

IBM WebSphere Business Integration Connect - Express



User Guide

Version 4.2.0

Note!

Before using this information and the product it supports, be sure to read the general information under "Notices and Trademarks" on page 131.

First Edition (September 2003)

This edition applies to Version 4, Release 2, Modification 0, of IBM® WebSphere® Business Integration Connect - Express (5724-E88), and to all subsequent releases and modifications until otherwise indicated in new editions.

IBM welcomes your comments. You can send to the following address:

*IBM Burlingame Laboratory
Information Development
577 Airport Blvd., Suite 800
Burlingame, CA 94010
U.S.A*

Include the title and order number of this book, and the page number or topic related to your comment.

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

© Copyright International Business Machines Corporation 2003. All rights reserved.

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

Table of Contents

Introduction 5

Overview	5
Features	5
Console-based trading partner management	5
Support for HTTP- and AS2-based documents	6
Secure message routing	6
Console-based transaction auditing	7
Checklist	7

Installing WebSphere Business Integration Connect – Express 9

Overview	9
Minimum requirements	9
Installing the program using the GUI	9
Installing the code silently	17
Generating an options file	18

Getting Started 19

Overview	19
Starting WebSphere Business Integration Connect – Express	19
Accessing the Console	20
First-time login procedure	22
Logging in for the first time	22
Changing the default login passwords	22
Creating a participant	24
Where to go from here	26
Subsequent login procedures	27
Understanding the user interface	28
Updating your login passwords	30

Configuring and Testing 31

Overview	31
Displaying the Configuration menu	31
Configuring participants	33
Displaying the Manage Participants screen	33
Adding participants	34
Editing participants	35
Deleting participants	36
Configuring your profile	37
Configuring AS2 parameters	40
Configuring HTTP parameters	43

Testing Business Integration Connect – Express	46
--	----

Implementing Security 47

Overview	47
Understanding terms and concepts	47
Understanding the SSL protocol	47
Understanding client authentication	48
Understanding encryption and decryption	48
Understanding digital signatures	48
Understanding digital certificates	48
Certificate Revocation List (CRL)	49
Displaying the Security menu	49
Securing inbound transactions	50
Managing keystores for an SSL connection	50
Managing truststores for client authentication	56
Using keytool	56
Managing keypairs for decryption	60
Securing outbound transactions	64
Managing keypairs for client authentication	64
Managing encryption certificates	69
Managing keypairs for digital signatures	72
Adding certificates from certifying authorities	76
Adding new certificates	76
Deleting a certificate	77
Working with certification revocation lists	78
Adding new CRLs	78
Deleting a CRL	79

Managing Documents 81

Overview	81
Managing AS2 documents	81
Sending AS2 documents	82
Resending AS2 documents	84
Viewing sent AS2 documents	86
Viewing pending AS2 documents	93
Viewing AS2 documents pending MDNs	95
Viewing received AS2 documents	97
Managing HTTP documents	99
Sending HTTP documents	100
Resending HTTP documents	101
Viewing sent HTTP documents	103

Viewing pending HTTP documents	110	WebSphere Business Integration	
Viewing received HTTP documents	112	Connect – Express Folders	123
Viewing Reports	115	Uninstalling WebSphere Business	
Overview	115	Integration Connect – Express . . .	125
Displaying the Reports menu	115	Notices and Trademarks	131
Viewing the Document Summary report	116	Notices	131
Viewing the Participant Summary report	117	Programming interface information. . . .	132
Viewing the Activity Log	118	Trademarks and service marks	133
Error Messages	121		

About this book

This document describes how to install, configure, and use IBM® WebSphere® 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.

Who should read this book

This document is intended for organizations that will be using WebSphere Business Integration Connect – Express to conduct B2B activities with their trading partners.

Conventions and terminology used in this book

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

bold	Indicates something you select in the User Interface.
blue text	Blue text, which is only visible when you view the manual online, indicates a cross-reference hyperlink. Click any blue text to jump to the object of the reference.

Terms

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

Action: The initiating document sent in a business process.

Business Process: A predefined set of transactions that represent the method of performing the work needed to achieve a business objective.

Document: A collection of information adhering to an organizational convention. In this context, there are multiple documents in a message.

Document Protocol: A set of rules and instructions (protocol) for the formatting and transmission of information across a computer network. Examples include RosettaNet, XML, flat file, and EDI.

Console: A Web-based tool used to manage the documents being exchanged between the owner and partners.

Message: A message consists of multiple documents. For example, a message might include a header, body, and attachment.

Owner: The entity that is using IBM WebSphere Business Integration Connect – Express.

Partner: The entity that is exchanging documents with the owner.

Transaction: A sequence of information exchange and related work that are treated as a unit for the purposes of conducting business between partners.

Getting help

Online help

Click the **Help** link next to **Logout** to access the online help.

Customer service

Software support

www.ibm.com/software/support

Passport Advantage®

www-3.ibm.com/software/howtobuy/passportadvantage/

Company web site

www.ibm.com/websphere/wbiconnect/

Chapter 1. Introduction

Overview

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

Companies today are commonly communicating business-sensitive information with a large number of partners, customers, and suppliers over insecure networks such as the Internet. 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, the dynamic protocol of the World Wide Web, 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.

In this way, AS2 enables users to connect, deliver, and reply to data securely and reliably. For the first time, the Internet can be used for fast, secure, non-proprietary communication, where companies can interact and exchange information and documents in real-time with full receipt notification.

Secure message routing

Business Integration Connect – Express provides all 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. In this way, transactions are protected and managed to the highest levels possible.

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
- Encryption — transforms plain text into an unintelligible form (ciphertext) so that the original data cannot be recovered without using decryption.

- Digital signature

Console-based transaction auditing

Companies regularly need to know if a business partner has received a document and acknowledged or responded to that document. Using the Business Integration Connect – Express Console, you can view document and participant summary reports. There is also an activity log you can use to search for transactions that meet specific criteria. These tools provide a complete audit trail for managing and reconciling all B2B transactions and relationships.

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. See [Chapter 2, Installing WebSphere Business Integration Connect – Express, on page 9](#).
2. Start Business Integration Connect – Express. See [“Starting WebSphere Business Integration Connect – Express” on page 19](#).
3. Use your Web browser to access the Business Integration Connect – Express Console. See [“Accessing the Console” on page 20](#).
4. The first time you log in, you must change the default login passwords and create your first participant. See [“First-time login procedure” on page 22](#).
Thereafter, you can login using the procedure under [“Subsequent login procedures” on page 27](#).
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 31](#).

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, Implementing Security, on page 47](#).
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 81](#).
 - If you will be exchanging HTTP-based documents with participants, see [“Managing HTTP documents” on page 99](#).
8. Access reports as necessary to view a summary of the document, participant, and system activities that have occurred. See [Chapter 7, Viewing Reports, on page 115](#).

Chapter 2. Installing WebSphere Business Integration Connect – Express

Overview

WebSphere Business Integration Connect – Express can be installed on a personal computer (PC) running Microsoft® Windows® 2000. There are two ways to install Business Integration Connect – Express:

- Using an Install Shield graphical user interface (GUI) — see “[Installing the program using the GUI,](#)” below.
- Silently, using a command line interface — see “[Installing the code silently](#)” on page 17.

This chapter begins with a description of the minimum requirements for running Business Integration Connect – Express.

Minimum requirements

To install Business Integration Connect – Express on a PC, 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 100 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
- A Simple Mail Transport Protocol (SMTP)-based e-mail relay server for delivering e-mail alerts and SMTP messages

Installing the program using the GUI

To install Business Integration Connect – Express using the Install Shield GUI, use the following procedure.

1. Run the Business Integration Connect – Express install image. The Business Integration Connect – Express Installer starts automatically and the Welcome screen in [Figure 2-1 on page 10](#) appears.

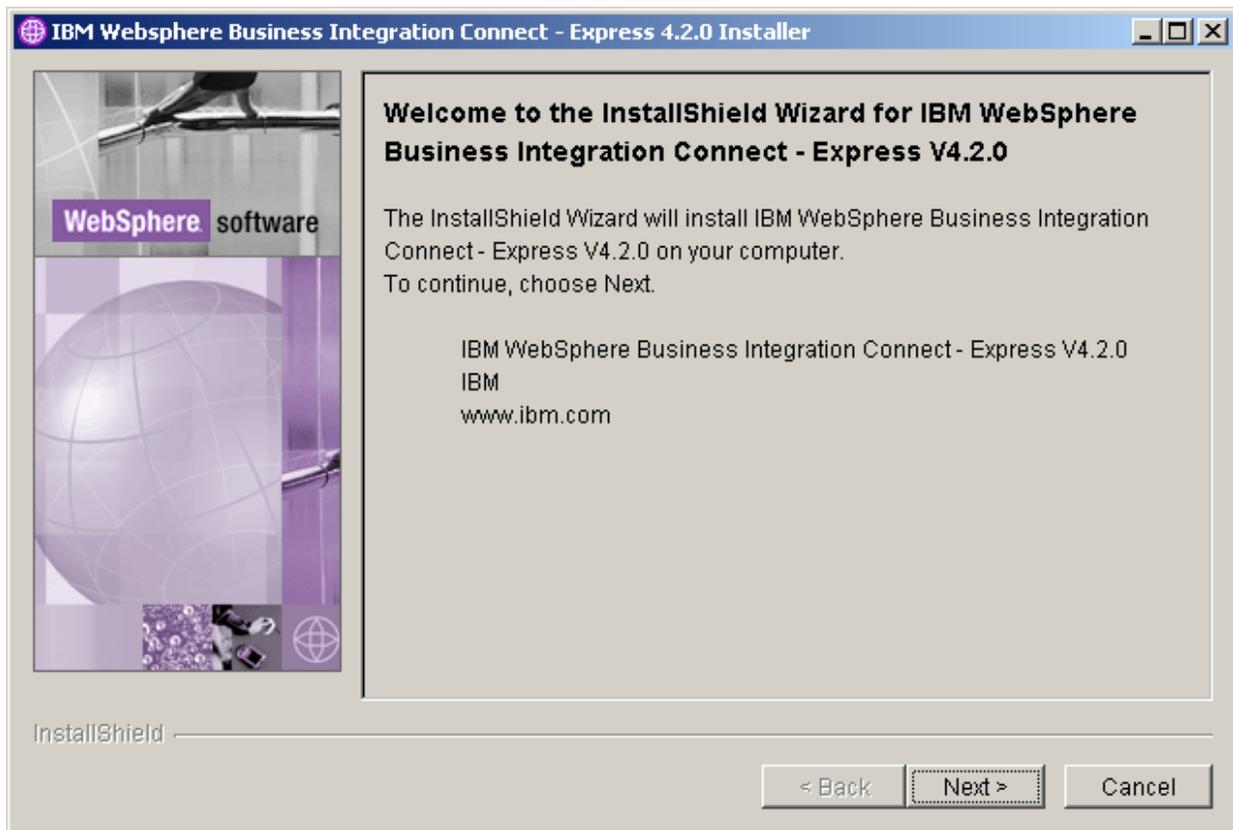


Figure 2-1. Welcome Screen

2. Click the **Next** button. The Software License Agreement in [Figure 2-2 on page 11](#) appears.

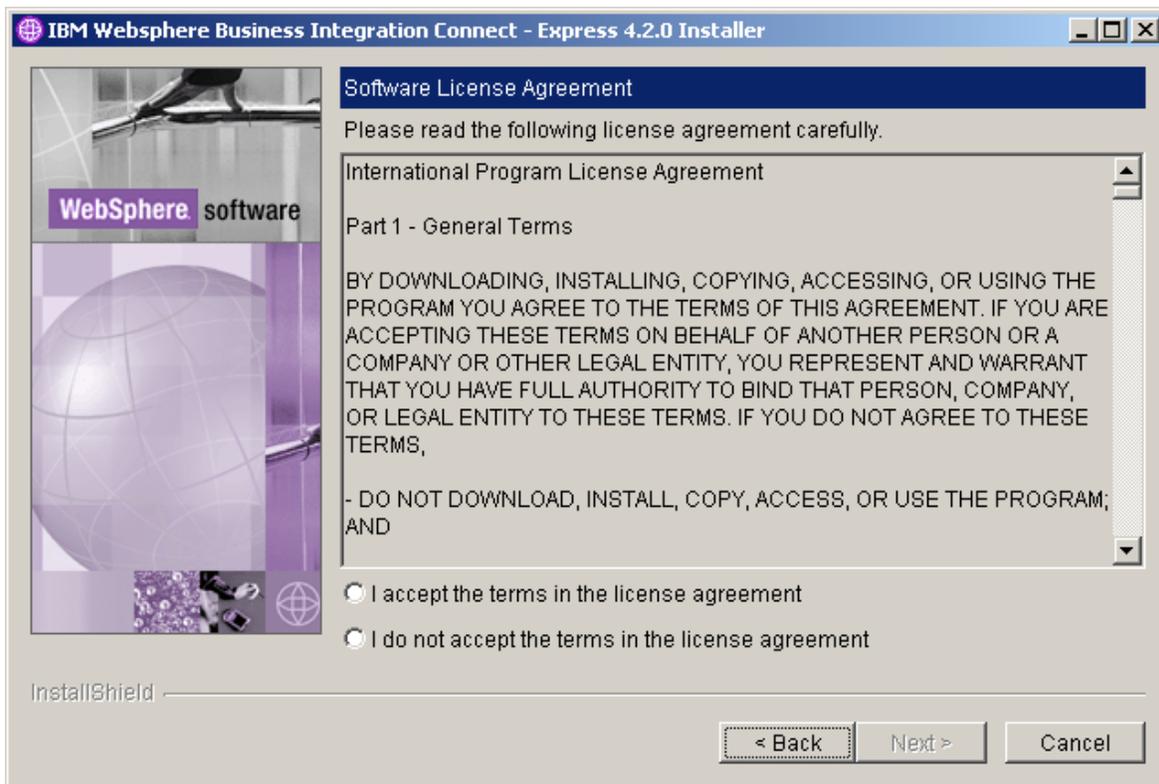


Figure 2-2. Software License Agreement

3. Click **I accept the terms in the license agreement**, then click the **Next** button. The screen in [Figure 2-3 on page 12](#) appears.

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

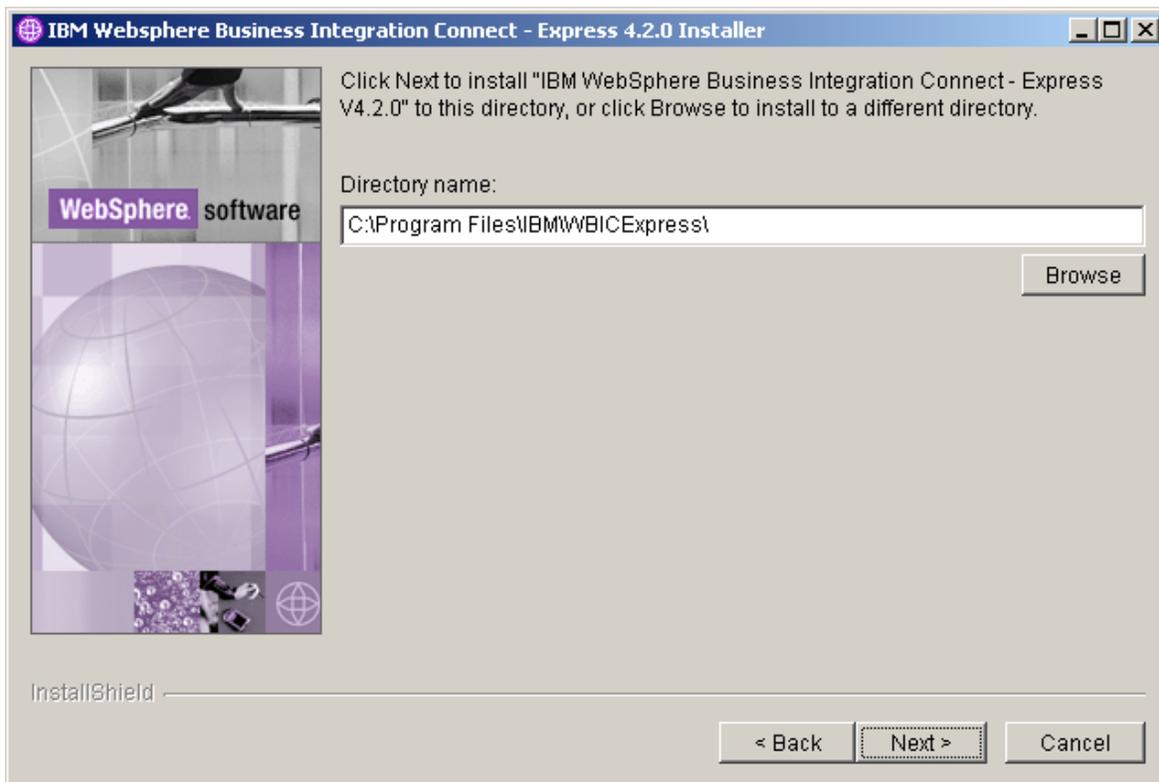


Figure 2-3. Directory Name

4. 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.
5. Click **Next**. The screen in [Figure 2-4 on page 13](#) appears.

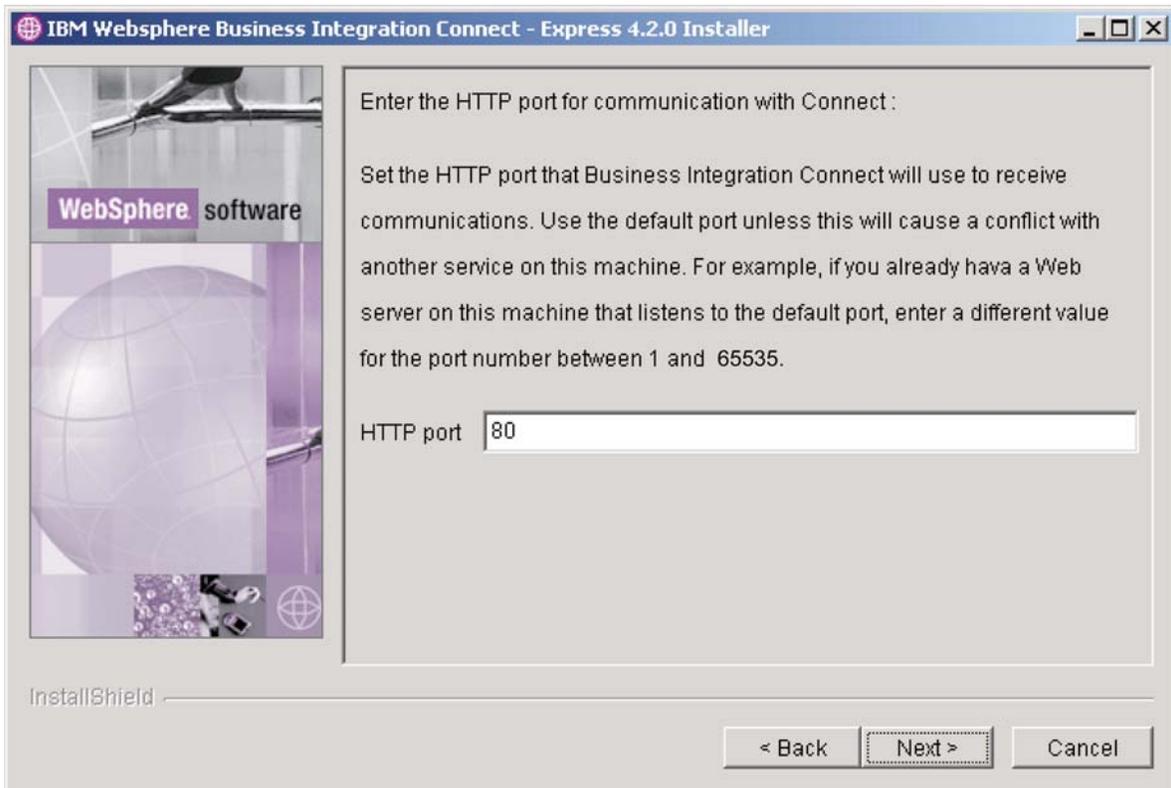


Figure 2-4. HTTP Port Screen

6. The HTTP Port screen 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.

7. Click **Next**. The screen in [Figure 2-5 on page 14](#) appears.

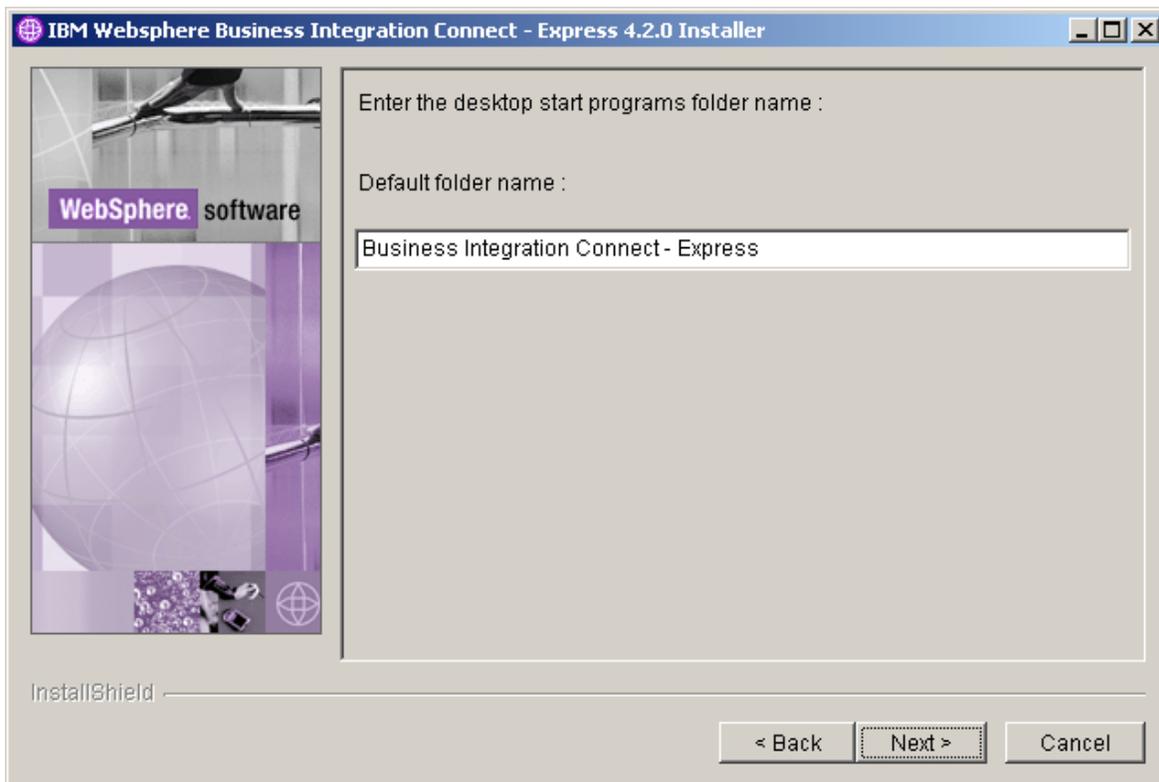


Figure 2-5. Default Folder Name

8. The Default Folder Name screen shows the name of the folder that Business Integration Connect – Express will install on your computer. Either accept the default name or change it.
9. Click **Next**. The screen in [Figure 2-6 on page 15](#) appears.

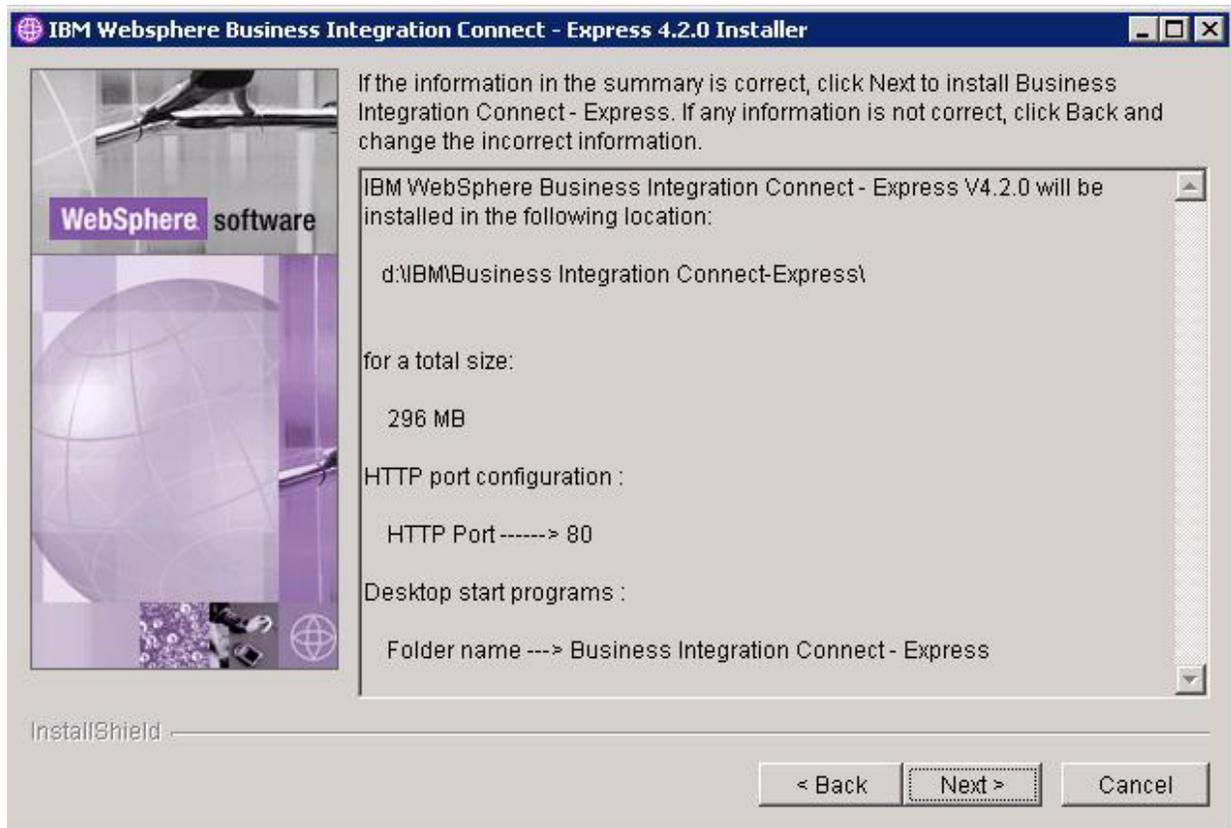


Figure 2-6. Summary Screen

10. Review your selections in the Summary screen. If you need to change any of them, click the **Back** button to return to the appropriate screen, make your changes, and click **Next** until you return to the Summary screen.
11. Click **Next**. The Installer installs the Business Integration Connect – Express software, then displays the First Use Application screen in [Figure 2-7 on page 16](#).

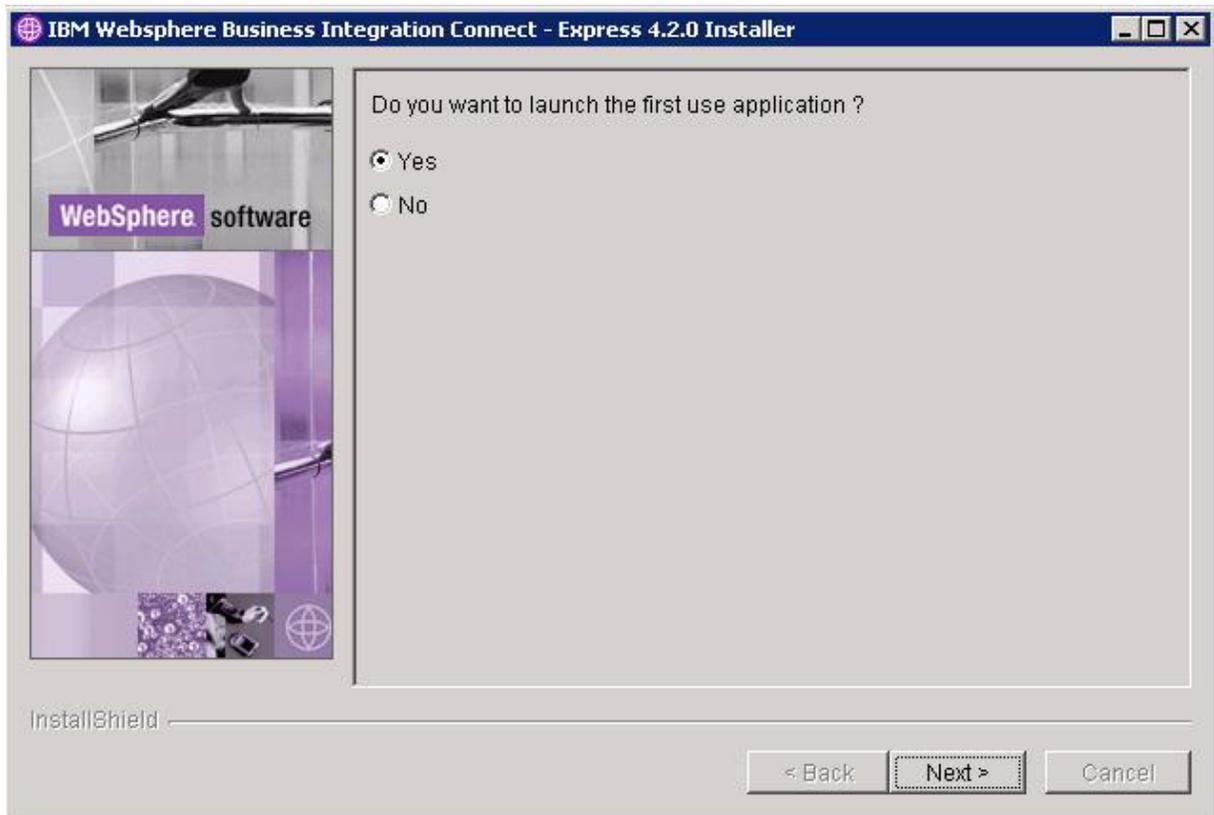


Figure 2-7. First Use Application Screen

12. To read the latest information about Business Integration Connect – Express, accept the **Yes** selection. Otherwise, click **No**.

NOTE: We recommend you read the latest information before you start using Business Integration Connect – Express.

13. Click **Next**. The screen in [Figure 2-8 on page 17](#) appears. If **Yes** was selected in the First Use Application screen, a screen containing information about using Business Integration Connect – Express also appears.

