported. You can also configure proxies to access the CRL distribution points.

Note 1: For Windows installations, use wsadmin.bat instead of ./wsadmin.sh in the commands listed in this section.

Note 2: On systems running i5/OS or OS/400, the following commands are executed from a QShell (use the STRQSH command) environment. Therefore, you must add the following parameter just after `./wsadmin`: `-wsadmin_classpath /QIBM/ProdData/WSPGExpress60/jaclScripts/classes`. Also, be sure to remove the `.sh` or `.bat` from `./wsadmin`.

To enable the use of CRL distribution points, run the following command from the <server_root>/bin directory:

```
./wsadmin.sh -f <ProductDir>/scripts/bcgSetCRLDP.jacl install <nodename>
<serverName> CRLDP
```

To disable the use of CRL distribution points, run the following command from the <server_root>/bin directory:

```
./wsadmin.sh -f <ProductDir>/scripts/bcgSetCRLDP.jacl uninstall <nodename>
<serverName> CRLDP
```

To enable the use of CRL distribution points with a proxy, run the following command from the <server_root>/bin directory:

```
./wsadmin.sh -f <ProductDir>/scripts/bcgSetCRLDP.jacl install <nodename>
<serverName> CRLDP <proxyHost> <proxyPort>
```

To specify that you do not want to use a proxy, run the following command from the <server_root>/bin directory:

```
./wsadmin.sh -f <ProductDir>/scripts/bcgSetCRLDP.jacl uninstall <nodename>
<serverName> PROXY
```

If you are using a Receiver user exit and if the user exit uses the SecurityService API, the above settings are applicable for the bcgreceiver server also. To run the above commands for the Receiver, replace `bcgdocmgr` with `bcgreceiver`.

Chapter 6. Managing Documents

WebSphere Partner Gateway - Express lets you send, receive, and resend AS2- and HTTP-based documents. It also lets you view pending transmissions and pending Message Disposition Notification (MDN).

This chapter describes how to manage AS2 and HTTP documents. Topics in this chapter include:

Managing AS2 documents

All AS2 document tasks are performed from the AS2 tab's pages. To access the AS2 pages, click the **AS2** tab. Initially, the Pending Transmission page appears. However, you can use the navigation bar to access other pages.

When you click the AS2 tab, the navigation bar contains the following:

- **Pending Transmission** lets you see which AS2 documents are waiting to be transmitted. See "Viewing pending AS2 documents" on page 60.
- **Pending MDN** lets you see which AS2 documents are waiting to receive MDN to prove that the participant received the document. See "Viewing AS2 documents pending MDNs" on page 61.
- **Sent** lets you view sent AS2 documents that meet your search criteria. If a MDN has been requested, the document is not considered to be sent until a MDN has been received. See "Viewing sent AS2 documents" on page 59.
- **Received** lets you see which received AS2 documents meet your search criteria. See "Viewing received AS2 documents" on page 61.
- **Send** lets you send AS2 documents. See "Sending AS2 documents" on page 57.
- **Resend** lets you resend AS2 documents that meet your search criteria. See "Resending AS2 documents" on page 58.

Sending AS2 documents

To send AS2 documents, use the following procedure.

1. Click the **AS2** tab, then click **Send** in the navigation bar. The Send Document page appears.
2. Complete the entries in the Send Document page (see Table 16).
3. Click the **Send** button. A message in the gray area above **Current Transmission Options** indicates whether the file was uploaded to the send directory successfully. The does not indicate whether the document transmission was successful or otherwise. The responsibility for document transmission rests with the engine which subsequently picks up the document from the send directory for packaging and posting. In most cases this transmission will occur within a few seconds.

4. To send additional AS2 documents, repeat steps 2 and 3.

Table 16. Send Document page

Parameter	Description
Participant	Select the participant who will be sending the file.
Content Type	Select the appropriate content type for the file that will be sent.
Filename	Type the name of the file to be sent or use the **Browse** button to select the file.

Resending AS2 documents

WebSphere Partner Gateway - Express makes it easy to resend AS2 documents. Using the Resend Documents page, you can search for sent documents that meet your search criteria and then resend them.

To resend AS2 documents, use the following procedure.

1. Click the **AS2** tab, then click **Resend** in the navigation bar. The Resend Documents page appears.
2. Complete the entries in the Resend Document page (see Table 17 on page 58).
3. Click the **Search** button. WebSphere Partner Gateway - Express finds the sent documents that meet your search criteria and displays them in the Resend Documents page.

   This page shows valuable information about the documents, including status information about whether the document was successfully sent previously. There is also View Document icon you can click to view the content of the documents.
4. To resend one or more documents, click the checkbox for each document you want to resend, and click the **Resend** button.

Table 17. Resend Document page

Parameter	Description
Participant	Select the participant who sent the documents you want to find.
Filename	If you know the name of the file you want to find, enter it. You can use the asterisk as a wildcard character if desired. The default ***.*** finds all documents that meet the other search criteria.
Document Status	Select whether WebSphere Partner Gateway - Express is to find documents that were sent successfully, failed transmission, or both.
File Size	Select the size of the AS2 documents you want to find. If you select **Specify Size**, specify the minimum or maximum size of the document(s) to be located.
Content Type	Select the content type of the documents you want to find.
Date/Time	Select the date and time when the documents you want to find were sent. For start and end dates, you can click the calendar icon to select dates from a pop-up calendar.

Viewing sent AS2 documents

Using the Sent page, you can have WebSphere Partner Gateway - Express search for sent AS2 documents that meet your search criteria.

To view AS2 documents that have been sent, use the following procedure.

