IBM WebSphere Business Integration Connect - Express

IBM

User Guide

Version 4.2.1

IBM WebSphere Business Integration Connect - Express

IBM

User Guide

Version 4.2.1

> **Note:**
> Before using this information and the product it supports, read the information in "Notices" on page 91.

Contents

Preface

About this book

This document describes how to install, configure, and use IBM(R) WebSphere(R)Business Integration Connect - Express.

WebSphere Business Integration Connect - 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 Business Integration Connect, without the extensive scalability and features required by community managers.

WebSphere Business Integration Connect - 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 Business Integration Connect - 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 Business Integration Connect - Express offers unparalleled flexibility in deployment and implementation.

Audience

This document is intended for organizations that use7y WebSphere Business Integration Connect - Express to conduct B2B activities with their trading partners.

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.
italic, `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.

Related documents

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

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

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

Getting help

Software support

www.ibm.com/software/integration/wbiconnect/support/

Passport Advantage

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

Product documentation

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

New in this release

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 45
- Added Appendix E, "Examples of preparing documents to be sent securely between two instances of Business Integration Connect - Express," on page 85
- 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, "Business Integration Connect - Express Messaging Integration," on page 83
- 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 Business Integration Connect - Express is that solution.

Business Integration Connect - Express is a Web-based trading partner management that accelerates the creation and maintenance of business-partner relationships through extensive B2B protocol support and secure data transport. As an AS2-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 24/7 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 Business Integration Connect - Express.

Console-based trading partner management

Creating and managing relationships with hundreds to thousands of trading partners is complex and error prone. Business Integration Connect - 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 Business Integration Connect. 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, Business Integration Connect - Express supports HTTP- and Applicability Statement 2 (AS2)-based

documents. Moreover, Business Integration Connect - Express is certified by the Drummond Group for AS2 interoperability. AS2 is the latest Internet Engineering Task Force (IETF) standard for transmitting 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.

Using HTTP, AS2 essentially creates an ″envelope″ that allows transactions to traverse the Internet securely. With an encryption base, AS2 underscores the essential factors of data privacy, data authentication, and non-repudiation of original and receipt that is required to ensure the integrity of data transactions over the Internet.

Secure message routing

Business Integration Connect - 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

Business Integration Connect - Express incorporates the following 4-level authentication process for documents received from trading partners.

- Secure Sockets Layer (SSL) protocol — Enables Business Integration Connect - Express to authenticate a partner's identity.
- Client authentication — Allows clients to authenticate themselves to Business Integration Connect - Express by providing their own digital certificates.
- Decryption — Transforms encrypted text into a plain-text format that can be understood.
- Digital signature — Applied to electronic documents to validate that the document contents have not been tampered with.

Outbound documents

Business Integration Connect - Express incorporates the following 3-level authentication process for documents to be transmitted.

- Client authentication — Allows Business Integration Connect - Express to authenticate clients.
- Encryption — Transforms plain text into an unintelligible form (ciphertext) so that the original data cannot be recovered without using decryption.
- 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 Business Integration Connect - 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.

Checklist

The following checklist describes the steps you perform to get Business Integration Connect - 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 Business Integration Connect - Express. SeeChapter 2, "Installing WebSphere Business Integration Connect - Express," on page 5.

2. Start Business Integration Connect - Express. See "Starting WebSphere Business Integration Connect - Express server" on page 25.

3. Use your Web browser to access the Business Integration Connect - Express Console. See "Accessing the Console" on page 26.

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 27.

   Thereafter, you can log in using the procedure described under "Subsequent login procedures" on page 31.

5. Configure and test Business Integration Connect - Express. If necessary, fine-tune your Business Integration Connect - Express configuration to suit your requirements. See Chapter 4, "Configuring and Testing," on page 35.

   Note: If you want to test Business Integration Connect - Express with your security configuration in place, skip to the next step, then test Business Integration Connect.

6. Implement security for your inbound and outbound documents. See Chapter 5, "Configuring Security," on page 45.

7. After you have tested Business Integration Connect - 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 61.
   - If you will be exchanging HTTP-based documents with participants, see "Managing HTTP documents" on page 66.

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 71.

Chapter 2. Installing WebSphere Business Integration Connect - Express

This chapter describes how to install IBM WebSphere Business Integration Connect - Express. You can install WebSphere Business Integration Connect - Express on a personal computer (PC) running Microsoft Windows 2000 or Linux, or a system running OS/400.

This chapter contains the following sections:
- "Minimum requirements"
- "Installing WebSphere Business Integration Connect - Express on a Windows system" on page 6
- "Installing WebSphere Business Integration Connect - Express on a Linux system" on page 13
- "Installing WebSphere Business Integration Connect - Express on a system running OS/400" on page 19
- "Upgrading WebSphere Business Integration Connect - Express from Version 4.2.0 to 4.2.1" on page 23

Minimum requirements

Windows

To install Business Integration Connect - Express on a PC, the PC must meet the following minimum requirements:
- 1.4 GHz or faster Intel (R) Xeon processor
- At least 512 MB of Random Access Memory (RAM)
- At least 150 MB of available hard disk space
- Microsoft Windows 2000 operating system, with Service Pack 3 installed
- Microsoft Internet Explorer, version 5.5 or higher, or Netscape, version 6.0 or higher, for Console access

   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.
- A Simple Mail Transport Protocol (SMTP)-based e-mail relay server for delivering e-mail alerts and SMTP messages

Linux

To install Business Integration Connect - Express on a Linux environment, the PC must have the following minimum requirements:
- 1.4 GHz or faster Intel Xeon processor
- At least 512 MB of Random Access Memory (RAM)
- At least 150 MB of available hard disk space
- RedHat Advanced Server V2.1or SuSe Linux Enterprise Server V8, SP2 operating system
- Microsoft Internet Explorer, version 5.5 or higher, or Netscape, version 6.0 or higher, for Console access

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.

- A Simple Mail Transport Protocol (SMTP)-based e-mail relay server for delivering e-mail alerts and SMTP messages

System running OS/400

To install Business Integration Connect - Express on a system running 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 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 Business Integration Connect - Express on a system running OS/400 must meet the following minimum requirements:

- Windows 98, Windows Me, Windows NT 4.0 with Service Pack 6 installed, Windows 2000, Windows XP, or Windows Server 2003
- Administrative privileges on the system
- Microsoft Internet Explorer 5.01 (IE 5.5 or higher recommended)

  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.

- 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 XGA with 1024 x 768 resolution or greater

Minimum requirements for the system running OS/400

The system running OS/400 on which the WebSphere Business Integration Connect - Express product is being installed must meet the following minimum requirements:

- A minimum processor Commercial Processing Workload (CPW) rating of 300
- At least 640 of Random Access Memory (RAM)
- At least 150 MB of available hard disk space
- IBM OS/400 V5R2M0 (5722-SS1) with PTF SI11277 installed
- -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)
- IBM Toolbox for Java (5722JC1)
- A Simple Mail Transport Protocol (SMPT)-based e-mail relay server for delivering e-mail alerts and SMTP messages

Installing WebSphere Business Integration Connect - Express on a Windows system

There are two ways to install Business Integration Connect - Express on a Windows system:

- Using an Install Shield graphical user interface (GUI) — see "Using the Business Integration Connect - Express graphical installer" on page 7, below.

- Silently, using a command line interface — see "Performing a silent installation" on page 12.

Using the Business Integration Connect - Express graphical installer

To install Business Integration Connect - Express using the graphical installer:

1. Insert the WebSphere Business Integration Connect - Express 4.2.1 CD-ROM into the CD-ROM drive on your computer.

   The Launchpad window in Figure 1 on page 7 appears.

Figure 1. Launchpad window

> **Note:** If the Launchpad does not start automatically, open Windows Explorer and double-click the CD-ROM icon. Navigate to the folder for the Windows installation and double-click the installation file: `setup.exe`

2. From the Launchpad, click **Install WebSphere Business Integration Connect - Express**.

   The Welcome window in Figure 2 on page 8 appears.

Figure 2. Welcome window

3. Click **Next**. The Software License Agreement in Figure 3 on page 8 appears.

Figure 3. Software License Agreement

4. Click **I accept the terms in the license agreement**, then click **Next**. The window in Figure 4 on page 9 appears.

   Note: You must accept the terms of the license agreement to proceed with the installation.
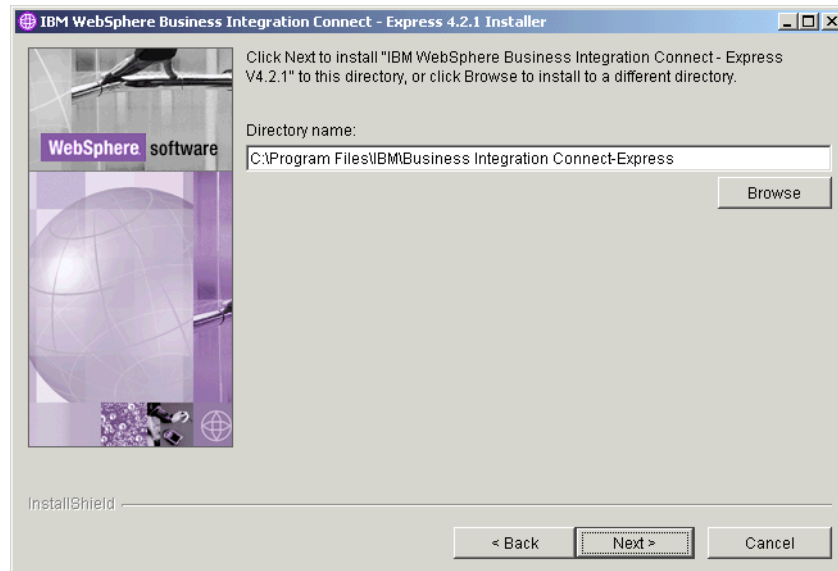
Figure 4. Directory Name

5. The path under **Directory Name** shows where the Business Integration Connect - 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.

6. Click **Next**. The window in **Figure 5 on page 9** appears.

Figure 5. HTTP Port window

7. The HTTP Port window shows the default HTTP port that Business Integration Connect - Express will use to communicate. If the default port will not conflict with another resource on the computer, accept it. Otherwise, change the default HTTP port shown.

> **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 Business Integration Connect - Express and choose a different HTTP port.

8. Click **Next**. The window in Figure 6 on page 10 appears.

Figure 6. Default Folder Name

9. The Default Folder Name window shows the name of the folder that Business Integration Connect - Express will install on your computer. Either accept the default name or change it.

10. Click **Next**. The Service settings window in Figure 7 on page 10 appears.
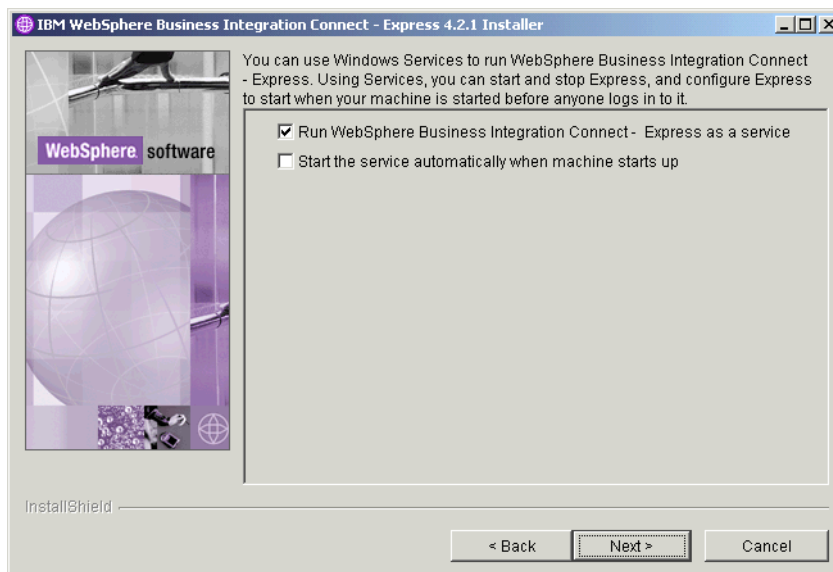
Figure 7. Service Settings

11. The Service settings window by default allows you to run Business Integration Connect - Express as a service in Windows Service Manager. You can also select the option to start the service automatically when you start your machine.

> **Note:** You must have administrator privileges in order to configure Business Integration Connect - 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 **Run WebSphere Business Integration Connect - Express as a service** check box.

12. Click **Next**. The window in Figure 8 on page 11 appears.

Figure 8. Summary window

13. 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.

14. Click **Next**. The Installer installs the Business Integration Connect - Express software, then displays the First Steps application window in Figure 9 on page 12.

Figure 9. First Steps application window

15. To learn how to get started with WebSphere Business Integration Connect - Express, accept the **Yes** selection. Otherwise, click **No**.

16. Click **Next**. The window in Figure 10 on page 12 appears. If **Yes** was selected in the First Steps Application launch window, the First Steps application also opens.

Figure 10. Installation Completed window

17. Click **Finish** to complete the installation process.

Performing a silent installation

Business Integration Connect - 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.

Business Integration Connect - Express includes a sample file called BCGWindowsExpressInstall.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 Business Integration Connect - 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."

To install Business Integration Connect - 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.

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 Business Integration Connect - 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 WebSphere Business Integration Connect - Express on a Linux system

There are three ways to install Business Integration Connect - Express:

- Using an Install Shield graphical user interface (GUI) — see "Using the Business Integration Connect - Express graphical installer" on page 7, below.
- Silently, using a command line interface — see "Performing a silent installation" on page 12.
- Console mode, using a command line interface — see "Installing with console mode" on page 18.

Using the Business Integration Connect - Express graphical installer

To install Business Integration Connect - Express using the graphical installer:

1. Insert the WebSphere Business Integration Connect - Express 4.2.1 CD-ROM into the CD-ROM drive on your computer.
2. Mount the CD.

3. Navigate to the disk1 directory of the product CD and double-click the `setup.bin` file. You can also navigate to the disk1directory of the product CD and execute the `setup.bin` file at the command line.