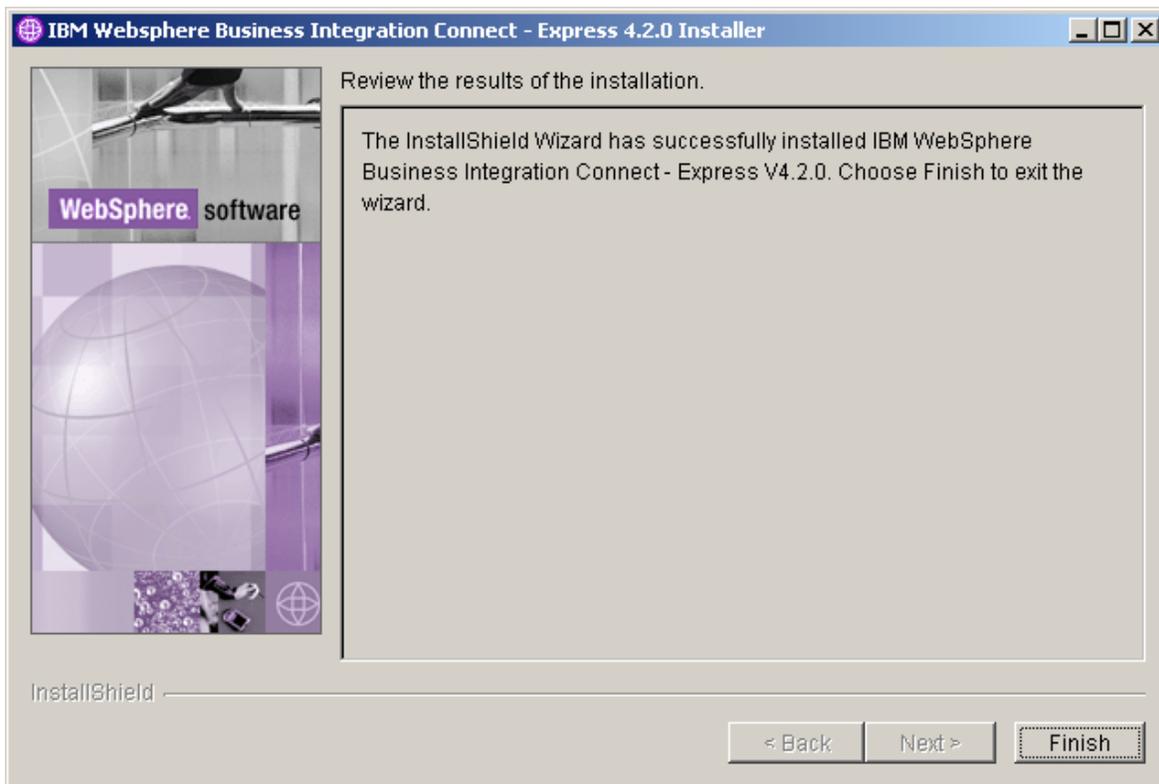


Figure 2-8. Installation Completed Screen

14. Click the **Finish** button to complete the installation.

Installing the code silently

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 `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, see [“Generating an options file” on page 18](#).

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.

To uninstall Business Integration Connect - Express silently:

1. Navigate to the directory:

```
<Business Integration Connect - Express install  
directory>\_uninst
```

2. Enter the following command:

```
uninstaller -silent
```

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

Chapter 3. Getting Started

Overview

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,”](#) below
- [“Accessing the Console,”](#) below
- [“First-time login procedure”](#) on page 22
- [“Subsequent login procedures”](#) on page 27
- [“Understanding the user interface”](#) on page 28
- [“Updating your login passwords”](#) on page 30

Starting WebSphere Business Integration Connect – Express

To start Business Integration Connect – Express:

1. Click the Start button on the Microsoft Windows taskbar and click **Programs**.
2. Point to **Business Integration Connect - Express** and click **Start Gateway**.
A Command Prompt window opens and Business Integration Connect – Express is launched.
3. 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.

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 3-1 on page 20](#)).

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

After you start Business Integration Connect – Express, use the following procedure to log into Business Integration Connect – Express:

1. Click the Start button on the Microsoft Windows taskbar and click **Programs**.
2. Point to **Business Integration Connect - Express** and click **Console**.
Business Integration Connect – Express displays the Welcome screen in your Web browser, with a blinking cursor in the **User Name** text box (see [Figure 3-1](#)).

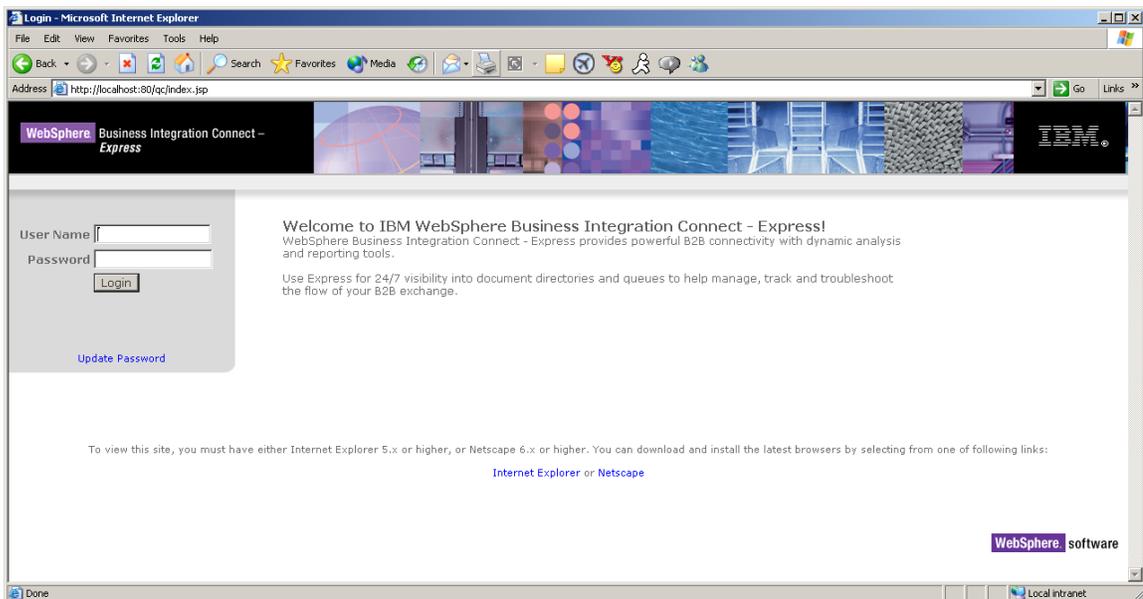


Figure 3-1. Welcome Screen

NOTE: If you used the My Profile screen 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 37](#)).

-
3. If this is the first time you are logging in, proceed to [“First-time login procedure”](#) on page 22. Otherwise, proceed to [“Subsequent login procedures”](#) on page 27.

First-time login procedure

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 screen in [Figure 3-1 on page 20](#) 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 screen appears (see [Figure 3-2 on page 23](#)). This screen lets you change login passwords.
4. Proceed to [“Changing the default login passwords” on page 22](#).

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.

Admin and Guest users have their own login passwords. By default, the login password for both is **admin**. When you log into the system for the first time, however, you must change these defaults to unique login passwords for Admin and Guest. These tasks are performed from the Initialize Passwords screen (see [Figure 3-2 on page 23](#)).

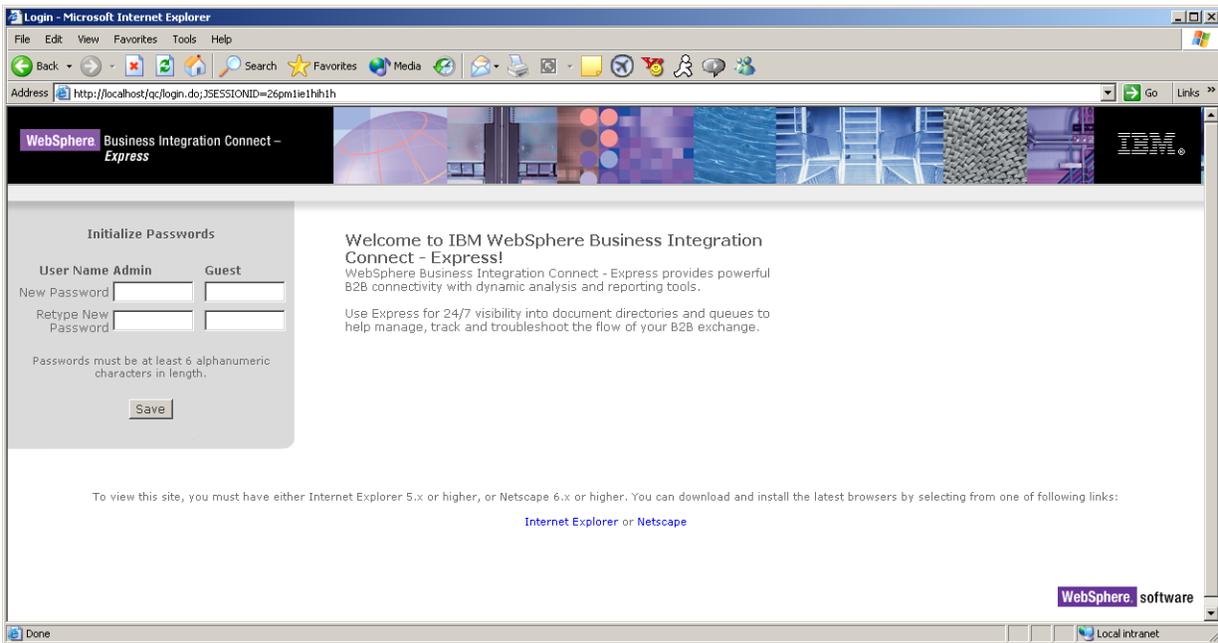


Figure 3-2. Initialize Passwords Screen

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 screen in [Figure 3-3 on page 24](#) appears.

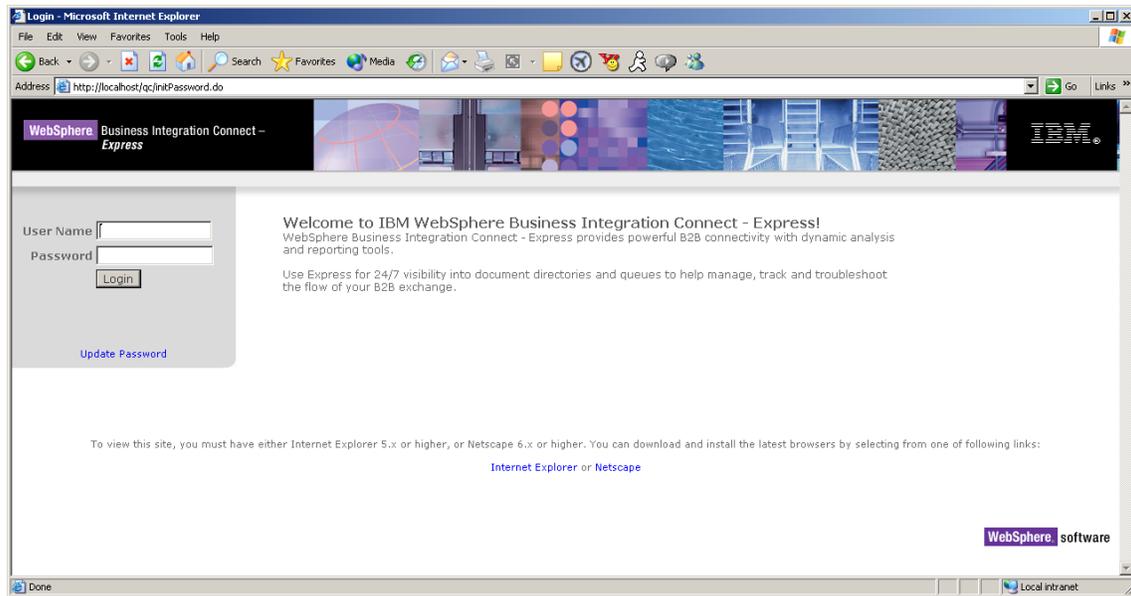


Figure 3-3. Login Welcome Screen

4. In the appropriate text boxes, enter your user name and the new login password you typed earlier in this procedure. The Create Participants screen appears (see [Figure 3-4 on page 25](#)). This screen lets you create and edit Business Integration Connect – Express participants.
5. Proceed to [“Creating a participant” on page 24](#).

NOTE: After you change the default login password, you can update it if necessary (see [“Updating your login passwords” on page 30](#)).

Creating a participant

When you log into Business Integration Connect – Express for the first time, the program allows you to use the Create Participant screen (shown in [Figure 3-4](#)) to create a participant with whom Business Integration Connect – Express will communicate.

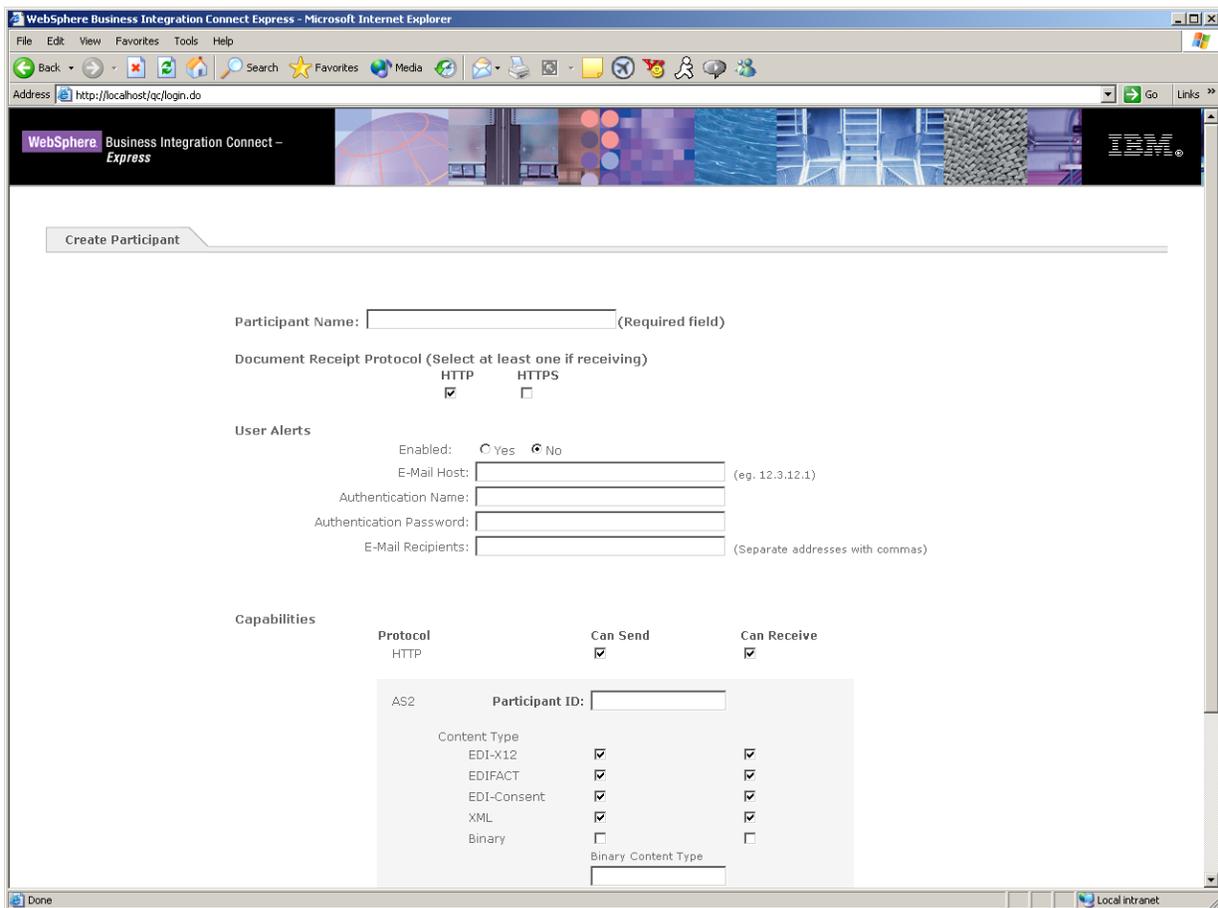


Figure 3-4. Create Participant Screen

To create a participant, use the following procedure.

1. Complete the entries in the Create Participant screen (see [Table 3-1 on page 26](#)).
2. Click the **Save** button. The Manage Participants screen appears. This screen 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 33](#).

Table 3-1. Create Participant Screen

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 your user name.
Authentication Password	Enter your login password.
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	Check whether the HTTP protocol will be used to send (Can Send) and receive (Can Receive) documents.
AS2 Participant ID	If you will be working with AS2-based documents, enter the AS2 participant ID.
Content Type	Check the content type that is to be sent (Can Send) and received (Can Receive). If Binary is checked, enter a binary content type.

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 screen (see [“Understanding the user interface” on page 28](#)).

NOTE: The Console automatically times-out after 5 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 screen in [Figure 3-1 on page 20](#) 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 screen appears (see [“Viewing the Document Summary report” on page 116](#)).
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 screen (see [“Understanding the user interface” on page 28](#)).

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 screens associated with the selected menu.

When you click a menu in the main menu:

- The horizontal navigation bar shows the screens associated with the menu you selected.
- In the horizontal navigation bar, the first screen 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** screen. To display a different screen in the menu, click the screen 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 two links appear at the top-right corner of each screen:

- **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 27](#).
- **Help** lets you access the online help for Business Integration Connect – Express.

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.

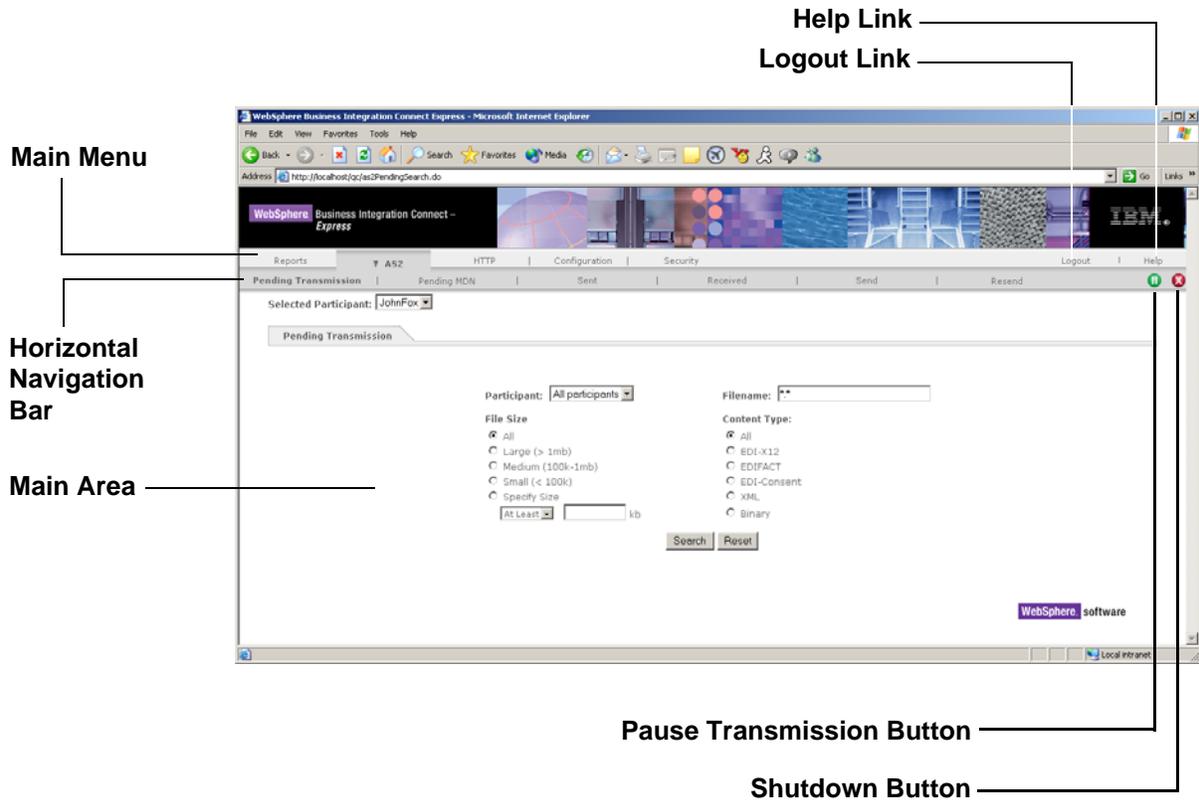


Figure 3-5. Business Integration Connect – Express User Interface

Updating your login passwords

There may be times when you want to change your login passwords. Business Integration Connect – Express simplifies this task by providing an **Update Password** link on the Login Welcome screen. 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 screen, click **Update Password**. The screen in [Figure 3-6](#) appears.

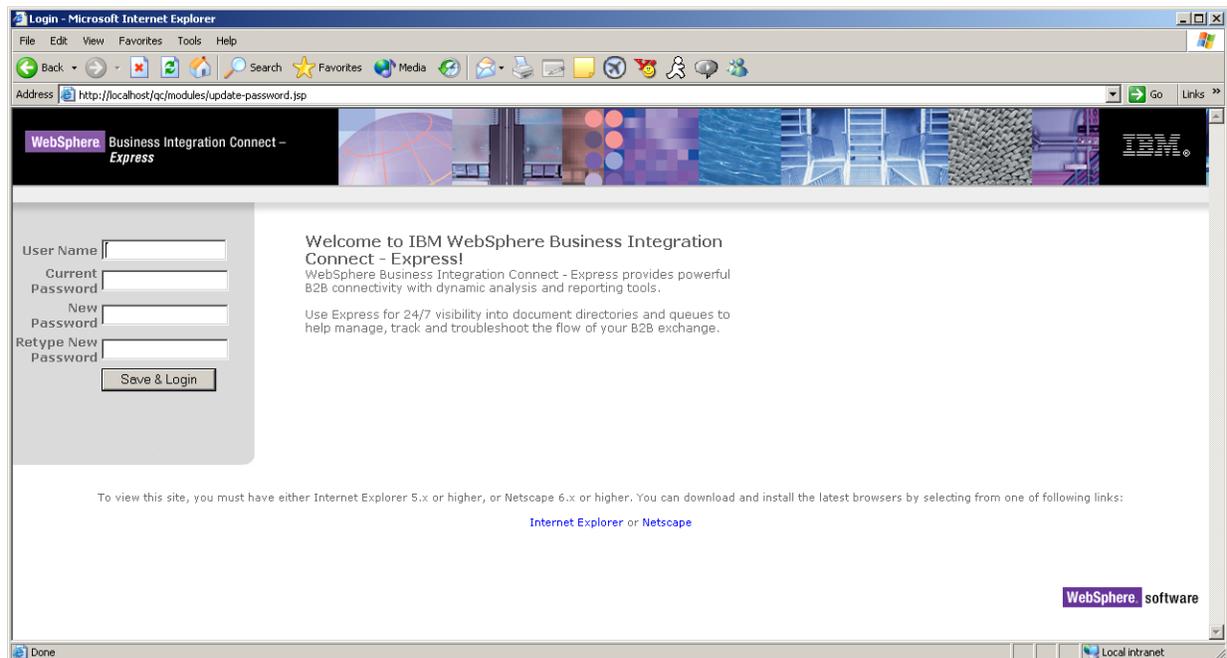


Figure 3-6. Screen for Updating the Login Password

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. Your password is changed and the Document Summary screen appears.

Chapter 4. Configuring and Testing

Overview

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 33
- [“Configuring your profile”](#) on page 37
- [“Configuring AS2 parameters”](#) on page 40
- [“Configuring HTTP parameters”](#) on page 43
- [“Testing Business Integration Connect – Express”](#) on page 46

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 screen appears (see [Figure 4-1 on page 32](#)). However, you can use the horizontal navigation bar to access other configuration screens.

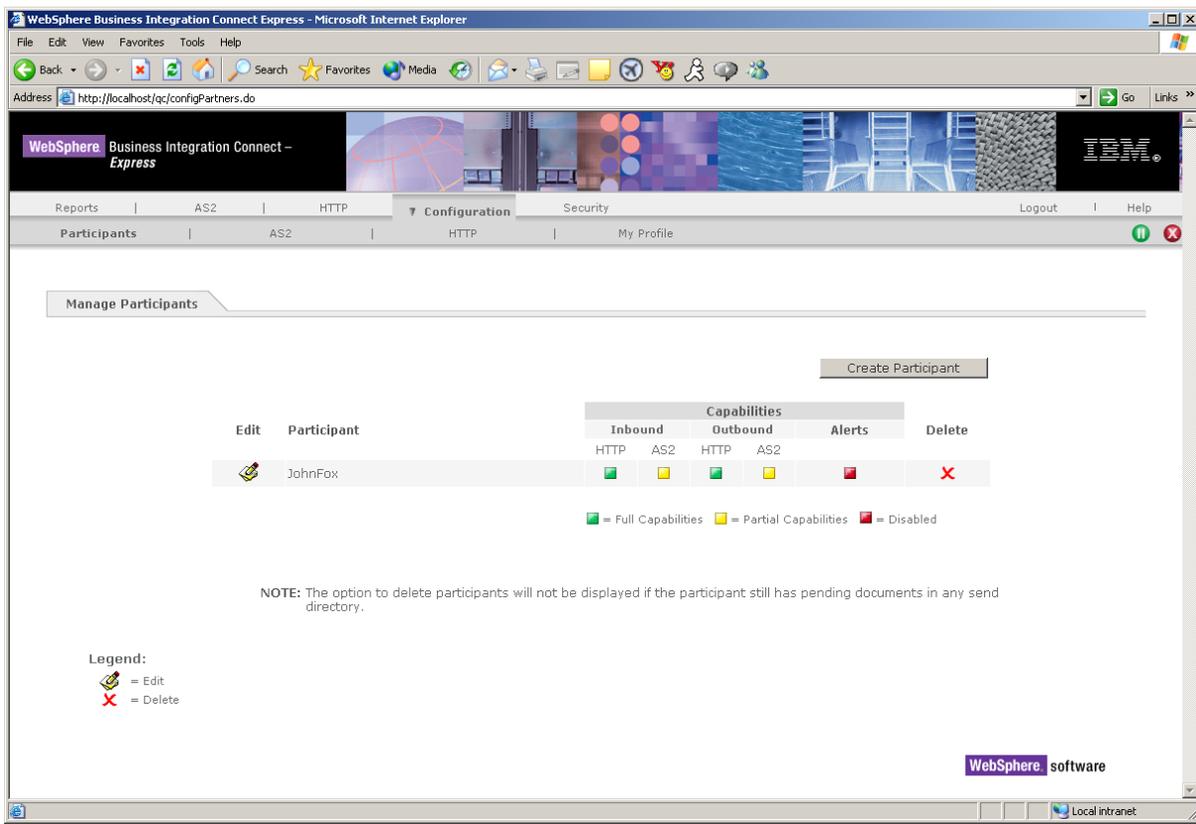


Figure 4-1. Configuration Menu, Participants Screen

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 33](#).
- **AS2** lets you select AS2 parameters for your participants. See [“Configuring AS2 parameters” on page 40](#).
- **HTTP** lets you select HTTP parameters for your participants. See [“Configuring HTTP parameters” on page 43](#).
- **My Profile** lets you create a profile for your company. See [“Configuring your profile” on page 37](#).

Configuring participants

The Manage Participants screen (shown in [Figure 4-2](#)) shows the participants you have created. Initially, this screen shows the participant you created when you logged into the system for the first time. However, you can display this screen when necessary to add, edit, or delete participants.

Displaying the Manage Participants screen

To display the Manage Participants screen, click the **Configuration** menu. The Manage Participants screen appears (see [Figure 4-2](#)). If it does not appear, click **Participants** in the horizontal navigation bar.

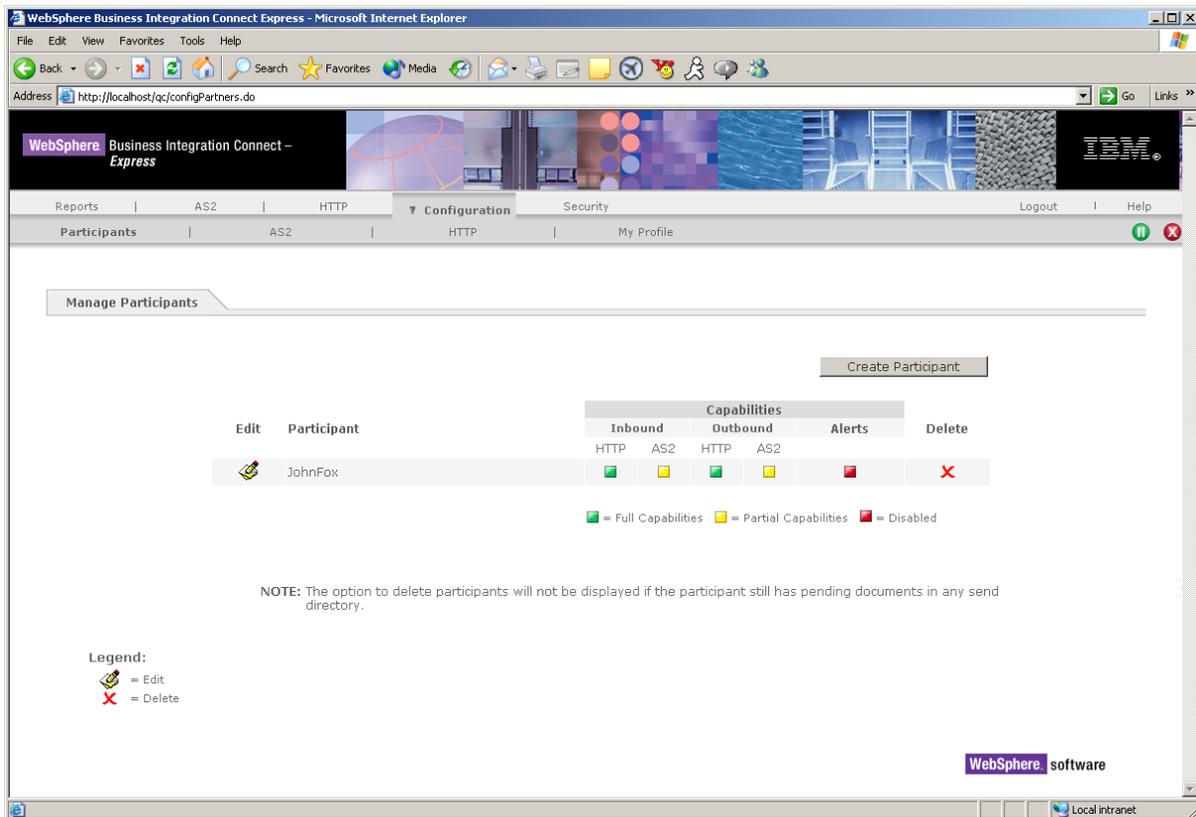


Figure 4-2. Manage Participants Screen

Adding participants

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

1. Click the **Configuration** menu to display the Manage Participants screen in [Figure 4-2 on page 33](#). If the screen does not appear, click **Participants** in the horizontal navigation bar.
2. Click the **Create Participant** button. The Create Participant screen appears (see [Figure 4-3](#)).

Participant Name: (Required field)

Document Receipt Protocol (Select at least one if receiving)

HTTP HTTPS

User Alerts

Enabled: Yes No

E-Mail Host: (eg, 12.3.12.1)

Authentication Name:

Authentication Password:

E-Mail Recipients: (Separate addresses with commas)

Capabilities

Protocol	Can Send	Can Receive
HTTP	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
AS2		
Participant ID: <input type="text"/>		
Content Type		
EDI-X12	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
EDIFACT	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
EDI-Consent	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
XML	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Binary	<input type="checkbox"/>	<input type="checkbox"/>

Figure 4-3. Screen for Adding Participants

3. Complete the entries in the Create Participant screen (see [Table 4-1 on page 35](#)).
4. Click the **Save** button.
5. To add more participants, repeat steps 2 through 4.

Table 4-1. Create Participants Screen Parameters

Parameter	Description
Participant Name	Enter the name of this participant without any spaces. The participant name must be unique; otherwise, unexpected results may occur.
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	Specify whether this participant is to receive system-generated alerts if his document transmission has failed.
E-Mail Host	Enter the e-mail host or server that will be used. Example: mail.mycompany.com
Authentication Name	Enter your user name for e-mail system.
Authentication Password	Enter your login password for e-mail system.
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	Check whether the HTTP protocol will be used to send (Can Send) and receive (Can Receive) documents.
AS2 Participant ID	Enter the AS2 participant ID if working with AS2-based documents. The ID entered here appears on the Manage AS2 screen (see “ Configuring AS2 parameters ” on page 40).
Content Type	Check the content type that is to be sent (Can Send) and received (Can Receive). If Binary is checked, enter a binary 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 screen in [Figure 4-2 on page 33](#). If the screen 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 screen similar to the one in [Figure 4-3 on page 34](#) appears, with the information you specified for the participant.
3. Change the information as required. If you need assistance, refer to [Table 4-1](#).
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 screen in [Figure 4-2 on page 33](#). If the screen 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 4-4](#) appears.