1. Click the **AS2** tab, then click **Sent** in the navigation bar. The Sent Documents page appears.
2. Complete the entries in the Sent Documents page.
3. Click the **Search** button. WebSphere Partner Gateway - Express displays summary statistics for the numbers of successful and failed documents grouped in either hourly or daily intervals depending on the value chosen in the "Display Results" drop down on the Search page. Express will display up to 100 of the most recent intervals depending on the search criteria in the Summary Statistics page.
4. To view detailed information about all documents in an interval represented by a row in the Summary Statistics page, click the **View** icon next to the appropriate summary row. This will display the Sent Documents Details page. If you only wish to view only the documents that were successfully transmitted or those that failed, click on the value in the successful or failed column respectively.
   - Display sent document results and search criteria fields in one page by clicking the **Expand Search** icon next to **Participant** at the top of the page. The page that appears contains icons for viewing the content of sent documents and search fields for conducting another search.
   - Display the search scope by clicking the **Expand Search** icon next to **Search Scope**.
5. To view the contents of an individual document, click the **View Document** icon next to the document in the sent Document Detail page. This document will only be displayed if it still exists on the file system. It is possible that the historical logs used for the search are still present but the file has been moved or deleted from the file system. If WebSphere Partner Gateway - Express cannot find the file in the location computed from the activity logs, the **View Document** icon will not be displayed.
6. To view the contents of an individual document, click the **View Document** icon next to the document in the sent Document Detail page. This document will only be displayed if it still exists on the file system. It is possible that the historical logs used for the search are still present but the file has been moved or deleted from the file system. If WebSphere Partner Gateway - Express cannot find the file in the location computed from the activity logs, the **View Document** will not be displayed.

Table 18. Sent Documents page

Parameter	Description
Participant	Select the participant who sent the AS2 documents, or select **all participants** to search all participants.
File Size	Select the size of the AS2 documents you want to find. If you select **Specify Size**, specify the minimum or maximum size of the document(s) to be located.
Content Type	Select the content type of the AS2 documents you want to find, or click **All** to search all content types.
Date/Time	Select the date and time when the documents you want to search were sent. If you select **Between**, specify the start and end dates and start and end times. For start and end dates, you can click the calendar icon to select dates from a pop-up calendar.
Display Results	Select whether results are to be displayed by the hour or by the day.

Viewing pending AS2 documents

Using the Pending Transmission page, you can search for AS2 documents that are waiting to be transmitted. This page will rarely return any documents, as the send directory is polled frequently (typically, at 1-second intervals) and the documents are moved to the sent or error directory as appropriate. However, this page does serve a useful role if troubleshooting is required.

To view pending AS2 transmissions, use the following procedure.

1. Click the **AS2** tab, then click **Pending Transmission** in the navigation bar. The Pending Transmission page appears.
2. Complete the entries in the Pending Transmission page (see Table 17 on page 58).
3. Click the **Search** button. WebSphere Partner Gateway - Express finds the pending documents that meet your search criteria and displays them in the Pending Transmission page.

   This page shows status information about the pending documents,. There is also a **View Document** icon you can click to view the content of the documents.

Table 19. Pending Transmission page

Parameter	Description
Participant	Select the participant whose pending documents you want to find.
Filename	If you know the name of the file you want to find, enter it. You can use the asterisk as a wildcard character if desired. The default ***.*** finds all documents that meet the other search criteria.
File Size	Select the size of the pending AS2 documents you want to find. If you select **Specify Size**, specify the minimum or maximum size of the document(s) to be located.
Content Type	Select the content type of the documents you want to find.

Viewing AS2 documents pending MDNs

Using the Pending MDN page, you can search for AS2 documents that are pending MDNs. Documents pending MDNs remain pending for 10 minutes - this value is not configurable via the console. The default value is 10 minutes. If the document does not receive an MDN within this time, WebSphere Partner Gateway - Express moves it to the Failed folder.

To view documents pending MDNs, use the following procedure:

1. Click the **AS2** tab, then click **Pending MDN** in the navigation bar. The Pending MDN page appears.
2. Complete the entries in the Pending MDN page (see Table 20 on page 61).
3. Click the **Search** button. WebSphere Partner Gateway - Express finds the documents pending MDNs that meet your search criteria and displays them in the Pending MDN page.

   This page shows status information about documents pending MDNs,. There is also a **View Document** icon you can click to view the content of the documents.

Table 20. Pending MDN page

Parameter	Description
Selected Participant	Select the participant whose pending MDNs you want to find.
Filename	If you know the name of the file you want to find, enter it. You can use the asterisk as a wildcard character if desired. The default ***.*** finds all documents that meet the other search criteria.
File SIze	Select the size of the pending AS2 documents you want to find. If you select **Specify Size**, specify the minimum or maximum size of the document(s) to be located.
Duration	Select the length of time that documents can wait for an MDN before being moved to the Failed folder. The default time is 10 minutes.
Content Type	Select the content type of the documents you want to find.

Viewing received AS2 documents

Using the Received page, you can search for AS2 documents that have been received by selected participants.

To view received AS2 documents, use the following procedure.

1. Click the **AS2** tab, then click **Received** in the navigation bar. The Received page appears.
2. Complete the entries in the Received page (see Table 21 on page 62).
3. Click the **Search** button. WebSphere Partner Gateway - Express displays summary statistics for the numbers of successful and failed documents grouped in either hourly or daily intervals depending on the value chosen in the “Display Results” drop down on the Search page. Express will display up to 100 of the most recent intervals depending on the search criteria in the Summary Statistics page.

   This page shows status information about the received documents,. There is also a **View Document** icon you can click to view the content of the documents.

4. To view detailed information about all documents in an interval represented by a row in the Summary Statistics page, click the **View** icon next to the appropriate summary row. This will display the Received Documents Details page. If you only wish to view the documents which were successfully transmitted or those which failed, click on the value in the successful or failed column respectively.
5. To view the contents of an individual document, click the **View Document** icon next to the document in the Received Document Detail page. This document will only be displayed if it still exists on the file system. It is possible that the historical logs used for the search are still present but the file has been moved or deleted from the file system. If WebSphere Partner Gateway - Express cannot find the file in the location computed from the activity logs, the document icon will not be displayed.