   The Welcome window in Figure 2 on page 8 appears.
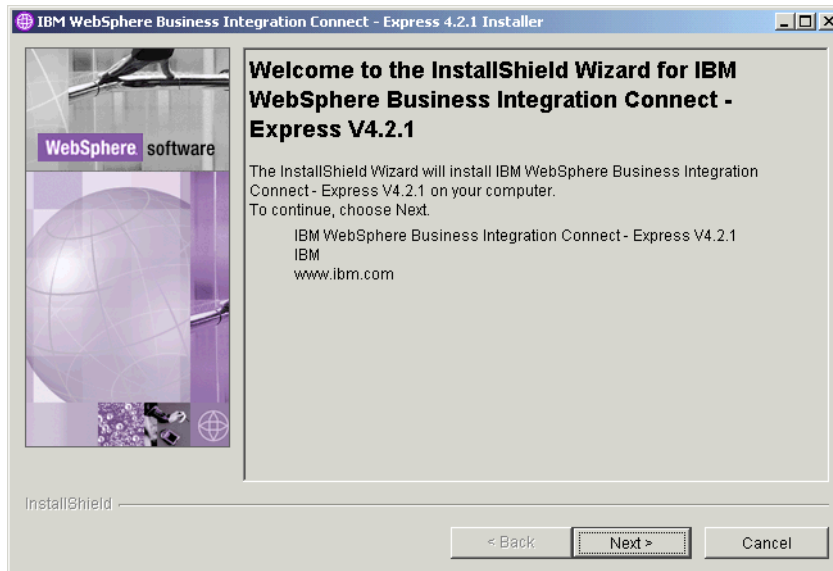

Figure 11. Welcome window

4. Click **Next**. The Software License Agreement in Figure 12 on page 14 appears.
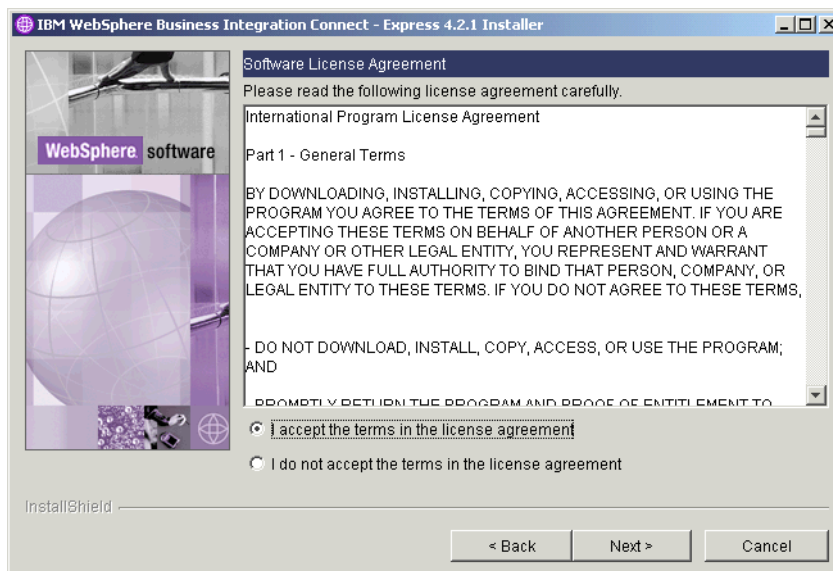

Figure 12. Software License Agreement

5. Click **I accept the terms in the license agreement**, then click **Next**. The window in Figure 13 on page 15 appears.

   **Note:** You must accept the terms of the license agreement to proceed with the installation.
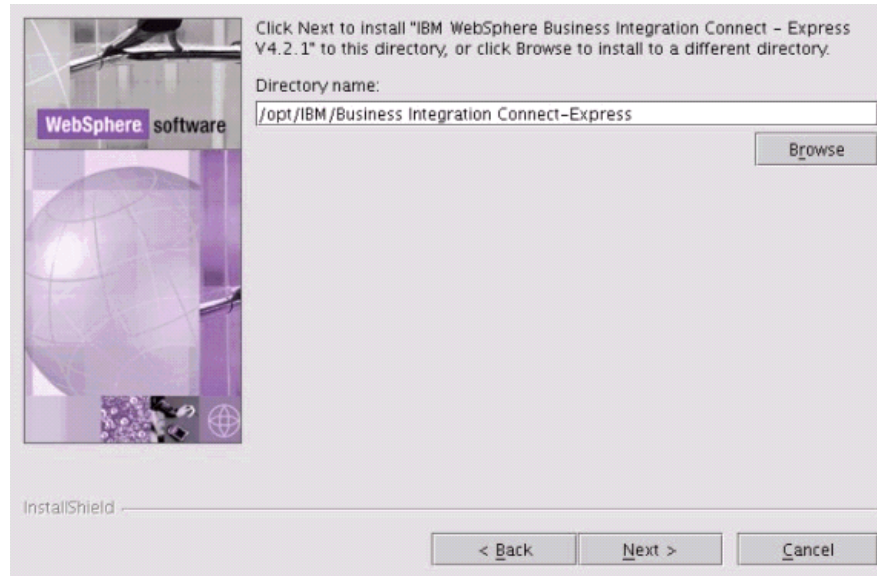
Figure 13. Directory Name

6. The path under **Directory Name** shows where the Business Integration Connect - 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.

7. Click **Next**. The window in **Figure 14 on page 15** appears.
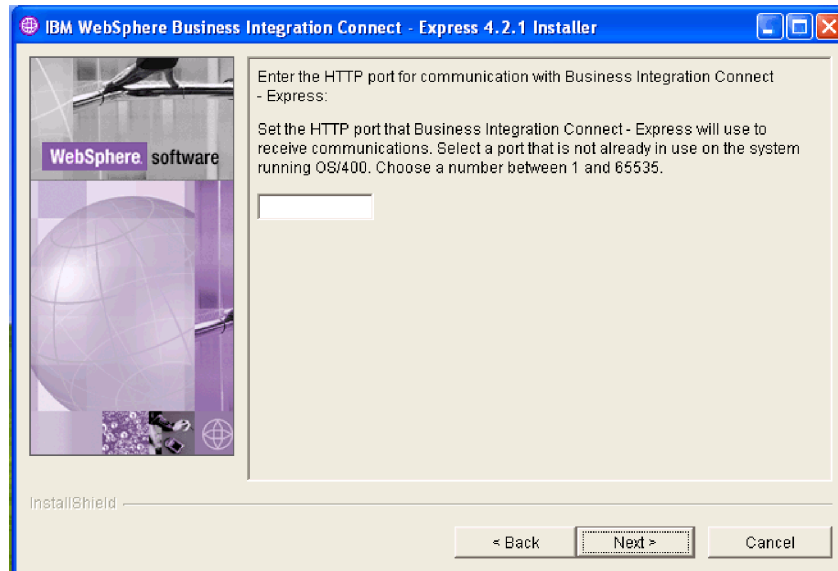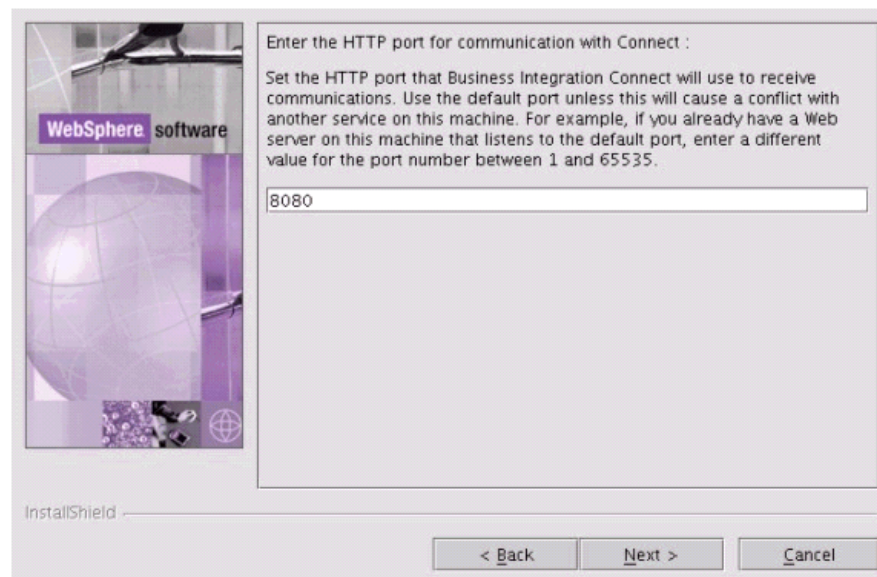

Figure 14. HTTP Port window

8. The HTTP Port window shows the default HTTP port that Business Integration Connect - Express will use to communicate. If the default port will not conflict with another resource on the computer, accept it. Otherwise, change the default HTTP port shown.

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 Business Integration Connect - Express and choose a different HTTP port.

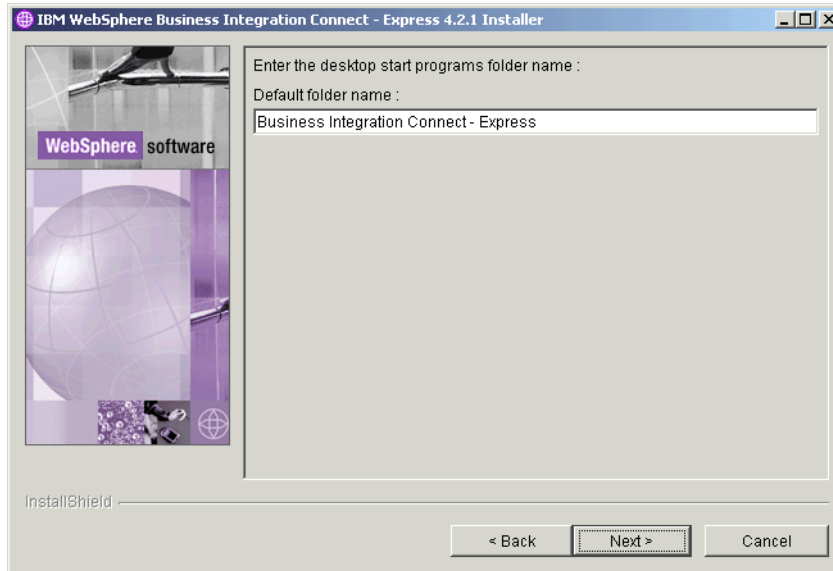9. Click **Next**. The window in Figure 15 on page 16 appears.
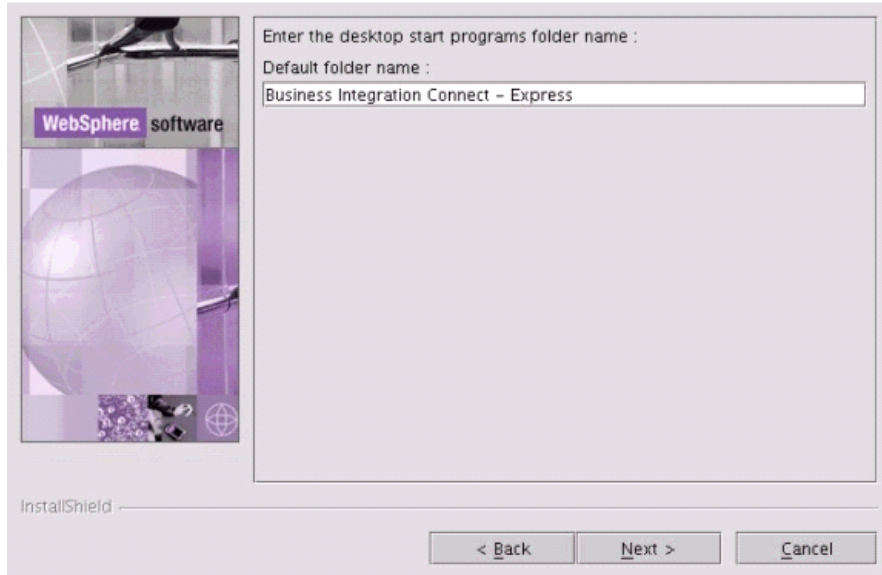
Figure 15. Default Folder Name

10. The Default Folder Name window shows the name of the folder that Business Integration Connect - Express will install on your computer. Either accept the default name or change it.

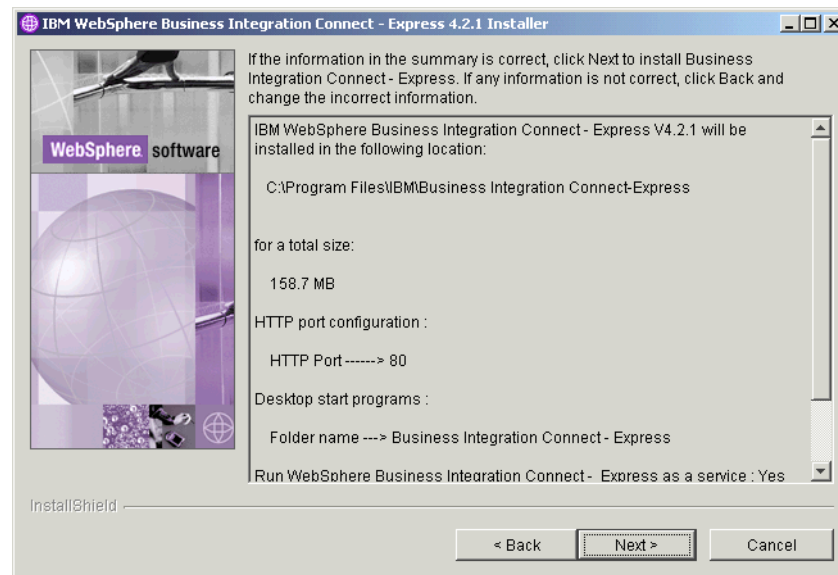11. Click **Next**. The Summary window in Figure 16 on page 16 appears.
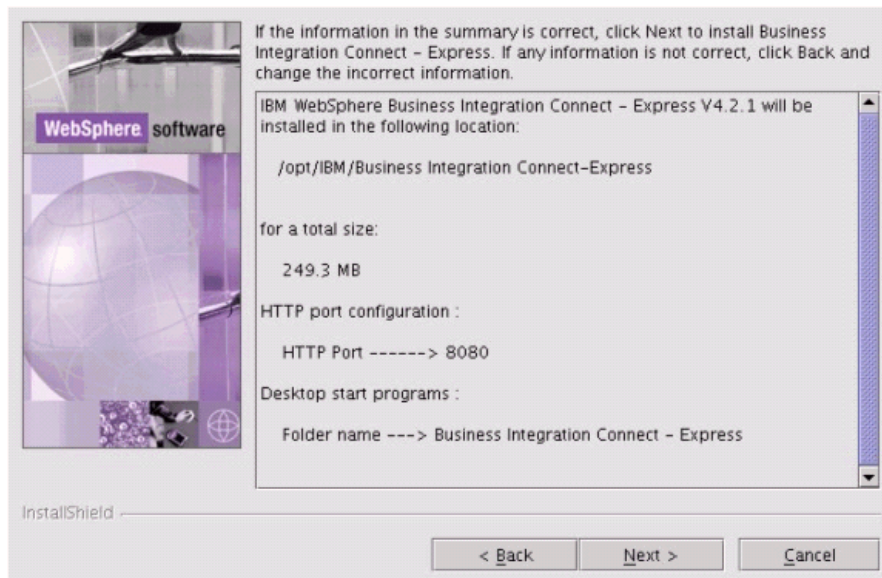
Figure 16. Summary window