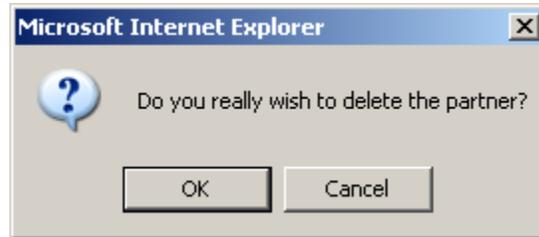


Figure 4-4. Precautionary Message when Deleting a Participant

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

Configuring your profile

Using the My Profile screen 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 profile information before specifying your AS2 and HTTP configuration parameters.

1. Click the **Configuration** menu, then click **My Profile** in the horizontal navigation bar. The Manage My Profile screen appears (see [Figure 4-5](#)).

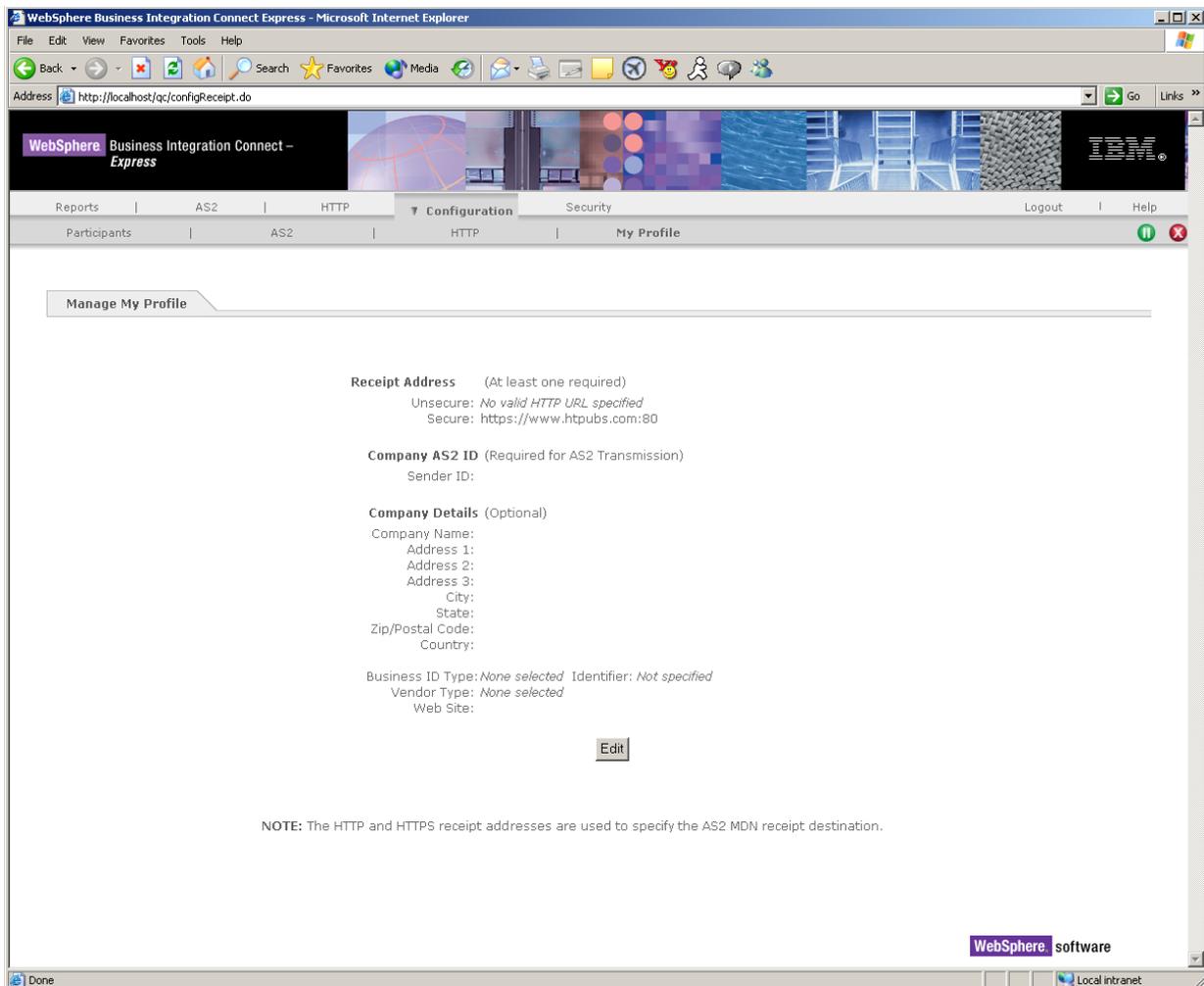


Figure 4-5. Manage My Profile Screen

2. Click the **Edit** button. The Manage My Profile screen in [Figure 4-6 on page 38](#) appears.

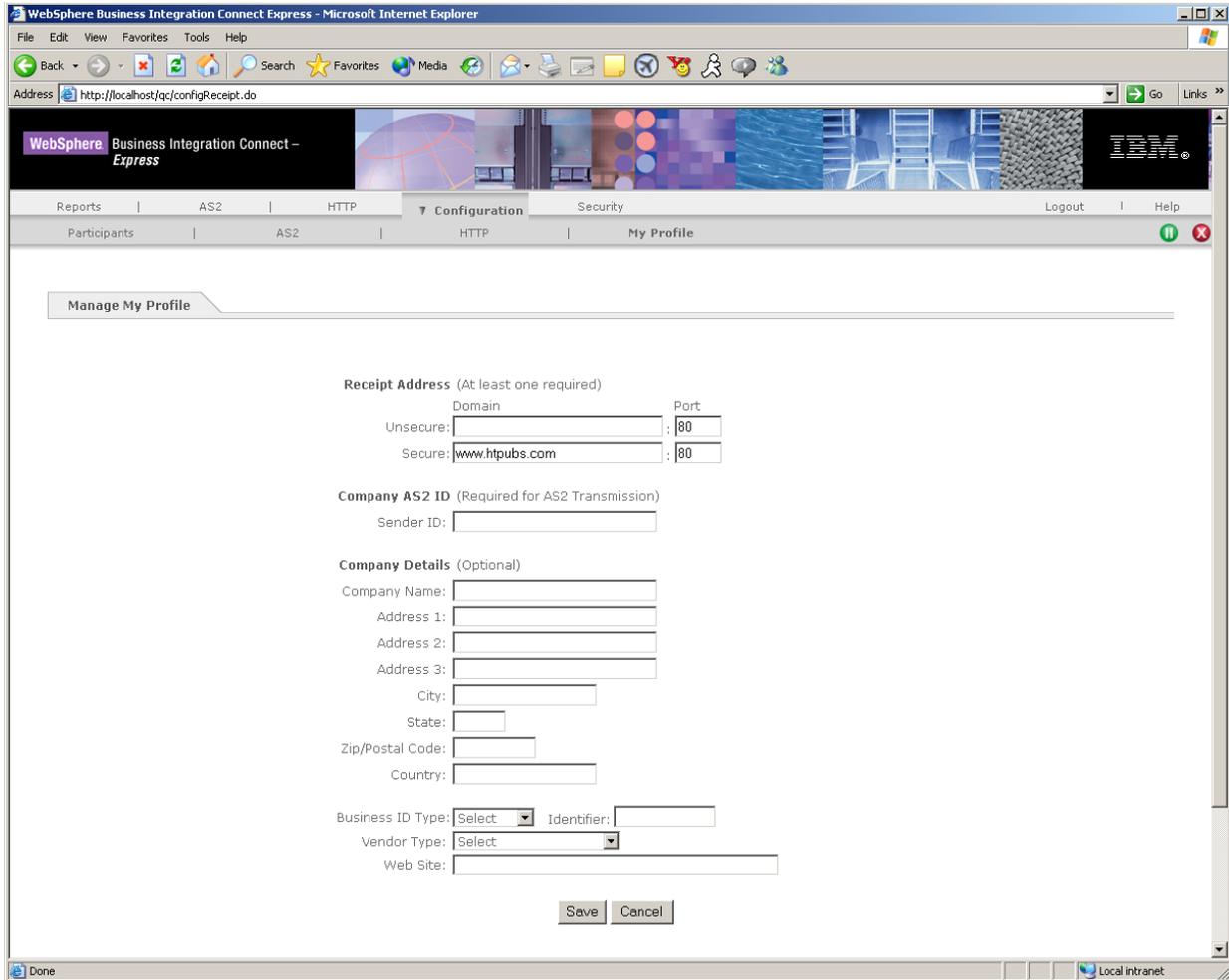


Figure 4-6. Screen for Entering My Profile Configuration Parameters

3. Complete the entries in the Manage My Profile screen (see [Table 4-4 on page 45](#)).
4. Click the **Save** button.

Table 4-2. Manage My Profile Screen 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 screens (see “Configuring AS2 parameters” on page 40 and “Configuring HTTP parameters” on page 43). 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 20).
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 screens (see “Configuring AS2 parameters” on page 40 and “Configuring HTTP parameters” on page 43). 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 20).
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 screen (see “Configuring AS2 parameters” on page 40).
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 screen.

To configure AS2 parameters, use the following procedure.

1. Click the **Configuration** menu, then click **AS2** in the horizontal navigation bar. The Manage AS2 screen appears (see [Figure 4-7](#)).

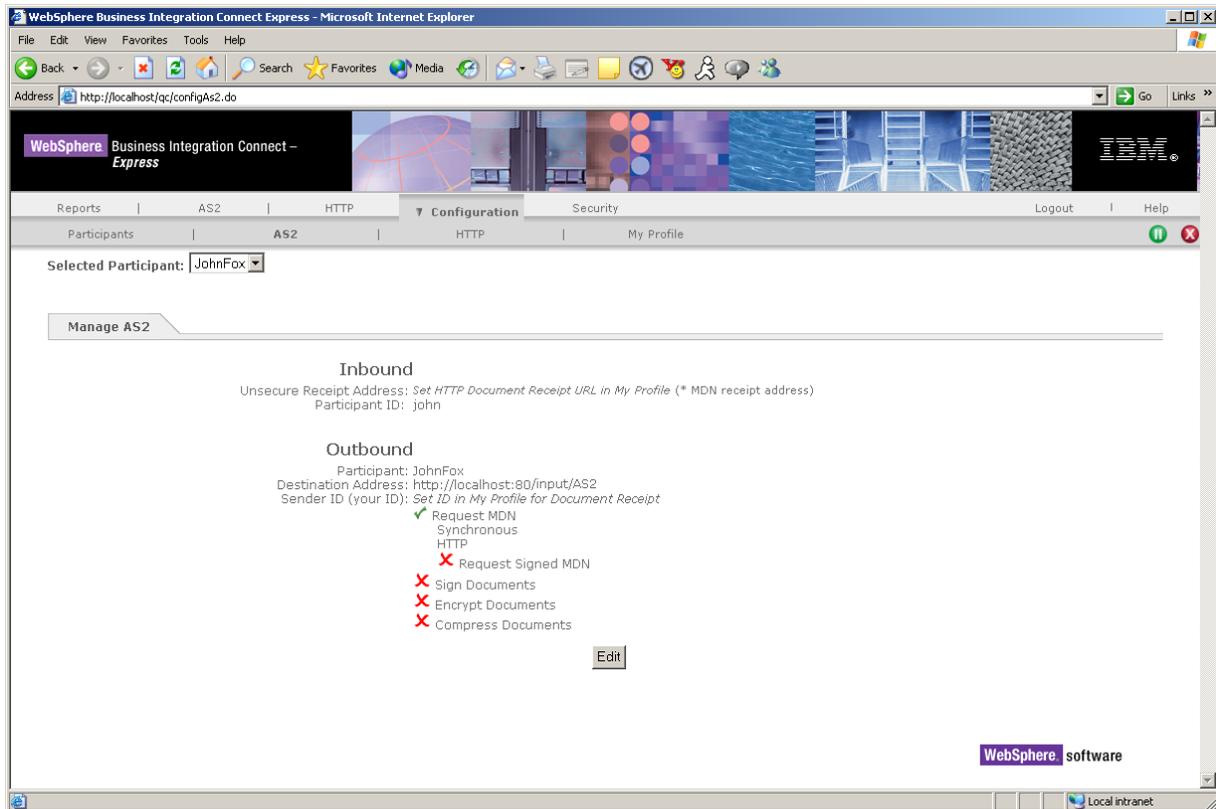


Figure 4-7. Manage AS2 Screen

2. Next to **Selected Participants**, select the participant whose AS2 configuration you want to specify.
3. Click the **Edit** button. The Manage AS2 screen in [Figure 4-8 on page 41](#) appears. This screen 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 (see [“Configuring your profile” on page 37](#)).

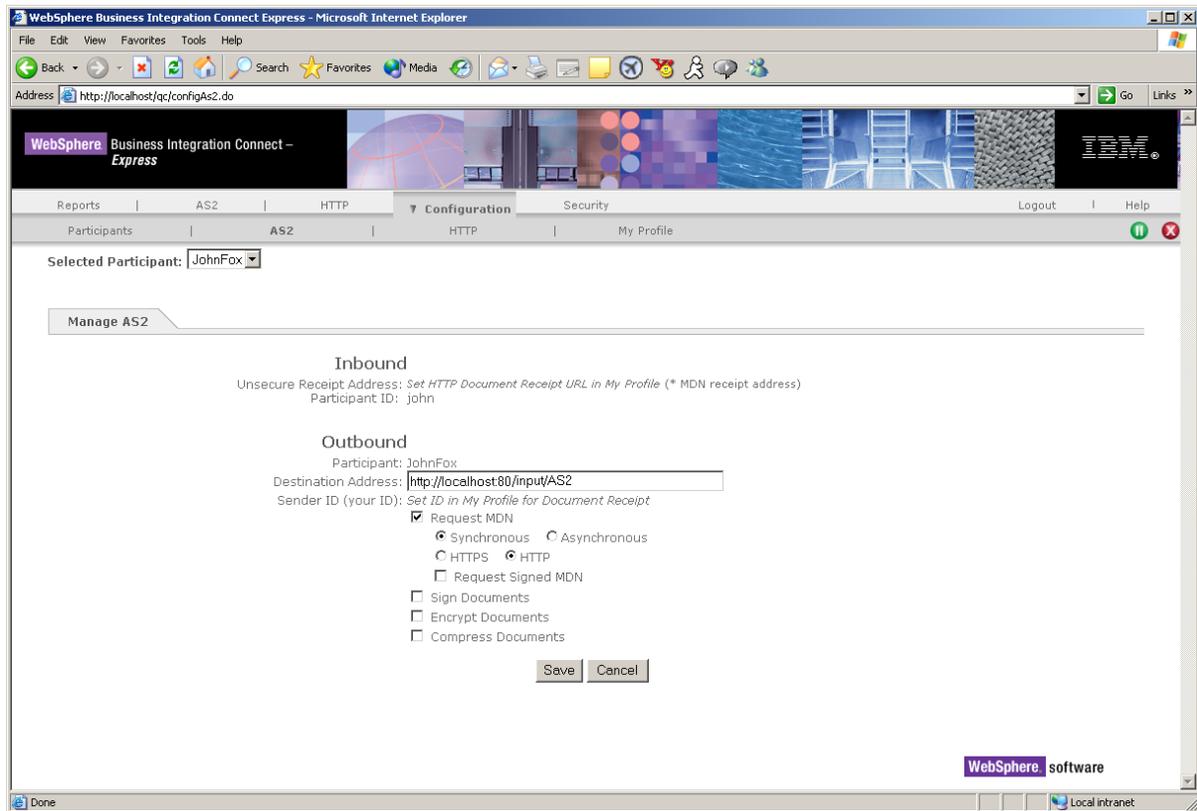


Figure 4-8. Screen for Entering AS2 Configuration Parameters

4. Complete the entries in the Manage AS2 screen (see [Table 4-3 on page 42](#)).
5. Click the **Save** button.
6. To specify AS2 configuration parameters for other participants, repeat steps 2 through 5.

Table 4-3. Manage AS2 Screen 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 37).
Participant ID	Read-only field that shows the ID associated with this participant. This parameter is set on the My Participants screen (see “Configuring participants” on page 33).
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 37).
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.
Encrypt Documents	Check to encrypt outbound AS2 documents from this participant.
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 screen.

To configure HTTP parameters, use the following procedure.

1. Click the **Configuration** menu, then click **HTTP** in the horizontal navigation bar. The Manage HTTP screen appears (see [Figure 4-9](#)).

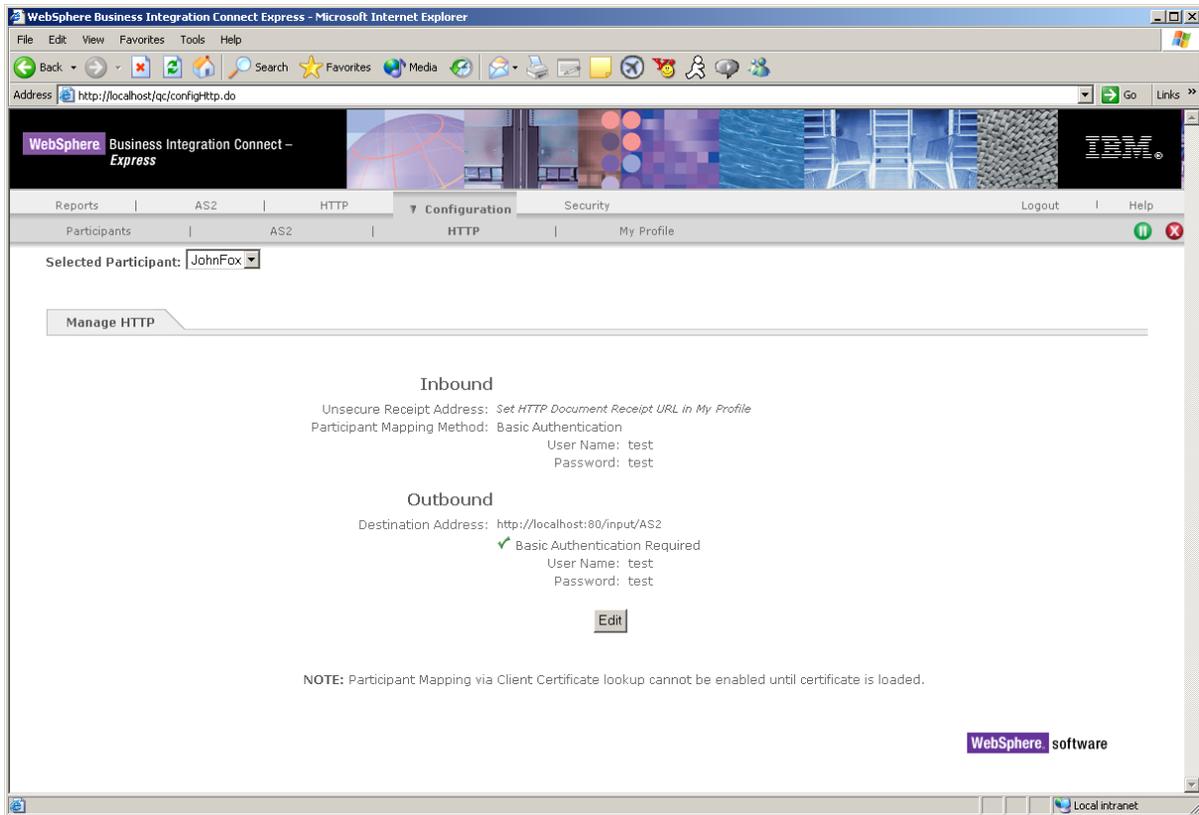


Figure 4-9. Manage HTTP Screen

2. Next to **Selected Participants**, select the participant whose HTTP configuration you want to specify.
3. Click the **Edit** button. The Manage HTTP screen in [Figure 4-10 on page 44](#) appears. This screen 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 (see [“Configuring your profile” on page 37](#)).

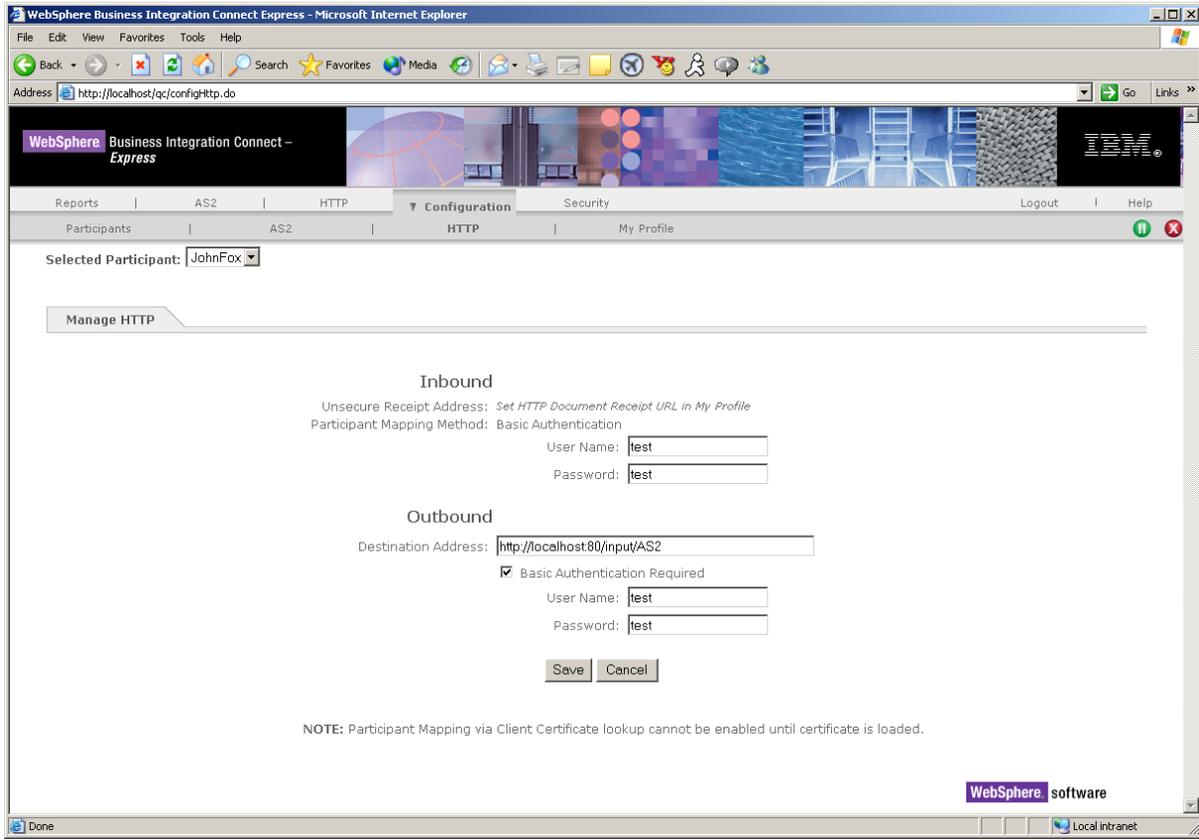


Figure 4-10. Screen for Entering HTTP Configuration Parameters

4. Complete the entries in the Manage HTTP screen (see [Table 4-4 on page 45](#)).
5. Click the **Save** button.
6. To specify HTTP configuration parameters for other participants, repeat steps 2 through 5.

Table 4-4. Manage HTTP Screen Parameters

Parameter	Description
Inbound	
Unsecure Receipt Address	Read-only field showing the HTTP document receipt URL.
Participant Mapping Method	Read-only field that shows that basic authentication (unique username and password) will be used to ascertain the sender of an inbound document. In Business Integration Connect – Express, basic authentication is mandatory for receipt of plain HTTP documents, as plain HTTP does not enforce a header field identifying the sender.
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.
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.

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 82](#).
 - If you sent an HTTP-based document, see [“Sending HTTP documents” on page 100](#).
3. After you send the document, go to the Sent Documents screen 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 86](#).
 - If you sent an HTTP-based document, see [“Viewing sent HTTP documents” on page 103](#).
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 97](#).
 - If you received an HTTP-based document, see [“Viewing received HTTP documents” on page 112](#).
5. If the document was received skip to the next step. Otherwise, go to the Pending Transmission screen and see whether the document is waiting to be transmitted.
 - For AS2-based documents, see [“Viewing pending AS2 documents” on page 93](#). If you requested a Message Disposition Notification for your document, also see [“Viewing AS2 documents pending MDNs” on page 95](#).
 - If you sent an HTTP-based document, see [“Viewing pending HTTP documents” on page 110](#).

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. Implementing Security

Overview

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.

This chapter describes the security features supported by Business Integration Connect – Express. Topics in this chapter include:

- [“Understanding terms and concepts” on page 47](#)
- [“Displaying the Security menu” on page 49](#)
- [“Securing inbound transactions” on page 50](#)
- [“Securing outbound transactions” on page 64](#)
- [“Adding certificates from certifying authorities” on page 76](#)
- [“Working with certification revocation lists” on page 78](#)

Understanding terms and concepts

Security is paramount when it comes to B2B Internet commerce. Sales management, for example, may wonder if a competitor could tap into the content of the purchase orders submitted via the Internet by its top customers and use that information to steal those customers. Accounting may wonder if someone could submit bogus invoices or doctor order status reports in transit. The Board of Directors may wonder if the information they are passing through their service providers can be used against the company.

To safeguard inbound and outbound documents, Business Integration Connect – Express incorporates a multi-level authentication process that incorporates Secure Sockets Layer (SSL), client authentication, encryption and decryption, and signing. The following sections describe these features.

Understanding the SSL protocol

Business Integration Connect – Express uses the SSL protocol to secure inbound documents. SSL is a protocol developed by Netscape for transmitting private documents via the Internet. It implements link-level encryption of documents sent to and from Partners. 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.

Understanding client authentication

Business Integration Connect – Express uses client authentication to secure inbound and outbound documents. Client authentication guarantees that a transmitted message was not modified en route and that the identity of the creator is not misrepresented. With client authentication, a separate piece of data generated during the handshake is signed by the client and authenticated by the server. Once the client has been authenticated, messages can be sent over the encrypted connection.

Understanding encryption and decryption

Business Integration Connect – Express uses encryption to secure outbound documents and decryption to secure inbound documents. Data encryption works by using the receiver’s public key.

With encryption, a random password is generated by the software, and the data is encrypted using a symmetric algorithm (such as 3DES or RC5) using the generated password. That password is encrypted asymmetrically (RSA) using the destination partner’s public key. When the destination partner receives the data, the partner uses his private key to decrypt the password, which is then used to decrypt the data.

Understanding digital signatures

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”). The mechanism for ensuring non-repudiation is the digital signature.

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.

Understanding digital certificates

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 CAs 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.

Certificate Revocation List (CRL)

Business Integration Connect – Express supports Certificate Revocation Lists (CRLs). A CRL is a list maintained by the certifying authority of digital certificates that have been declared invalid for a reason other than expiration. The CRL consists of a special message together with a signature. The special message for a CRL contains a list of revoked certificates, where the certificates are typically referenced indirectly by a serial number. A CRL enables the certification authority to “void” its signatures on someone's certificate or extended certificates, which might be required when someone's name changes or their private key is compromised.

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 screen appears (see [Figure 5-1](#)). However, you can use the horizontal navigation bar to access other security screens.

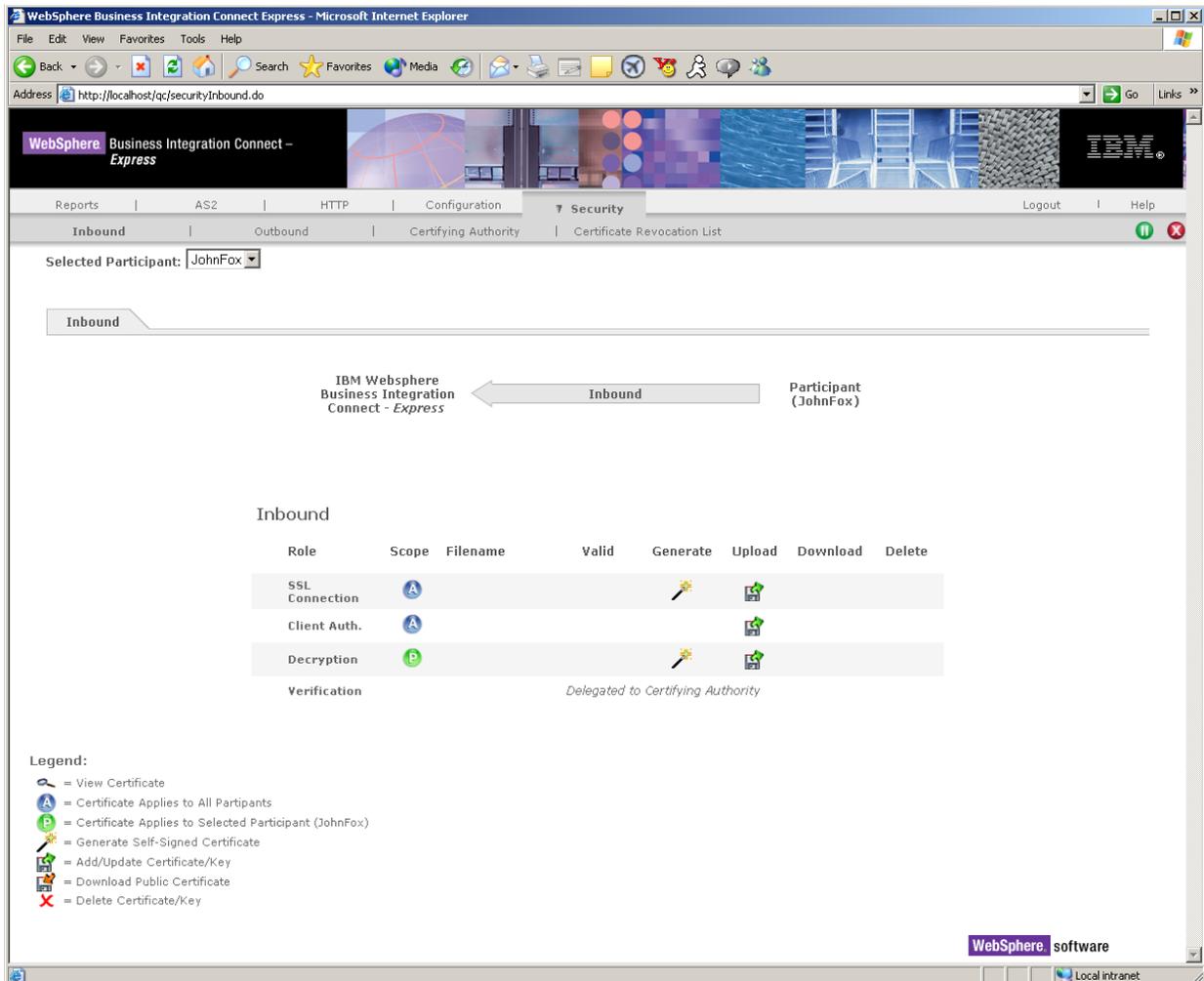


Figure 5-1. Security Menu, Inbound Screen

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. See [“Securing inbound transactions” on page 50](#).
- **Outbound** lets you configure security for documents sent by Business Integration Connect – Express. See [“Securing outbound transactions” on page 64](#).
- **Certifying Authority** lets you add and delete CA certificates. See [“Adding certificates from certifying authorities” on page 76](#).
- **Certificate Revocation List** lets you add and delete CRLs. See [“Working with certification revocation lists” on page 78](#).