Table 21. Received Documents page

Parameter	Description
Participant	Select the participant whose received documents you want to find.
File SIze	Select the size of the received AS2 documents you want to find. If you select **Specify Size**, specify the minimum or maximum size of the document(s) to be located.
Content Type	Select the content type of the received documents you want to find.
Date/Time	Select the date and time when the documents you want to find were received. For start and end dates, you can click the calendar icon to select dates from a pop-up calendar.
Display Results	Select whether results are to be displayed by the hour or by the day.

Managing HTTP documents

All HTTP document tasks are performed from the HTTP tab's pages. To display the HTTP pages, click **HTTP** tab. Initially, the Pending Transmission page appears. However, you can use the navigation bar to access other pages.

When you click the HTTP tab, the navigation bar contains the following:

- **Pending Transmission** lets you see which HTTP documents are waiting to be transmitted. See "Viewing pending HTTP documents" on page 65.
- **Sent** lets you view sent HTTP documents that meet your search criteria. See "Viewing sent HTTP documents" on page 64.
- **Received** shows the HTTP documents that have been received. See "Viewing received HTTP documents" on page 65.
- **Send** lets you send HTTP documents. See "Sending HTTP documents" on page 62.
- **Resend** lets you resend HTTP documents that meet your search criteria. See "Resending HTTP documents" on page 63.

Sending HTTP documents

To send HTTP documents, use the following procedure.

1. Click the **HTTP** tab, then click **Send** in the navigation bar. The Send Document page appears.

2. Complete the entries in the Send Document page (see Table 22).
3. Click the **Send** button. A message in the gray area above **Current Transmission Options** indicates whether the file was uploaded to the send directory successfully. The does not indicate whether the document transmission was successful or otherwise. The responsibility for document transmission rests with the engine which subsequently picks up the document from the send directory for posting. In most cases this transmission will occur within a few seconds.
4. To send additional HTTP documents, repeat steps 2 and 3.

Table 22. Send Document page

Parameter	Description
Participant	Select the participant to whom the file will be sent.
Filename	Type the name of the file to be sent or use the **Browse** button to select the file.

Resending HTTP documents

WebSphere Partner Gateway - Express makes it easy to resend HTP documents. Using the Resend Documents page, you can search for sent documents that meet your search criteria and then resend them.

To resend HTTP documents, use the following procedure.

1. Click the **HTTP** tab, then click **Resend** in the navigation bar. The Resend Documents page appears.
2. Complete the entries in the Resend Document page.
3. Click the **Search** button. WebSphere Partner Gateway - Express finds the sent documents that meet your search criteria and displays them in the Resend Documents page.

   This page shows valuable information about the documents, including status information about whether the document was successfully sent previously. There is also a **View Document** icon you can click to view the content of the documents.
4. To resend one or more documents, click the checkbox for each document you want to resend, and click the **Resend** button. To resend all documents, click the checkbox adjacent to the ″All″ label. This will select (or deselect) all documents.

Table 23. Resend Document page

Parameter	Description
Participant	Select the participant who sent the documents you want to find.
Filename	If you know the name of the file you want to find, enter it. You can use the asterisk as a wildcard character if desired. The default ***.*** finds all documents that meet the other search criteria.
Document Status	Select whether WebSphere Partner Gateway - Express is to find documents that were sent successfully, failed transmission, or both.
File Size	Select the size of the HTTP documents you want to find. If you select **Specify Size**, specify the minimum or maximum size of the document(s) to be located.
Date/Time	Select the date and time when the documents you want to find were sent. For start and end dates, you can click the calendar icon to select dates from a pop-up calendar.

Viewing sent HTTP documents

Using the Sent page, you can have WebSphere Partner Gateway - Express search for sent HTTP documents that meet your search criteria.

To view HTTP documents that have been sent, use the following procedure.

1. Click the **HTTP** tab, then click **Sent** in the navigation bar. The Sent Documents page appears.
2. Complete the entries in the Sent Documents page (see Table 24 on page 65).
3. Click the **Search** button. WebSphere Partner Gateway - Express displays summary statistics for the numbers of successful and failed documents grouped in either hourly or daily intervals depending on the value chosen in the "Display Results" drop down on the Search page. WebSphere Partner Gateway - Express will display up to 100 of the most recent intervals depending on the search criteria in the Summary Statistics page.
4. To view detailed information about all documents in an interval represented by a row in the Summary Statistics page, click the **View Sent Details** icon next to the appropriate summary row. This will display the Received Documents Details page.If you only wish to view the documents which were successfully transmitted or those which failed, click on the value in the successful or failed column respectively.

   In addition to showing detailed information about sent documents, the Document Details page also lets you:

   - Display sent document results and search criteria fields in one page by clicking the **Expand Search** icon next to **Participant** at the top of the page. The page that appears contains icons for viewing the content of sent documents and search fields for conducting another search.
   - Display the search scope by clicking the **Expand Search** icon next to **Search Scope**.
5. To view the contents of an individual document, click the **View Document** icon next the document in the Received Document Detail page. This document will only be displayed if it still exists on the file system. It is possible that the historical logs used for the search are still present but the file has been moved or deleted from the file system. If WebSphere Partner Gateway - Express cannot

find the file in the location computed from the activity logs, the **View Document** icon will not be displayed.

Table 24. Sent Documents page

Parameter	Description
Participant	Select the participant who sent the HTTP documents, or select **all participants** to search all participants.
File Size	Select the size of the HTTP documents you want to find. If you select **Specify Size**, specify the minimum or maximum size of the document(s) to be located.
Date/Time	Select the date and time when the documents you want to search were sent. If you select **Between**, specify the start and end dates and start and end times. For start and end dates, you can click the calendar icon to select dates from a pop-up calendar.
Display Results	Select whether results are to be displayed by the hour or by the day.

Viewing pending HTTP documents

Using the Pending Transmission page, you can search for HTTP documents that are waiting to be transmitted.

To view pending HTTP transmissions, use the following procedure.

1. Click the **HTTP** tab, then click **Pending Transmission** in the navigation bar. The Pending Transmission page appears.
2. Complete the entries in the Pending Transmission page (see Table 25 on page 65).
3. Click the **Search** button. WebSphere Partner Gateway - Express finds the pending documents that meet your search criteria and displays them in the Pending Transmission page.