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 Business Integration Connect - Express software, then displays the First Steps application launch window in Figure 17 on page 17.
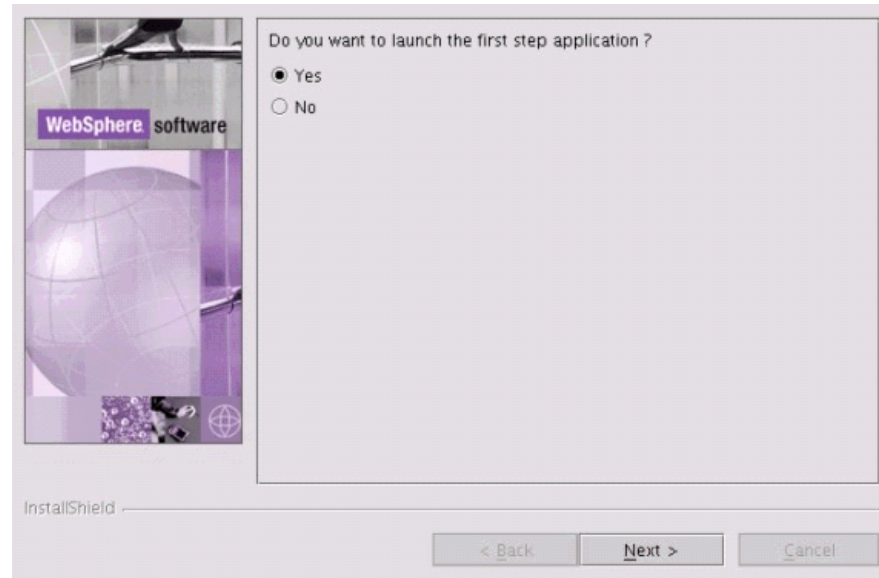
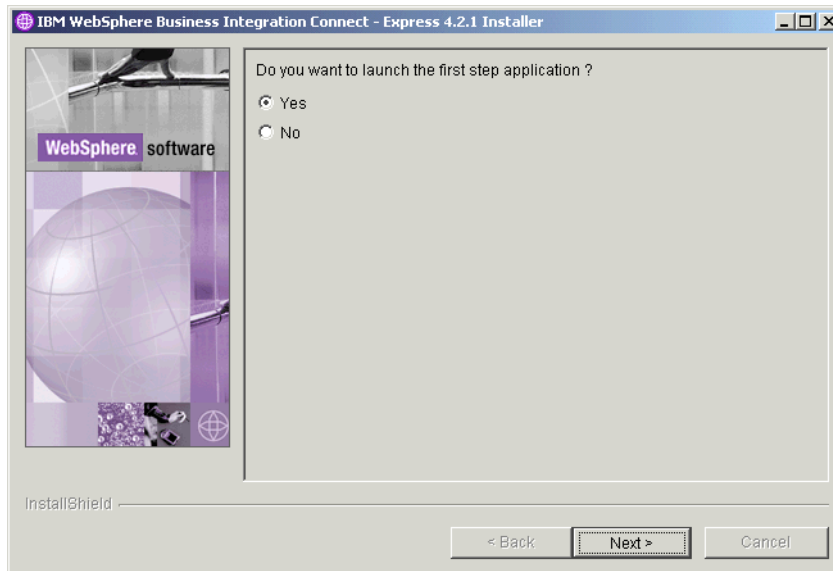*Figure 17. First Steps application launch window*

14. To learn how to get started with Business Integration Connect - Express, accept the **Yes** selection. Otherwise, click **No**.

15. Click **Next**. The window in Figure 18 on page 17 appears. If **Yes** was selected in the First Steps Application launch window, the First Steps application also opens.
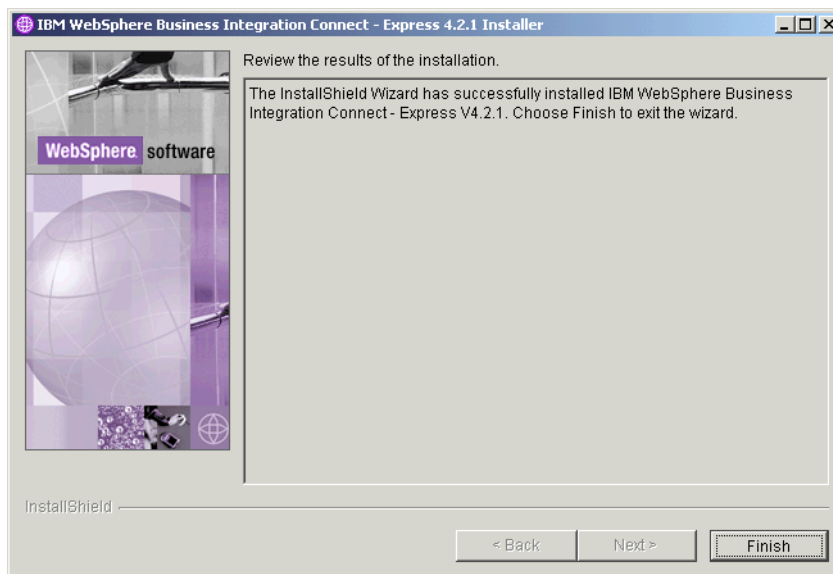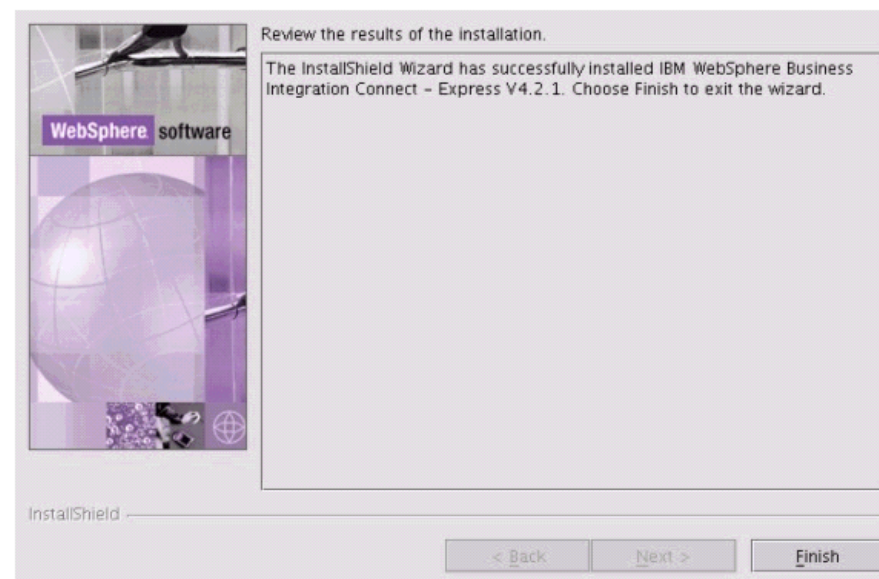

Figure 18. Installation Completed window

16. Click **Finish** to complete the installation process.

Performing a silent installation

Business Integration Connect - 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.

Business Integration Connect - Express includes a sample file called `BCGLinuxEexpressInstall.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 Business Integration Connect - 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 13.

To install Business Integration Connect - 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  "<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 Business Integration Connect - 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 Business Integration Connect - Express on your computer.

To install WebSphere Business Integration Connect - 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 Business Integration Connect - Express on a system running OS/400

There are two ways to install Business Integration Connect - Express on a system running OS/400:

- Remotely from a Windows PC, using an Install Shield graphical user interface (GUI) — see "Using the Business Integration Connect - Express graphical installer," below.
- Silently, using a command line interface — see "Performing a silent installation" on page 22.

Using the Business Integration Connect - Express graphical installer

To install Business Integration Connect - Express using the graphical installer:

1. Insert the WebSphere Business Integration Connect - Express 4.2.1 CD-ROM into the CD-ROM drive on the Windows PC that is connected to the system running OS/400.

   The Launchpad window in Figure 1 on page 7 appears.
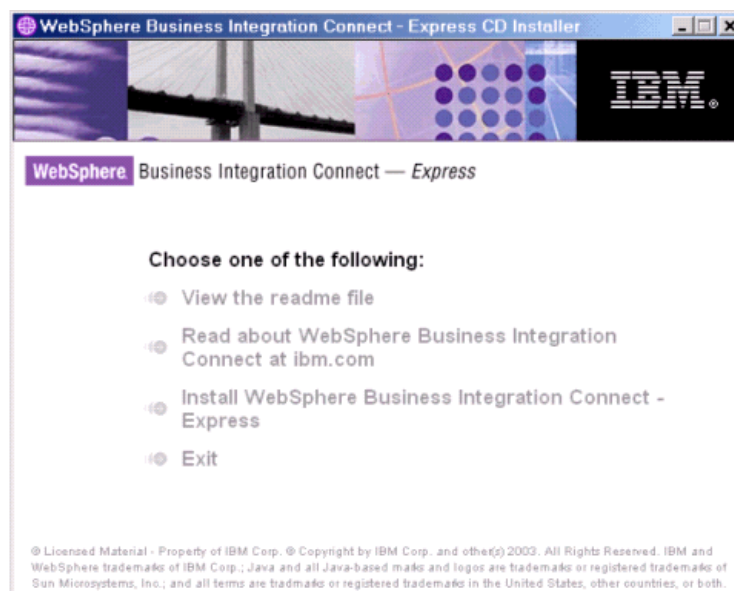
Figure 19. Launchpad window

> **Note:** If the Launchpad does not start automatically, open Windows Explorer and double-click the CD-ROM icon. Navigate to the folder for the Windows installation and double-click the installation file: `setup.exe`

2. From the Launchpad, click **Install WebSphere Business Integration Connect - Express**.

   The Sign on to the Server window in Figure 20 on page 20 appears.
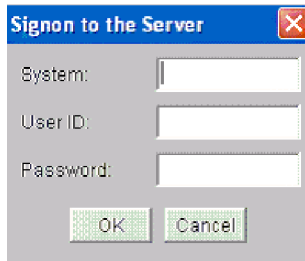
Figure 20. Sign on to the Server

3. In the System field, enter the host name of the system running OS/400 on which you are installing WebSphere Business Integration Connect - Express. In the User ID and Password fields, enter the OS/400 User ID and password that has ALLOBJ (All Object) authority on the system running OS/400, then click OK.

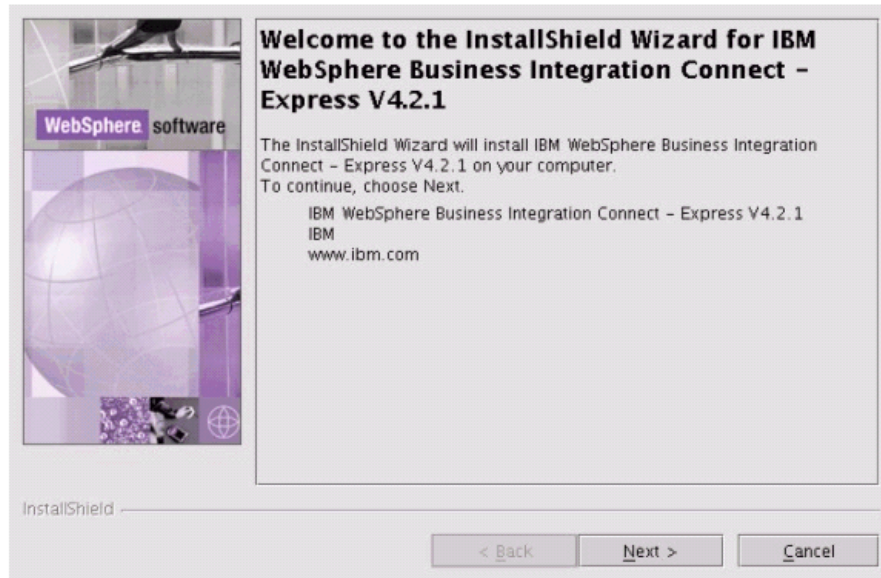   The Welcome window in Figure 21 appears.
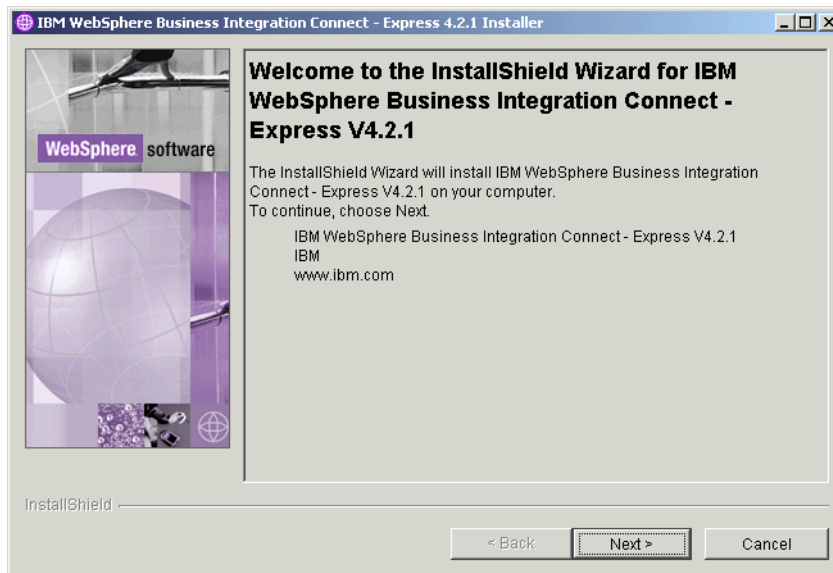
Figure 21. Welcome window

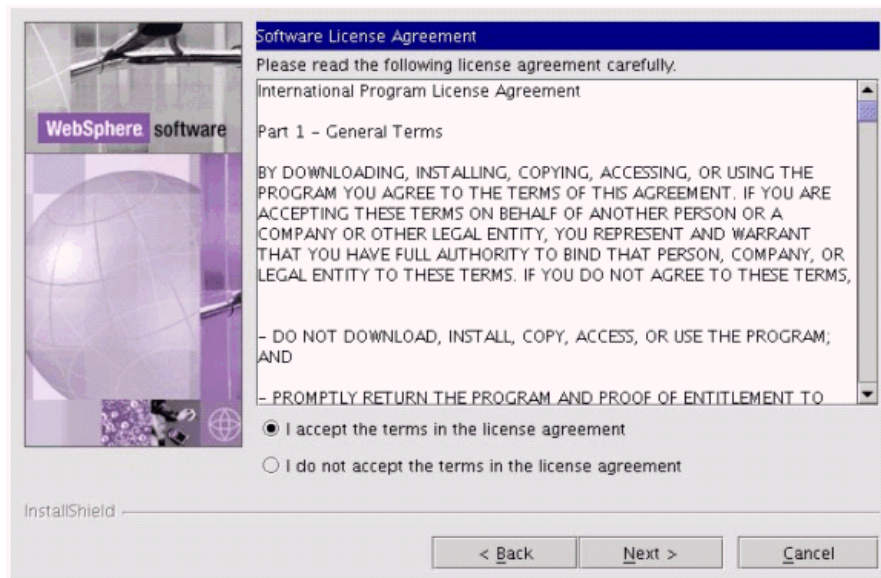4. Click **Next**. The Software License Agreement in Figure 3 on page 8 appears.
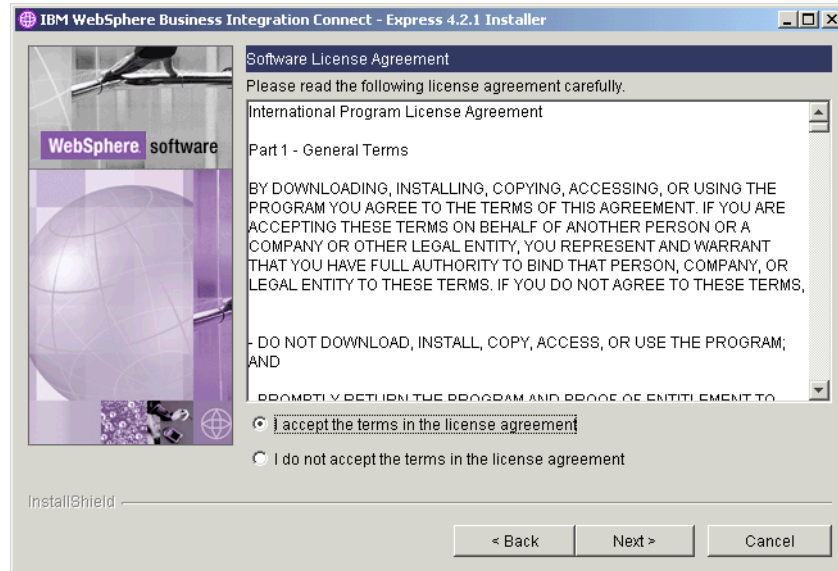
Figure 22. Software License Agreement