Securing inbound transactions

Business Integration Connect – Express uses the concepts of keystores, truststores, and keypairs to secure inbound transactions.

- 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 screen to make the keystore available to the appropriate participants. See [“Managing keystores for an SSL connection,”](#) below.
- 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. See [“Managing truststores for client authentication” on page 56](#).
- A keypair is used for decryption. The keypair consists of a private key and a public key. The private key is your personal key to use and not available to anyone but you. The public key is listed and authorized by a third-party CA and open to all users. With this keypair, you can perform your operations in a totally secure environment. See [“Managing keypairs for decryption” on page 60](#).

Managing keystores for an SSL connection

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 or deleted when it is no longer required.

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 screen in [Figure 5-1 on page 49](#). If the screen 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.

- Under **Generate**, click the  icon in the **SSL Connection** row. The Inbound screen in [Figure 5-2](#) appears.

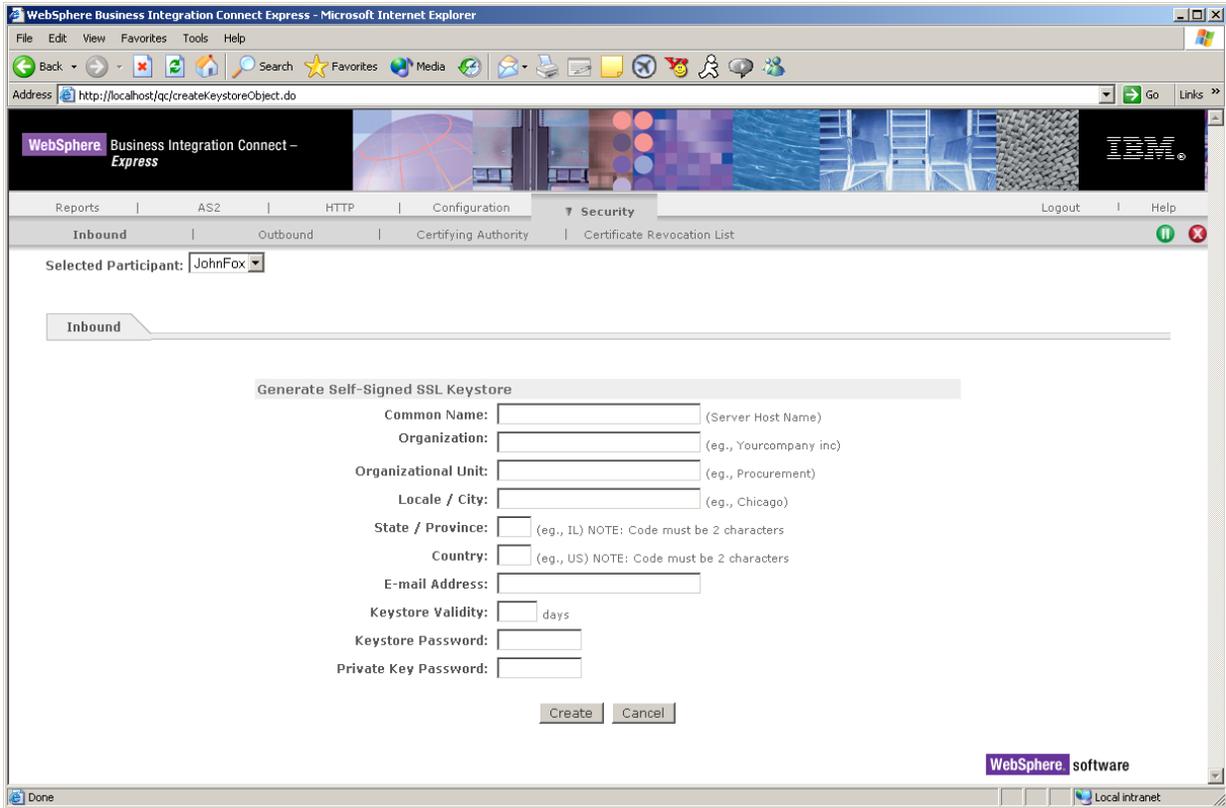


Figure 5-2. Inbound Screen for Generating a Self-Signed SSL Keystore

- Complete the entries in the Inbound screen (see [Table 5-1](#)).
- Click the **Create** button. The self-signed keystore is uploaded and appears in the Inbound screen.

Table 5-1. Inbound Screen 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.

Table 5-1. Inbound Screen for Generated Self-Signed SSL Keystore (continued)

Parameter	Description
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 screen in [Figure 5-1 on page 49](#). If the screen 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  icon in the **SSL Connection** row. The Inbound screen in [Figure 5-3 on page 53](#) appears.

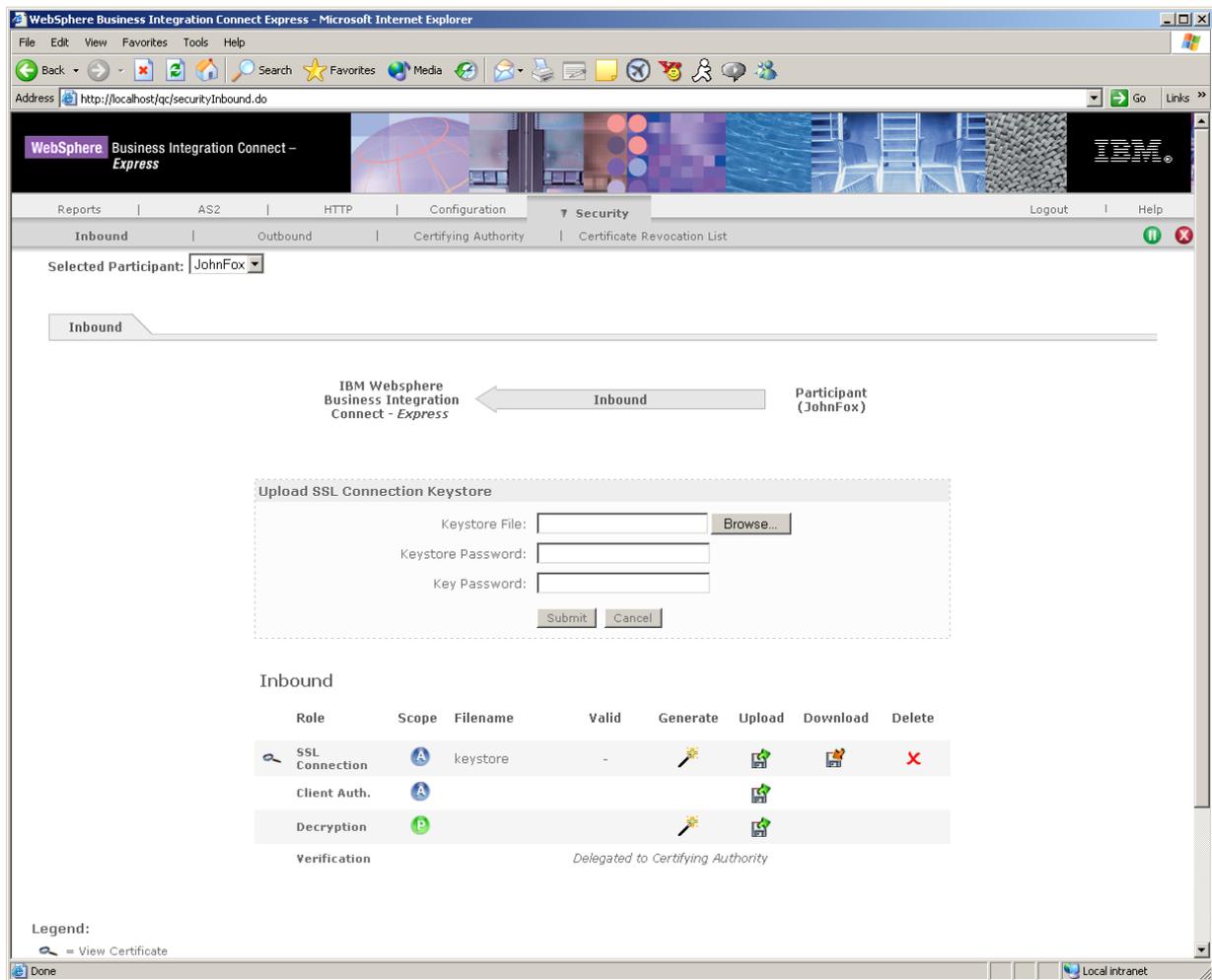


Figure 5-3. Inbound Screen for Uploading an SSL Keystore

4. Complete the entries in the Inbound screen (see [Table 5-2 on page 54](#)).
5. Click the **Submit** button. The keystore is uploaded and appears in the Inbound screen.

Table 5-2. Inbound Screen 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 screen in [Figure 5-1 on page 49](#). If the screen 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 in the **SSL Connection** row. The File Download screen in [Figure 5-4](#) appears.



Figure 5-4. File Download Screen

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.)

Deleting an SSL keystore

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

1. Click the **Security** menu to display the Inbound screen in [Figure 5-1 on page 49](#). If the screen does not appear, click **Inbound** in the horizontal navigation bar.
2. Next to **Selected Participant**, select the participant whose keystore you want to delete.
3. Under **Delete**, click the  icon in the **SSL Connection** row. The precautionary message in [Figure 5-5](#) appears.



Figure 5-5. Precautionary Message

4. Click **OK** to delete the keystore or **Cancel** to retain it.

Managing truststores for client authentication

Using the Inbound screen, 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” on page 57](#) 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 screen in [Figure 5-1 on page 49](#). If the screen 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. Under **Upload**, click the  icon in the **Client Auth.** row. The Inbound screen in [Figure 5-6](#) appears.

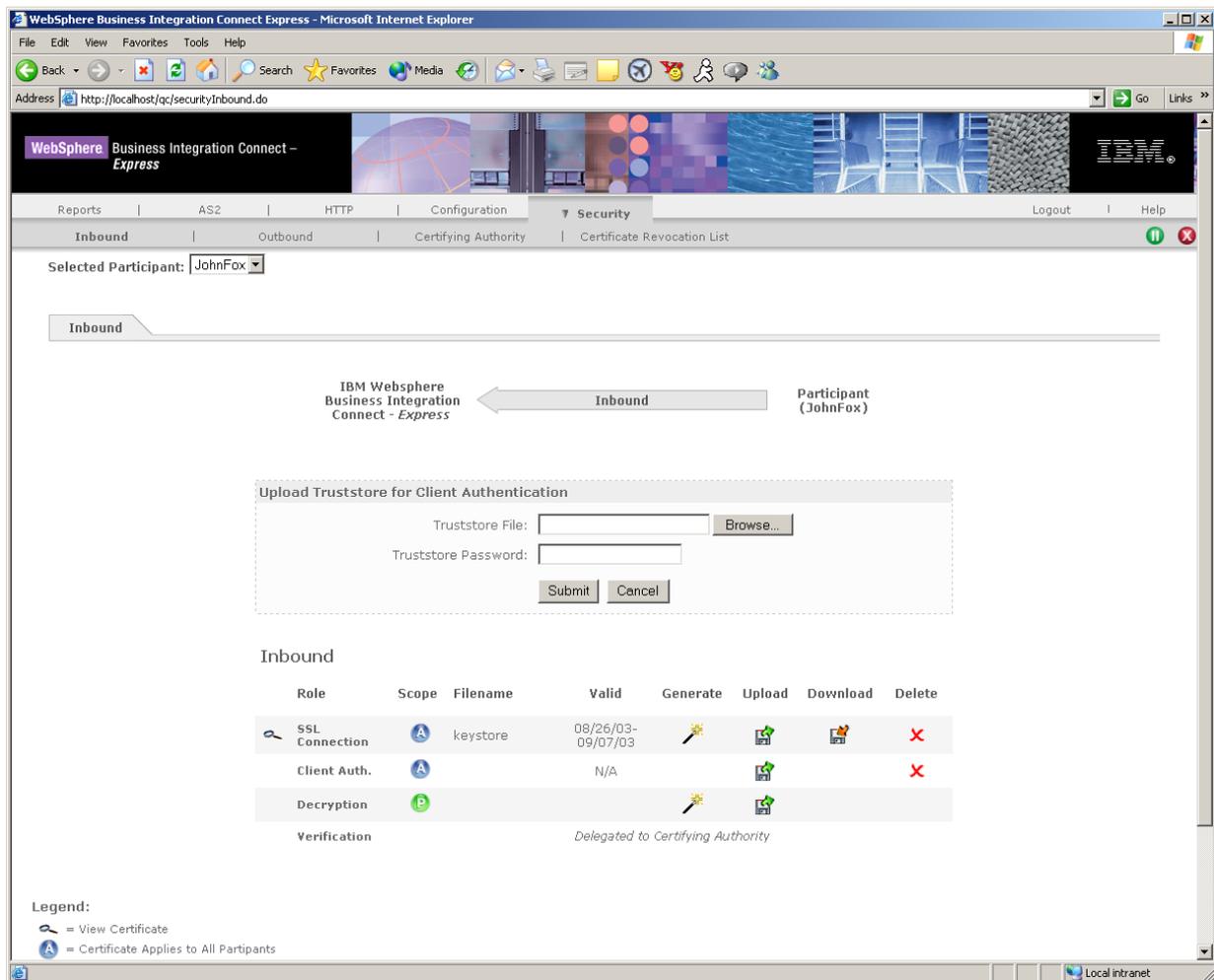


Figure 5-6. Inbound Screen for Uploading a Truststore for Client Authentication

4. Complete the entries in the Inbound screen (see [Table 5-3](#)).
5. Click the **Submit** button. The truststore is uploaded and appears in the Inbound screen.

Table 5-3. Inbound Screen 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.

Deleting the truststore for client authentication

If you no longer need the truststore, use the following procedure to delete it.

1. Click the **Security** menu to display the Inbound screen in [Figure 5-1 on page 49](#). If the screen does not appear, click **Inbound** in the horizontal navigation bar.
2. Under **Delete**, click the  icon in the **Client Auth.** row. The precautionary message in [Figure 5-7](#) appears.



Figure 5-7. Precautionary Message

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

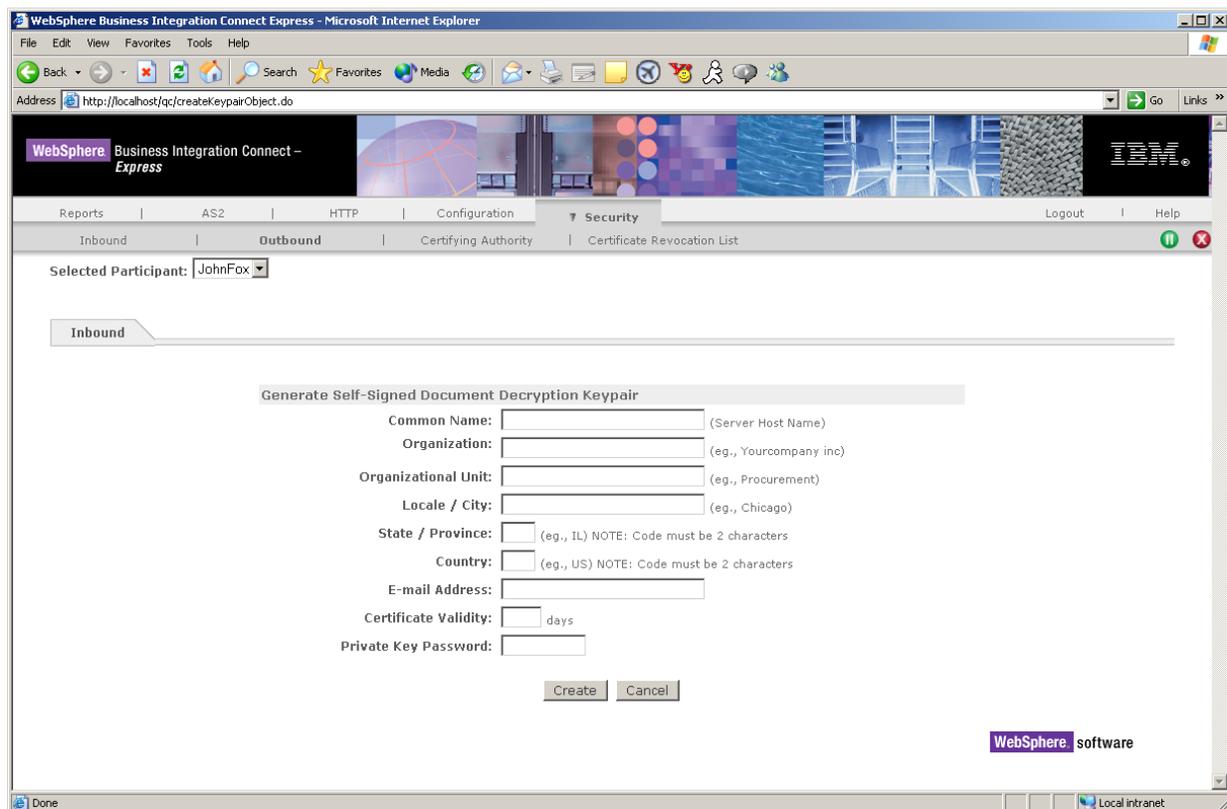
Managing keypairs for decryption

A keypair for decrypting inbound documents can be generated within Business Integration Connect – Express or uploaded into the application. The keypair can then be downloaded or deleted when it is no longer required.

Generating a self-signed document decryption keypair

The following procedure describes how to use WebSphere Business Integration Connect– Express to generate a self-signed decryption keypair for securing inbound documents. When you generate a self-signed decryption keypair, it is uploaded into Business Integration Connect – Express automatically.

1. Click the **Security** menu to display the Inbound screen in [Figure 5-1 on page 49](#). If the screen 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 **Generate**, click the  icon in the **Decryption** row. The Inbound screen in [Figure 5-8](#) appears.



The screenshot shows the WebSphere Business Integration Connect Express interface in a Microsoft Internet Explorer browser window. The address bar shows the URL `http://localhost/qc/createkeypairObject.do`. The navigation bar includes tabs for Reports, AS2, HTTP, Configuration, Security, Logout, and Help. The Security tab is active, and the Inbound screen is displayed. The Selected Participant is set to JohnFox. The Inbound screen contains a form titled "Generate Self-Signed Document Decryption Keypair" with the following fields:

- Common Name: (Server Host Name)
- Organization: (eg., Yourcompany inc)
- Organizational Unit: (eg., Procurement)
- Locale / City: (eg., Chicago)
- State / Province: (eg., IL) NOTE: Code must be 2 characters
- Country: (eg., US) NOTE: Code must be 2 characters
- E-mail Address:
- Certificate Validity: days
- Private Key Password:

At the bottom of the form are "Create" and "Cancel" buttons. The WebSphere software logo is visible in the bottom right corner of the page.

Figure 5-8. Inbound Screen for Generating a Self-Signed Document Decryption Keypair

4. Complete the entries in the Inbound screen (see [Table 5-4](#)).
5. Click the **Create** button. The self-signed keypair is uploaded and appears in the Inbound screen.

Table 5-4. Inbound Screen 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 a decryption keypair

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

1. Click the **Security** menu to display the Inbound screen in [Figure 5-1 on page 49](#). If the screen 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 screen in [Figure 5-9](#) appears.

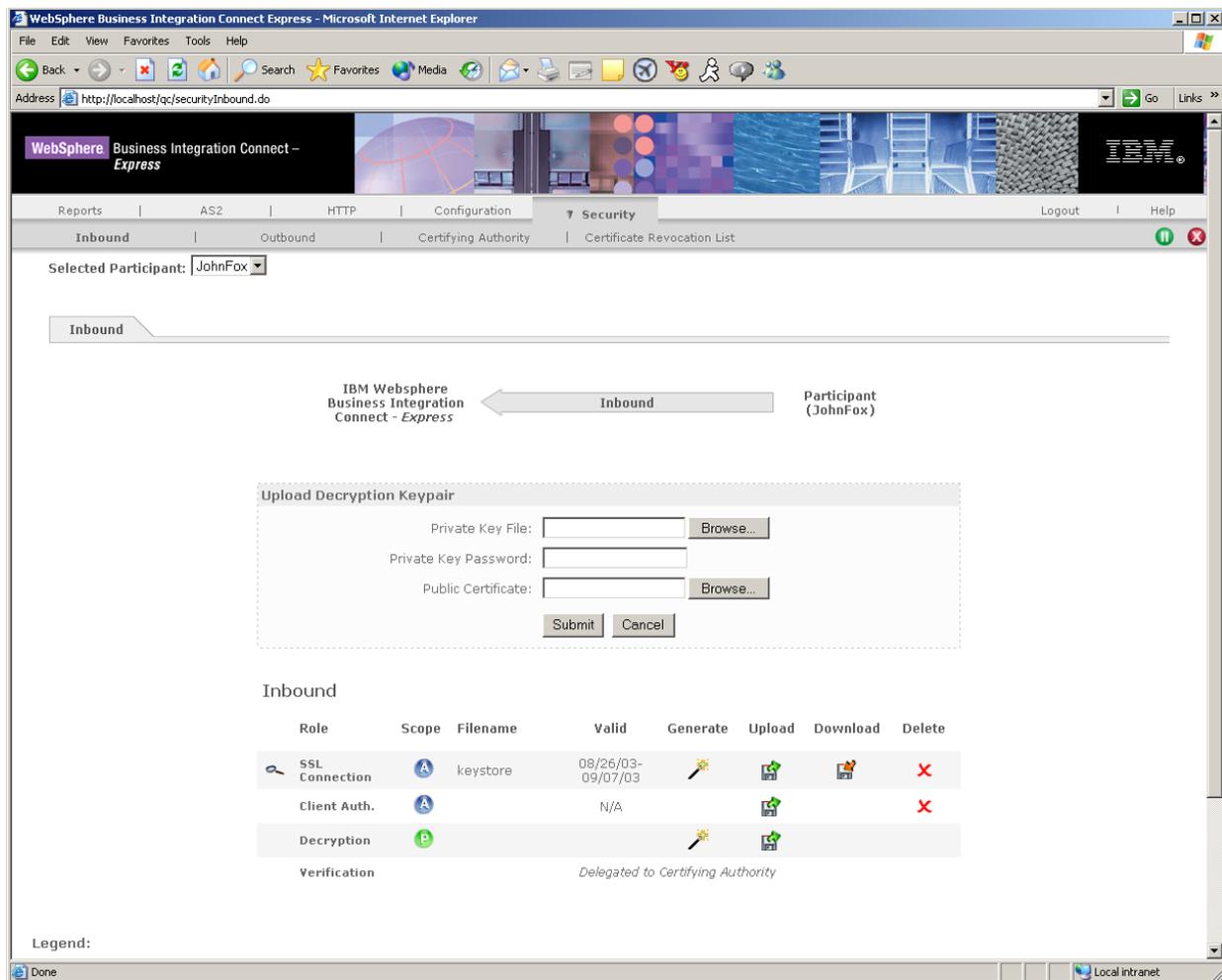


Figure 5-9. Inbound Screen for Uploading a Keypair for Decryption

4. Complete the entries in the Inbound screen (see [Table 5-5 on page 63](#)).
5. Click the **Submit** button. The decryption pair is uploaded and appears in the Inbound screen.

Table 5-5. Inbound Screen for Uploaded Keypair for Decryption

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 public certificate for decryption

After you upload a keypair into WebSphere Business Integration Connect–Express, you can use the following procedure to download the public certificate. 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 screen in [Figure 5-1 on page 49](#). If the screen 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. Under **Download**, click the  icon in the **Decryption** row. A File Download screen appears.
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.)

Deleting a keypair for decryption

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

1. Click the **Security** menu to display the Inbound screen in [Figure 5-1 on page 49](#). If the screen does not appear, click **Inbound** in the horizontal navigation bar.
2. Next to **Selected Participant**, select the participant whose keypair you want to delete.
3. Under **Delete**, click the  icon in the **Decryption** row. The precautionary message in [Figure 5-10](#) appears.



Figure 5-10. Precautionary Message

4. Click **OK** to delete the keypair or **Cancel** to retain it.

Securing outbound transactions

Business Integration Connect – Express uses keypairs and public certificates to secure outbound transactions.

- A keypair is used for client authentication and verification. See [“Managing keypairs for client authentication,”](#) below.
- Public certificates are used for encrypting outbound documents. See [“Managing encryption certificates”](#) on page 69.

Managing keypairs for client authentication

For outbound documents, client authentication is where Business Integration Connect – Express identifies itself to a remote server.

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 screen in [Figure 5-11 on page 65](#) appears.

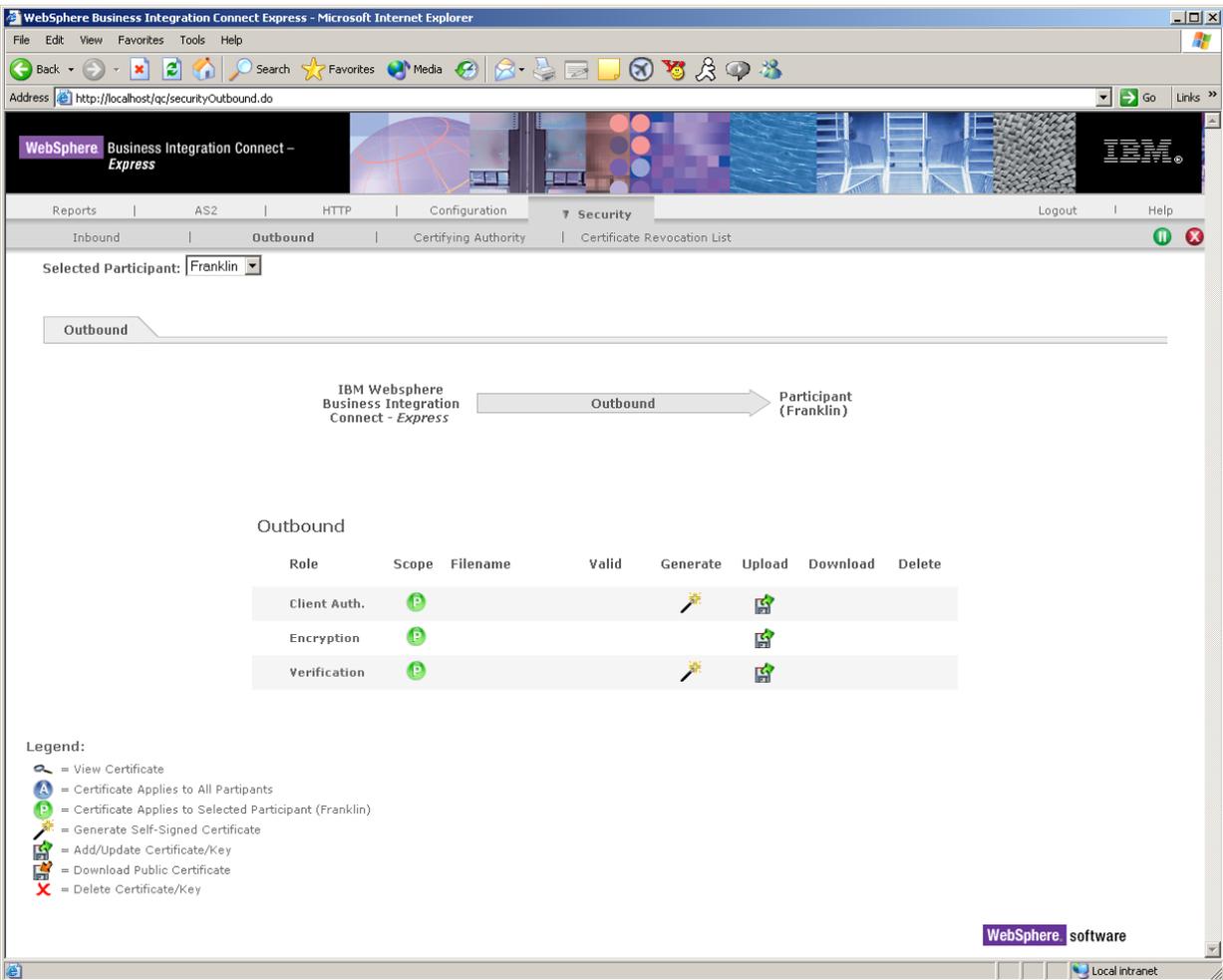


Figure 5-11. Outbound Screen

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 screen in [Figure 5-12 on page 66](#) appears.

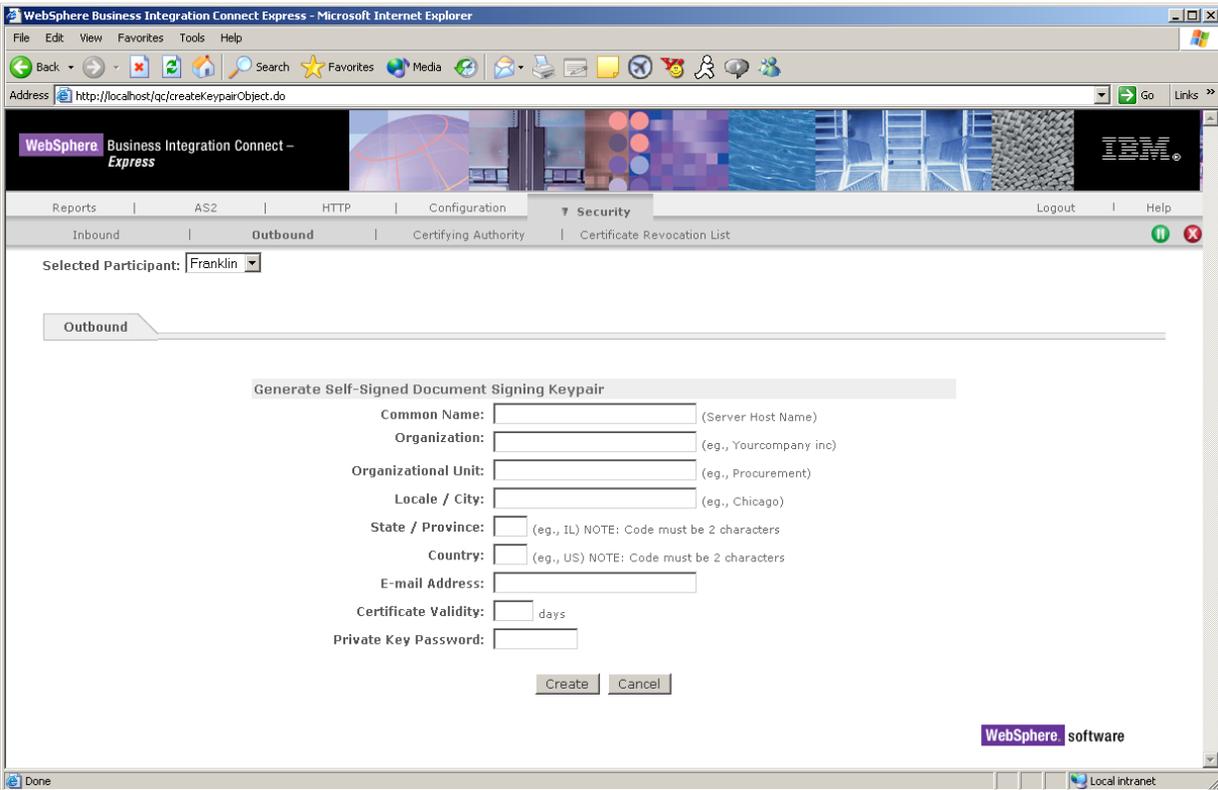


Figure 5-12. Outbound Screen for Generating a Self-Signed SSL Client Certificate Keypair

4. Complete the entries in the Outbound screen (see [Table 5-6](#)).
5. Click the **Create** button. The self-signed keystore is uploaded and appears in the Outbound screen.