   This page shows status information about the pending documents,. There is also a **View Document** icon you can click to view the content of the documents.

Table 25. Pending Transmission page

Parameter	Description
Participant	Select the participant whose pending documents you want to find.
Filename	If you know the name of the file you want to find, enter it. You can use the asterisk as a wildcard character if desired. The default ***.*** finds all documents that meet the other search criteria.
File Size	Select the size of the pending HTTP documents you want to find. If you select **Specify Size**, specify the minimum or maximum size of the document(s) to be located.

Viewing received HTTP documents

Using the Received Documents page, you can search for HTTP documents that have been received by selected participants.

To view received HTTP documents, use the following procedure.

1. Click the **HTTP** tab, then click **Received Documents** in the navigation bar. The Received Documents page appears.
2. Complete the entries in the Received Documents page (see Table 25 on page 65).
3. Click the Search button. WebSphere Partner Gateway - Express displays summary statistics for the numbers of successful and failed documents grouped in either hourly or daily intervals depending on the value chosen in the ″Display Results″ drop down on the Search page (Figure 6-5). Express will display up to 100 of the most recent intervals depending on the search criteria in the Summary Statistics page (see Figure 6-7).

   This page shows status information about the received documents,. There is also a **View Document** icon you can click to view the content of the documents.
4. To view detailed information about all documents in an interval represented by a row in the Summary Statistics page, click the magnifying glass icon next to the appropriate summary row. This will display the Received Documents Details page. If you only wish to view the documents which were successfully transmitted or those which failed, click on the value in the successful or failed column respectively.
5. To view the contents of an individual document, click the **View Document** icon next to the document in the Received Document Detail page. This document will only be displayed if it still exists on the file system. It is possible that the historical logs used for the search are still present but the file has been moved or deleted from the file system. If WebSphere Partner Gateway - Express cannot find the file in the location computed from the activity logs, the document icon will not be displayed.

Table 26. Received Documents page

Parameter	Description
Participant	Select the participant whose received documents you want to find.
File SIze	Select the size of the received HTTP documents you want to find. If you select **Specify Size**, specify the minimum or maximum size of the document(s) to be located.
Date/Time	Select the date and time when the documents you want to find were received. For start and end dates, you can click the calendar icon to select dates from a pop-up calendar.
Display Results	Select whether results are to be displayed by the hour or by the day.

Chapter 7. Viewing Reports

WebSphere Partner Gateway - Express provides reports that display valuable information. This chapter describes these reports and how to access them. Topics in this chapter include:

Displaying the Reports pages

All report activities are performed using the Reports tab's pages. To display the pages, click the **Reports** tab. Initially, the Document Summary page appears. However, you can use the navigation bar to access other report pages.

When you click the Reports tab, the navigation bar contains the following:

- **Document Summary** displays a summary of the documents sent, received and pending by each participant. See "Viewing the Document Summary report," below.
- **Participant Summary** displays a summary of the activities performed by participants. See "Viewing the Participant Summary report" on page 68.
- **Activity Logs** displays activity information that matches your search criteria. See "Viewing the Activity Log" on page 68.

Viewing the Document Summary report

To view a summary of the document activities conducted by participants, click the **Reports** tab to display the Document Summary page. If the page does not appear, click **Document Summary** in the navigation bar.

Each row in the Document Summary page shows the following information for each participant:

- Number of pending transmissions.
- Number of pending Message Disposition Notification (MDNs).
- Number of received documents.
- Number of sent documents.

If desired, you can clear sent items in the Document Summary page for one or more participants.

1. Click the checkbox under the **Clear** column for the participants whose sent items you want to clear (or click **All** to check all participants).
2. Click the **Clear** button. A precautionary message asks whether you are sure you want to delete sent items from the selected participant(s).

   Note: The ″Clear″ option only deletes files in the ″sent″ and ″error″ directories for the selected participant. It does not delete files from the ″received″ or ″rec_err″ directories. The reasoning for this is that it is anticipated that every received file will need to be further processed by user interaction

— specifically, the file will need to be accessed and moved to the appropriate business unit for application. Sent files, however, are most likely stored at their source and the copies saved to the file system do not represent unique copies of a file in an organization. Additionally, it is unlikely that a user will ever have a need to go to the filesystem to interrogate a sent file (unlike a received file).

3. Click **OK** to delete them or **Cancel** to retain them. If you click **OK**, all documents in the sent and error directories for the selected participant(s) are deleted.

Viewing the Participant Summary report

The Participant Summary report displays a summary of participant activity. To display this report, click the **Reports** tab, then click **Participant Summary** on the navigation bar.

The Participant Summary report shows the status of queued, sent, and received documents for the participant whose name appears next to **Selected Participant** at the top-left side of the report. To display information about another participant, select one from the **Selected Participant** drop-down menu.

The top-right side of the Participant Summary report also has a **Refresh Rate** value that indicates how often the information in the report is updated. By default, refresh is disabled. To enable it, select the appropriate rate (30 seconds, 1 minute, or 5 minutes) from the drop-down list and click the **Play** icon. To turn off refresh, click the **Pause** icon, which appears in place of the **Play** icon when refresh is enabled.

Viewing the Activity Log

The Activity Logs page lets you view system activity that meets certain search criteria. To display the page where you enter search criteria, click the **Reports** tab, then click **Activity Logs** on the navigation bar. This page lets you search for activity information by date, by text, or by latest entries.

To view the Activity Log, use the following procedure.