5. Select **I accept the terms in the license agreement**, then click **Next**.

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

The HTTP port window in **Figure 5 on page 9** appears, where you specify the port that WebSphere Business Integration Connect - Express will use to communicate.
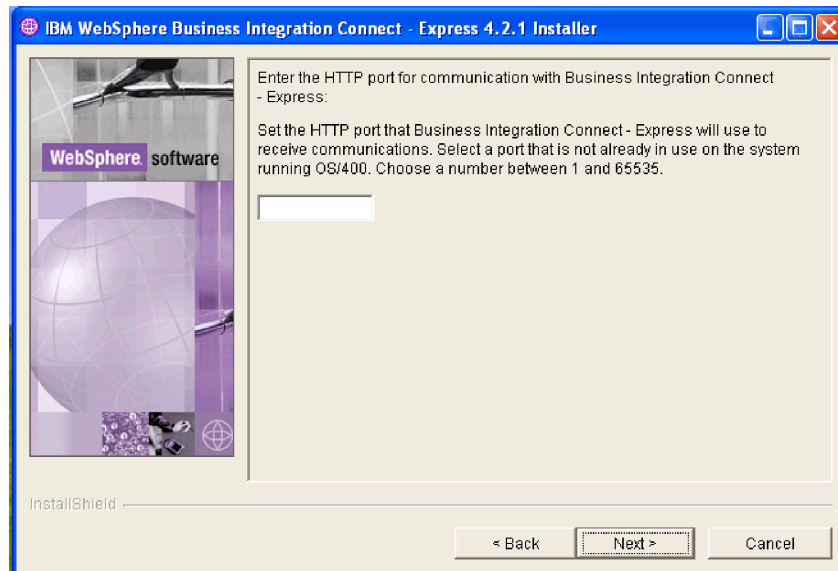
Figure 23. HTTP Port window

6. Enter an HTTP port that will not conflict with another resource on the compute, then click **Next**.

> **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 Business Integration Connect - Express and choose a different HTTP port.

The installer installs the product, then the window in Figure 10 on page 12 appears.
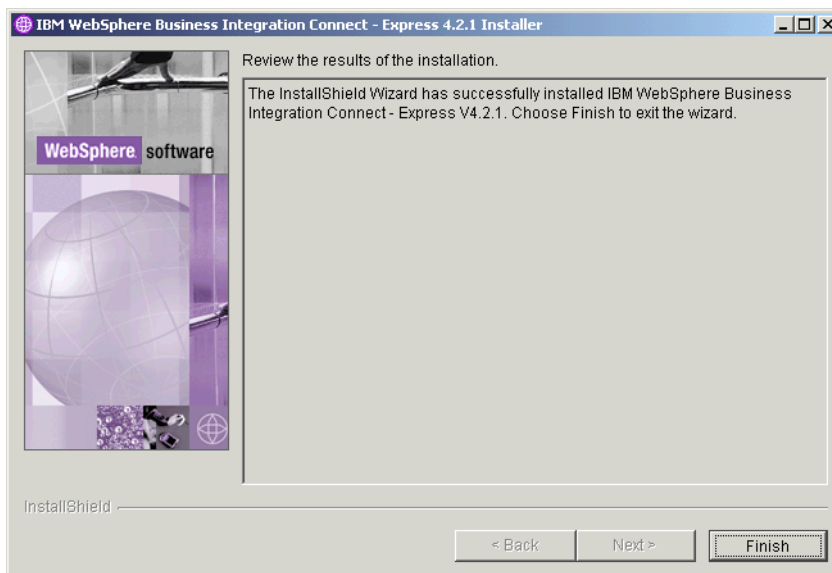
Figure 24. Installation Completed window

7. Click **Finish** to complete the installation process.

Performing a silent installation

Business Integration Connect - 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.

Business Integration Connect - Express includes a sample file called `BCGExpressInstall.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 Business Integration Connect - 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 13.

To install Business Integration Connect - Express silently:
1. Edit the `BCGExpressInstall.iss` options file to specify the HTTP port.
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 -os400 <System> <User_ID> <Password> -options <options file name> -silent`

   where *<System>* is the host name of the system running OS400, *<User_ID>* is an 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 -os400 <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 Business Integration Connect - 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 Business Integration Connect - Express on your computer.