Table 5-6. Outbound Screen 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 screen in [Figure 5-11 on page 65](#) appears.
2. Next to **Selected Participant**, select the participant for whom you want to upload the keypair.
3. Under **Generate**, click the  icon in the **Client Auth.** row. The Outbound screen in [Figure 5-13](#) appears.

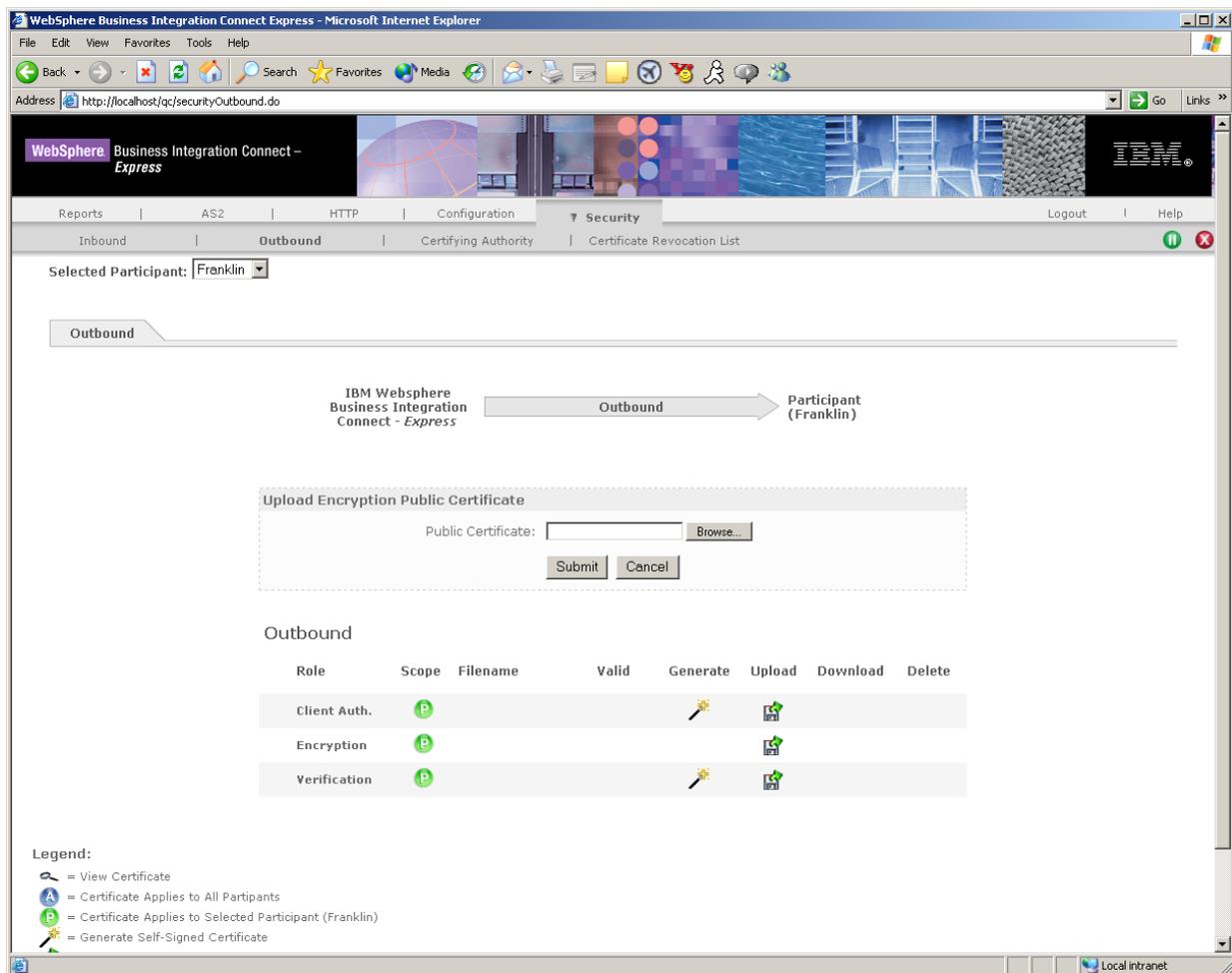


Figure 5-13. Outbound Screen for Uploading a Client Authentication Keypair

4. Complete the entries in the Outbound screen (see [Table 5-7 on page 68](#)).
5. Click the **Submit** button. The keypair is uploaded and appears in the Outbound screen.

Table 5-7. Outbound Screen 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 screen in [Figure 5-11 on page 65](#) appears.
2. Next to **Selected Participant**, select the participant whose keypair you want to download.
3. Under **Download**, click the  icon in the **Client Auth.** row. A File Download screen 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.)

Deleting a keypair for client authentication

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

1. Click the **Security** menu, then click **Outbound** in the horizontal navigation bar. The Outbound screen in [Figure 5-11 on page 65](#) appears.
2. Next to **Selected Participant**, select the participant whose keypair you want to delete.
3. Under **Delete**, click the  icon in the **Client Auth.** row. The precautionary message in [Figure 5-14](#) appears.



Figure 5-14. Precautionary Message

4. Click **OK** to delete the keypair or **Cancel** to retain it.

Managing encryption certificates

A public certificate for encrypting outbound documents can be uploaded into Business Integration Connect – Express. Typically, the public certificate will originate from a host that wants to receive encrypted outbound documents from you for decryption with their private key. (This is the reverse of the inbound decryption process.)

Uploading an encryption public certificate

To upload an encryption public certificate for securing outbound documents, use the following procedure.

1. Click the **Security** menu, then click **Outbound** in the horizontal navigation bar. The Outbound screen in [Figure 5-11 on page 65](#) appears.
2. Next to **Selected Participant**, select the participant for whom you want to upload the encryption public certificate.
3. Under **Generate**, click the  icon in the **Encryption** row. The Outbound screen in [Figure 5-15 on page 70](#) appears.

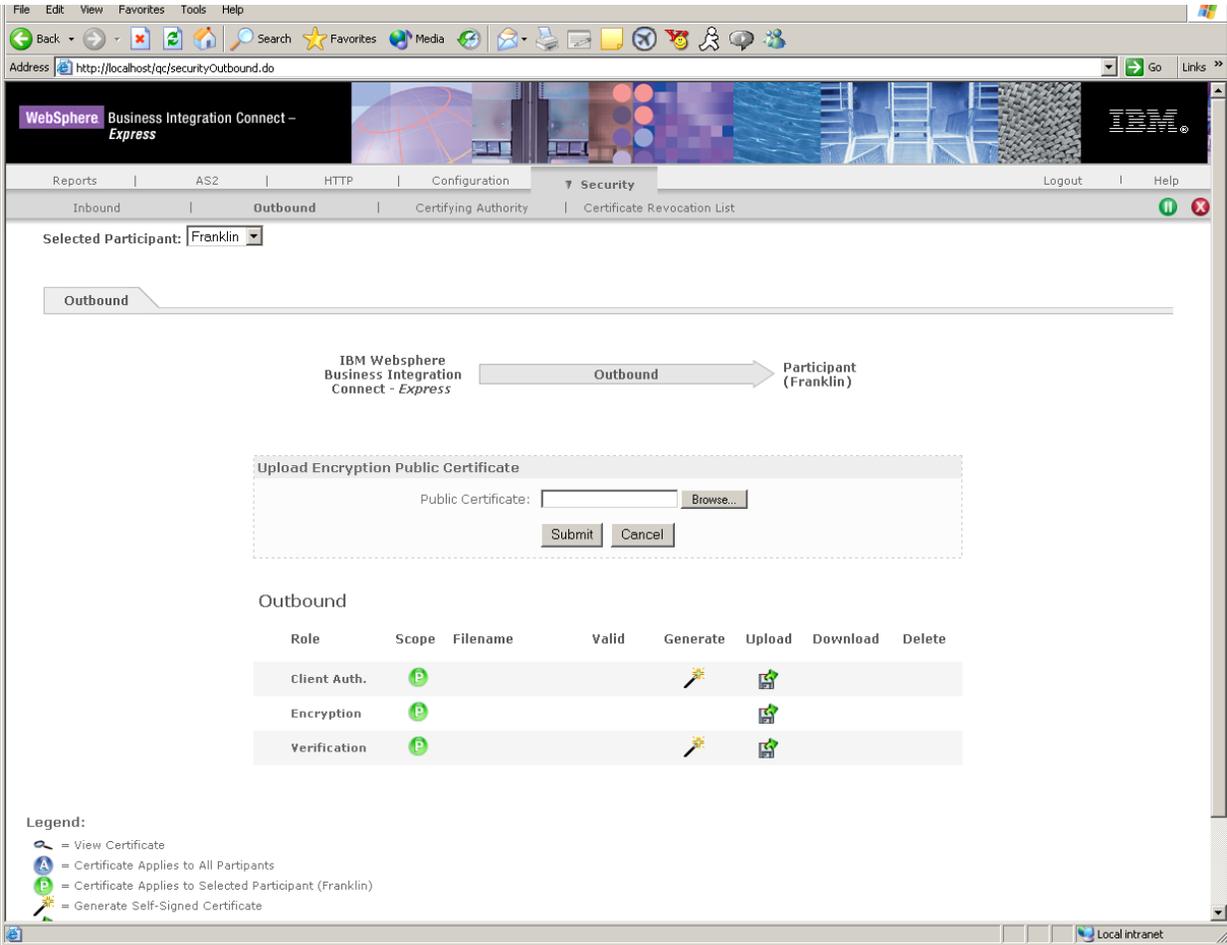


Figure 5-15. Outbound Screen for Uploading an Encryption Public Certificate

4. Complete the entry in the Outbound screen (see [Table 5-8](#)).
5. Click the **Submit** button.

Table 5-8. Outbound Screen for Uploaded Encryption Public Certificate

Parameter	Description
Public Certificate File	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 an encryption public certificate

After you upload an encryption public certificate into WebSphere Business Integration Connect-Express, you can use the following procedure to download it.

1. Click the **Security** menu, then click **Outbound** in the horizontal navigation bar. The Outbound screen in [Figure 5-11 on page 65](#) appears.
2. Next to **Selected Participant**, select the participant whose encryption public certificate you want to download.
3. Under **Download**, click the  icon in the **Encryption** row. A File Download screen appears.
4. Click **Save** to display the Save As dialog box, select a location where you want to download the encryption public certificate, and click **Save**. (Or click **Open** to open the encryption public certificate file, **Cancel** to cancel the operation, or **More Info** to obtain more information.)

Deleting an encryption public certificate

If you no longer need an encryption public certificate for a participant, use the following procedure to delete it.

1. Click the **Security** menu, then click **Outbound** in the horizontal navigation bar. The Outbound screen in [Figure 5-11 on page 65](#) appears.
2. Next to **Selected Participant**, select the participant whose encryption public certificate you want to delete.
3. Under **Delete**, click the  icon in the **Encryption** row. The precautionary message in [Figure 5-16](#) appears.



Figure 5-16. Precautionary Message

4. Click **OK** to delete the encryption public certificate or **Cancel** to retain it.

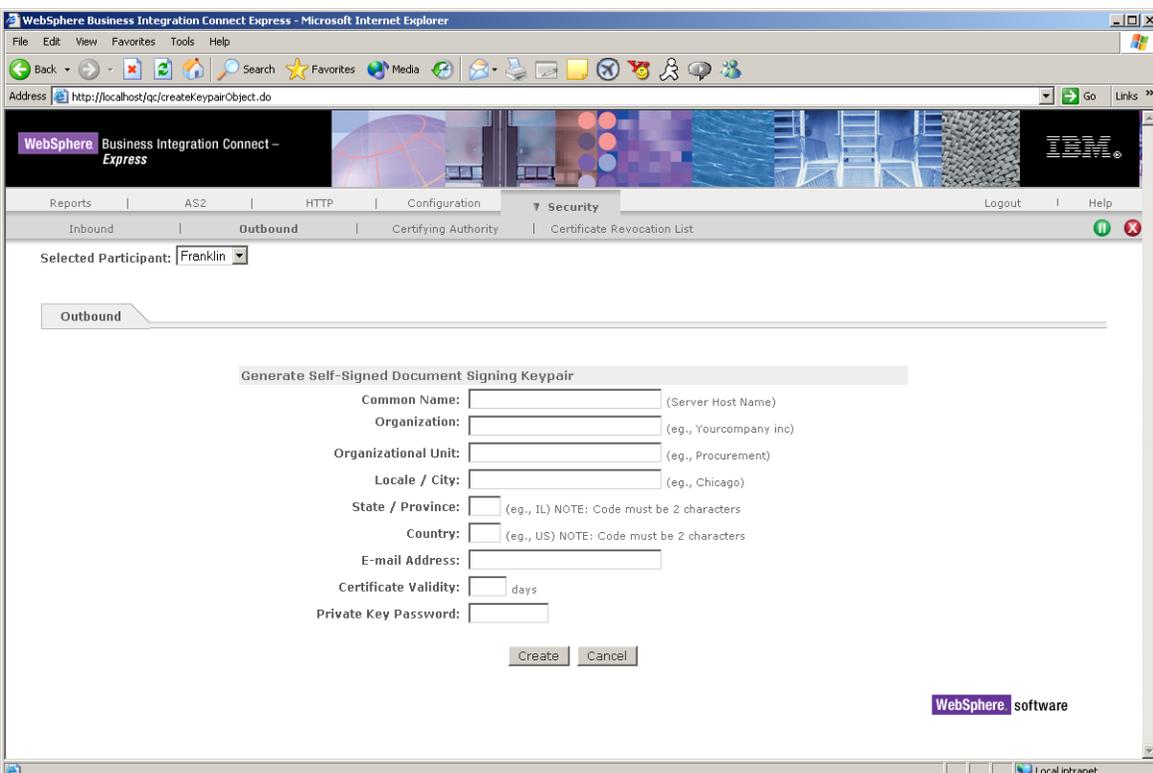
Managing keypairs for digital signatures

A keypair for digital signatures can be generated within Business Integration Connect – Express or uploaded into the application. The keypair can then be downloaded or deleted when it is no longer required.

Generating a self-signed document signing keypair

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 screen in [Figure 5-11 on page 65](#) 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 **Verification** row. The Outbound screen in [Figure 5-17](#) appears.



The screenshot shows the WebSphere Business Integration Connect Express interface in Microsoft Internet Explorer. The browser address bar shows <http://localhost/qc/createKeypairObject.do>. The application header includes the WebSphere logo and the text "Business Integration Connect – Express". The navigation bar shows "Reports", "AS2", "HTTP", "Configuration", "Security", "Logout", and "Help". The "Security" menu is expanded, showing "Inbound", "Outbound", "Certifying Authority", and "Certificate Revocation List". The "Outbound" tab is selected. Below the navigation bar, the "Selected Participant" is set to "Franklin". The main content area is titled "Outbound" and contains a form titled "Generate Self-Signed Document Signing Keypair". The form fields are: Common Name (Server Host Name), Organization (eg., Yourcompany inc), Organizational Unit (eg., Procurement), Locale / City (eg., Chicago), State / Province (eg., IL) NOTE: Code must be 2 characters, Country (eg., US) NOTE: Code must be 2 characters, E-mail Address, Certificate Validity (days), and Private Key Password. There are "Create" and "Cancel" buttons at the bottom of the form. The WebSphere software logo is visible in the bottom right corner of the application window.

Figure 5-17. Outbound Screen for Generating a Self-Signed Document Signing Keypair

4. Complete the entries in the Outbound screen (see [Table 5-9 on page 73](#)).
5. Click the **Create** button. The self-signed keypair is uploaded and appears in the Outbound screen.

Table 5-9. Outbound Screen 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 a document signing keypair

To upload a 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 screen in [Figure 5-11 on page 65](#) appears.
2. Next to **Selected Participant**, select the participant for whom you want to upload the keypair.
3. Under **Generate**, click the  icon in the **Verification** row. The Inbound screen in [Figure 5-18 on page 74](#) appears.

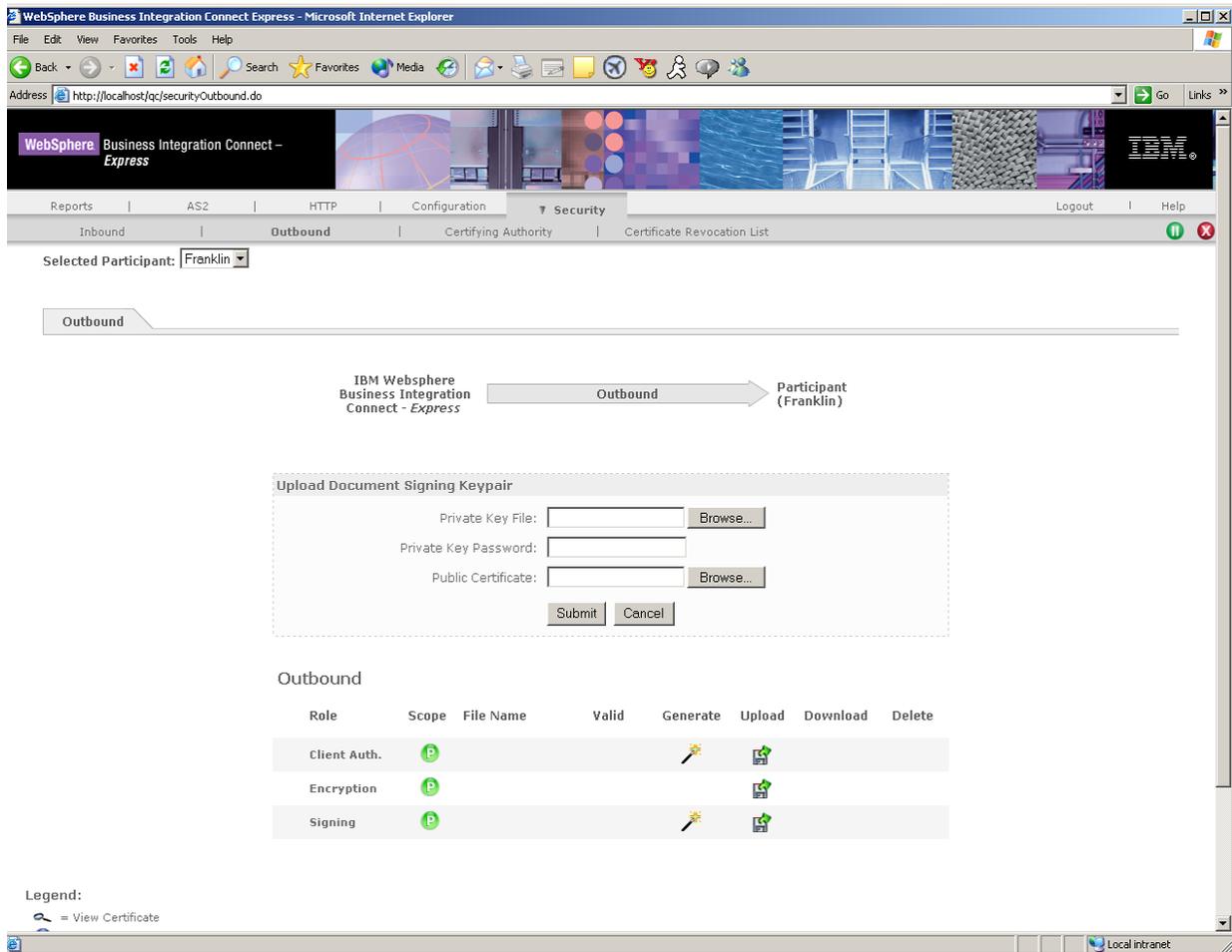


Figure 5-18. Outbound Screen for Uploading a Document Signing Keypair

4. Complete the entries in the Outbound screen (see [Table 5-10](#)).
5. Click the **Submit** button. The keypair is uploaded and appears in the Outbound screen.

Table 5-10. Outbound Screen 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 can use the following procedure to download the keypair’s public certificate. 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 76).

1. Click the **Security** menu, then click **Outbound** in the horizontal navigation bar. The Outbound screen in [Figure 5-11 on page 65](#) 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 **Verification** row. A File Download screen appears.
4. Click **Save** to display the Save As dialog box, select a location where you want to download the document signing public certificate, and click **Save**. (Or click **Open** to open the document signing public certificate file, **Cancel** to cancel the operation, or **More Info** to obtain more information.)

Deleting a document signing keypair

If you no longer need a document signing keypair for a participant, use the following procedure to delete it.

1. Click the **Security** menu, then click **Outbound** in the horizontal navigation bar. The Outbound screen in [Figure 5-11 on page 65](#) appears.
2. Next to **Selected Participant**, select the participant whose document signing keypair you want to delete.
3. Under **Delete**, click the  icon in the **Verification** row. The precautionary message in [Figure 5-19](#) appears.



Figure 5-19. Precautionary Message

4. Click **OK** to delete the document signing keypair or **Cancel** to retain it.

Adding certificates from certifying authorities

Using the Certifying Authority screen, 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 screen in [Figure 5-20](#) appears.

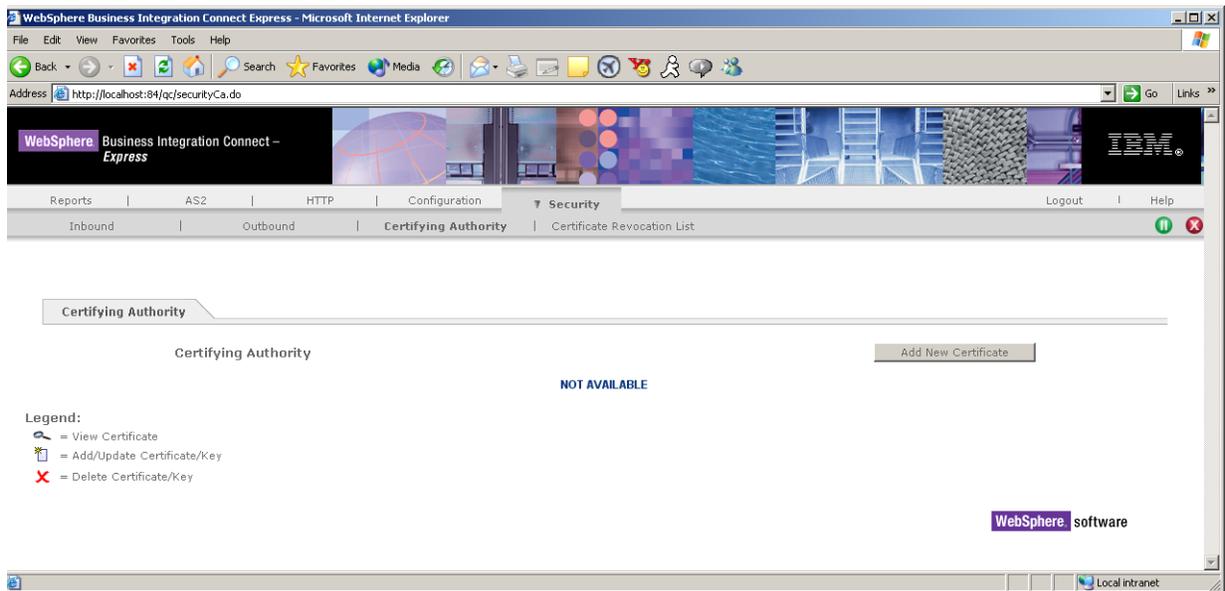


Figure 5-20. Certifying Authority Screen

2. Click the **Add New Certificate** button. The Certifying Authority screen changes to the one shown in [Figure 5-21 on page 77](#).

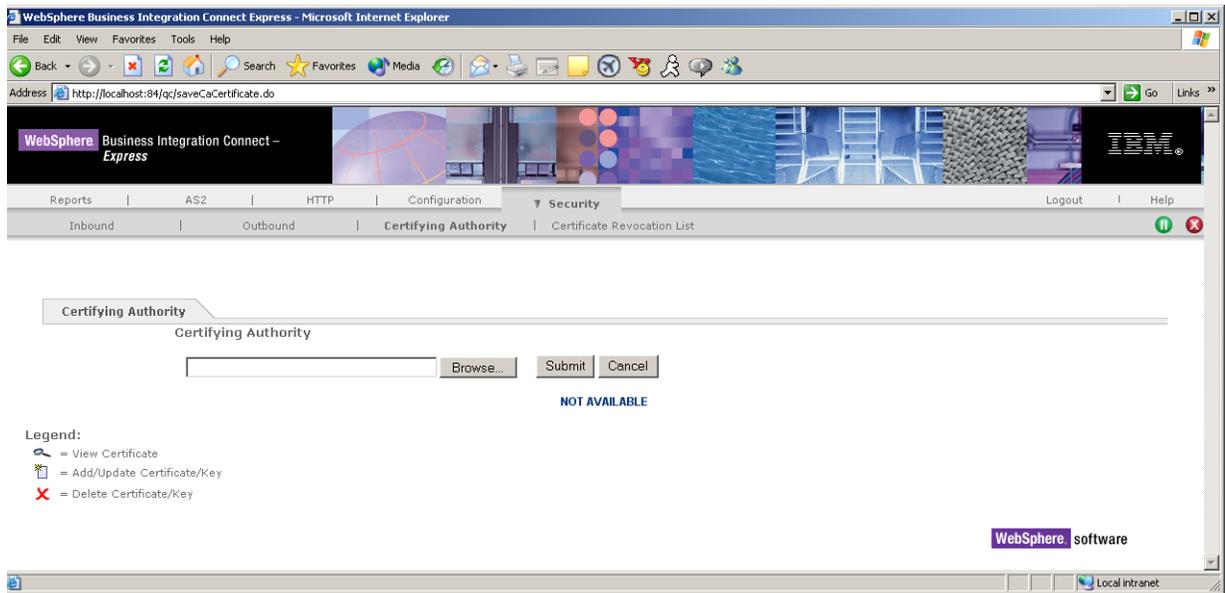


Figure 5-21. Screen for Adding a New Certificate

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 screen.
5. Click the **Submit** button. The certificate is added to Business Integration Connect - Express and its name appears in the Certifying Authority screen.
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 screen in [Figure 5-20 on page 76](#) appears.
2. In the **Delete** column, click the  icon for the certificate you want to delete. The precautionary message in [Figure 5-22 on page 78](#) appears.



Figure 5-22. Precautionary Message when Deleting a Certificate

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

Working with certification revocation lists

Using the Certificate Revocation List screen, 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 screen in [Figure 5-23](#) appears.

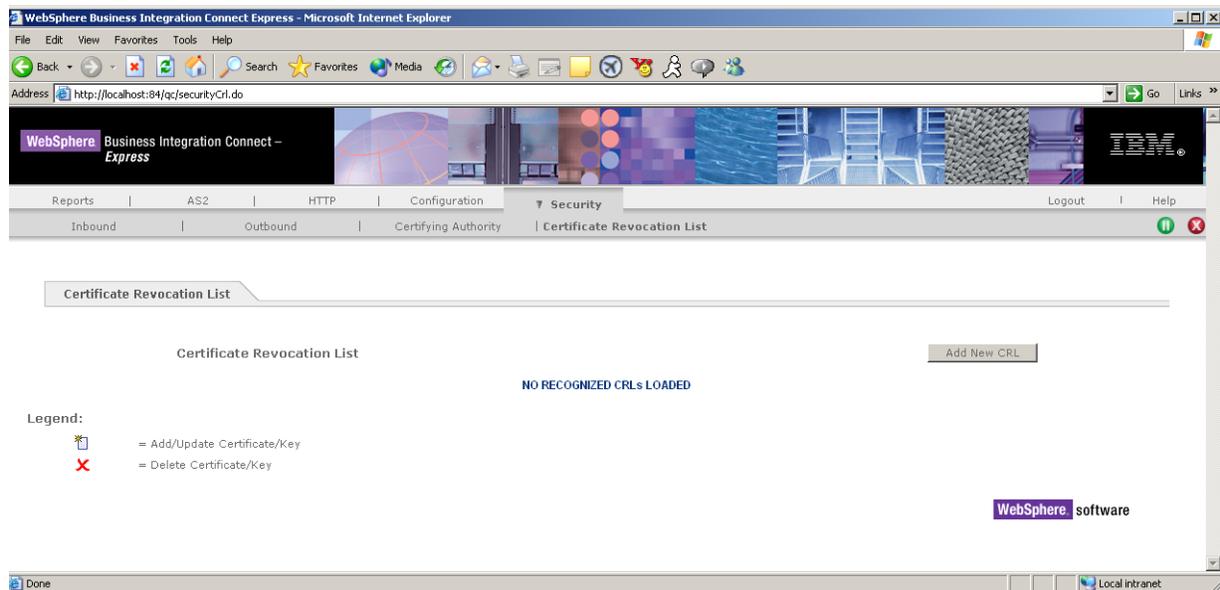


Figure 5-23. Certificate Revocation List Screen

2. Click the **Add New CRL** button. The Certificate Revocation List changes to the one shown in [Figure 5-24 on page 79](#).

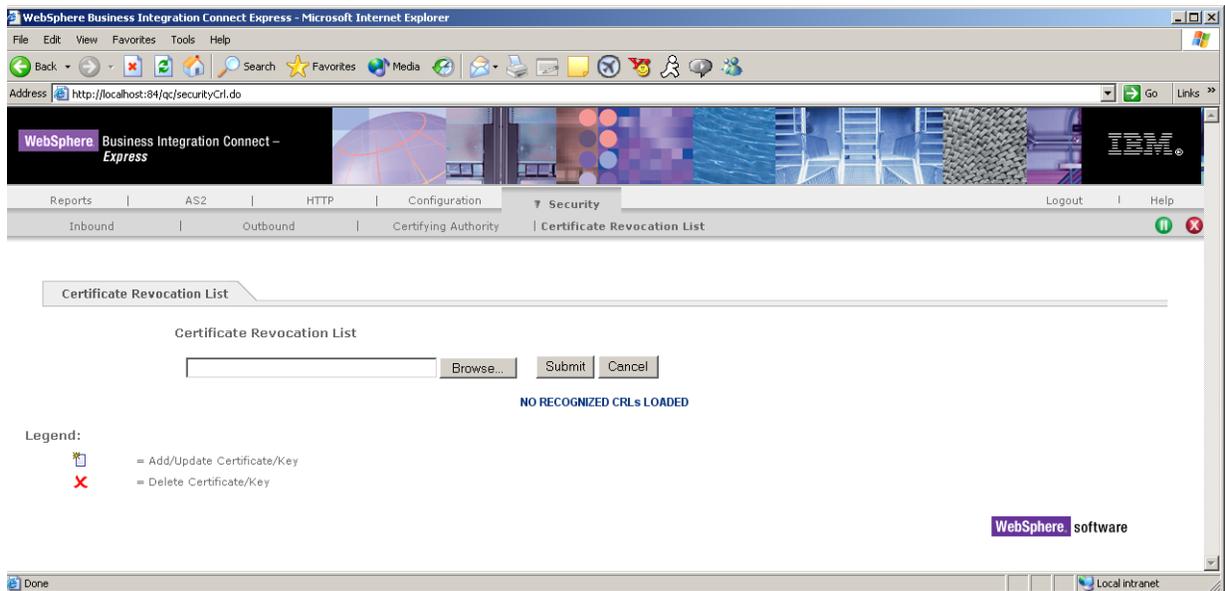


Figure 5-24. Screen for Adding a New CRL

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 screen.
5. Click the **Submit** button. The CRL is added to Business Integration Connect - Express and its name appears in the Certificate Revocation List screen (see [Figure 5-25 on page 80](#)).
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 screen similar to the one in [Figure 5-25 on page 80](#) appears.