1. Click the **Reports** tab, then click **Activity Logs** in the navigation bar.
2. Next to **Limit Size to**, select the maximum size for the log.
3. Indicate whether the search is to be conducted by date, by text, or by latest entries by entering the appropriate search criteria.
   - **By Date** lets you view activity that occurred on a start date, on an end date, or between a range of dates that you specify. If desired you can click the **Calendar** icon to select dates from a pop-up calendar. When the search is performed, the size of the result returned is either the number of characters between the start and end dates or the value selected in the **Limit Size** drop-down list, whichever is smaller. The results will be presented starting with the first entry after the date specified in the search parameters.
   - **By Text** lets you view lines from the Activity Log that appear before or after a text string you enter. You can specify the number of lines before and after the matching text that are to be returned. The search results are presented with the newest matching entry displayed first, working backwards to the oldest entries, until the end of the oldest activity log is reached or the Limit Size bound is reached, whichever occurs first.

- **Latest Entries** lets you view the latest entries in the Activity Log. You can enable refresh to update the Log and specify how often the Log is refreshed. The search results are presented with the newest log entry displayed first and working backwards.

4. Click the **Search** button in the area where you entered your search criteria. (Or click **Reset** to clear your criteria.) WebSphere Partner Gateway - Express finds the activity that matches your criteria and displays it in a new page.

Appendix A. Error Messages

This appendix describes error messages generated by WebSphere Partner Gateway - Express

Table 27. Error Messages

Error Message	Description
alert.advisory.1	MDN Failed Processing
alert.advisory.2	MDN MIC Mismatch
alert.advisory.3	MDN Returned with error status
alert.advisory.4	MDN Disposition = null
alert.advisory.5	MDN not returned in response
alert.advisory.6	MDN Mime parsing error
alert.advisory.7	Unable to return synchronous MDN
alert.advisory.100	Transmission failed
alert.advisory.101	Exception caught posting message
alert.advisory.102	Partner info not found
alert.advisory.103	Signing certificate not found
alert.advisory.104	Received HTTP error code
alert.advisory.200	Unknown doc type received
alert.advisory.201	Message failed processing
alert.advisory.300	Received unknown content type
alert.advisory.301	Received disallowed content type
alert.advisory.302	Received disallowed protocol
alert.advisory.303	Sent unknown content type
alert.advisory.304	Sent disallowed content type
alert.advisory.305	Sent disallowed protocol

Appendix B. WebSphere Partner Gateway - Express Folders

When you install WebSphere Partner Gateway - Express, the program automatically sets up folders and files. This appendix describes the folders that are automatically installed when you install the program.

Directory name	Contents
_jvm	This directory contains the Java Virtual Machine (JVM) that is used by Installer. This directory is removed/deleted after the product is installed.
_unist	This directory contains the uninstaller.exe file that is used to remove WebSphere Partner Gateway - Express from your system.
bin	This directory contains batch and shell script files for executing programs associated with WebSphere Partner Gateway - Express.
copyright	This directory contains IBM WebSphere Partner Gateway - Express copyright information.
config	This directory contains property and system-configuration files, as well as generated and uploaded certificates.
data	This directory contains the participant files.
firstSteps	This directory contains the Getting Started file that is linked to from the First Steps page. The Getting Started file contains general information about how to begin using WebSphere Partner Gateway - Express.
jaclScripts	This directory contains .jacl scripts that allow you to manually configure various components of WebSphere Partner Gateway - Express.
lib	This directory contains library files supporting WebSphere Partner Gateway - Express.
license	This directory contains the license agreement for WebSphere Partner Gateway - Express.
logs	This directory contains a history file of installation and uninstallation of WebSphere Partner Gateway - Express.
readme	This directory contains the ReadMe file that describes how to obtain the WebSphere Partner Gateway - Express documentation.
was	This directory contains all the files and folders that are automatically installed when WebSphere Application Server (WAS) is installed during the installation of WebSphere Partner Gateway - Express.

Appendix C. Uninstalling WebSphere Partner Gateway - Express

This appendix describes how to uninstall WebSphere Partner Gateway - Express from your system.

Note: The instructions in this appendix also apply to WebSphere Business Integration Connect - Express version 4.2.1.

It contains the following sections:

Uninstalling from a Windows system

This section describes how to uninstall WebSphere Partner Gateway - Express from your Windows system. It contains the following:

Using the WebSphere Partner Gateway - Express graphical uninstaller

IBM provides an uninstall program that you can use to remove your entire WebSphere Partner Gateway - Express installation from your computer.

To uninstall WebSphere Partner Gateway - Express:

1. Shut down WebSphere Partner Gateway - Express.
   a. If your existing version of WebSphere Partner Gateway - Express is running, ensure that any documents that are in progress have finished processing.
   b. Close all open Web browser sessions that are connected to the WebSphere Partner Gateway - Express console.
   c. Stop the WebSphere Partner Gateway - Express server.
2. Once the server is stopped, click **Start** > **Settings** > **Control Panel**.
3. Double-click **Add/Remove Programs**. The Add/Remove Programs dialog box appears.
4. Scroll down and select WebSphere Partner Gateway - Express.
5. Click **Change/Remove**.
6. If WebSphere Partner Gateway - Express is installed on a Windows environment and registered as a service, the Service check panel appears. Click **Next** to remove the service from the Windows Service Manager and to continue with the uninstallation process.
7. The Uninstaller Welcome panel appears. Click **Next**.
8. If WebSphere Partner Gateway - Express is installed on a Windows environment and registered as a service, the Unregistering Service panel appears. Click **Next**.
9. At the Product Installation Location window, click **Next**.

10. At the Uninstallation Complete window, click **Finish** to complete the uninstallation process.
11. Restart your computer.

Performing a silent uninstallation on a Windows system

IBM also provides a silent uninstall program that you can use to remove your entire WebSphere Partner Gateway - Express installation from your computer.

To unintall WebSphere Partner Gateway - Express:

1. Shut down WebSphere Partner Gateway - Express.
   a. If your existing version of WebSphere Partner Gateway - Express is running, ensure that any documents that are in progress have finished processing.
   b. Close all open Web browser sessions that are connected to the WebSphere Partner Gateway - Express console.
   c. Stop the WebSphere Partner Gateway - Express server.
2. Open an MS-DOS command prompt window and navigate to the following directory:

   *ProductDir*_uninst

   Here *ProductDir* represents the directory in which you installed WebSphere Partner Gateway - Express.
3. Enter the following command at the prompt:

   ```
   uninstall -silent
   ```
4. Restart your computer.