To install WebSphere Business Integration Connect - 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 -os400
   ```

Upgrading WebSphere Business Integration Connect - Express from Version 4.2.0 to 4.2.1

This section describes how to upgrade WebSphere Business Integration Connect - Express from V4.2.0 to V4.2.1

To upgrade Business Integration Connect - Express:

1. Navigate to the directory where WebSphere Business Integration Connect Express V4.2.0 is installed
2. Copy the `config` and the `data` directories to another location outside of the Express 4.2.0 directory tree.
3. Uninstall WebSphere Business Integration Connect - Express V4.2.0.
4. Install WebSphere Business Integration Connect - Express V4.2.1. See "Installing WebSphere Business Integration Connect - Express on a Windows system" on page 6.
5. Copy the `config` and `data` directories saved in Step 2 into the new Express 4.2.1 installation directory and overwrite the existing config and data files.
6. Start Express V4.2.1. See Chapter 3, "Getting Started," on page 25.

Chapter 3. Getting Started

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

- "Starting WebSphere Business Integration Connect - Express server," below
- "Accessing the Console" on page 26, below
- "First-time login procedure - setting the login passwords" on page 27
- "Subsequent login procedures" on page 31
- "Understanding the user interface" on page 32
- "Updating your login passwords" on page 32

Starting WebSphere Business Integration Connect - Express server

The following instructions describe how to start Business Integration Connect - Express, depending on your operating system:

Windows

To start Business Integration Connect - Express server on a Windows system:

1. Click **Start** > **Programs** > **Business Integration Connect - Express** > Start Server.

   A Command Prompt window opens and Business Integration Connect - Express is launched.

2. Confirm that the server has started by verifying that the line SERVER STARTED appears in the Command Prompt window.

Note: If the system generates a warning and an Exception, it means you specified an HTTP port during the installation that is already in use. If this occurs, re-install Business Integration Connect - Express and choose a different HTTP port.

Important: Leave the Command Prompt window open during your Business Integration Connect - Express session. Closing it ends your session.

OS/400

To start Business Integration Connect - Express server on a system running OS/400:

1. Open a command line interface to the system with a user profile that has QBCGX42 as a group profile or has *ALLOBJ (All Object) authority.

2. Start the Business Integration Connect - Express subsystem with the following command: STRSBS QBCGX42/QBCGX42.

3. Confirm that the server has started by using the WRKACTJOB (Work with Active Jobs) command, and verify that the QBCGX42 is started with the following four jobs running in it:
   QBCGX42
   QPOZSPWP
   QPOZSPWP
   QZSHSH

Accessing the Console

Business Integration Connect - Express provides a Web-based Console for managing documents. To access the Console, use one of the following browsers:

- Microsoft Internet Explorer versions 5.5 or higher
- Netscape Navigator versions 6.x or higher

Be sure to install the latest available Service Pack and updates for your browser.

Tip: The Welcome window provides links to download the latest version of these browsers (see Figure 25 on page 26).

For best results, set your window resolution to 1024 x 768 dots per inch or higher.

After you start Business Integration Connect - Express, use one of the following procedures to log into Business Integration Connect - Express, depending on your operating system:

Windows

1. Click **Start** > **Programs** > **Business Integration Connect - Express** > Console.

   Business Integration Connect - Express displays the Welcome window in your Web browser, with a blinking cursor in the **User Name** text box (see Figure 25).
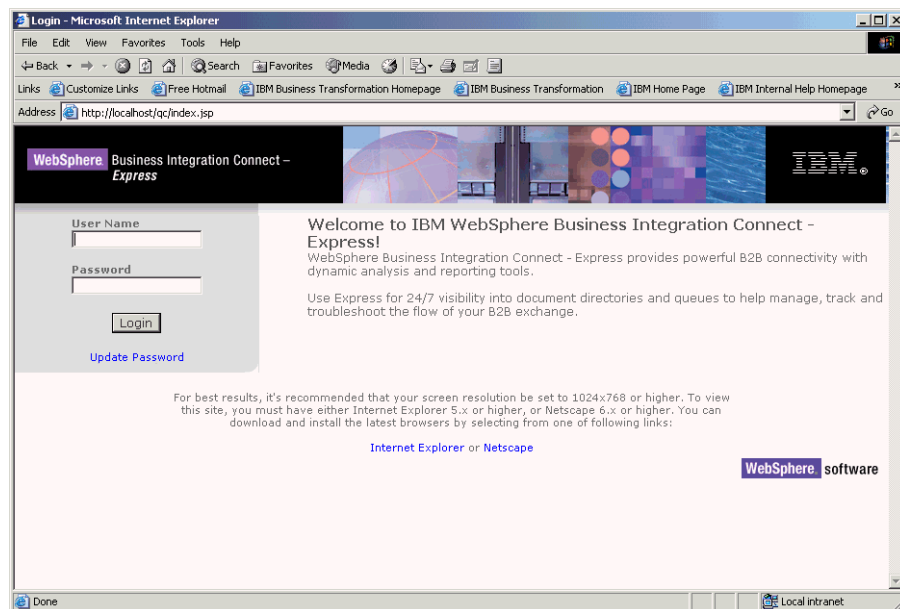
Figure 25. Welcome window

Note: If you used the My Profile window to change the default HTTP port, use the HTTP port value you specified instead of value of **80** shown above (see "Configuring your profile" on page 38).

2. If this is the first time you are logging in, proceed to "First-time login procedure - setting the login passwords" on page 27. Otherwise, proceed to "Subsequent login procedures" on page 31.

OS/400

1. Open a Web browser window.

2. Direct the browser to the following URL:
   `http://<Systemname:port>/qc/index.jsp`, where *Systemname* is the host name of the system running OS/400, and *port* is the HTTP port you specified when you installed Business Integration Connect - Express.

First-time login procedure - setting the login passwords

When you log into Business Integration Connect - 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 window in Figure 25 on page 26 displayed, use the following procedure to log into Business Integration Connect - Express.

1. Next to **User Name**, enter the default user name: **admin**.
2. Next to **Password**, enter the default login password: **admin**.
3. Click the **Login** button. The Initialize Passwords window appears (see Figure 26 on page 28). This window lets you 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 Business Integration Connect - Express features. Users with Guest access have the following limitations:

- Read-only permission to Configuration and Certificates modules.

  Pause and stop functionality will be disabled.
- Pause and stop functionality will be disabled.
- Document send and resend functionality will be 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 are requested. This task is performed from the Initialize Passwords window (see Figure 26 on page 28). Should valid admin and guest passwords be supplied, they will be encrypted and stored to be used to validate all future logins for both admin and guest users. No system functionality can be accessed until valid encrypted passwords exist.
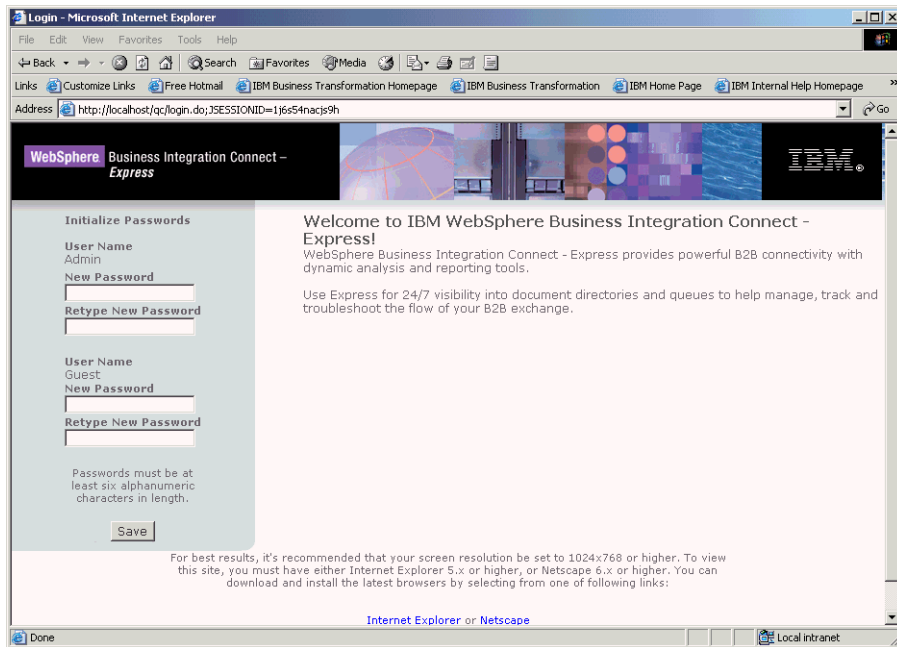
Figure 26. Initialize Passwords window

1. Click in the **New Password** text box under **Admin** and enter a new admin login password in the top text box. Then retype the same password in the **Retype New Password** text box.

   Note: Login passwords must be at least six characters long. They can consist of alphanumeric values and are case sensitive.

2. Click in the **New Password** text box under **Guest** and enter a new guest login password in the top text box. Then retype the same password in the **Retype New Password** text box.

3. Click the **Save** button. The Login Welcome window in Figure 27 on page 29 appears.
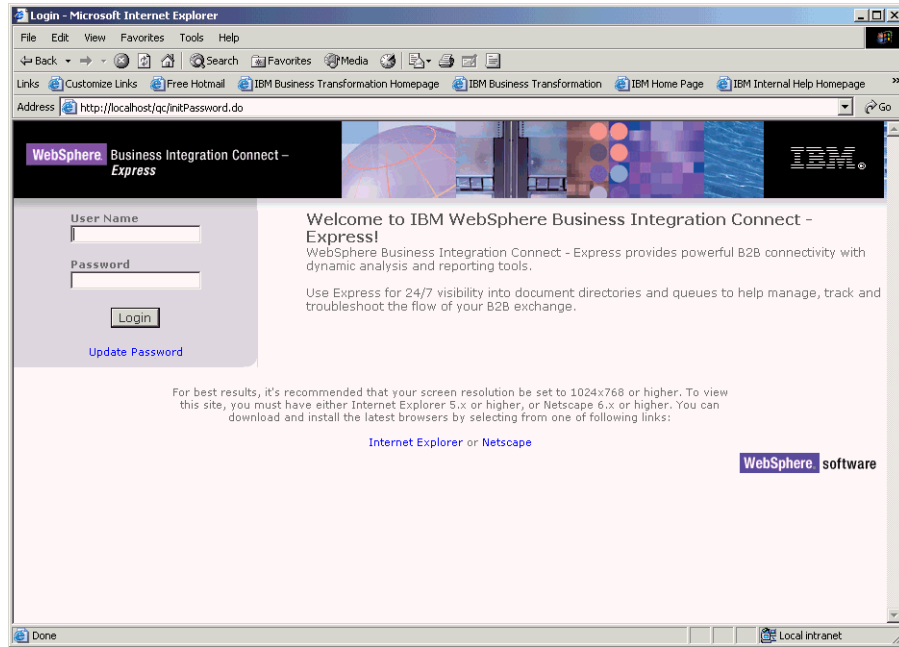
Figure 27. Login Welcome window

4. In the appropriate text boxes, enter admin as the user name and the new admin login password you typed 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 window appears (see Figure 28 on page 30). This window lets you create and edit Business Integration Connect - Express participants.

5. Proceed to "Creating a participant" on page 29.

   Note: After you change the default login password, you can update it if necessary (see "Updating your login passwords" on page 32).

Creating a participant

When you log into Business Integration Connect - Express for the first time, the program allows you to use the Create Participant window (shown in Figure 28) to create a participant with whom Business Integration Connect - Express will communicate.
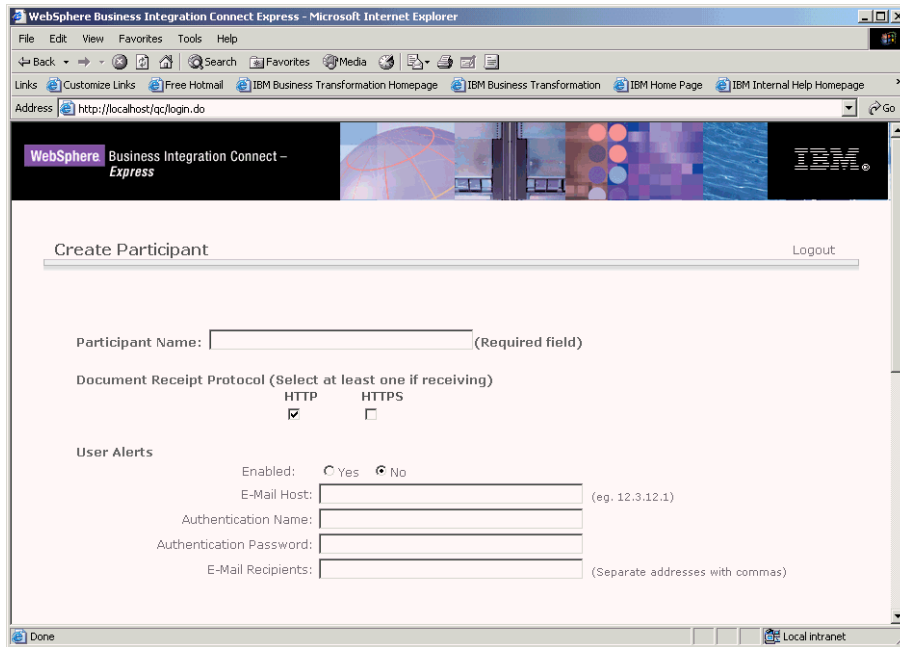
Figure 28. Create Participant window

To create a participant, use the following procedure.

1. Complete the entries in the Create Participant window (see Table 1 on page 30).
2. Click the **Save** button. The Manage Participants window appears. This window lets you 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 35.

Table 1. Create Participant window

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.
HTTPS	Check if you will be using the HTTPS protocol.
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 Business Integration Connect – Express. Separate each e-mail address with a comma. Example: johndoe@mycompany.com,maryf@mycompany.com
Capabilities	

Table 1. Create Participant window (continued)

Parameter	Description
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 with transmitting the document. If **Can Receive** is selected, documents which 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 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.
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. For example, binary-octet.

Where to go from here

After you create your first participant, you can perform Business Integration Connect - 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 32).

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

Subsequent login procedures

After you log in to Business Integration Connect - Express for the first time, subsequent logins are performed using the following procedure.

1. With the Welcome window in Figure 25 on page 26 displayed, enter your user name in the **User Name** text box and your login password in the **Password** text box.

2. Click the **Login** button. The Document Summary window appears (see "Viewing the Document Summary report" on page 71).

3. Perform the desired Business Integration Connect - 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 will be disabled.

4. When you finish your session, click the **Logout** link at the top-right area of the current window (see "Understanding the user interface" on page 32).

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

Understanding the user interface

The Business Integration Connect - Express user interface consists of a main menu and a horizontal navigation bar. The main menu contains menus you can click. The horizontal navigation bar contains windows associated with the selected menu.

When you click a menu in the main menu:
- The horizontal navigation bar shows the windows associated with the menu you selected.
- In the horizontal navigation bar, the first window associated with the current menu appears in the main area.

If you click the **AS2** menu, for example, **Pending Transmission**, **Pending MDN**, **Sent**, **Received**, **Send**, and **Resend** appear in the horizontal navigation bar and the main area shows the **Pending Transmission** window. To display a different window in the menu, click the window name in the horizontal navigation bar. Similarly, to navigate to a different menu, click the name of the menu in the main menu.

The following link appear at the top-right corner of each window:
- **Logout** lets you log out from the current Business Integration Connect - Express session. The application continues to run in the background. To log in again, use the procedure under "Subsequent login procedures" on page 31.

Below these links are the following buttons:
- A green button that lets you temporarily stop sending documents. Click this button once to pause document transmission and click it again to resume document transmission.
- A red button that shuts down Business Integration Connect - Express. If you click this button, a precautionary message appears before the application shuts down.

Note: You can also use your browser's **Forward** and **Backward** controls to navigate through Business Integration Connect - Express.

Updating your login passwords

There may be times when you want to change your login passwords. Business Integration Connect - Express simplifies this ask by providing an **Update Password** link on the Login Welcome window. To change your login password, use the following procedure.

Note: If you have started a Business Integration Connect - Express session, click **Logout** to end the session.

1. From the Login Welcome window. click **Update Password**. The window in Figure 29 appears.
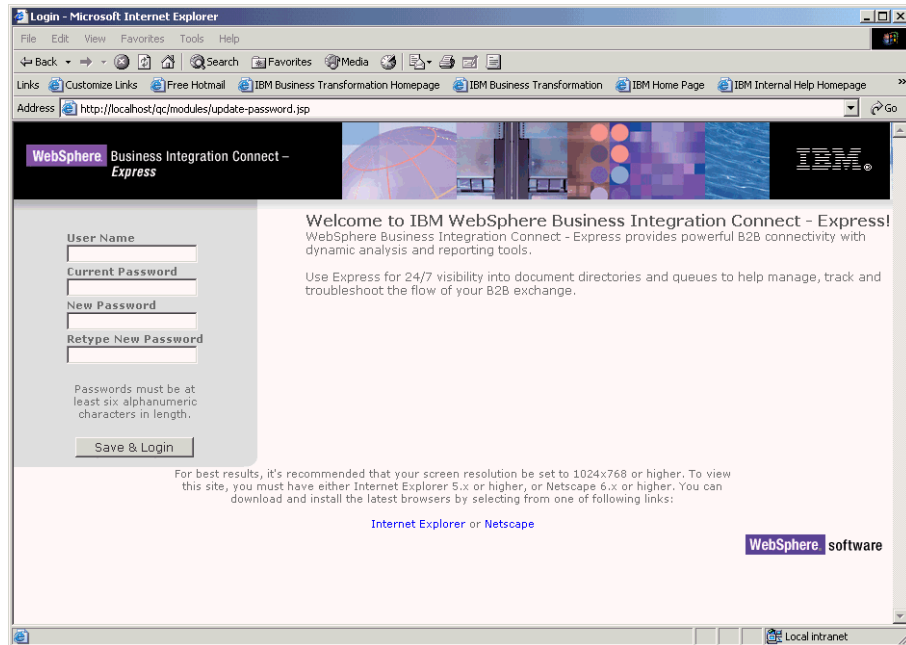
Figure 29. Window for updating the login password

2. Click in the **User Name** text box and enter your user name.
3. Click in the **Current Password** text box and enter the password you use to log into Business Integration Connect - Express.
4. Click in the **New Password** text box and enter the new password you want to use.

   Note: Login passwords must be at least six characters long. They can consist of alphanumeric values and are case sensitive.

5. Click in the **Retype New Password** text box and enter the new password again.
6. Click the **Save & Login** button. You password is changed and the Document Summary window appears.

Chapter 4. Configuring and Testing

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

This chapter describes how to configure and test Business Integration Connect - Express. Topics in this chapter include:

- "Displaying the Configuration menu," below
- "Configuring participants" on page 35
- "Configuring your profile" on page 38
- "Configuring AS2 parameters" on page 39
- "Configuring HTTP parameters" on page 40
- "Manually configuring the properties files" on page 41
- "Testing Business Integration Connect - Express" on page 43

Displaying the Configuration menu

All configuration activities are performed using the Configuration menu. To display the Configuration menu, click **Configuration** in the menu bar. Initially, the Participants window appears. However, you can use the horizontal navigation bar to access other configuration windows.

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

- **Participants** lets you create, edit, and delete participants. See "Configuring participants" on page 35.
- **AS2** lets you select AS2 parameters for your participants. See "Configuring AS2 parameters" on page 39.
- **HTTP** lets you select HTTP parameters for your participants. See "Configuring HTTP parameters" on page 40.
- **My Profile** lets you create a profile for your company. See **"Configuring your profile" on page 38**.

Configuring participants

The Manage Participants window (shown in Figure 30) shows the participants you have created. Initially, this window shows the participant you created when you logged into the system for the first time. However, you can display this window when necessary to add, edit, or delete participants.

Displaying the Manage Participants window

To display the Manage Participants window, click the **Configuration** menu. The Manage Participants window appears (see Figure 30). If it does not appear, click **Participants** in the horizontal navigation bar.
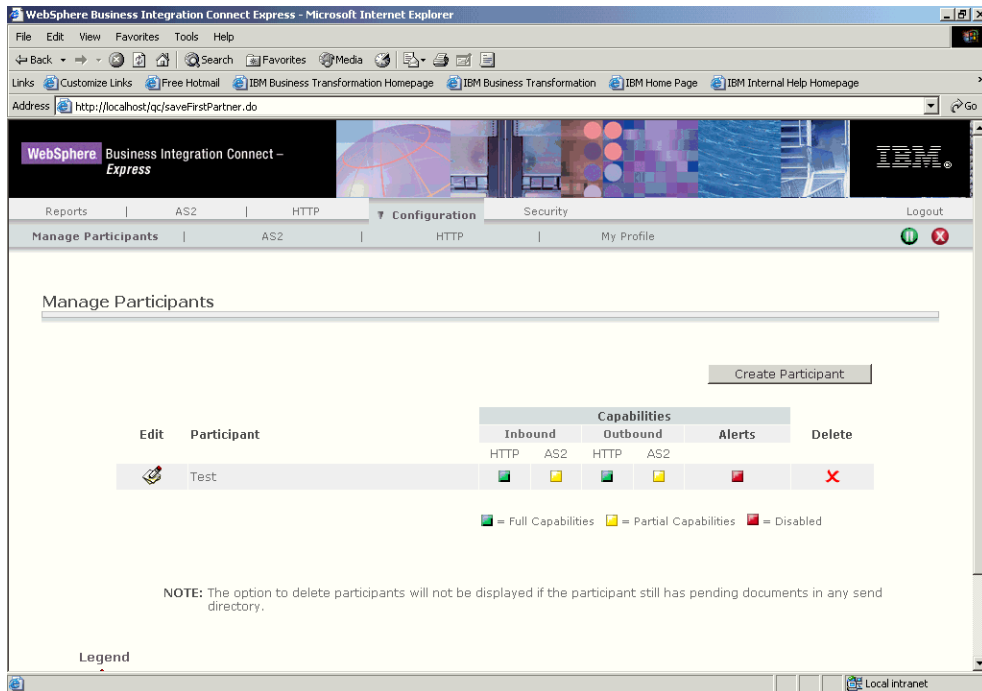
Figure 30. Manage Participants window

Adding participants

To add participants from the Manage Participants window, use the following procedure.

1. Click the **Configuration** menu to display the Manage Participants window in Figure 30 on page 36. If the window does not appear, click **Participants** in the horizontal navigation bar.
2. Click the **Create Participant** button. The Create Participant window appears.
3. Complete the entries in the Create Participant window (see Table 2 on page 36).
4. Click the **Save** button.
5. To add more participants, repeat steps 2 through 4.

Table 2. Create Participant window

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.
HTTPS	Check if you will be using the HTTPS protocol.
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.

Table 2. Create Participant window (continued)

Parameter	Description
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 Business Integration Connect - 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 with transmitting the document. If **Can Receive** is selected, documents which 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 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.
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, use the following information.

1. Click the **Configuration** menu to display the Manage Participants window in Figure 30 on page 36. If the window does not appear, click **Participants** in the horizontal navigation bar.

2. Click the icon next to the participant you want to edit. An Edit Participant window similar to the one in 2 on page 36 appears, with the information you 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.

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** menu to display the Manage Participants window in Figure 30 on page 36. If the window does not appear, click **Participants** in the horizontal navigation bar.

2. In the **Delete** column, click the ✖ icon for the participant you want to delete. The precautionary message in Figure 31 appears.
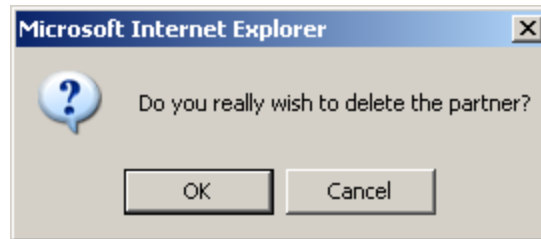
Figure 31. Precautionary Message when Deleting a Participant

3. Click **OK** to delete the participant or **Cancel** to retain the participant.

Configuring your profile

Using the My Profile window in the Configuration menu, 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** menu, then click **My Profile** in the horizontal navigation bar. The Manage My Profile window appears.
2. Click the **Edit** button. The Manage My Profile window appears.
3. Complete the entries in the Manage My Profile window (see Table 5 on page 41).
4. Click the **Save** button.

Table 3. Manage My Profile window parameters

Parameter	Description
Receipt Address	At least one receipt address (either unsecure or secure) is required. The receipt address entered here also appears in the Manage AS2 and Manage HTTP windows (see "Configuring AS2 parameters" on page 39 and "Configuring HTTP parameters" on page 40). 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 26).

Table 3. Manage My Profile window parameters (continued)

Parameter	Description
Unsecure	Enter the domain and port number that will be used to handle unsecure transactions. The receipt address entered here also appears in the Manage AS2 and Manage HTTP windows (see "Configuring AS2 parameters" on page 39 and "Configuring HTTP parameters" on page 40). 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 26).
Secure	Enter the domain and port number that will be used to handle secure transactions.
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 window (see "Configuring AS2 parameters" on page 39).
Company Details	
Company Name	Enter the name of your company.
Address 1 ... Address 3	Enter your company address. For convenience, three text boxes are provided.
City	Enter the city where your company is located.
State	Enter the state where your company is located.
Zip / Postal Code	Enter the zip code or postal code for your company.
Country	Enter the country where your company is located.
Business ID Type	Select a business ID type (**DUNS**, **DUNS+4**, or **Freeform**).
Identifier	Enter the identifier corresponding to the business type you selected.
Vendor Type	Select the vendor type category appropriate for your company.
Web Site	Enter your company's Web site.

Configuring AS2 parameters

Business Integration Connect - Express lets you define AS2 parameters for each participant. You define AS2 configuration parameters using the Manage AS2 window.

To configure AS2 parameters, use the following procedure.

1. Click the **Configuration** menu, then click **AS2** in the horizontal navigation bar. The Manage AS2 window appears.

2. Next to **Selected Participants**, select the participant whose AS2 configuration you want to specify.

3. Click the **Edit** button. The Manage AS2 window in 3 on page 39 appears. This window shows the parameters for inbound AS2 documents coming into the system and outbound AS2 documents leaving the system. The Inbound parameters are read-only and can be changed using **My Profile** in the **Configuration** menu.