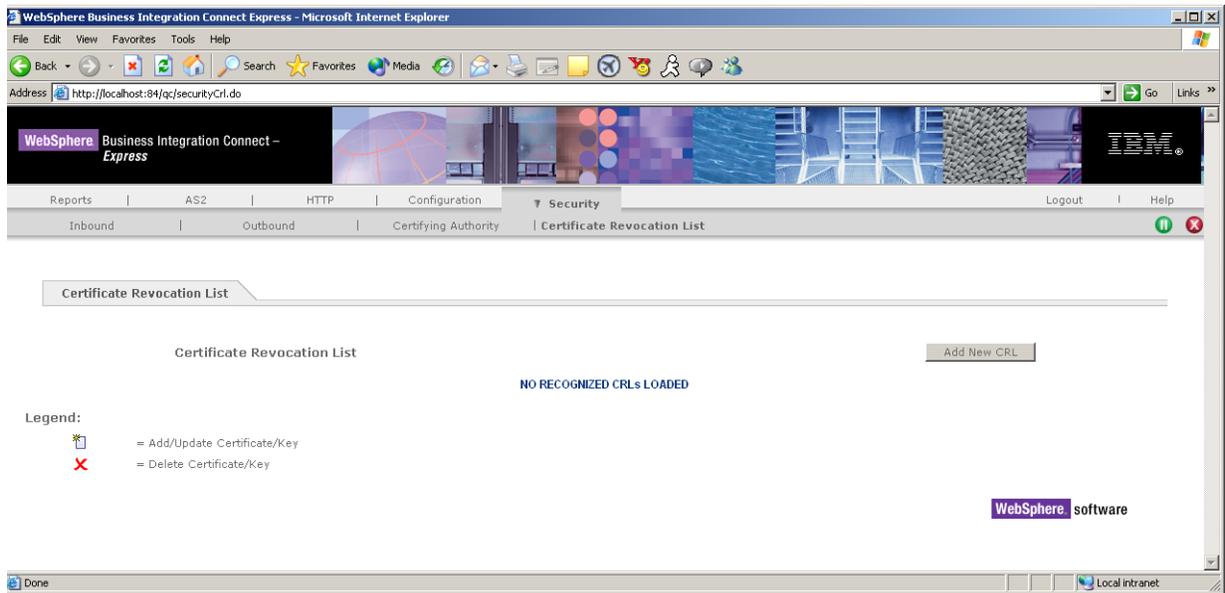


Figure 5-25. Certificate Revocation List Screen

2. In the **Delete** column, click the  icon for the CRL you want to delete. The precautionary message in [Figure 5-26](#) appears.

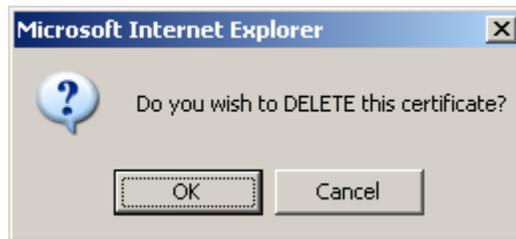


Figure 5-26. Precautionary Message when Deleting a CRL

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

Chapter 6. Managing Documents

Overview

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 81](#)
- [“Managing HTTP documents” on page 99](#)

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 screen appears (see [Figure 6-1 on page 82](#)). However, you can use the horizontal navigation bar to access other screens.

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 82](#).
- **Resend** lets you resend AS2 documents that meet your search criteria. See [“Resending AS2 documents” on page 84](#).
- **Sent** lets you view sent AS2 documents that meet your search criteria. See [“Viewing sent AS2 documents” on page 86](#).
- **Pending Transmission** lets you see which AS2 documents are waiting to be transmitted. See [“Viewing pending AS2 documents” on page 93](#).
- **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 95](#).
- **Received** lets you see which received AS2 documents meet your search criteria. See [“Viewing received AS2 documents” on page 97](#).

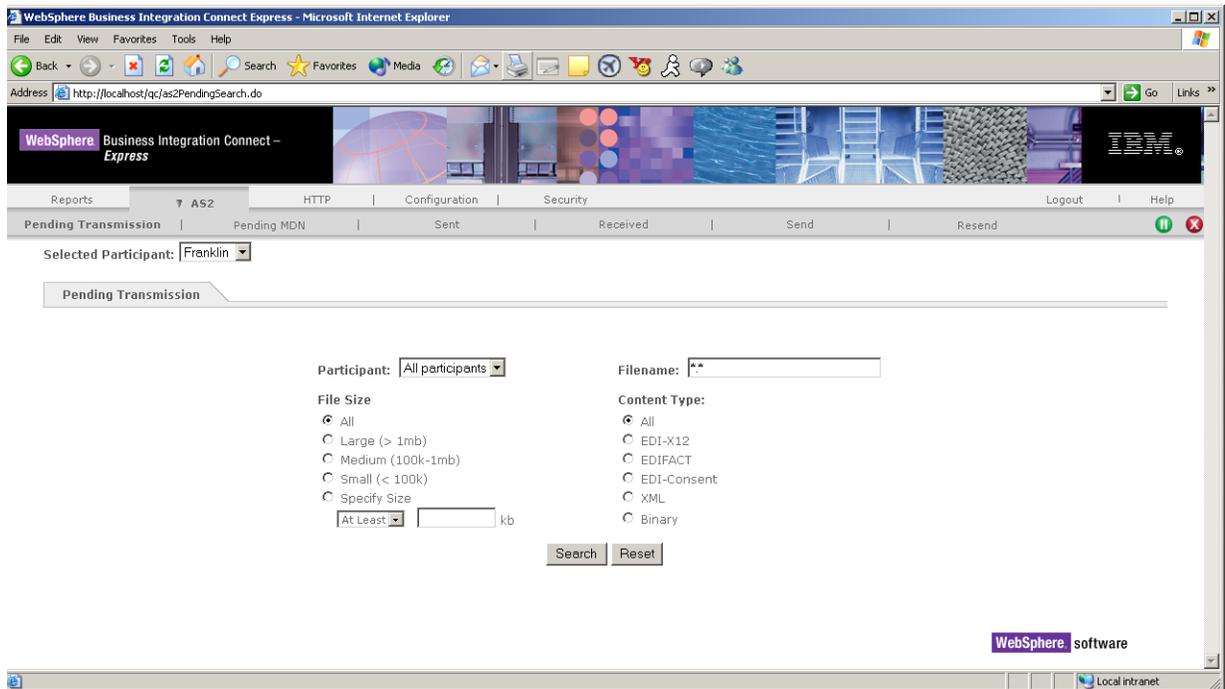


Figure 6-1. AS2 Menu, Pending Transmission Screen

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 screen in [Figure 6-2 on page 83](#) appears.

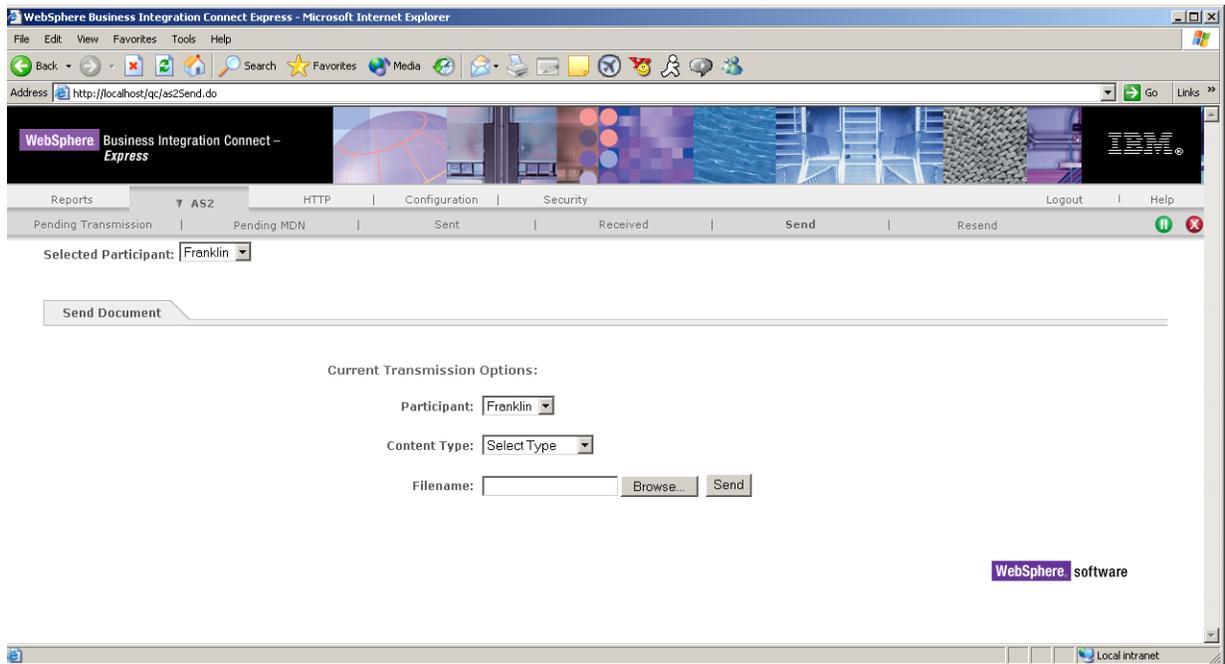


Figure 6-2. Send Document Screen

2. Complete the entries in the Send Document screen (see [Table 6-1](#)).
3. Click the **Send** button. A message in the gray area above **Current Transmission Options** indicates whether the file was uploaded successfully. The document is sent and a message appears, telling you that the document was uploaded.
4. To send additional AS2 documents, repeat steps 2 and 3.

Table 6-1. Send Document Screen

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 screen in [Figure 6-3](#) appears.

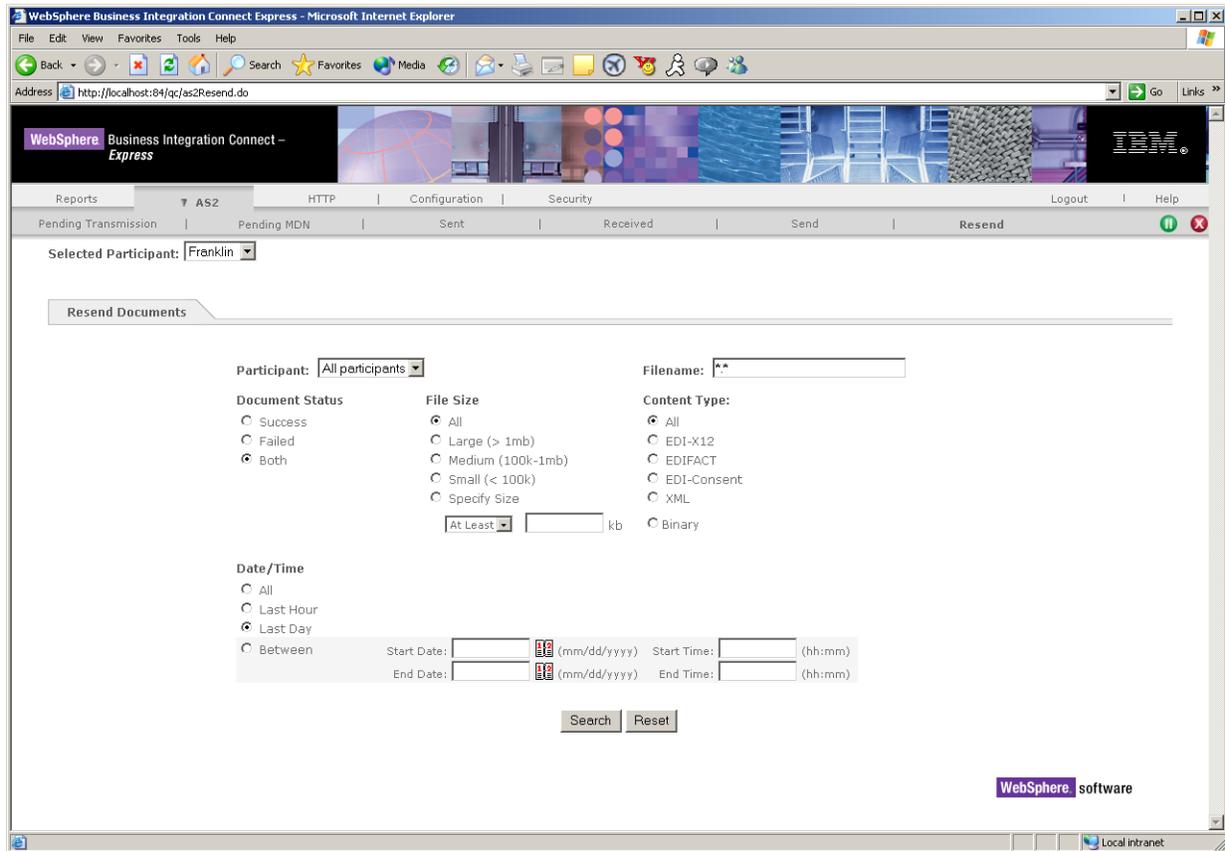


Figure 6-3. Resend Documents Screen

2. Complete the entries in the Resend Document screen (see [Table 6-2 on page 85](#)).
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 screen (see [Figure 6-4 on page 85](#)).

This screen 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.

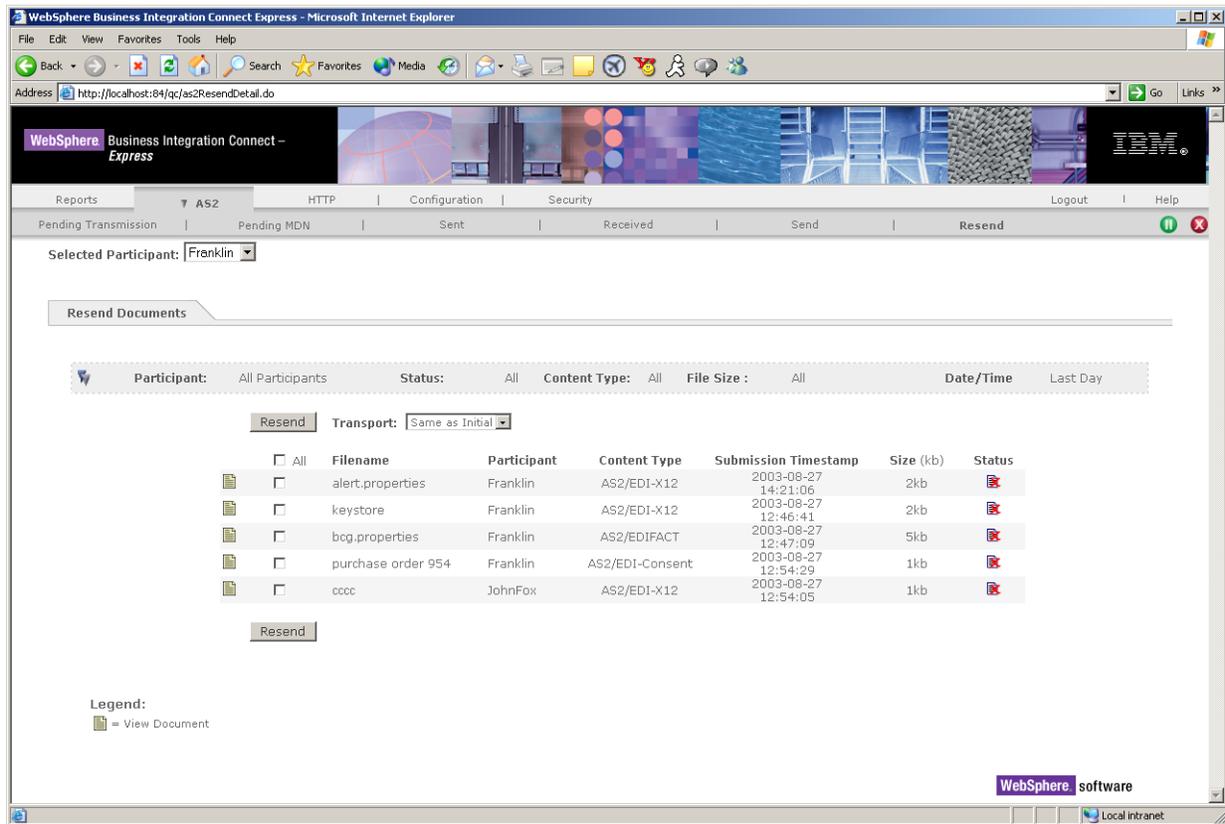


Figure 6-4. Matching Documents Displayed in the Resend Documents Screen

- 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 6-2. Resend Document Screen

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.

Table 6-2. Resend Document Screen

Parameter	Description
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  icon to select dates from a pop-up calendar:



Viewing sent AS2 documents

Using the Sent screen, 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 screen in [Figure 6-5 on page 87](#) appears.

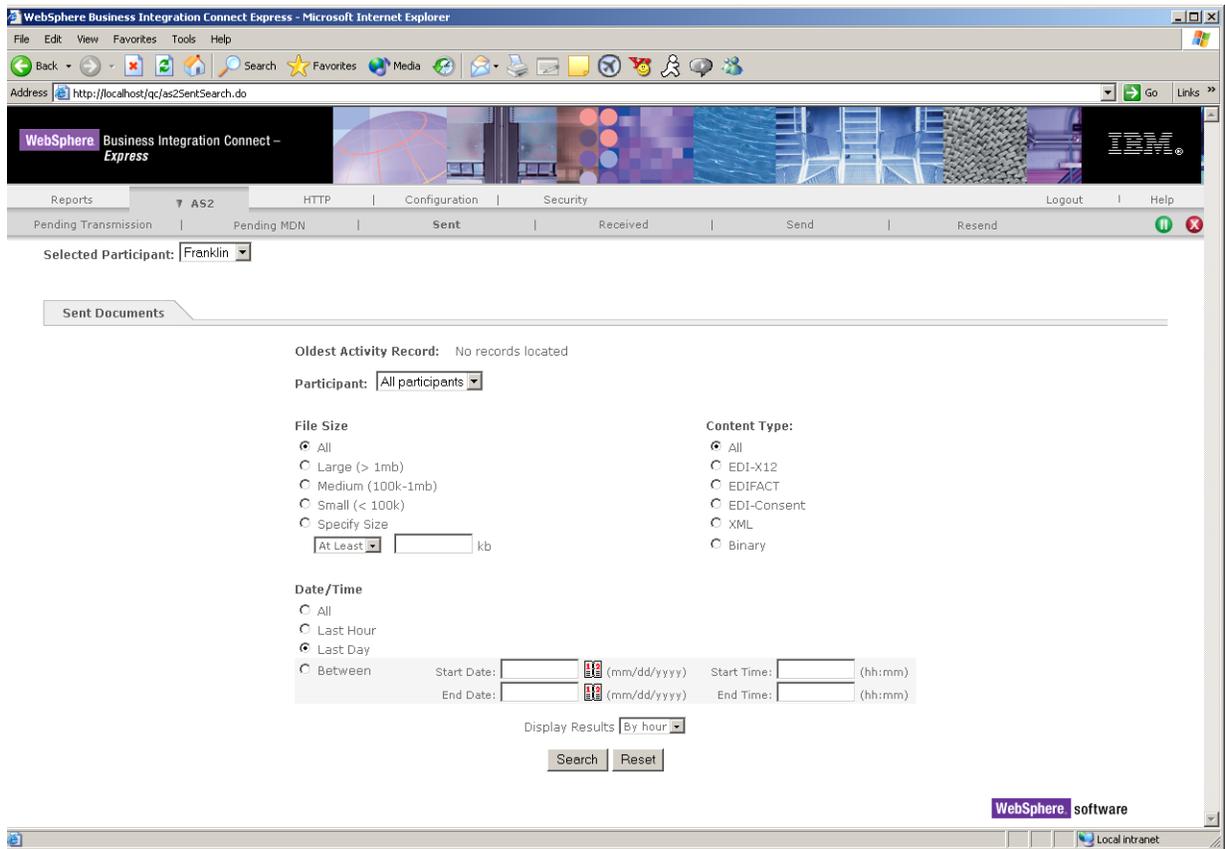


Figure 6-5. Sent Screen

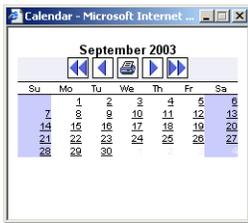
2. Complete the entries in the Sent Documents screen (see [Table 6-3 on page 88](#)).
3. Click the **Search** button. Business Integration Connect – Express displays all the sent AS2 documents that meet your search criteria (see [Figure 6-7 on page 90](#)).
4. To view detailed information about a sent document, click the  icon next to the appropriate document to display the Document Details screen. [Figure 6-6 on page 89](#) shows an example of this screen.

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

- Display sent document results and search criteria fields in one screen by clicking the  icon next to **Participant** at the top of the screen. The screen that appears contains icons for viewing the content of sent documents and search fields for conducting another search. [Figure 6-8 on page 91](#) shows an example of this screen.
- Display the search scope by clicking the  icon next to **Search Scope**. [Figure 6-6 on page 89](#) shows an example of this screen.
- View the contents of a document by clicking the  icon next to the document under **Sent Document Details**.

Table 6-3. Sent Documents Screen

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



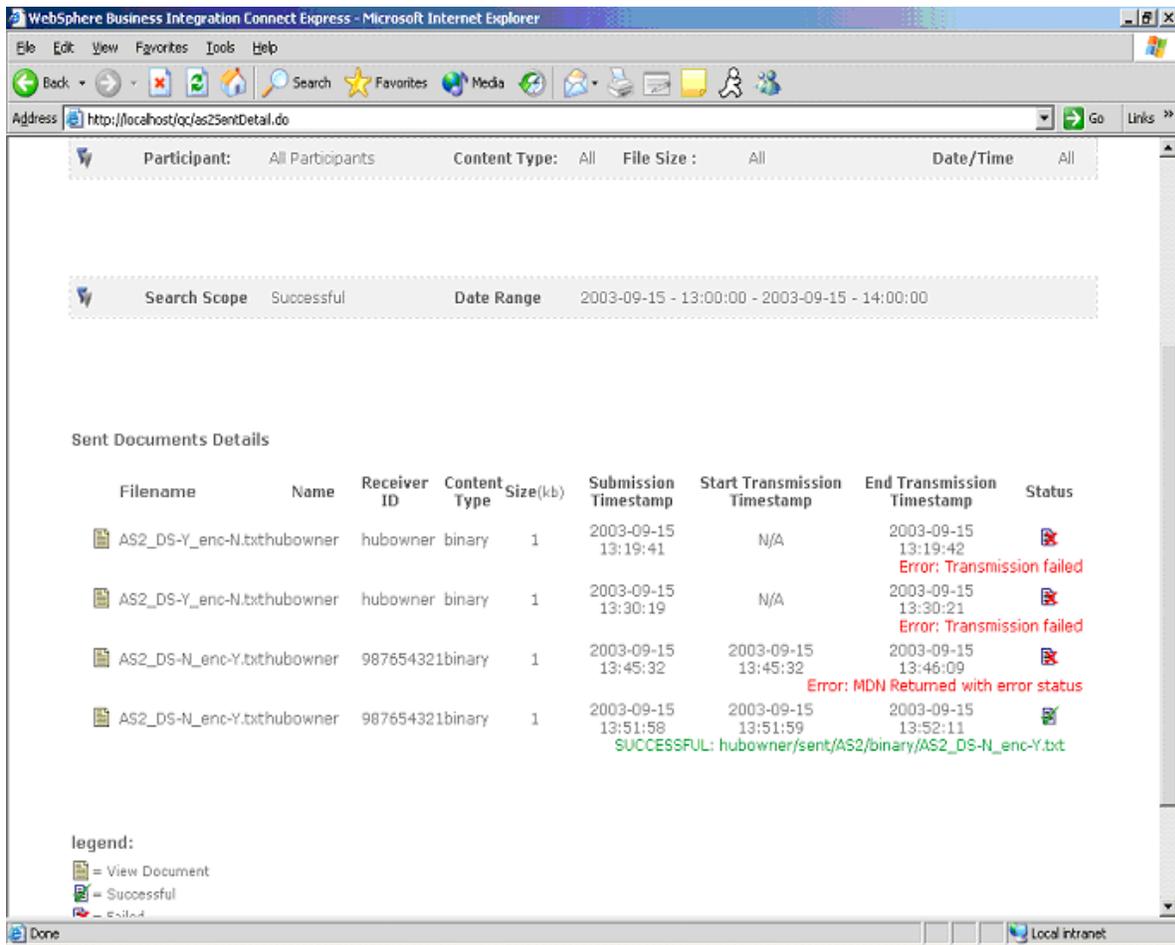


Figure 6-6. Example of Document Details Screen

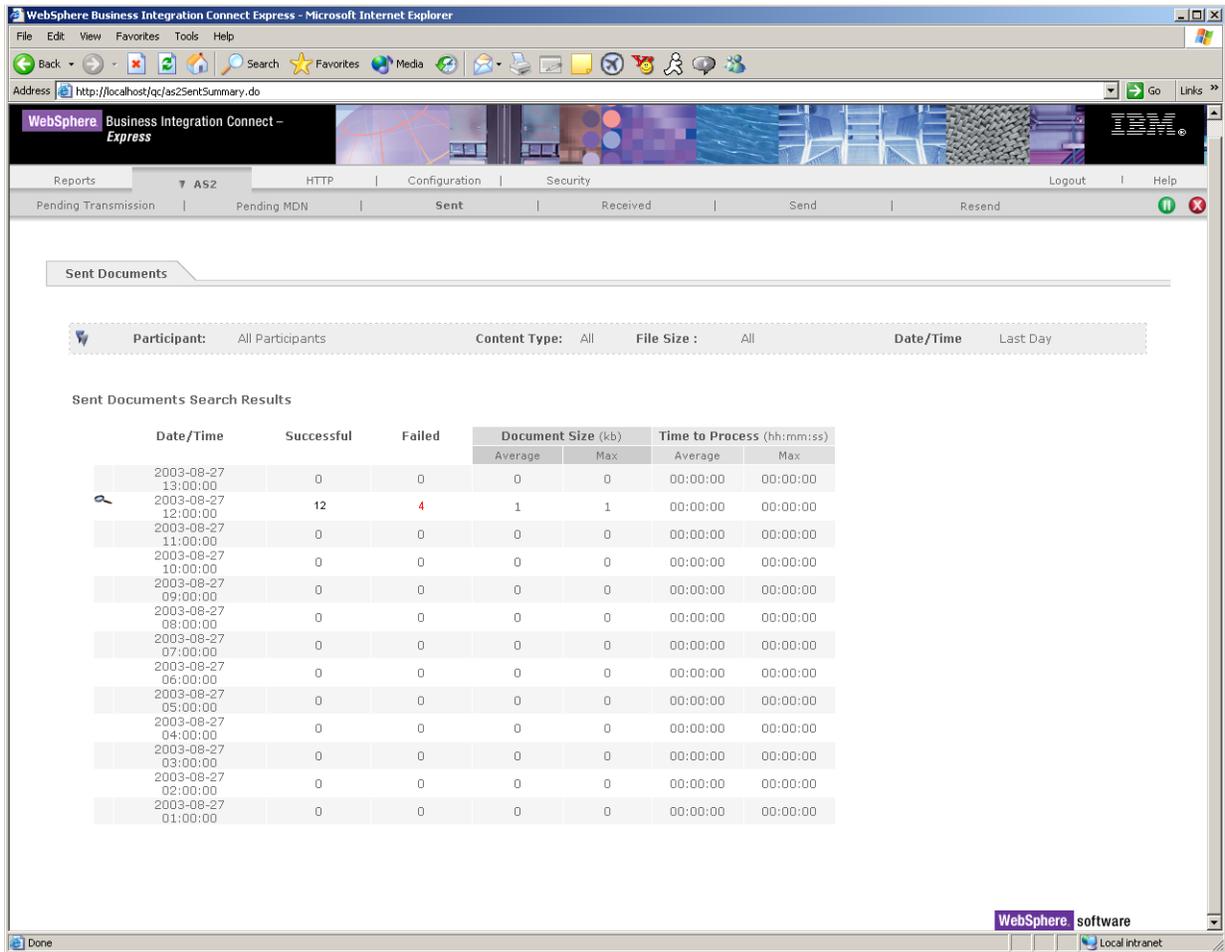


Figure 6-7. Example of Viewing Sent AS2 Documents

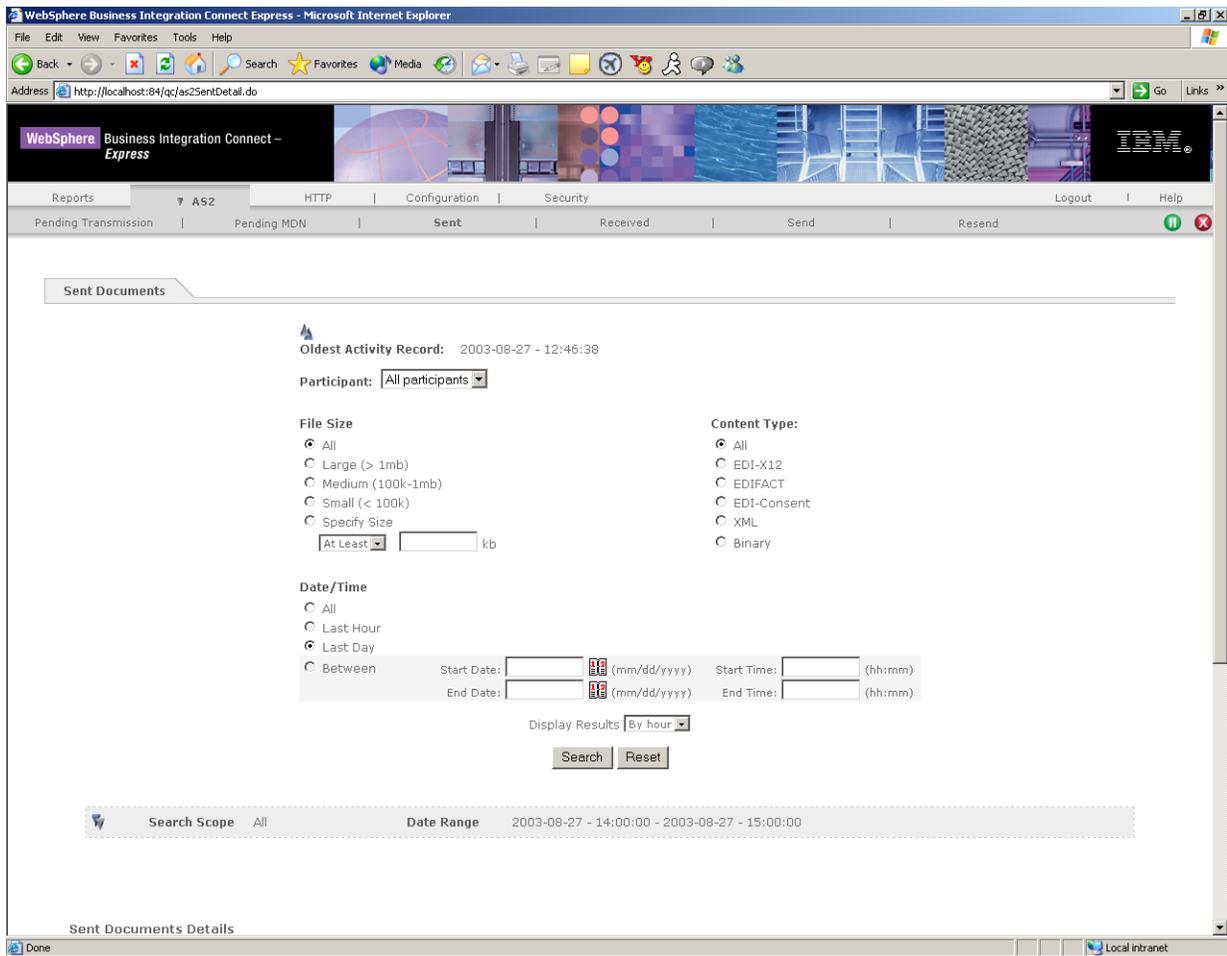


Figure 6-8. Example of a Screen with Search Fields and Sent Document Details

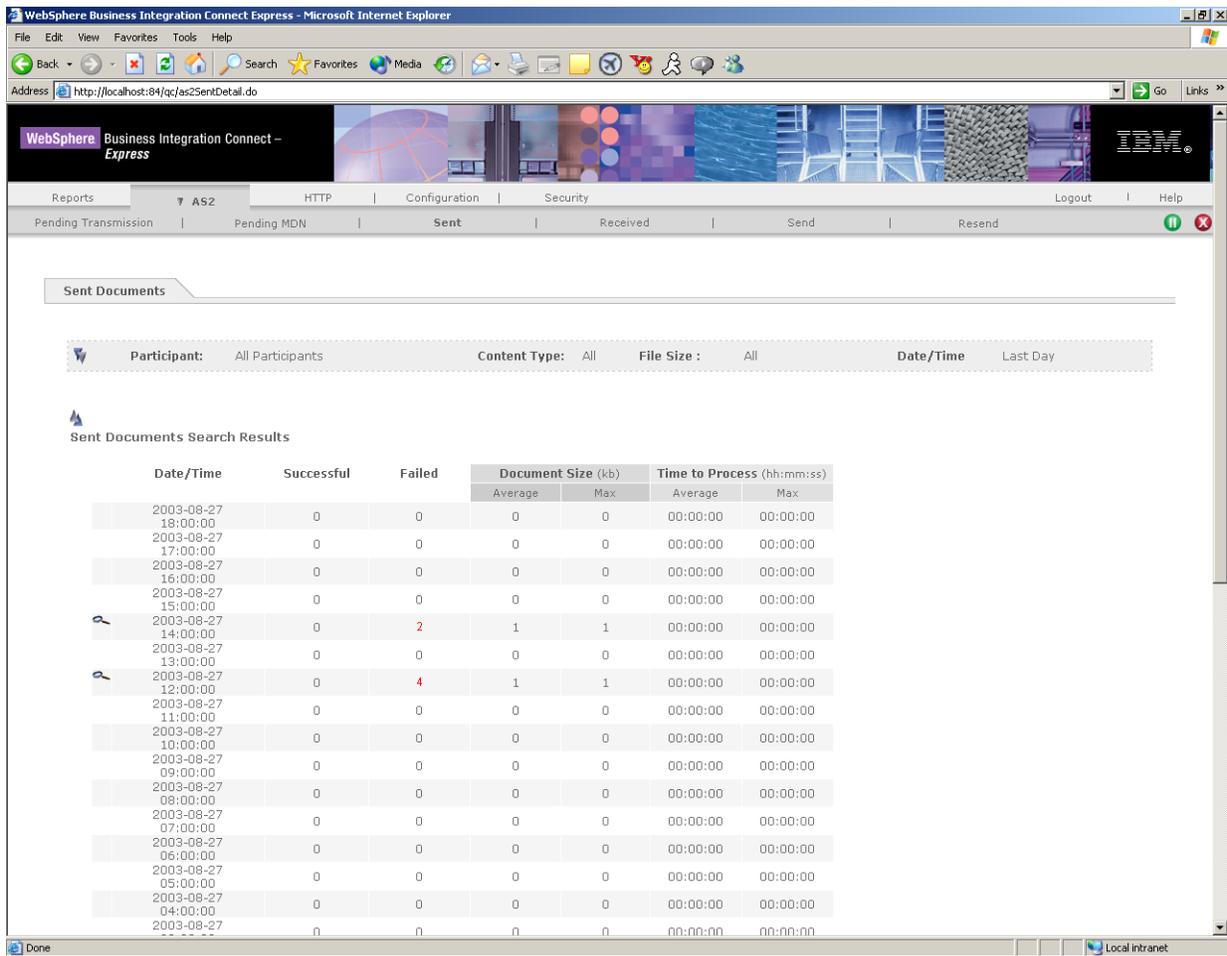


Figure 6-9. Example of a Search Scope

Viewing pending AS2 documents

Using the Pending Transmission screen, you can search for AS2 documents that are waiting to be transmitted. This screen will rarely return any documents, as the `send` directory is polled frequently (typically, at 1-second intervals) and the documents are moved to the `send` or `error` directory as appropriate. However, this screen 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 screen in [Figure 6-10](#) appears.