Uninstalling from a Linux system

This section describes how to uninstall WebSphere Partner Gateway - Express from your Linux system. It contains the following:

- "Using the WebSphere Partner Gateway - Express graphical uninstaller" on page 75
- "Performing a silent uninstallation" on page 77
- "Uninstalling in console mode" on page 77

Using the WebSphere Partner Gateway - Express graphical uninstaller

IBM provides an uninstall program that you can use to remove your entire WebSphere Partner Gateway - Express installation from your computer.

To uninstall WebSphere Partner Gateway - Express:

1. Shut down WebSphere Partner Gateway - Express.
   a. If your existing version of WebSphere Partner Gateway - Express is running, ensure that any documents that are in progress have finished processing.
   b. Close all open Web browser sessions that are connected to the WebSphere Partner Gateway - Express console.
   c. Stop the WebSphere Partner Gateway - Express server.
2. Run the Linux uninstaller executable file.
3. The Uninstaller Welcome panel appears. Click **Next**.
4. At the Product Installation Location window, click **Next**.

5. At the Uninstallation Complete window, click **Finish** to complete the uninstallation process.
6. Restart your computer.

Performing a silent uninstallation

IBM also provides a silent uninstall program that you can use to remove your entire WebSphere Partner Gateway - Express installation from your computer.

To unintall WebSphere Partner Gateway - Express:

1. Shut down WebSphere Partner Gateway - Express.
   a. If your existing version of WebSphere Partner Gateway - Express is running, ensure that any documents that are in progress have finished processing.
   b. Close all open Web browser sessions that are connected to the WebSphere Partner Gateway - Express console.
   c. Stop the WebSphere Partner Gateway - Express server.
2. Open a Linux command prompt window and navigate to the following directory:

   ProductDir/_uninst

   Here *ProductDir* represents the directory in which you installed WebSphere Partner Gateway - Express.
3. Enter the following command at the prompt:

   ```
   ./uninstall -silent
   ```
4. Restart your computer.

Uninstalling in console mode

IBM also provides a command line (console mode) uninstall program that you can use to remove your entire WebSphere Partner Gateway - Express installation from your computer.

To unintall WebSphere Partner Gateway - Express:

1. Shut down WebSphere Partner Gateway - Express.
   a. If your existing version of WebSphere Partner Gateway - Express is running, ensure that any documents that are in progress have finished processing.
   b. Close all open Web browser sessions that are connected to the WebSphere Partner Gateway - Express console.
   c. Stop the WebSphere Partner Gateway - Express server.
2. Open a Linux command prompt window and navigate to the following directory:

   ProductDir/_uninst

   Here *ProductDir* represents the directory in which you installed WebSphere Partner Gateway - Express.
3. Enter the following command at the prompt:

   ```
   ./uninstall -console
   ```
4. Restart your computer.

Uninstalling from a system running i5/OS or OS/400

IBM provides a command line program that you can use to remove the entire WebSphere Partner Gateway - Express program from your system running i5/OS or OS/400. This uninstall program is run in the qshell environment on the system running i5/OS or OS/400 that has WebSphere Partner Gateway - Express installed.

The following steps describe how to uninstall WebSphere Partner Gateway - Express.

1. Shut down WebSphere Partner Gateway - Express.
   a. If your existing version of WebSphere Partner Gateway - Express is running, ensure that any documents that are in progress have finished processing.
   b. Close all open Web browser sessions that are connected to the WebSphere Partner Gateway - Express console.
   c. Open a command line interface to the system running i5/OS or OS/400 with a user profile that has QBCGX60 as a group profile or has *ALLOBJ (All Object) authority.
   d. Start the qsh shell interpreter with the following command:
      `STRQSH`
   e. In the qsh shell interpreter, stop the WebSphere Partner Gateway server with the following commands:
      `cd/QIBM/UserData/WSPGExpress60/bin`
      `bcgStopServer`
2. In the qsh shell interpreter, enter the following commands:
   `cd/QIBM/ProdData/WSPGExpress60`
   `java -cp_uninst/uninstall.jar run -console`

   Note: This command will perform the uninstallation in console mode. To perform the uninstallation without additional user interaction, replace the `-console` parameter with `-silent`.

The uninstaller removes the WebSphere Partner Gateway - Express program from your system running i5/OS or OS/400, but it will leave the following directories that may contain user information:

- `/QIBM/UserData/WSPGExpress60/config`
- `/QIBM/UserData/WSPGExpress60/data`
- `/QIBM/UserData/WPGExpress60/logs`

Appendix D. WebSphere Partner Gateway - Express Messaging Integration

This appendix describes how to use the WebSphere Partner Gateway - Express file system to transfer messages to other enterprise applications over an existing network.

WebSphere Partner Gateway - Express directory structure

You can use the WebSphere Partner Gateway - Express file system to transfer messages to and from enterprise applications, including WebSphere Partner Gateway Enterprise, over an existing network. The messaging directories are located under the *EXPRESS_HOME*`/data/FileSystemAdapter2/partners` directory. On a system running i5/OS or OS/400, the *EXPRESS_HOME* directory is `/QIBM/UserData/WSPGExpress60`. The "partners" directory contains a subdirectory named for each partner configured in the system. The directory structure should resemble the following:

```
 EXPRESS_HOME
data
FileSystemAdapter2
partners
partner1
partner2
...
partnerX
```

If you would like to send a message to a partner, for example, "partner1", move the message into the appropriate "send" subdirectory in the "partner1" directory. Each partner has a set of directories that hold messages that are to be sent, have been sent, have been received, and have had some kind of error. Each send directory also has a subdirectory that corresponds to the method of sending and the message content being sent. For example, "partner1" in the above example has the following subdirectories:

```
    partner1
error
rec_err
received
send
sent
```

The "error" subdirectory contains messages that failed transmission. The "rec_err" subdirectory contains messages that failed receipt. The "received" subdirectory contains messages that were received successfully. The "send" subdirectory contains messages that are being sent currently. The "sent" subdirectory contains messages that have been successfully sent. Each one of the above subdirectories has in turn its own set of identical subdirectories. The subdirectories exist in order to identify the content type and messaging protocol used in sending the messages. Each of the directories above has the following subdirectory structure:

AS2
binary
EDI-Consent
EDIFACT
EDI-X12
MDN
XML
HTTP

Subdirectories of the AS2 directory are used to send and receive AS2 messages. The “binary” subdirectory holds binary messages. The “EDI-Consent”, “EDIFACT” and “EDI-X12” are for EDI format messages. The MDN subdirectory holds received acknowledgements; it is not used in the “send” directory tree. The “XML” directory holds arbitrary XML messages.