4. Complete the entries in the Manage AS2 window.

5. Click the **Save** button.

6. To specify AS2 configuration parameters for other participants, repeat steps 2 through 5.

Table 4. Manage AS2 window parameters

Parameter	Description
Inbound	
Unsecure Receipt Address	Read-only field showing the HTTP document receipt URL. This parameter is set using My Profile (see "Configuring your profile" on page 38).
Participant ID	Read-only field that shows the ID associated with this participant. This parameter is set on the My Participants window (see "Configuring participants" on page 35).
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.
Sender ID	Read-only field that shows your AS2 ID. This parameter is set using My Profile (see "Configuring your profile" on page 38),
Request MDN	Check if a Message Disposition Notification (MDN) is required as proof of receipt for outbound AS2 documents from this participant.
Synchronous or Asynchronous	Select whether outbound AS2 documents from this participant will be sent synchronously or asynchronously.
HTTP or HTTPS	Select whether the HTTPS or HTTP protocol is to be used with outbound AS2 documents from this participant.
Request Signed MDN	Check if a digitally signed MDN is required as proof of receipt for outbound AS2 documents from this participant.
Sign Documents	Check to digitally sign outbound AS2 documents from this participant. 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.
Encrypt Documents	Check to encrypt outbound AS2 documents from this participant. 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 from this participant.

Configuring HTTP parameters

Business Integration Connect - Express lets you define HTTP parameters for each participant. You define HTTP configuration parameters using the Manage HTTP window.

To configure HTTP parameters, use the following procedure.

1. Click the **Configuration** menu, then click **HTTP** in the horizontal navigation bar. The Manage HTTP window appears.
2. Next to **Selected Participants**, select the participant whose HTTP configuration you want to specify.
3. Click the **Edit** button. The Manage HTTP window appears. This window 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** in the **Configuration** menu.

4. Complete the entries in the Manage HTTP window (see Table 5 on page 41).

5. Click the **Save** button.

6. To specify HTTP configuration parameters for other participants, repeat steps 2 through 5.

Table 5. Manage HTTP window 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 as well as AS2 documents. The basic authentication name is used to determine the originating partner rather than the AS2 ID in the case of AS2 documents.
User Name	Enter the user name that the participant will use as part of the basic authentication to authenticate himself to Business Integration Connect - 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 Business Integration Connect - 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 Business Integration Connect - Express GUI, two configuration tasks require that you manually edit the `bcg.properties` or `partner.properties` file:

- All inbound AS2 messages require basic authentication configuration, which is configurable only in the `bcg.properties` file.

- Any timeout problems you experience when sending messages to a trading partner can be fixed by configuring the timeout values in the both the `bcg.properties` and `partner.properties` files.

The following sections describe how to configure both basic authentication and timeout property values by manually editing these properties files.

Configuring basic authentication values

The following steps describe how to configure basic authentication for inbound AS2 messages.

1. Open the `bcg.properties` file. This file is located in the following directory `<ProductDir>/config`

2. Change the following propery values:
   From:
   ```
   bcg.connector.servlet.RequireAS2BasicAuth=false
   bcg.connector.servlet.UseBasicAuthenticationUID=false
   ```

   To either of the following:
   ```
   bcg.connector.servlet.RequireAS2BasicAuth=true
   bcg.connector.servlet.UseBasicAuthenticationUID=true
   ```

   This change means that basic authentication is required for all incoming AS2 messages and that the partner is identified using the basic authentication UserID.
   -or-
   ```
   bcg.connector.servlet.RequireAS2BasicAuth=true
   bcg.connector.servlet.UseBasicAuthenticationUID=false
   ```

   This change means that basic authentication is required for all incoming AS2 messages and that the partner is identified using the attribute AS2-Form.

Configuring timeout values

If a trading partner takes a long time to process a message and send the MDN back, Business Integration Connect - Express may fail with the following 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.

Testing Business Integration Connect - Express

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

1. Install and run two instances of Business Integration Connect - Express. The two can run on the same computer or on different computers. If they run on the same computer, assign each instance a different HTTP port value.

2. Send a document from one instance of Business Integration Connect - Express to the other.
   - If you sent an AS2-based document, see "Sending AS2 documents" on page 61.
   - If you sent an HTTP-based document, see "Sending HTTP documents" on page 66.

3. After you send the document, go to the Sent Documents window 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 63.
   - If you sent an HTTP-based document, see "Viewing sent HTTP documents" on page 67.

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 65.
   - If you received an HTTP-based document, see "Viewing received HTTP documents" on page 69.

   Note: Business Integration Connect - Express does not save the original file name on all received documents. Rather a unique identification number is generated and used as the file name on incoming documents.

5. If the document was received skip to the next step. Otherwise, go to the Pending Transmission window and see whether the document is waiting to be transmitted.
   - For AS2-based documents, see "Viewing pending AS2 documents" on page 64. If you requested a Message Disposition Notification for your document, also see "Viewing AS2 documents pending MDNs" on page 64.
   - If you sent an HTTP-based document, see "Viewing pending HTTP documents" on page 68.

   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 Business Integration Connect - 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 Business Integration Connect - Express. Topics in this chapter include:

- "Displaying the Security menu" on page 45
- "Configuring encryption and decryption"
- "Configuring and verifying digital signatures" on page 48
- "Using the Secure Sockets Layer (SSL) protocol" on page 51
- "Adding certificates from certifying authorities" on page 57
- "Working with certification revocation lists" on page 58

Displaying the Security menu

All security activities are performed using the Security menu. To display the Security menu, click **Security** in the menu bar. Initially, the Inbound window appears. However, you can use the horizontal navigation bar to access other security windows.When you click the Security menu, the horizontal navigation bar contains the following:

- **Inbound** lets you configure security for documents received by Business Integration Connect - Express.
- **Outbound** lets you configure security for documents sent by Business Integration Connect - Express.
- **Certifying Authority** lets you add and delete CA certificates. See "Adding certificates from certifying authorities" on page 57.
- **Certificate Revocation List** lets you add and delete CRLs. See "Working with certification revocation lists" on page 58.

Configuring encryption and decryption

WebSphere Business Integration Connect - 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 Business Integration Connect - 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 Business Integration Connect - Express, and includes the following topics:

- "Configuring encryption for outbound documents" on page 46
- "Configuring decryption for inbound documents" on page 46

Configuring encryption for outbound documents

To configure encryption for outbound documents, you must first upload the trading partner's public certificate, also known as 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, also known as the public key, use the following procedure.

1. Click the **Security** menu, then click **Outbound** in the horizontal navigation bar. The Outbound window appears.
2. Next to **Selected Participant**, select the participant for whom you want to upload the public certificate.
3. Under the **Generate** column, click the **Upload** icon ![icon] in the **Encryption** row. The Upload Encryption Public Certificate window 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**.
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** menu, then click **AS2** in the horizontal navigation bar.
2. In the **Selected Participant** menu, select the participant for whose outbound documents you want to enable encryption.
3. Click the **Edit** button. The Outbound options become editable.
4. 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 47

"Uploading an existing decryption keypair" on page 47

"Downloading a public certificate for decryption" on page 48

Generating a new self-signed document decryption keypair

The following procedure describes how to use WebSphere Business Integration Connect - 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 Business Integration Connect - Express automatically. The generated decryption certificate is also stored in the Express Certifying Authority (CA) directory.

1. Click the **Security** menu to display the Inbound window. If the window does not appear, click **Inbound** in the horizontal navigation bar.

2. Next to **Selected Participant**, select the participant for whom you want to generate the self-signed keypair.

3. Under the **Generate** column, click the **Generate** icon   in the **Decryption** row. The Inbound window appears.

4. Complete the entries in the Inbound window (see Table 6).

5. Click the **Create** button. The self-signed keypair is uploaded and appears in the Inbound window. A new file called decrypt.der is added to the **Decryption** row, and the certificate is automatically added to the **Security/Certifying Authority** tab.

Table 6. Inbound window 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.
Locale / City	Enter the locale or city where the participant works.
State / Province	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** menu to display the Inbound window. If the window does not appear, click **Inbound** in the horizontal navigation bar.

2. Next to **Selected Participant**, select the participant for whom you want to upload the keypair.

3. Under **Upload**, click the   icon in the **Decryption** row. The Inbound window appears.

4. Complete the entries in the Inbound window (see Table 6).

5. Click the **Submit** button. The decryption pair is uploaded and appears in the Inbound window. A copy of the decryption certificate will also be uploaded to the Express Certifying Authority (CA) directory.

Downloading a public certificate for decryption

After you generate or upload a keypair into WebSphere Business Integration Connect - 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** menu to display the Inbound window. If the window does not appear, click **Inbound** in the horizontal navigation bar.
2. Next to **Selected Participant**, select the participant whose certificate you want to download.
3. Click the **Download** icon in the **Decryption** row. A File Download window appears.
4. Click **Save** 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. Business Integration Connect - 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"
- "Configuring digital signature verification on inbound documents" on page 50
- "Enabling digital signature" on page 50

Configuring digital signatures for outbound documents

To configure digital signatures for outbound documents, you must first create 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" on page 49

"Uploading an existing document signing keypair" on page 49

Generating a self-signed document signing keypair

The following procedure describes how to use WebSphere Business Integration Connect - 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."

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

1. Click the **Security** menu, then click **Outbound** in the horizontal navigation bar. The Outbound window appears.

2. Next to **Selected Participant**, select the participant for whom you want to generate the self-signed keypair.

3. Click the **Generate** icon ✦ in the **Verification** row. The Outbound window appears.

4. Complete the entries in the Outbound window (see Table 7).

5. Click the **Create** button. The self-signed keypair is uploaded and appears in the Outbound window.

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

Table 7. Outbound window 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.
Locale / City	Enter the locale or city where the participant works.
State / Province	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."

1. Click the **Security** menu, then click **Outbound** in the horizontal navigation bar. The Outbound window appears.

2. Next to **Selected Participant**, select the participant for whom you want to upload the keypair.

3. Under **Upload**, click the icon in the **Signing** row. The Outbound window appears.

4. Complete the entries in the Outbound window (see Table 8).

5. Click the **Submit** button. The keypair is uploaded and appears in the Outbound window.

Table 8. Outbound window for Document Signing Keypair

Parameter	Description
Private Key File	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	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 Business Integration Connect - Express, you must download the keypair's public certificate before you can send it to the partner. If the partner is using Business Integration Connect - 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 57).

1. Click the **Security** menu, then click **Outbound** in the horizontal navigation bar. The Outbound window appears.
2. Next to **Selected Participant**, select the participant whose document signing public certificate you want to download.
3. Under **Download**, click the icon in the **Signing** row. A File Download window appears.
4. Click **Save** 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 on 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** menu, then click **Certifying Authority** in the horizontal navigation bar. The Certifying Authority window 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.

Enabling digital signature

To enable digital signature, use the following procedure.
1. Click the **Configuration** menu, then click **AS2** in the horizontal navigation bar.
2. In the **Selected Participant** menu, select the participant for whose outbound documents you want to enable encryption.
3. Click the **Edit** button. The Outbound options become editable.
4. Select the **Sign Documents** and **Request MDN** check boxes, then click **Save**.

Using the Secure Sockets Layer (SSL) protocol

Business Integration Connect - Express uses the Secure Sockets Layer (SSL) protocol to secure inbound 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

A keystore for securing inbound documents over an SSL connection can be generated within Business Integration Connect - Express and uploaded automatically 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 window to make the keystore available to the appropriate participants. The following topics describe how to use keystores for inbound server authentication.

Generating a self-signed SSL keystore

The following procedure describes how to use WebSphere Business Integration Connect - Express to generate a self-signed SSL keystore for securing inbound

documents. When you generate a self-signed keystore, it is uploaded into Business Integration Connect - Express automatically.

1. Click the **Security** menu to display the Inbound window. If the window does not appear, click **Inbound** in the horizontal navigation bar.
2. Next to **Selected Participant**, select the participant for whom you want to generate the self-signed keystore.
3. Under **Generate**, click the ![wand icon] icon in the **SSL Connection** row. The Inbound window appears.
4. Complete the entries in the Inbound window (see Table 9).
5. Click the **Create** button. The self-signed keystore is uploaded and appears in the Inbound window.

Table 9. Inbound window 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.
Locale / City	Enter the locale or city where the participant works.
State / Province	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.
Keystore 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 Business Integration Connect - Express, use the following procedure.

1. Click the **Security** menu to display the Inbound window. If the window does not appear, click **Inbound** in the horizontal navigation bar.
2. Next to **Selected Participant**, select the participant for whom you want to upload the keystore.
3. Under **Upload**, click the ![upload icon] icon in the **SSL Connection** row. The Inbound window appears.
4. Complete the entries in the Inbound window (see Table 10).
5. Click the **Submit** button. The keystore is uploaded and appears in the Inbound window.

Table 10. Inbound window 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 Business Integration Connect - Express, you can use the following procedure to download the public certificate encapsulated in the keystore database.

1. Click the **Security** menu to display the Inbound window. If the window does not appear, click **Inbound** in the horizontal navigation bar.

2. Next to **Selected Participant**, select the participant whose keystore you want to download.

3. Under **Download**, click the ![icon] icon in the **SSL Connection** row. The File Download window in Figure 32 appears.
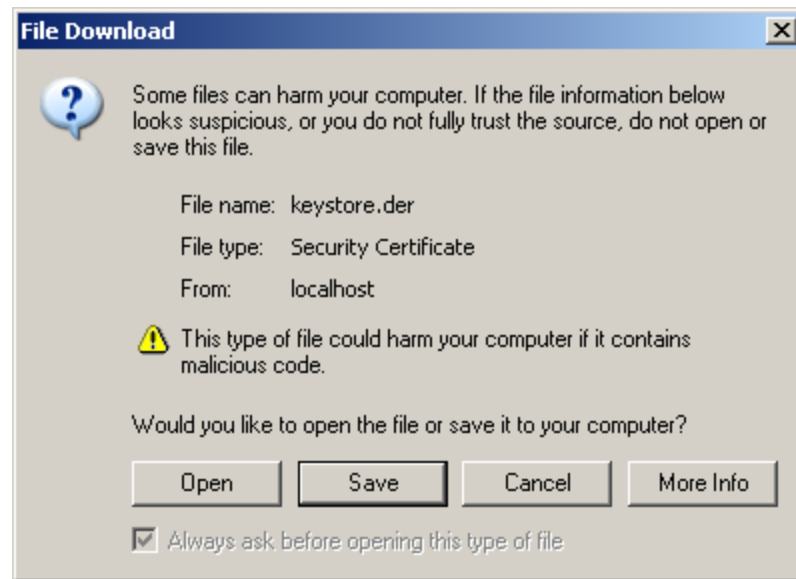
Figure 32. File Download window

4. Click **Save** to display the Save As dialog box, select a location where you want to download the certificate, and click **Save**. (Or click **Open** to open the certificate file, **Cancel** to cancel the operation, or **More Info** to obtain more information.)

Using truststores for inbound client authentication

A truststore is used for client authentication, when Business Integration Connect - 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 window, you can upload a truststore for client authentication. The truststore can then be downloaded or 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.

Using keytool

keytool is a key and certificate management utility. It lets you create keys for use in self-authentication (where Business Integration Connect - 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" to upload the file into Business Integration Connect - Express.

The following procedures describe how to use keytool to 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 jre directory of the Business Integration Connect - Express CD.

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

1. Execute the following command.

   ```
   keytool -list -v -keystore truststore
   ```

2. 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. 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>
```