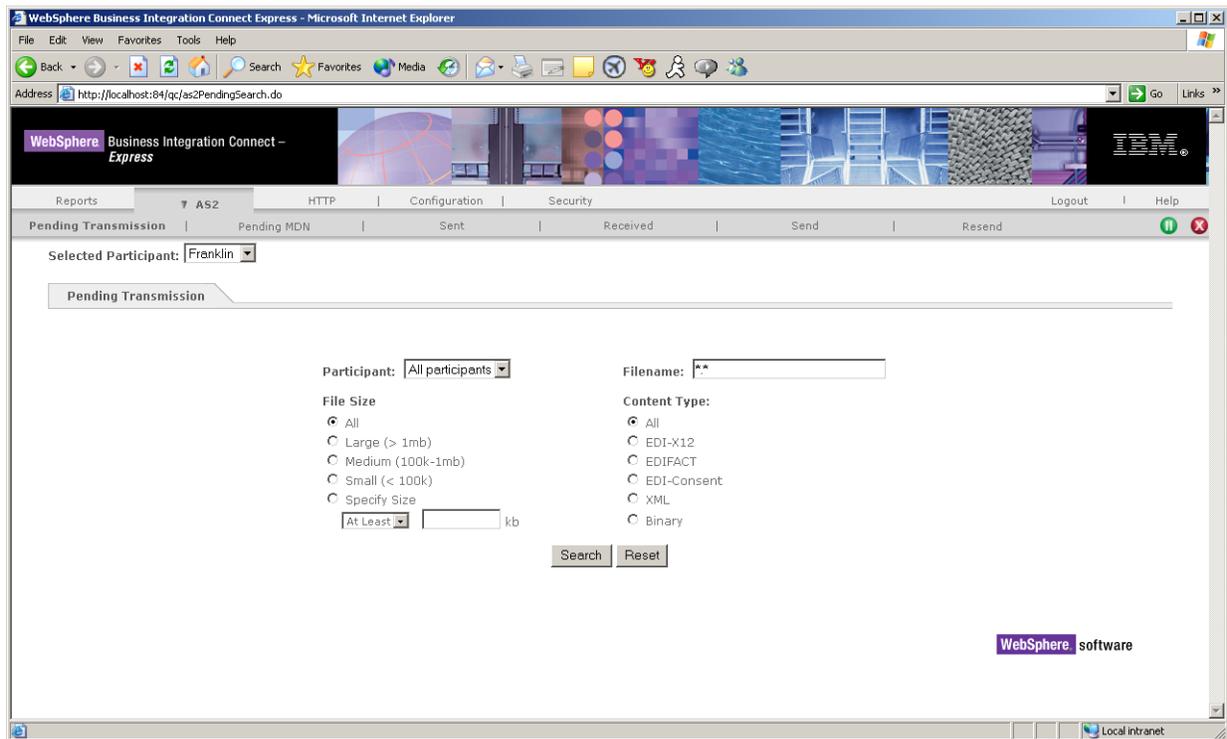


Figure 6-10. Pending Transmission Screen

2. Complete the entries in the Pending Transmission screen (see [Table 6-2 on page 85](#)).
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 screen (see [Figure 6-10 on page 93](#)).

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

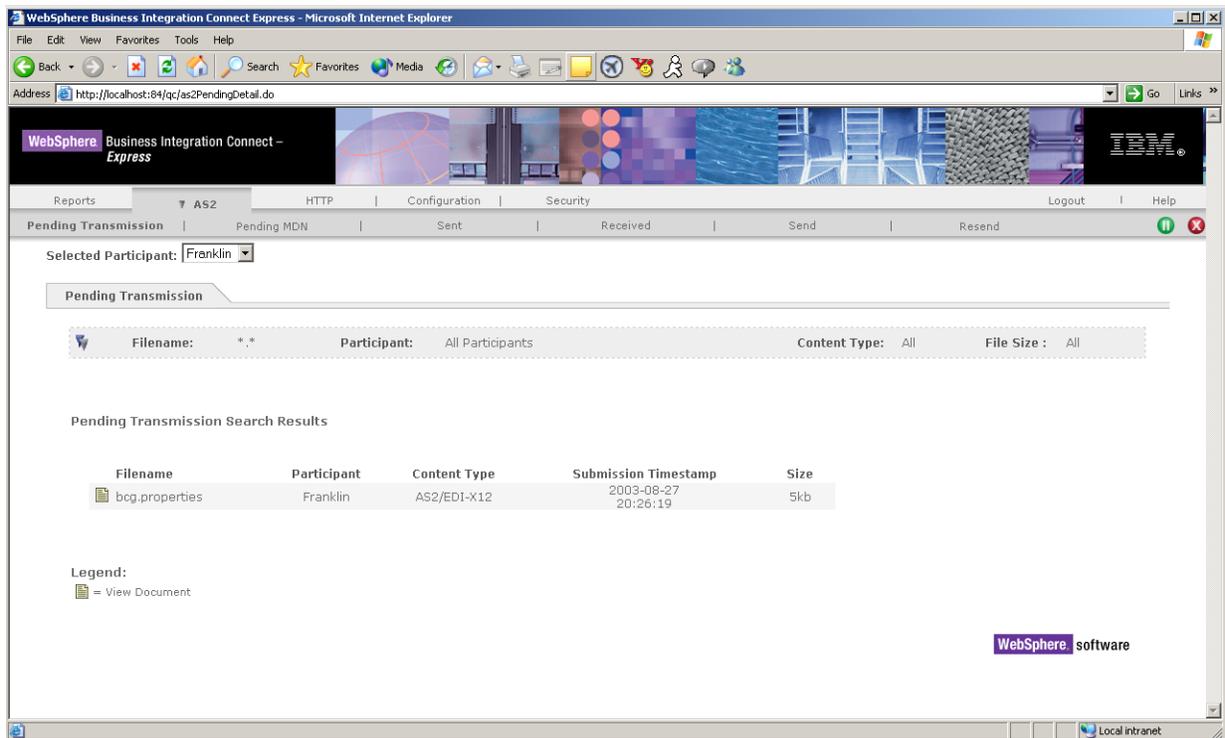


Figure 6-11. Matching Pending Documents

Table 6-4. Pending Transmission Screen

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 screen, you can search for AS2 documents that are pending MDNs. Documents pending MDNs remain pending for the number of minutes specified by the **Duration** parameter in the **Pending MDN** screen (see “[Viewing pending AS2 documents](#)” on page 93). 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 screen in [Figure 6-12](#) appears.

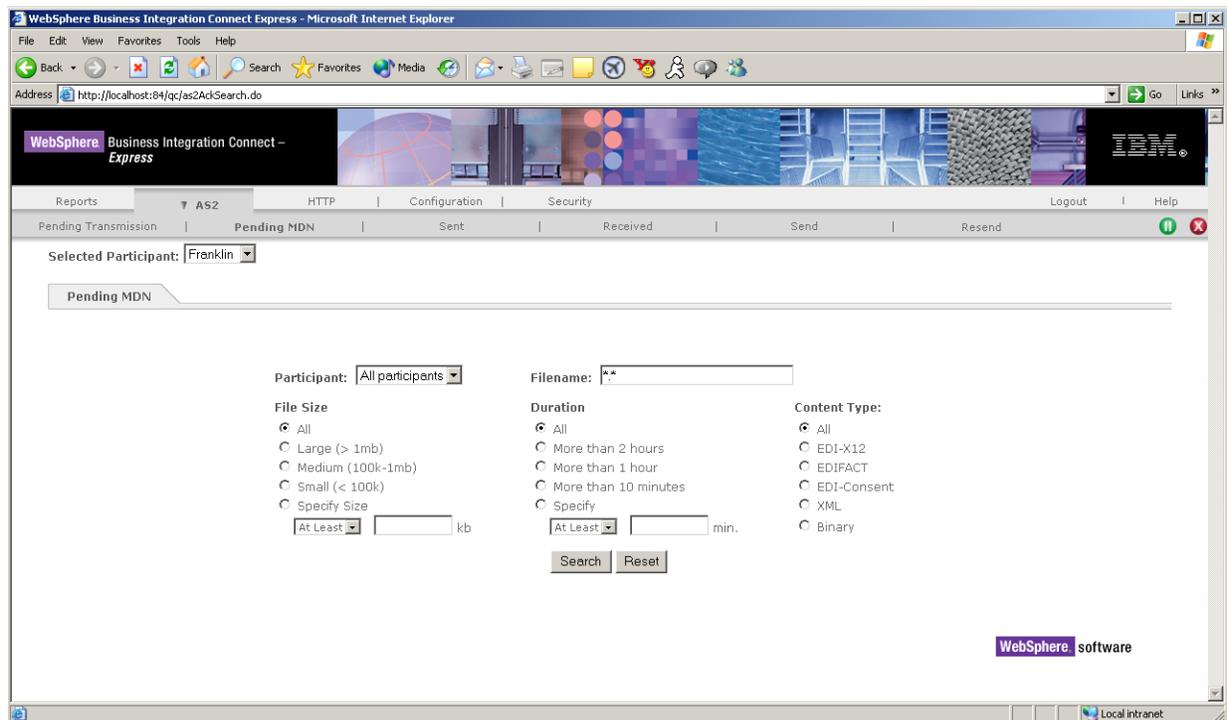


Figure 6-12. Pending MDN Screen

2. Complete the entries in the Pending MDN screen (see [Table 6-5](#) on page 96).
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 screen.

This screen shows status information about documents pending MDNs. There is also a  icon you can click to view the content of the documents.

Table 6-5. Pending MDN Screen

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 screen, 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 screen in [Figure 6-13](#) appears.

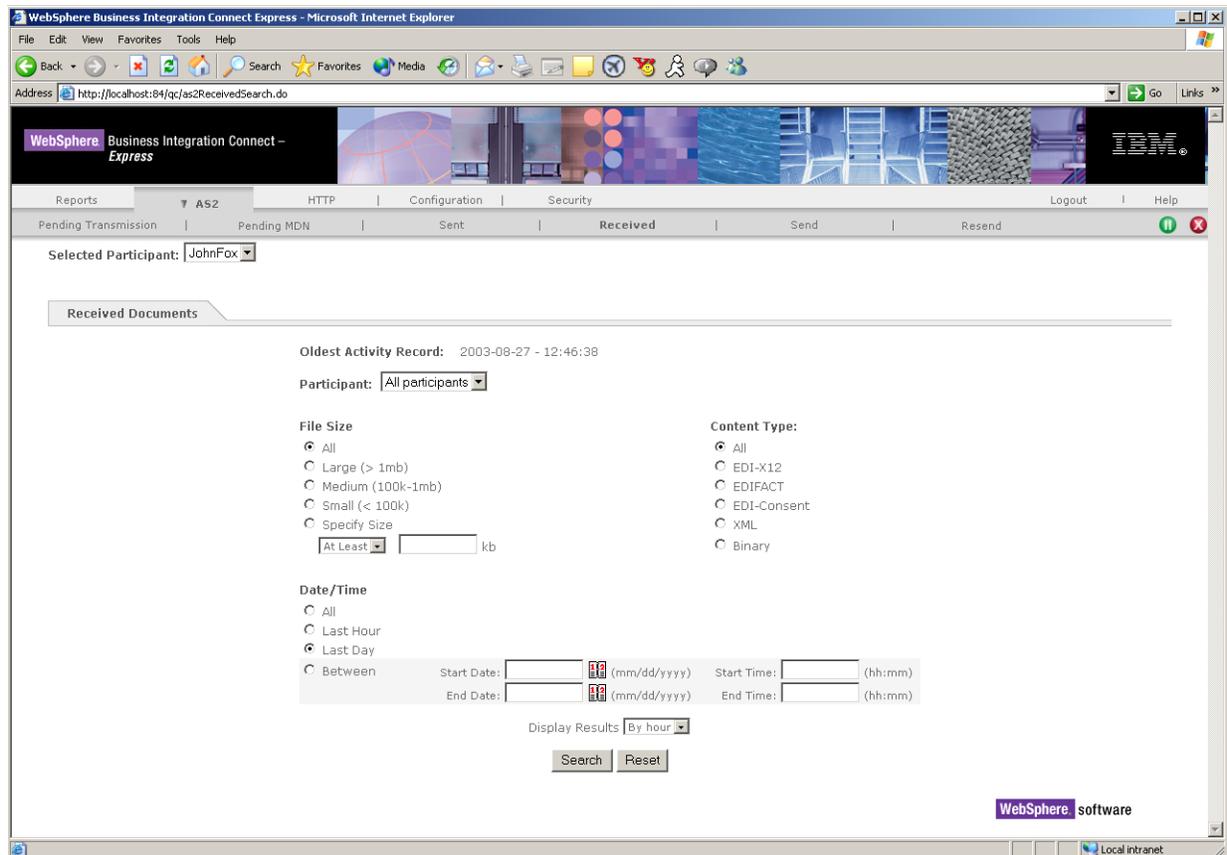


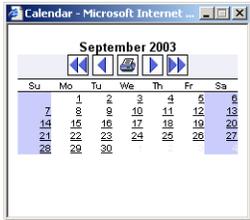
Figure 6-13. Received Documents Screen

2. Complete the entries in the Received Documents screen (see [Table 6-6 on page 98](#)).
3. Click the **Search** button. Business Integration Connect – Express finds the received documents that meet your search criteria and displays them in the Received Documents screen.

This screen shows status information about the received documents. There is also a  icon you can click to view the content of the documents.

Table 6-6. Received Documents Screen

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	<p>Select the date and time when the documents you want to find were received. For start and end dates, you can click the  icon to select dates from a pop-up calendar:</p>
Display Results	Select whether results are to be displayed by the hour or by the day they were sent.



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 screen appears (see [Figure 6-14](#)). However, you can use the horizontal navigation bar to access other screens.

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

- **Send** lets you send HTTP documents. See [“Viewing sent AS2 documents” on page 86](#).
- **Resend** lets you resend HTTP documents that meet your search criteria. See [“Resending HTTP documents” on page 101](#).
- **Sent** lets you view sent HTTP documents that meet your search criteria. See [“Viewing sent HTTP documents” on page 103](#).
- **Pending Transmission** lets you see which HTTP documents are waiting to be transmitted. See [“Viewing pending HTTP documents” on page 110](#).
- **Received** shows the HTTP documents that have been received. See [“Viewing received HTTP documents” on page 112](#).

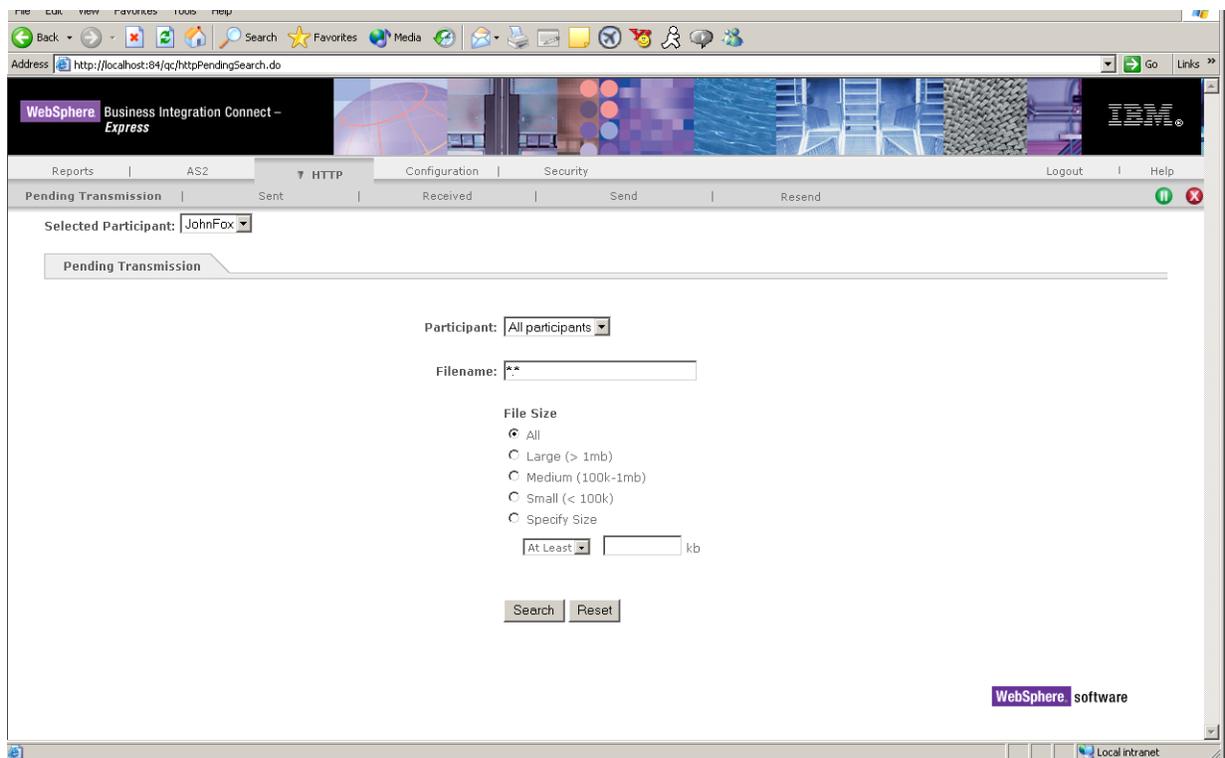


Figure 6-14. HTTP Menu, Pending Transmission Screen

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 screen in [Figure 6-15](#) appears.

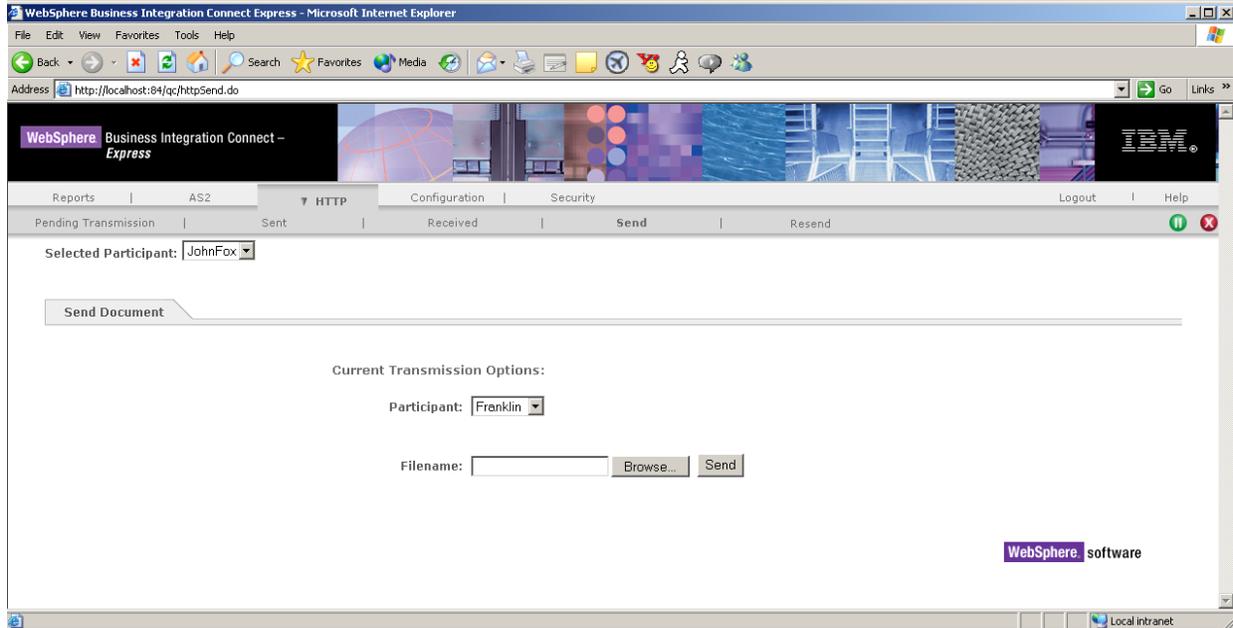


Figure 6-15. Send Document Screen

2. Complete the entries in the Send Document screen (see [Table 6-7](#)).
3. Click the **Send** button. A message in the gray area above **Current Transmission Options** indicates whether the file was uploaded successfully. The document is sent and a message appears, telling you that the document was uploaded.
4. To send additional HTTP documents, repeat steps 2 and 3.

Table 6-7. Send Document Screen

Parameter	Description
Participant	Select the participant who will be sending the file.
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 HTTP 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 screen in [Figure 6-16](#) appears.

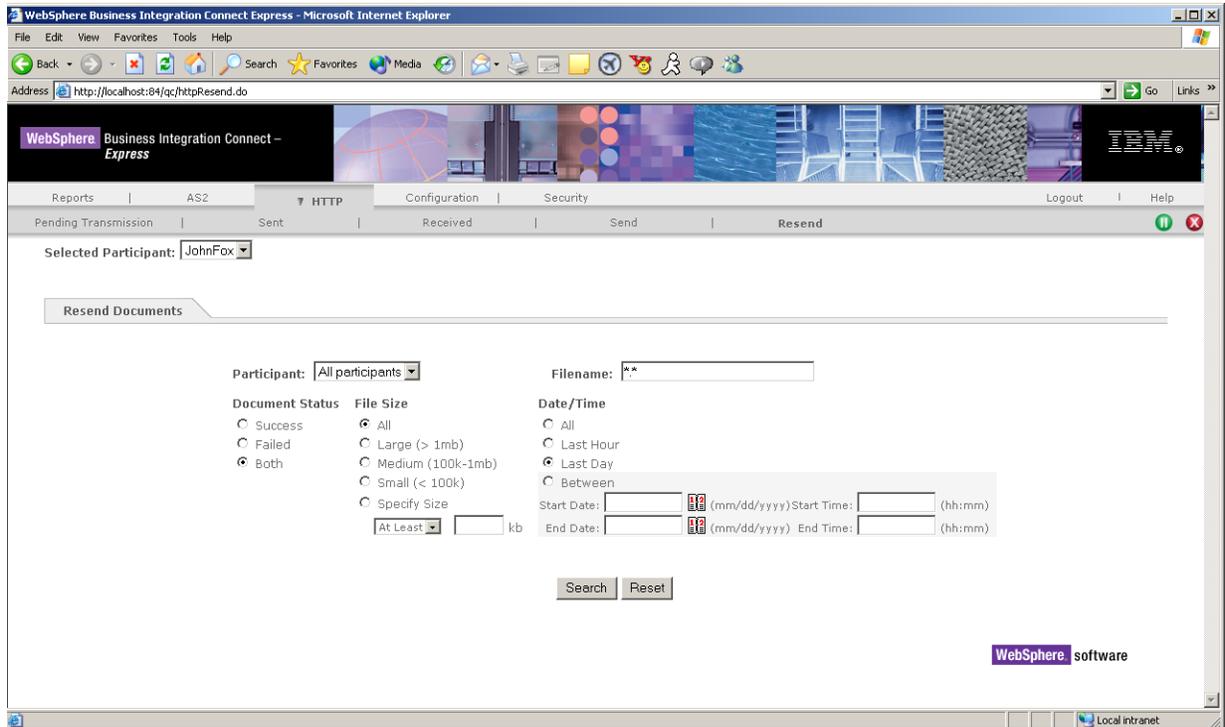


Figure 6-16. Resend Documents Screen

2. Complete the entries in the Resend Document screen (see [Table 6-8 on page 102](#)).
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 screen (see [Figure 6-17 on page 102](#)).

This screen 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.

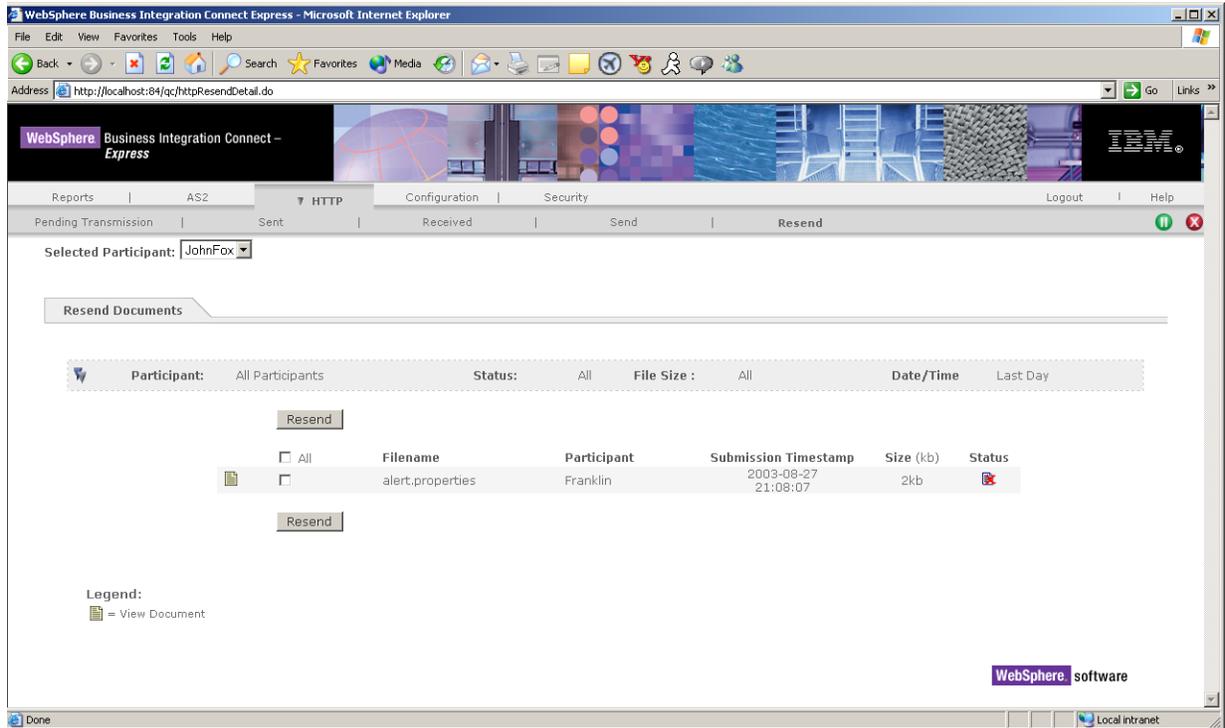


Figure 6-17. Matching Documents Displayed in the Resend Documents Screen

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 6-8. Resend Document Screen

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.

Table 6-8. Resend Document Screen

Parameter	Description
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  icon to select dates from a pop-up calendar:



Viewing sent HTTP documents

Using the Sent screen, 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 screen in [Figure 6-18 on page 104](#) appears.