The HTTP directory holds messages sent or received using the HTTP POST method.

Message Transmission

In order to send and receive messages programmatically, or manually without the WebSphere Partner Gateway - Express user interface, the file system must be used. Using “partner1” from the example above as a trading partner, an EDI-X12 message can be sent by placing EDI-X12 content in the form of a file into the *EXPRESS_HOME*/data/FileSystemAdapter2/partners/partner1/send/AS2/EDI-X12 subdirectory.

Note: Do not copy files into the “send” subdirectories. Using copy may cause a partially read file to be sent. Instead, use an atomic move operation.

Once Express sends the document, it will be moved either into the sent/AS2/EDI-X12 subdirectory if it succeeded, or the error/AS2/EDI-X12 subdirectory if it failed. Documents requiring MDNs are not moved until the MDN is received, or Express times out waiting for the MDN. Received MDNs are always placed in the MDN directory. When files are moved from the “send” directories, they are suffixed with a timestamp to differentiate between multiple transmissions of the same filename.

Message Receipt

Received messages can be retrieved by opening the “received” subdirectories. For example, if an EDI-X12 message was expected from “partner1” over AS2, the EXPRESS_HOME/data/FileSystemAdapter2/partner1/received/AS2/EDI-X12 directory would store the received message. Any file appearing in that directory will be an EDI-X12 message from ″partner1″ that succeeded. The message could then be retrieved and processed. A robust implementation would also monitor the partner1/rec_err/AS2/EDI-X12 directory in case parsing errors were encountered in an incoming message from ″partner1.″

Note: Incoming files do not retain their original filenames from the sender system. The content itself must be used to identify messages.

Appendix E. Security configuration examples

This appendix describes examples of how to prepare documents to be sent securely between two instances of WebSphere Partner Gateway - Express. In these examples, the first instance of WebSphere Partner Gateway - Express is referred to as ″Express1″ while the second instance is referred to as ″Express2.″ Also, ″5443″ is used as the sample port number. The following examples are described.

Sending documents between two instances of WebSphere Partner Gateway - Express

This section describes how to prepare encrypted documents to be sent between two instances of WebSphere Partner Gateway - Express and includes the following topics:

Sending encrypted documents from Express1 to Express2

The following steps describe how to prepare an encrypted document to be sent from Express1 to Express2.

1. In Express2, generate a new self-signed document decryption keypair. To do this, follow the instructions in “Generating a new self-signed document decryption keypair” on page 43.
2. In Express2, download the new certificate, then rename it to ″Express2PublicEncrypt.der.″ To do this, follow the instructions in “Downloading a public certificate for decryption” on page 44.
3. In Express1, upload the certificate named Express2PublicEncrypt.der from Express2. To do this, follow the instructions in “Uploading the trading partner’s public certificate” on page 42.
4. In Express1, enable encryption for outbound documents. To do this, follow the instructions in “Enabling encryption for outbound documents” on page 42.

Sending encrypted documents from Express2 to Express1

The following steps describe how to prepare an encrypted document to be sent from Express2 to Express1.

1. In Express1, generate a new self-signed document decryption keypair. To do this, follow the instructions in “Generating a new self-signed document decryption keypair” on page 43.

2. In Express1, download the new certificate, then rename it to ″Express1PublicEncrypt.der.″ To do this, follow the instructions in “Downloading a public certificate for decryption” on page 44.
3. In Express2, upload the certificate named Express1PublicEncrypt.der from Express1. To do this, follow the instructions in “Uploading the trading partner’s public certificate” on page 42.
4. In Express2, enable encryption for outbound documents. To do this, follow the instructions in “Enabling encryption for outbound documents” on page 42.

Sending digitally signed documents

This section describes how to prepare digitally signed documents to be sent between two instances of WebSphere Partner Gateway - Express, and includes the following topics:

“Sending digitally signed documents from Express1 to Express2”

“Sending digitally signed documents from Express2 to Express1”

Sending digitally signed documents from Express1 to Express2

The following steps describe how to prepare digitally signed documents to be sent from Express1 to Express2.

1. In Express1, generate a self-signed document signing keypair. To do this, follow the instruction in “Generating a self-signed document signing keypair” on page 45.
2. In Express1, download the new document signing public certificate and rename it to ″Express1PublicSignVerify.der.″ To do this, follow the instructions in “Downloading a document signing public certificate” on page 47.
3. In Express2, upload the document signing keypair. To do this, follow the instructions in “Uploading an existing document signing keypair” on page 46.
4. In Express1, enable digital signature. To do this, follow the instructions in “Enabling digital signature” on page 47.

Sending digitally signed documents from Express2 to Express1

The following steps describe how to prepare digitally signed documents to be sent from Express2 to Express1.

1. In Express2, generate a self-signed document signing keypair. To do this, follow the instruction in “Generating a self-signed document signing keypair” on page 45.
2. In Express2, download the new document signing public certificate and rename it to ″Express2PublicSignVerify.der.″ To do this, follow the instructions in “Downloading a document signing public certificate” on page 47.
3. In Express1, upload the document signing keypair. To do this, follow the instructions in “Uploading an existing document signing keypair” on page 46.
4. In Express2, enable digital signature. To do this, follow the instructions in “Enabling digital signature” on page 47.