2. 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. Execute the following command.

   ```
   keytool —delete —alias <cert name> -keystore truststore
   ```

2. 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** menu to display the Inbound window. If the window does not appear, click **Inbound** in the horizontal navigation bar.

2. Next to **Selected Participant**, select the participant for whom you want to upload the truststore.

3. In the Client Auth. row, click the **Upload** icon . The Inbound window appears.

4. Complete the entries in the Inbound window (see Table 11 on page 55).

5. Click the **Submit** button. The truststore is uploaded and appears in the Inbound window.

Table 11. Inbound window 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 Business Integration Connect - 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"

"Uploading a client authentication keypair"

"Downloading the client certificate for client authentication" on page 56

Generating a self-signed SSL client certificate keypair

The following procedure describes how to use WebSphere Business Integration Connect - Express to generate a self-signed SSL client certificate keypair. When you generate a self-signed decryption keypair, it is uploaded into Business Integration Connect - Express automatically.

1. Click the **Security** menu, then click **Outbound** in the horizontal navigation bar. The Outbound window appears.
2. Next to **Selected Participant**, select the participant for whom you want to generate the self-signed keypair.
3. Under **Generate**, click the   icon in the **Client Auth.** row. The Outbound window appears.
4. Complete the entries in the Outbound window (see Table 12).
5. Click the **Create** button. The self-signed keystore is uploaded and appears in the Outbound window.

Table 12. Outbound window 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.
Locale / City	Enter the locale or city where the participant works.
State / Province	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** menu, then click **Outbound** in the horizontal navigation bar. The Outbound window appears.
2. Next to **Selected Participant**, select the participant for whom you want to upload the keypair.
3. Under **Generate**, click the ![icon] icon in the **Client Auth.** row. The Outbound window appears.
4. Complete the entries in the Outbound window (see Table 13).
5. Click the **Submit** button. The keypair is uploaded and appears in the Outbound window.

Table 13. Outbound window 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 Business Integration Connect - 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** menu, then click **Outbound** in the horizontal navigation bar. The Outbound window appears.
2. Next to **Selected Participant**, select the participant whose keypair you want to download.
3. Under **Download**, click the ![icon] icon in the **Client Auth.** row. A File Download window appears.
4. Click **Save** to display the Save As dialog box, select a location where you want to download the keypair, and click **Save**. (Or click **Open** to open the keypair file, **Cancel** to cancel the operation, or **More Info** to obtain more information.)

Enabling HTTPS

The following steps describe how to enable HTTPS.

1. Click the **Configuration** menu, then click **My Profile** in the horizontal navigation bar. The Manage My Profile window appears.
2. Under the Receipt Address section, in the Secure row, enter a domain in the Domain column and a port number in the Port column.
3. If appropriate or necessary, fill in fields under Company AS2 ID and Company Details, then click **Save**.
4. Click the **Configuration** menu, then click **Manage Participants** in the horizontal navigation bar. The Manage Participants window appears.
5. Click **Edit** for the participant whose HTTPS you want to enable. The Edit Participant window appears.
6. Select the HTTPS check box, then click **Save**.

Adding certificates from certifying authorities

Business Integration Connect - 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 window, you can add and delete certificates.

Adding new certificates

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

1. Click the **Security** menu, then click **Certifying Authority** in the horizontal navigation bar. The Certifying Authority window appears.
2. Click the **Add New Certificate** button. The Certifying Authority window appears.
3. Click the **Browse** button. The Choose File 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 window.
5. Click the **Submit** button. The certificate is added to Business Integration Connect - Express and its name appears in the Certifying Authority window.
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 Business Integration Connect - Express.

1. Click the **Security** menu, then click **Certifying Authority** in the horizontal navigation bar. The Certifying Authority window appears.

2. In the **Delete** column, click the ✖ icon for the certificate you want to delete. The precautionary message appears.

Figure 33. Precautionary Message when Deleting a Certificate

3. Click **OK** to delete the certificate or **Cancel** to retain it.

Working with certification revocation lists

Business Integration Connect - 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 Business Integration Connect.

Each revoked certificate is identified in a CRL by its certificate serial number. Business Integration Connect - 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. Business Integration Connect - 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 window, 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** menu, then click **Certificate Revocation List** in the horizontal navigation bar. The Certificate Revocation List window appears.
2. Click the **Add New CRL** button. The Certificate Revocation List window appears.
3. Click the **Browse** button. The Choose File 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 window.
5. Click the **Submit** button. The CRL is added to Business Integration Connect - Express and its name appears in the Certificate Revocation List window.
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 Business Integration Connect - Express.

1. Click the **Security** menu, then click **Certificate Revocation List** in the horizontal navigation bar. A Certificate Revocation List window appears.

2. In the **Delete** column, click the ✖ icon for the CRL you want to delete. The precautionary message in Figure 34 appears.

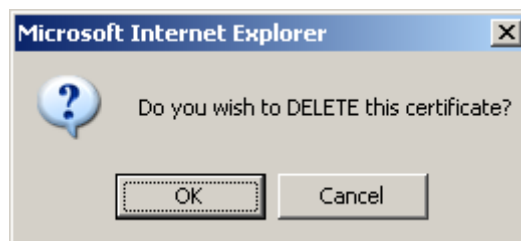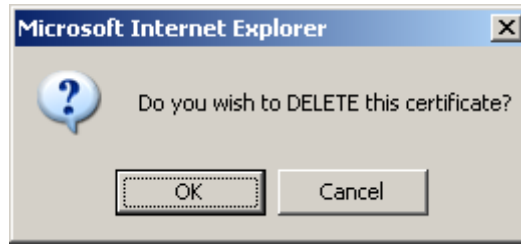*Figure 34. Precautionary Message when Deleting a CRL*

3. Click **OK** to delete the CRL or **Cancel** to retain it.

Chapter 6. Managing Documents

WebSphere Business Integration Connect - 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" on page 61
- "Managing HTTP documents" on page 66

Managing AS2 documents

All AS2 document tasks are performed from the AS2 menu. To display the AS2 menu, click **AS2** in the menu bar. Initially, the Pending Transmission window appears. However, you can use the horizontal navigation bar to access other windows.

When you click the AS2 menu, the horizontal navigation bar contains the following:

- **Send** lets you send AS2 documents. See "Sending AS2 documents" on page 61.
- Resend lets you resend AS2 documents that meet your search criteria. See "Resending AS2 documents" on page 62.
- 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 63.
- **Pending Transmission** lets you see which AS2 documents are waiting to be transmitted. See "Viewing pending AS2 documents" on page 64.
- **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 64.
- **Received** lets you see which received AS2 documents meet your search criteria. See "Viewing received AS2 documents" on page 65.

Sending AS2 documents

To send AS2 documents, use the following procedure.

1. Click the **AS2** menu, then click **Send** in the horizontal navigation bar. The Send Document window appears.
2. Complete the entries in the Send Document window (see Table 14).
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 14. Send Document window

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

Business Integration Connect - 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** menu, then click **Resend** in the horizontal navigation bar. The Resend Documents window appears.
2. Complete the entries in the Resend Document window (see Table 15 on page 62).
3. Click the **Search** button. Business Integration Connect - Express finds the sent documents that meet your search criteria and displays them in the Resend Documents window.

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

Table 15. Resend Document window

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 Business Integration Connect - 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 window, you can have Business Integration Connect - 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** menu, then click **Sent** in the horizontal navigation bar. The Sent Documents window appears.
2. Complete the entries in the Sent Documents window.
3. Click the **Search** button. Business Integration Connect - 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 window. Express will display up to 100 of the most recent intervals depending on the search criteria in the Summary Statistics window.
4. To view detailed information about all documents in an interval represented by a row in the Summary Statistics window, click the ⌕ icon next to the appropriate summary row. This will display the Sent Documents Details window. 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.
   - Display sent document results and search criteria fields in one window by clicking the 🔽 icon next to **Participant** at the top of the window. The window 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 🔽 icon next to **Search Scope**.
5. To view the contents of an individual document, click the (document icon) icon next to the document in the sent Document Detail window. 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 Express cannot find the file in the location computed from the activity logs, the (document icon) icon will not be displayed.
6. To view the contents of an individual document, click the 📄 icon next to the document in the sent Document Detail window. 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 Express cannot find the file in the location computed from the activity logs, the 📄 icon will not be displayed.

Table 16. Sent Documents window

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.

Table 16. Sent Documents window (continued)

Parameter	Description
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 window, you can search for AS2 documents that are waiting to be transmitted. This window 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 window does serve a useful role if troubleshooting is required.

To view pending AS2 transmissions, use the following procedure.

1. Click the **AS2** menu, then click **Pending Transmission** in the horizontal navigation bar. The Pending Transmission window appears.
2. Complete the entries in the Pending Transmission window (see Table 15 on page 62).
3. Click the **Search** button. Business Integration Connect - Express finds the pending documents that meet your search criteria and displays them in the Pending Transmission window.

   This window shows status information about the pending documents,. There is

   also a ▤ icon you can click to view the content of the documents.

Table 17. Pending Transmission window

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 window, 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, Business Integration Connect - Express moves it to the Failed folder.

To view documents pending MDNs, use the following procedure.

1. Click the **AS2** menu, then click **Pending MDN** in the horizontal navigation bar. The Pending MDN window appears.

2. Complete the entries in the Pending MDN window (see Table 18 on page 65).

3. Click the **Search** button. Business Integration Connect - Express finds the documents pending MDNs that meet your search criteria and displays them in the Pending MDN window.

   This window shows status information about documents pending MDNs,.

   There is also a 📄 icon you can click to view the content of the documents.

Table 18. Pending MDN window

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 Documents window, 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** menu, then click **Received Documents** in the horizontal navigation bar. The Received Documents window appears.

2. Complete the entries in the Received Documents window (see Table 19 on page 66).

3. Click the **Search** button. Business Integration Connect - 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 window. Express will display up to 100 of the most recent intervals depending on the search criteria in the Summary Statistics window.

   This window shows status information about the received documents,. There is also a 📄 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 window, click the 🔍 icon next to the appropriate summary row. This will display the Received Documents Details window. 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 document icon next to the document in the Received Document Detail window. 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 Express cannot find the file in the location

computed from the activity logs, the document icon will not be displayed.

Table 19. Received Documents window

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 menu. To display the HTTP menu, click **HTTP** in the menu bar. Initially, the Pending Transmission window appears. However, you can use the horizontal navigation bar to access other windows.

When you click the HTTP menu, the horizontal navigation bar contains the following:

- **Send** lets you send HTTP documents. See "Sending HTTP documents" on page 66.
- Resend lets you resend HTTP documents that meet your search criteria. See "Resending HTTP documents" on page 67.
- **Sent** lets you view sent HTTP documents that meet your search criteria. See "Viewing sent HTTP documents" on page 67.
- **Pending Transmission** lets you see which HTTP documents are waiting to be transmitted. See "Viewing pending HTTP documents" on page 68.
- **Received** shows the HTTP documents that have been received. See "Viewing received HTTP documents" on page 69.

Sending HTTP documents

To send HTTP documents, use the following procedure.

1. Click the **HTTP** menu, then click **Send** in the horizontal navigation bar. The Send Document window appears.
2. Complete the entries in the Send Document window (see Table 20).
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 20. Send Document window

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

Business Integration Connect - 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** menu, then click **Resend** in the horizontal navigation bar. The Resend Documents window appears.
2. Complete the entries in the Resend Document window.
3. Click the **Search** button. Business Integration Connect - Express finds the sent documents that meet your search criteria and displays them in the Resend Documents window.

   This window shows valuable information about the documents, including status information about whether the document was successfully sent

   previously. There is also a 📄 icon you can click to view the content of the documents.
4. To resend one or more documents, select the desired transport, 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 21. Resend Document window

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 Business Integration Connect - 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 window, you can have Business Integration Connect - 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** menu, then click **Sent** in the horizontal navigation bar. The Sent Documents window appears.
2. Complete the entries in the Sent Documents window (see Table 22 on page 68).
3. Click the **Search** button. Business Integration Connect - 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 window. Express will display up to 100 of the most recent intervals depending on the search criteria in the Summary Statistics window.
4. To view detailed information about all documents in an interval represented by a row in the Summary Statistics window, click the ⌕ icon next to the appropriate summary row. This will display the Received Documents Details window.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 window also lets you:

   • Display sent document results and search criteria fields in one window by clicking the 📊 icon next to **Participant** at the top of the window. The window 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 📊 icon next to **Search Scope**.