Sending documents to be sent over Secure Socket Layer (SSL)

This section describes how to prepare documents to be sent over Secure Socket Layer (SSL) when sending them between two instances of WebSphere Partner Gateway - Express. The following topics are included:

Sending documents over SSL from Express1 to Express2

The following steps describe how to prepare documents to be sent over SSL from Express1 to Express2.

1. In Express2, enable HTTPS. To do this, follow the instructions in "Enabling HTTPS" on page 53. When filling out the Domain and Port fields, use ″Express2″ as the domain and ″5443″ as the port number.
2. In Express2, generate a self-signed SSL client certificate keypair. To do this, follow the instructions in "Generating a self-signed SSL client certificate keypair" on page 52.
3. In Express2, download the newly created client certificate, and rename it to ″Express2PublicSSL.der.″ To do this, follow the instructions in "Downloading the client certificate for client authentication" on page 53.
4. In Express1, upload the public certificate named ″Express2PublicSSL.der.″ To do this, follow the instructions in "Adding new certificates" on page 54.
5. In Express1, configure the outbound destination address, using the domain and port number that were used to enable HTTPS in Express2. The following steps describe how to do this.
   a. Click the **Configuration** menu, then click **AS2**. The Manage AS2 page appears.
   b. In the Selected Participant field, select Express2, then click **Edit**.
   c. In the Outbound Destination field, enter ″https://Express2:5443/input/AS2.″
6. Refresh the views for both Express1 and Express2.

Sending documents over SSL from Express2 to Express1

The following steps describe how to prepare documents to be sent over SSL from Express2 to Express1.

1. In Express1, enable HTTPS. To do this, follow the instructions in "Enabling HTTPS" on page 53. When filling out the Domain and Port fields, use ″Express1″ as the domain and ″6443″ as the port number.
2. In Express1, generate a self-signed SSL client certificate keypair. To do this, follow the instructions in "Generating a self-signed SSL client certificate keypair" on page 52.
3. In Express1, download the newly created client certificate, and rename it to ″Express1PublicSSL.der.″ To do this, follow the instructions in "Downloading the client certificate for client authentication" on page 53.
4. In Express2, upload the public certificate named ″Express1PublicSSL.der.″ To do this, follow the instructions in "Adding new certificates" on page 54.
5. In Express2, configure the outbound destination address, using the domain and port number that were used to enable HTTPS in Express1. The following steps describe how to do this.

a. Click the **Configuration** menu, then click **AS2**. The Manage AS2 page appears.
b. In the Selected Participant field, select Express1, then click **Edit**.
c. In the Outbound Destination field, enter "https://Express1:6443/input/AS2."

6. Refresh the views for both Express2 and Express1.

Preparing documents to use Client Authentication

This section describes how to prepare documents to use Client Authentication when sending them between two instances of WebSphere Partner Gateway - Express. The following topics are included:

"Using Client Authentication when sending documents from Express1 to Express2"

"Using Client Authentication when sending documents from Express2 to Express1"

Using Client Authentication when sending documents from Express1 to Express2

The following steps describe how to prepare documents to use Client Authentication when sending them from Express1 to Express2.

1. In Express1, generate a self-signed SSL client certificate keypair. To do this, follow the instructions in "Generating a self-signed SSL client certificate keypair" on page 52.
2. In Express1, download the newly created client certificate, and rename it to "Express1PublicClientAuth.der." To do this, follow the instructions in "Downloading the client certificate for client authentication" on page 53.
3. In Express2, create a truststore by importing the client certificate named "Express1PublicClientAuth.der." The following steps describe how to do this:
   a. Copy the client certificate named "Express1PublicClientAuth.der" to the following directory on Express2: `<Express_Home>/was/java/bin`

      Important: Keytool fails if you copy the client certificate to any other directory.
   b. Use keytool to add the client certificate into a truststore. To do this, follow the instructions in "Adding a certificate to a truststore" on page 51, using "Express1PublicClientAuth.der" as the certification filename. This will create the truststore file in the `<Express_Home>/was/java/bin` directory.
4. In Express2, upload the newly created truststore file. To do this, follow the instructions in "Uploading a truststore for client authentication" on page 51.

Using Client Authentication when sending documents from Express2 to Express1

The following steps describe how to prepare documents to use Client Authentication when sending them from Express2 to Express1.

1. In Express2, generate a self-signed SSL client certificate keypair. To do this, follow the instructions in "Generating a self-signed SSL client certificate keypair" on page 52.

2. In Express2, download the newly created client certificate, and rename it to ″Express2PublicClientAuth.der.″ To do this, follow the instructions in “Downloading the client certificate for client authentication” on page 53.
3. In Express1, create a truststore by importing the client certificate named ″Express2PublicClientAuth.der.″ The following steps describe how to do this:
   a. Copy the client certificate named ″Express2PublicClientAuth.der″ to the following directory on Express1: `<Express_Home>/was/java/bin`

      Important: Keytool fails if you copy the client certificate to any other directory.
   b. Use keytool to add the client certificate into a truststore. To do this, follow the instructions in “Adding a certificate to a truststore” on page 51, using ″Express1PublicClientAuth.der″ as the certification filename. This will create the truststore file in the `<Express_Home/was/java/bin` directory.
4. In Express1, upload the newly created truststore file. To do this, follow the instructions in “Uploading a truststore for client authentication” on page 51.

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

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

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

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

Programming interface information

Programming interface information, if provided, is intended to help you create application software using this program. General-use programming interfaces allow you to write application software that obtain the services of this program's tools. However, this information may also contain diagnosis, modification, and tuning information. Diagnosis, modification and tuning information is provided to help you debug your application software.

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

Trademarks and service marks

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

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

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

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

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

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

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

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

WebSphere Partner Gateway - Express includes software developed by the Eclipse Project (http://www.eclipse.org/).

WebSphere Partner Gateway - Express, Version 6.0.

Printed in USA