5. To view the contents of an individual document, click the 📄 next to the document in the Received Document Detail window. 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 Express cannot find the file in the location computed from the activity logs, the 📄 icon will not be displayed.

Table 22. Sent Documents window

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 window, 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** menu, then click **Pending Transmission** in the horizontal navigation bar. The Pending Transmission window appears.
2. Complete the entries in the Pending Transmission window (see Table 23 on page 69).
3. Click the **Search** button. Business Integration Connect - Express finds the pending documents that meet your search criteria and displays them in the Pending Transmission window.

   This window shows status information about the pending documents,. There is also a ![icon] icon you can click to view the content of the documents.

Table 23. Pending Transmission window

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 window, 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** menu, then click **Received Documents** in the horizontal navigation bar. The Received Documents window appears.
2. Complete the entries in the Received Documents window (see Table 23 on page 69).
3. Click the Search button. Business Integration Connect - 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 window (Figure 6-5). Express will display up to 100 of the most recent intervals depending on the search criteria in the Summary Statistics window (see Figure 6-7).

   This window shows status information about the received documents,. There is also a ![icon] 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 window, click the magnifying glass icon next to the appropriate summary row. This will display the Received Documents Details window. 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 document icon next to the document in the Received Document Detail window. 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 Express cannot find the file in the location computed from the activity logs, the document icon will not be displayed.

Table 24. Received Documents window

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 Business Integration Connect - 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 menu," below
- "Viewing the Document Summary report" on page 71
- "Viewing the Participant Summary report" on page 72
- "Viewing the Activity Log" on page 72

Displaying the Reports menu

All report activities are performed using the Reports menu. To display the Reports menu, click **Reports** in the menu bar. Initially, the Document Summary window appears. However, you can use the horizontal navigation bar to access other report windows.

When you click the Reports menu, the horizontal 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 72.
- **Activity Logs** displays activity information that matches your search criteria. See "Viewing the Activity Log" on page 72.

Viewing the Document Summary report

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

Each row in the Document Summary window 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 window 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 move 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 Report displays a summary of participant activity. To display this report, click the **Reports** menu, then click **Participant Summary** on the horizontal 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** list.

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 Log lets you view system activity that meets certain search criteria. To display the window where you enter search criteria, click the **Reports** menu, then click **Activity Logs** on the horizontal navigation bar. This window 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** menu, then click **Activity Logs** in the horizontal 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 🗓 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.) Business Integration Connect - Express finds the activity that matches your criteria and displays it in a new window.

Appendix A. Error Messages

This appendix describes error messages generated by WebSphere Business Integration Connect - Express

Table 25. 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 Business Integration Connect - Express Folders

When you install WebSphere Business Integration Connect - 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 Business Integration Connect - Express from your system.
batch	This directory contains the batch files used during the installation and uninstallation processes. It also contains batch files for registering and unregistering WebSphere Business Integration Connect - Express as a Windows service.
bin	This directory contains batch and shell script files for executing programs associated with WebSphere Business Integration Connect - Express.
config	This directory contains property and system-configuration files, as well as generated and uploaded certificates.
data	This directory contains the participant files.
firstuse	This directory contains the files used for the First Use Application.
jre	This directory contains the Java runtime environment.
lib	This directory contains library files supporting WebSphere Business Integration Connect - Express.
license	This directory contains the license agreement for WebSphere Business Integration Connect - Express.
logs	This directory contains a history file of installation and uninstallation of WebSphere Business Integration Connect - Express.
webapps	This directory contains the WebSphere Business Integration Connect - Express user interface.

Appendix C. Uninstalling WebSphere Business Integration Connect - Express

This appendix describes how to uninstall WebSphere Business Integration Connect - Express from your system. It contains the following sections:

- "Uninstalling WebSphere Business Integration Connect - Express from a Windows system"
- "Uninstalling WebSphere Business Integration Connect - Express from a Linux system" on page 80
- "Uninstalling WebSphere Business Integration Connect - Express from a system running OS/400" on page 81

Uninstalling WebSphere Business Integration Connect - Express from a Windows system

This section describes how to uninstall WebSphere Business Integration Connect - Express from your Windows system. It contains the following:

- "Using the Business Integration Connect - Express graphical uninstaller"
- "Performing a silent uninstallation on a Windows system" on page 80

Using the Business Integration Connect - Express graphical uninstaller

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

To uninstall WebSphere Business Integration Connect - Express:

1. If you are not running WebSphere Business Integration Connect - Express as a service, you should stop the server as you normally would before proceeding.
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 Business Integration Connect - Express.
5. Click **Change/Remove**.
6. If WebSphere Business Integration Connect - 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 Business Integration Connect - 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 Business Integration Connect - Express from your computer.

To unintall WebSphere Business Integration Connect - Express:

1. If you are not running WebSphere Business Integration Connect - Express as a service, you should stop the server as you normally would before proceeding.
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 Business Integration Connect - Express.
3. Enter the following command at the prompt:

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

Uninstalling WebSphere Business Integration Connect - Express from a Linux system

This section describes how to uninstall WebSphere Business Integration Connect - Express from your Linux system. It contains the following:

- "Using the Business Integration Connect - Express graphical uninstaller" on page 79
- "Performing a silent uninstallation"
- "Uninstalling in console mode" on page 81

Using the Business Integration Connect - Express graphical uninstaller

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

To uninstall WebSphere Business Integration Connect - Express:

1. Stop the WebSphere Business Integration Connect - 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 Business Integration Connect - Express from your computer.

To unintall WebSphere Business Integration Connect - Express:

1. Stop the WebSphere Business Integration Connect - 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 Business Integration Connect - Express.

3. Enter the following command at the prompt:

   ```
   ./uninstaller -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 Business Integration Connect - Express from your computer.

To unintall WebSphere Business Integration Connect - Express:

1. Stop the WebSphere Business Integration Connect - 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 Business Integration Connect - Express.

3. Enter the following command at the prompt:

   ```
   ./uninstaller -console
   ```

4. Restart your computer.

Uninstalling WebSphere Business Integration Connect - Express from a system running OS/400

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

The following steps describe how to uninstall WebSphere Business Integration Connect - Express.

1. Open a command line interface to the system running OS/400 with a user profile that has QBCGX42 as a group profile or has *ALLOBJ (All Object) authority.

2. End WebSphere Business Integration Connect - Express subsystem with the following command:
   ```
   ENDSBS QBCGX42
   ```

3. Start the qsh shell interpreter with the following command:
   ```
   STRQSH
   ```

4. In the qsh shell interpreter, enter the following commands:
   ```
   cd /QIBM/ProdData/WBICExpress42
   java -cp _uninst/uninstall.jar run -console
   ```

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

- `/QIBM/UserData/WBICExpress42/config`
- `/QIBM/UserData/WBICExpress42/data`

- /QIBM/UserData/WBICExpress42/logs

Appendix D. Business Integration Connect - Express Messaging Integration

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

Business Integration Connect - Express directory structure

You can use the WebSphere Business Integration Connect - Express file system to transfer messages to and from enterprise applications, including WebSphere Business Integration Connect Enterprise, over an existing network. The messaging directories are located under the *EXPRESS_HOME*/data/FileSystemAdapter2/partners directory. On a system running OS/400, the EXPRESS_HOME directory is /QIBM/UserData/WBICExpress42. 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:

83

```
 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 Business Integration Connect - 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, rather use an atomic move operation. Using copy may cause a partially read file to be sent.

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. Examples of preparing documents to be sent securely between two instances of Business Integration Connect - Express

This appendix describes examples of how to prepare documents to be sent securely between two instances of Business Integration Connect - Express. In these examples, the first instance of Business Integration Connect - Express is referred to as "Express1" while the second instance is referred to as "Express2." The following examples are described.

"Preparing encrypted documents to be sent between two instances of Business Integration Connect - Express"

"Preparing digitally signed documents to be sent between two instances of Business Integration Connect - Express" on page 86

"Preparing documents to be sent over Secure Socket Layer (SSL) between two instances of Business Integration Connect - Express" on page 87

"Preparing documents to use Client Authentication between two instances of Business Integration Connect - Express" on page 88

Preparing encrypted documents to be sent between two instances of Business Integration Connect - Express

This section describes how to prepare encrypted documents to be sent between two instances of Business Integration Connect - Express and includes the following topics:

"Preparing encrypted documents to be sent from Express1 to Express2"

"Preparing encrypted documents to be sent from Express2 to Express1" on page 86

Preparing encrypted documents to be sent 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 47.
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 48.
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 46.
4. In Express1, enable encryption for outbound documents. To do this, follow the instructions in "Enabling encryption for outbound documents" on page 46.

Preparing encrypted documents to be sent 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 47.

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 48.

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 46.

4. In Express2, enable encryption for outbound documents. To do this, follow the instructions in "Enabling encryption for outbound documents" on page 46.

Preparing digitally signed documents to be sent between two instances of Business Integration Connect - Express

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

"Preparing digitally signed documents to be sent from Express1 to Express2"

"Preparing digitally signed documents to be sent from Express2 to Express1"

Preparing digitally signed documents to be sent 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 49.

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 50.

3. In Express2, upload the document signing keypair. To do this, follow the instructions in "Uploading an existing document signing keypair" on page 49.

4. In Express1, enable digital signature. To do this, follow the instructions in "Enabling digital signature" on page 50.

Preparing digitally signed documents to be sent 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 49.

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 50.

3. In Express1, upload the document signing keypair. To do this, follow the instructions in "Uploading an existing document signing keypair" on page 49.

4. In Express2, enable digital signature. To do this, follow the instructions in "Enabling digital signature" on page 50.

Preparing documents to be sent over Secure Socket Layer (SSL) between two instances of Business Integration Connect - Express

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

"Preparing documents to be sent over SSL from Express1 to Express2"

"Preparing documents to be sent over SSL from Express2 to Express1"

Preparing documents to be sent 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 56. 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 55.

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 56.

4. In Express1, upload the public certificate named "Express2PublicSSL.der." To do this, follow the instructions in "Adding new certificates" on page 57.

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 window 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.

Preparing documents to be sent 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 56. 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 55.

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 56.

4. In Express2, upload the public certificate named "Express1PublicSSL.der." To do this, follow the instructions in "Adding new certificates" on page 57.

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 window 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 between two instances of Business Integration Connect - Express

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

"Preparing documents to use Client Authentication when sending them from Express1 to Express2"

"Preparing documents to use Client Authentication when sending them from Express2 to Express1" on page 89

Preparing documents to use Client Authentication when sending them 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 55.

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 56.

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: `Express2/jre/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 54, using "Express1PublicClientAuth.der" as the certification filename. This will create the truststore file in the `jre/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 54.

Preparing documents to use Client Authentication when sending them 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 55.

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 56.

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: `Express1/jre/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 54, using "Express1PublicClientAuth.der" as the certification filename. This will create the truststore file in the `jre/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 54.

Notices

IBM may not offer the products, services, or features discussed in this document in all countries. Consult your local IBM representative for information on the products and services currently available in your area. Any reference to an IBM product, program, or service is not intended to state or imply that only that IBM product, program, or service may be used. Any functionally equivalent product, program, or service that does not infringe any IBM intellectual property right may be used instead. However, it is the user's responsibility to evaluate and verify the operation of any non-IBM product, program, or service.

IBM may have patents or pending patent applications covering subject matter described in this document. The furnishing of this document does not give you any license to these patents. You can send license inquiries, in writing, to:

IBM Director of Licensing
IBM Corporation
North Castle Drive
Armonk, NY 10504-1785
U.S.A.

The following paragraph does not apply to the United Kingdom or any other country where such provisions are inconsistent with local law:

INTERNATIONAL BUSINESS MACHINES CORPORATION PROVIDES THIS PUBLICATION "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF NON-INFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. Some states do not allow disclaimer of express or implied warranties in certain transactions, therefore, this statement may not apply to you.

This information could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein; these changes will be incorporated in new editions of the publication. IBM may make improvements and/or changes in the product(s) and/or program(s) described in this publication at any time without notice.

Any references in this information to non-IBM Web sites are provided for convenience only and do not in any manner serve as an endorsement of those Web sites. The materials at those Web sites are not part of the materials for this IBM product and use of those Web sites is at your own risk.

IBM may use or distribute any of the information you supply in any way it believes appropriate without incurring any obligation to you.

Licensees of this program who wish to have information about it for the purpose of enabling: (i) the exchange of information between independently created programs and other programs (including this one) and (ii) the mutual use of the information which has been exchanged, should contact:

IBM Burlingame Laboratory Director
IBM Burlingame Laboratory
577 Airport Blvd., Suite 800

Burlingame, CA 94010
U.S.A

Such information may be available, subject to appropriate terms and conditions, including in some cases, payment of a fee.

The licensed program described in this document and all licensed material available for it are provided by IBM under terms of the IBM Customer Agreement, IBM International Program License Agreement, or any equivalent agreement between us.

Any performance data contained herein was determined in a controlled environment. Therefore, the results obtained in other operating environments may vary significantly. Some measurements may have been made on development-level systems and there is no guarantee that these measurements will be the same on generally available systems. Furthermore, some measurement may have been estimated through extrapolation. Actual results may vary. Users of this document should verify the applicable data for their specific environment.

Information concerning non-IBM products was obtained from the suppliers of those products, their published announcements or other publicly available sources. IBM has not necessarily tested those products and cannot confirm the accuracy of performance, compatibility or any other claims related to non-IBM products. Questions on the capabilities of non-IBM products should be addressed to the suppliers of those products.

This information may contain examples of data and reports used in daily business operations. To illustrate them as completely as possible, the examples may include the names of individuals, companies, brands, and products. All of these names are fictitious and any similarity to the names and addresses used by an actual business enterprise is entirely coincidental.

All statements regarding IBM's future direction or intent are subject to change or withdrawal without notice, and represent goals and objectives only.

COPYRIGHT LICENSE

This information may contain sample application programs in source language, which illustrates programming techniques on various operating platforms. You may copy, modify, and distribute these sample programs in any form without payment to IBM, for the purposes of developing, using, marketing or distributing application programs conforming to the application programming interface for the operating platform for which the sample programs are written. These examples have not been thoroughly tested under all conditions. IBM, therefore, cannot guarantee or imply reliability, serviceability, or function of these programs.

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

COPYRIGHT AND PERMISSION NOTICE

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

All rights reserved.

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

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

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

Programming interface information

Programming interface information, if provided, is intended to help you create application software using this program.

General-use programming interfaces allow you to write application software that obtain the services of this program's tools.

However, this information may also contain diagnosis, modification, and tuning information. Diagnosis, modification and tuning information is provided to help you debug your application software.

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

Trademarks and service marks

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

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

MQSeries
Tivoli
WebSphere

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

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

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

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

WebSphere Business Integration Connect - Express includes software developed by
the Eclipse Project (www.eclipse.org).

WebSphere Business Integration Connect - Express Version 4.2.1.

IBM ®

Printed in USA