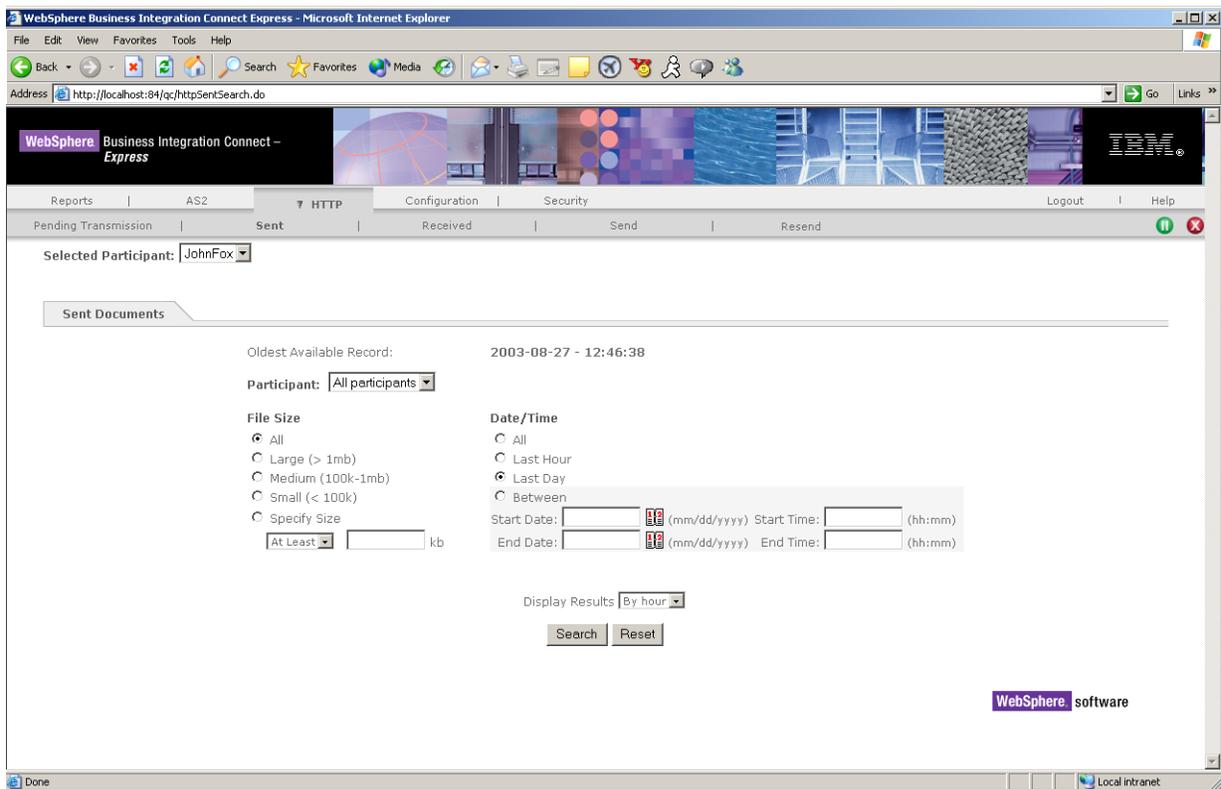


Figure 6-18. Sent Screen

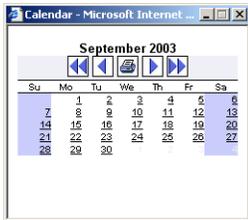
2. Complete the entries in the Sent Documents screen (see [Table 6-8 on page 102](#)).
3. Click the **Search** button. Business Integration Connect – Express displays all the sent HTTP documents that meet your search criteria (see [Figure 6-19 on page 106](#)).
4. To view detailed information about a sent document, click the  icon next to the appropriate document to display the Document Details screen. [Figure 6-20 on page 107](#) shows an example of this screen.

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

- Display sent document results and search criteria fields in one screen by clicking the  icon next to **Participant** at the top of the screen. The screen that appears contains icons for viewing the content of sent documents and search fields for conducting another search. [Figure 6-21 on page 108](#) shows an example of this screen.
- Display the search scope by clicking the  icon next to **Search Scope**. [Figure 6-22 on page 109](#) shows an example of this screen.
- View the contents of a document by clicking the  icon next to the document under **Sent Document Details**.

Table 6-9. Sent Documents Screen

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	<p>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.</p> <p>For start and end dates, you can click the  icon to select dates from a pop-up calendar:</p>
Display Results	Select whether results are to be displayed by the hour or by the day they were sent.



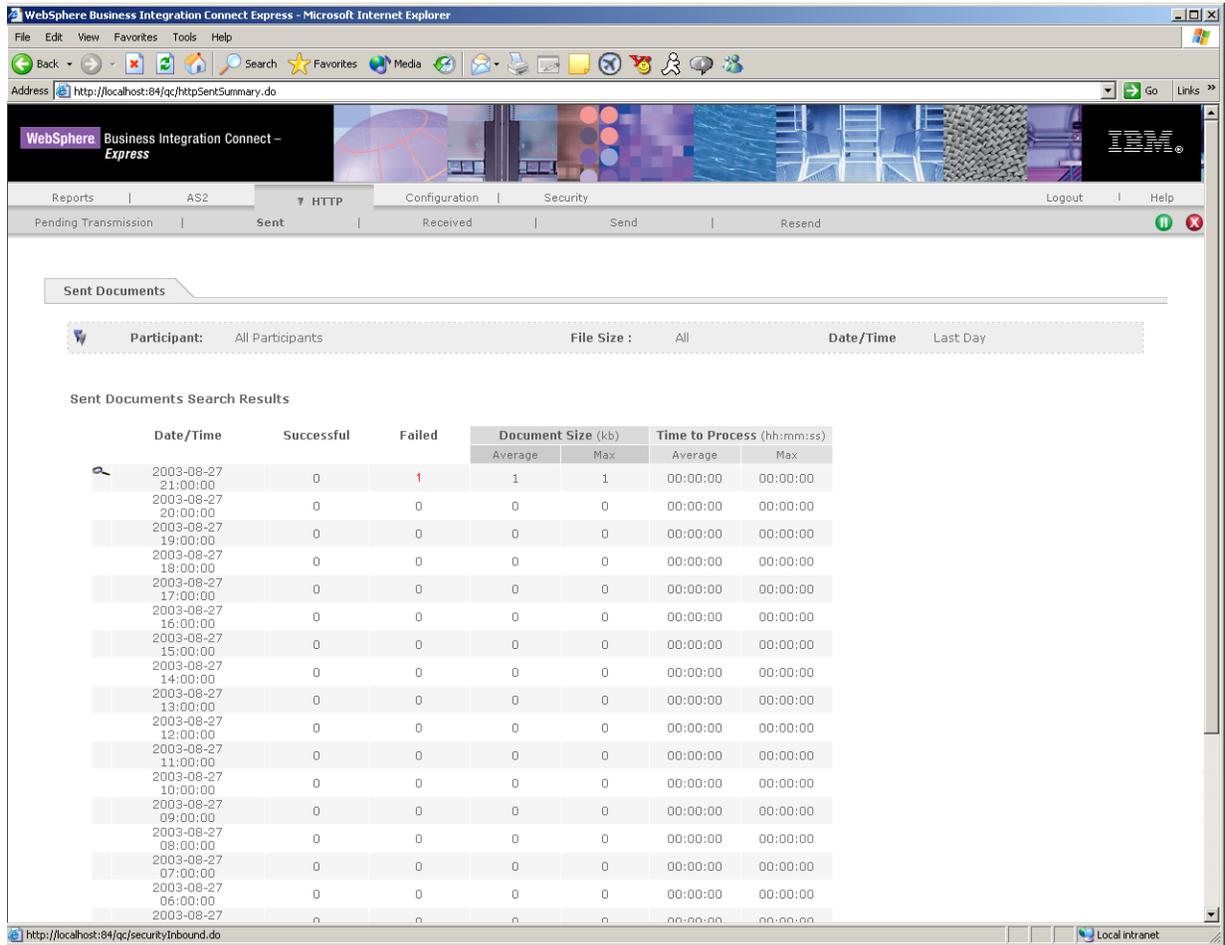


Figure 6-19. Example of Document Details Screen

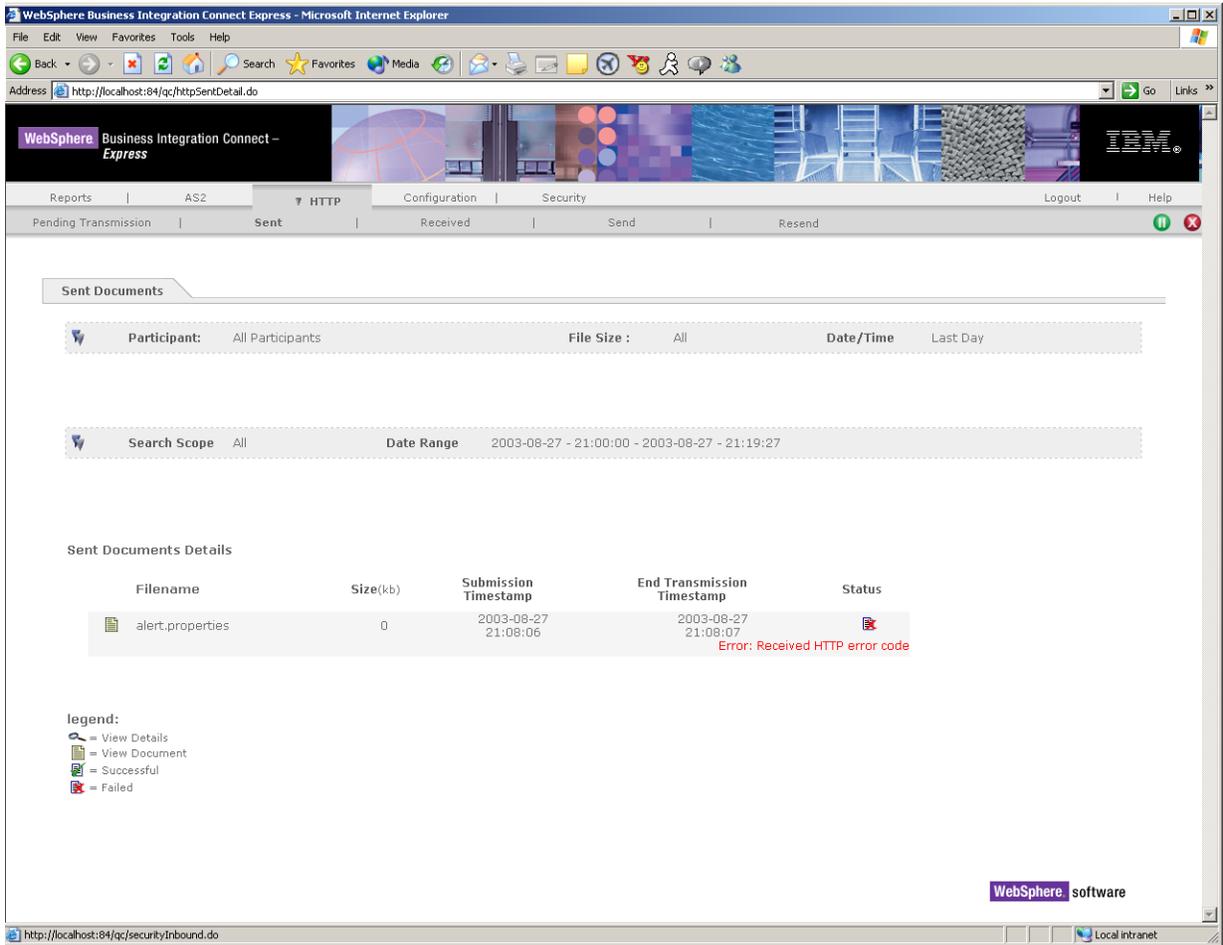


Figure 6-20. Example of Viewing Sent HTTP Documents

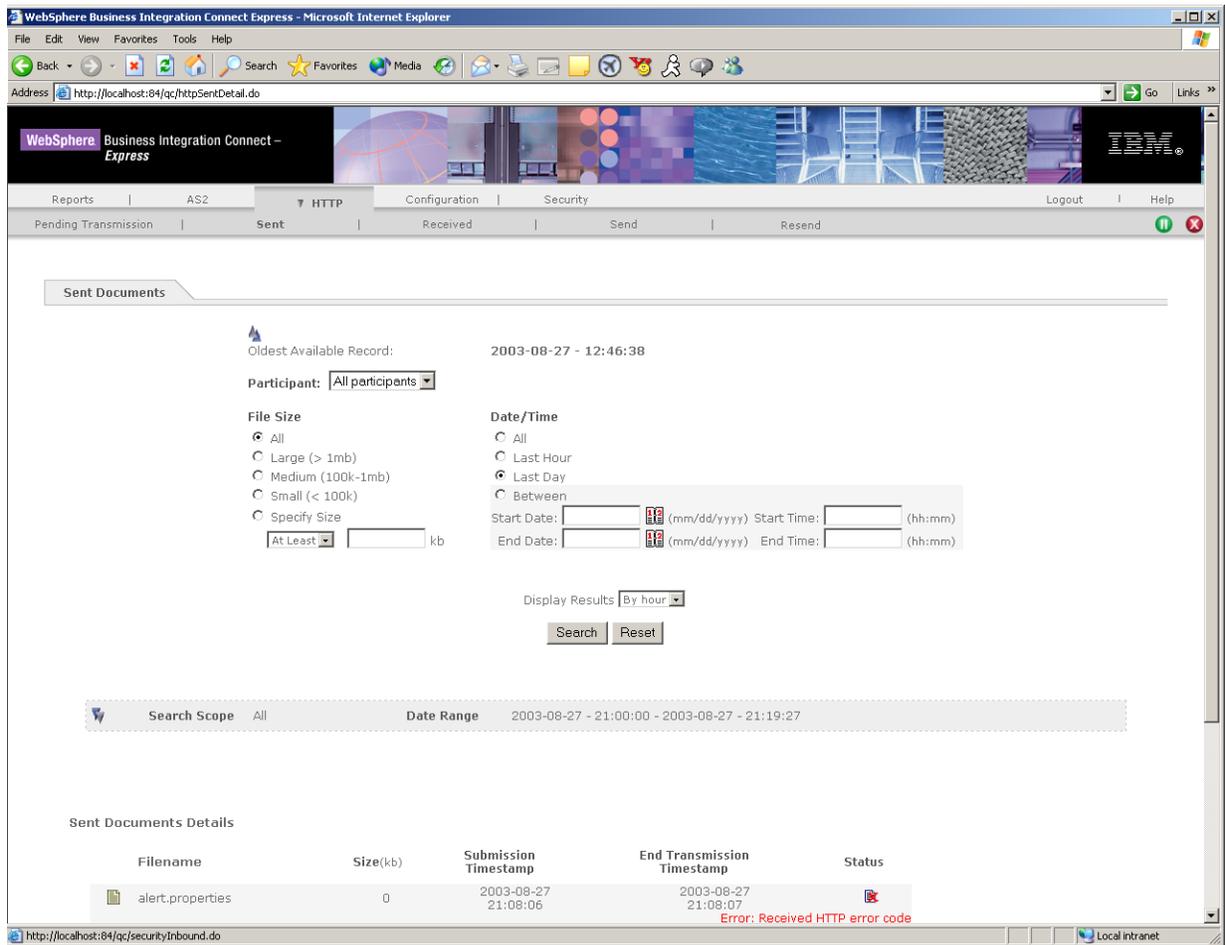


Figure 6-21. Example of a Screen with Search Fields and Sent Document Details

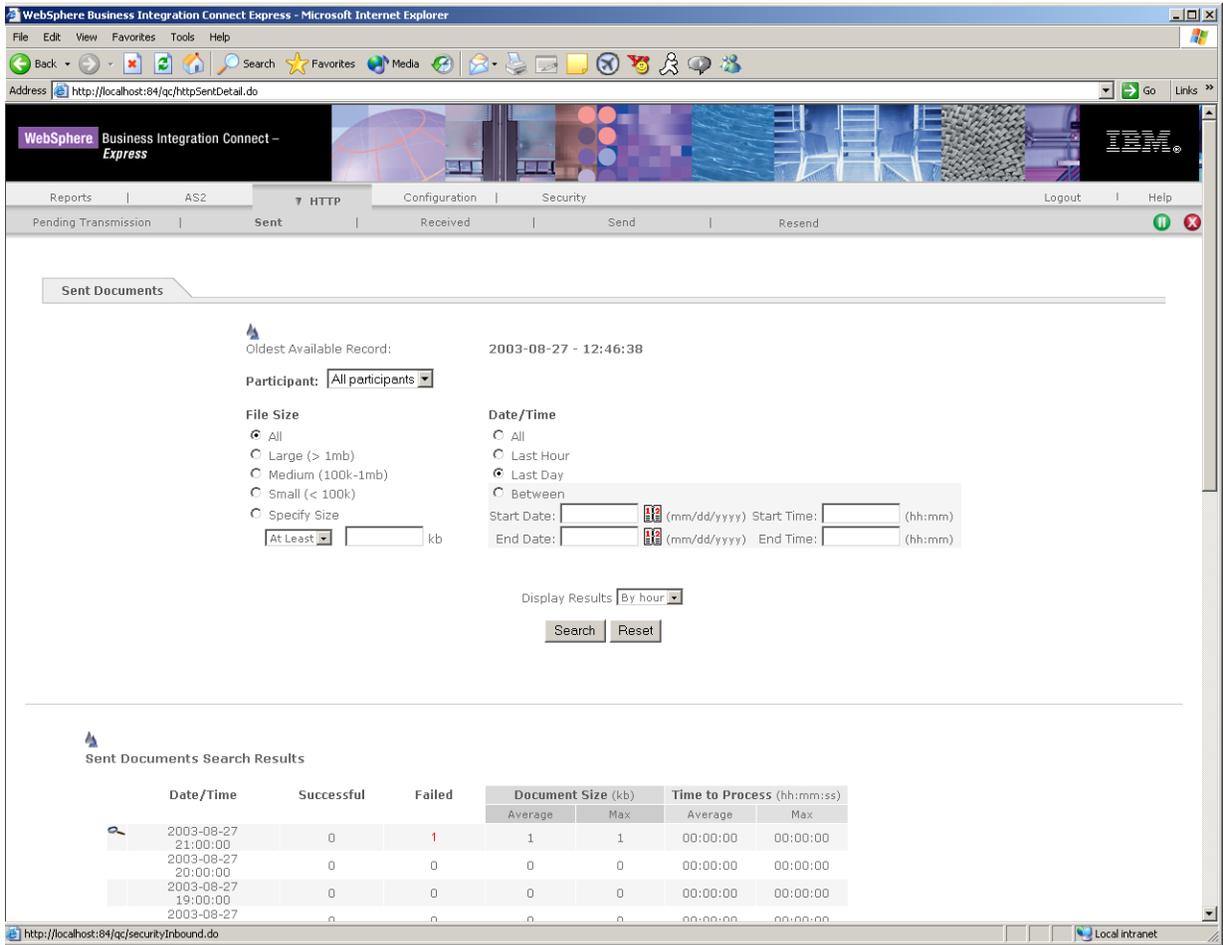


Figure 6-22. Example of a Search Scope

Viewing pending HTTP documents

Using the Pending Transmission screen, 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 screen in [Figure 6-23](#) appears.

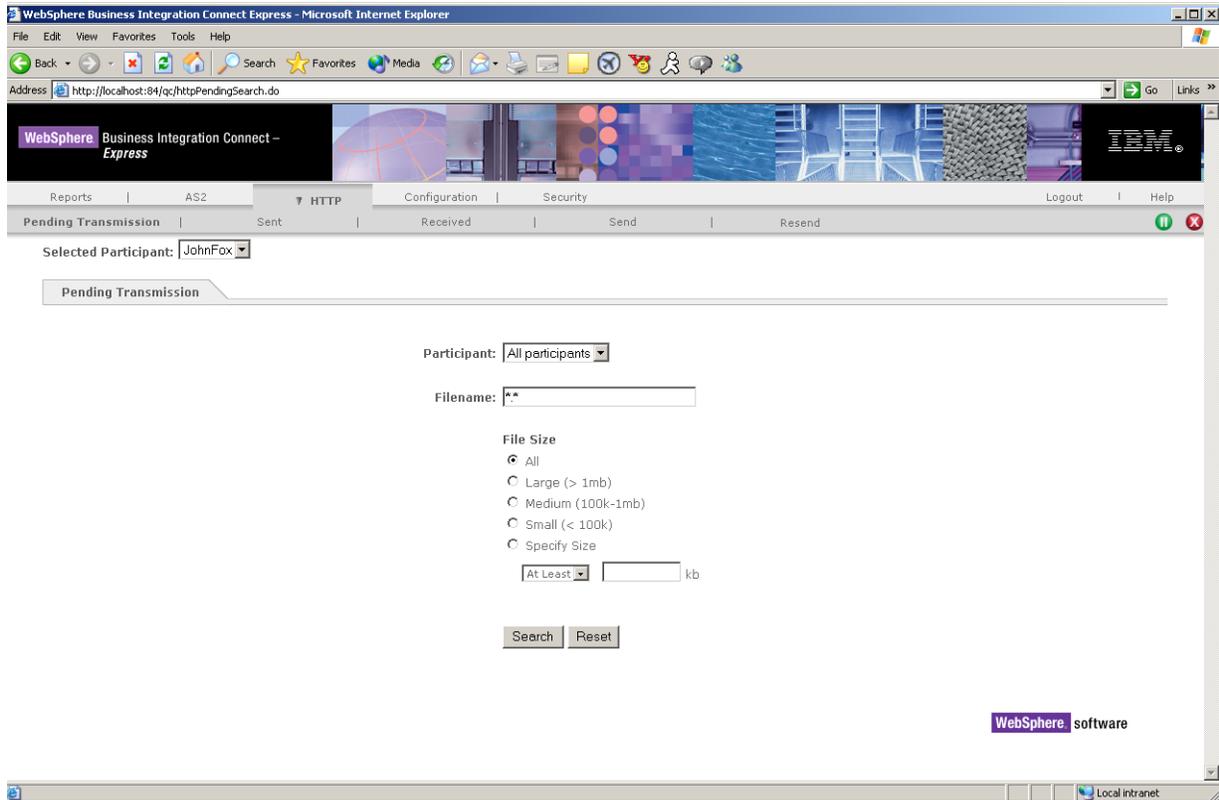


Figure 6-23. Pending Transmission Screen

2. Complete the entries in the Pending Transmission screen (see [Table 6-10 on page 111](#)).
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 screen (see [Figure 6-24 on page 111](#)).

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

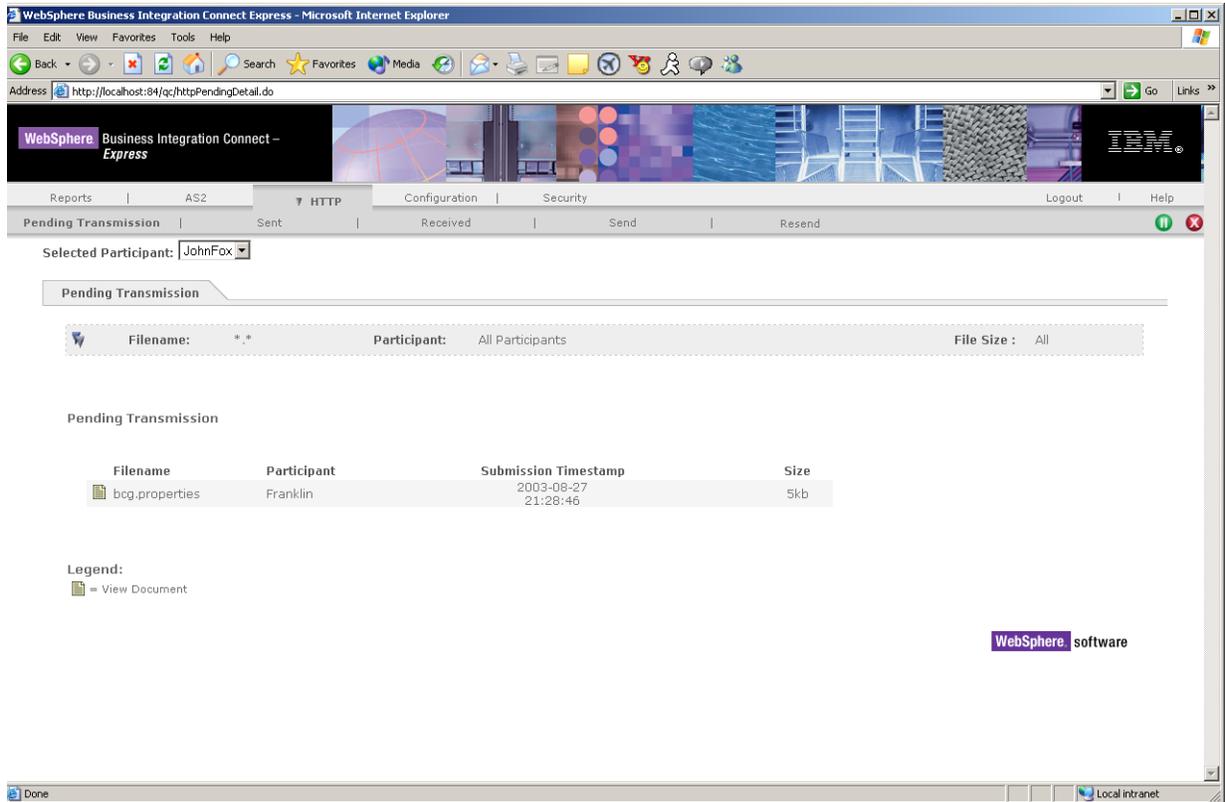


Figure 6-24. Matching Pending Documents

Table 6-10. Pending Transmission Screen

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 screen, 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 screen in [Figure 6-25](#) appears.

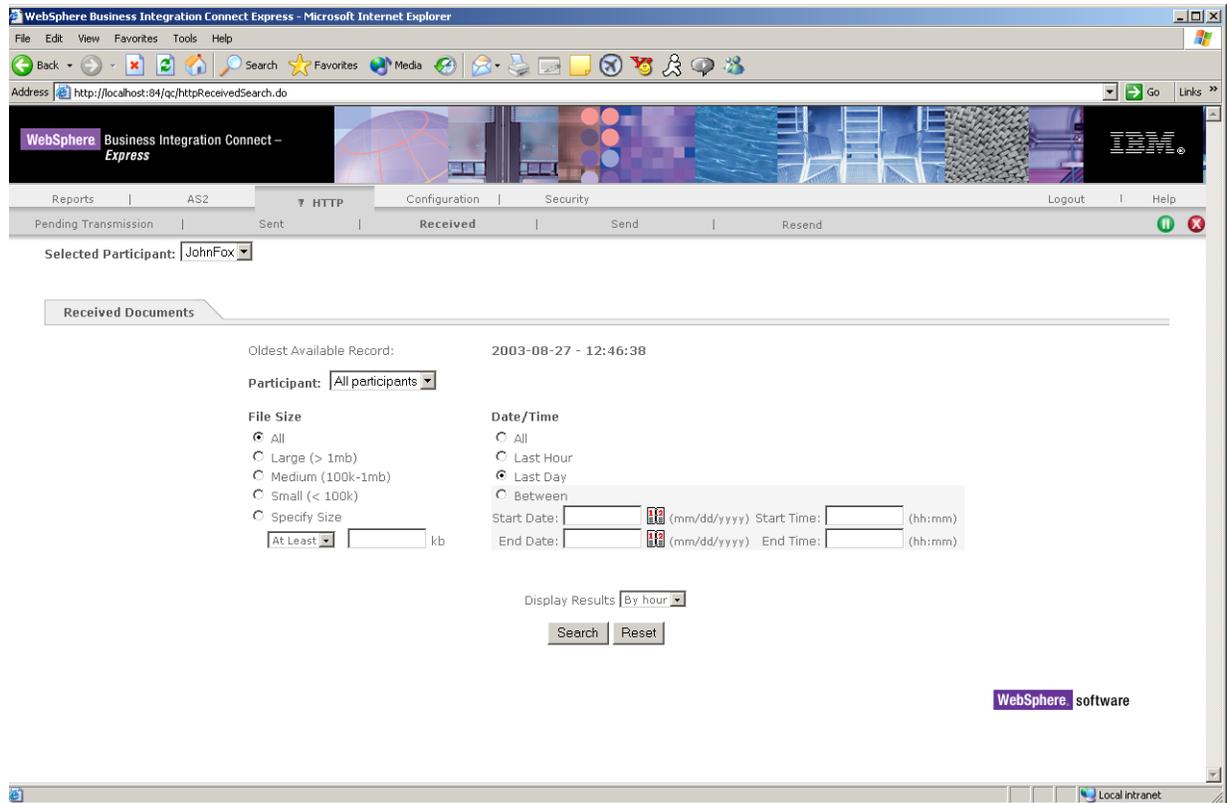


Figure 6-25. Received Documents Screen

2. Complete the entries in the Received Documents screen (see [Table 6-10 on page 111](#)).
3. Click the **Search** button. Business Integration Connect – Express finds the received documents that meet your search criteria and displays them in the Received Documents screen.

This screen shows status information about the received documents. There is also a  icon you can click to view the content of the documents.

Table 6-11. Received Documents Screen

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	<p>Select the date and time when the documents you want to find were received. For start and end dates, you can click the  icon to select dates from a pop-up calendar:</p>
Display Results	Select whether results are to be displayed by the hour or by the day they were sent.



Chapter 7. Viewing Reports

Overview

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 116
- “Viewing the Participant Summary report” on page 117
- “Viewing the Activity Log” on page 118

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 screen appears (see Figure 7-1). However, you can use the horizontal navigation bar to access other report screens.

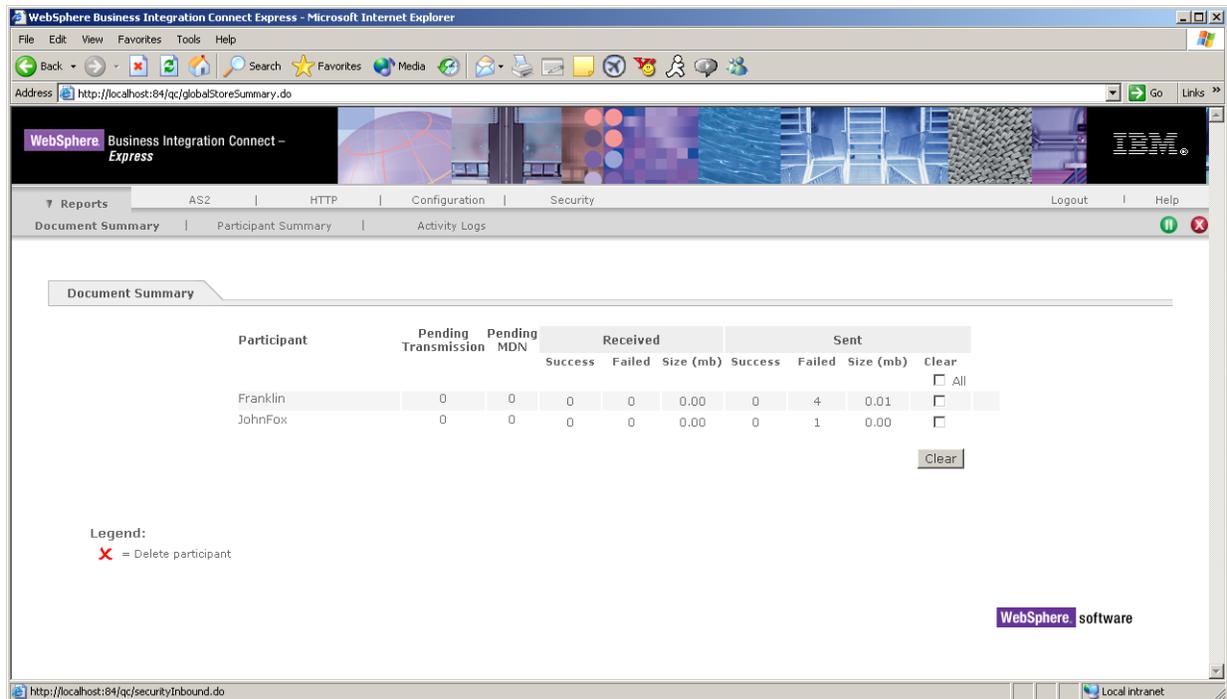


Figure 7-1. Reports Menu, Document Summary Screen

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 117.
- **Activity Logs** displays activity information that matches your search criteria. See “[Viewing the Activity Log](#)” on page 118.

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 screen (see [Figure 7-2](#)). If the screen does not appear, click **Document Summary** in the horizontal navigation bar.

Each row in the Document Summary screen 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.

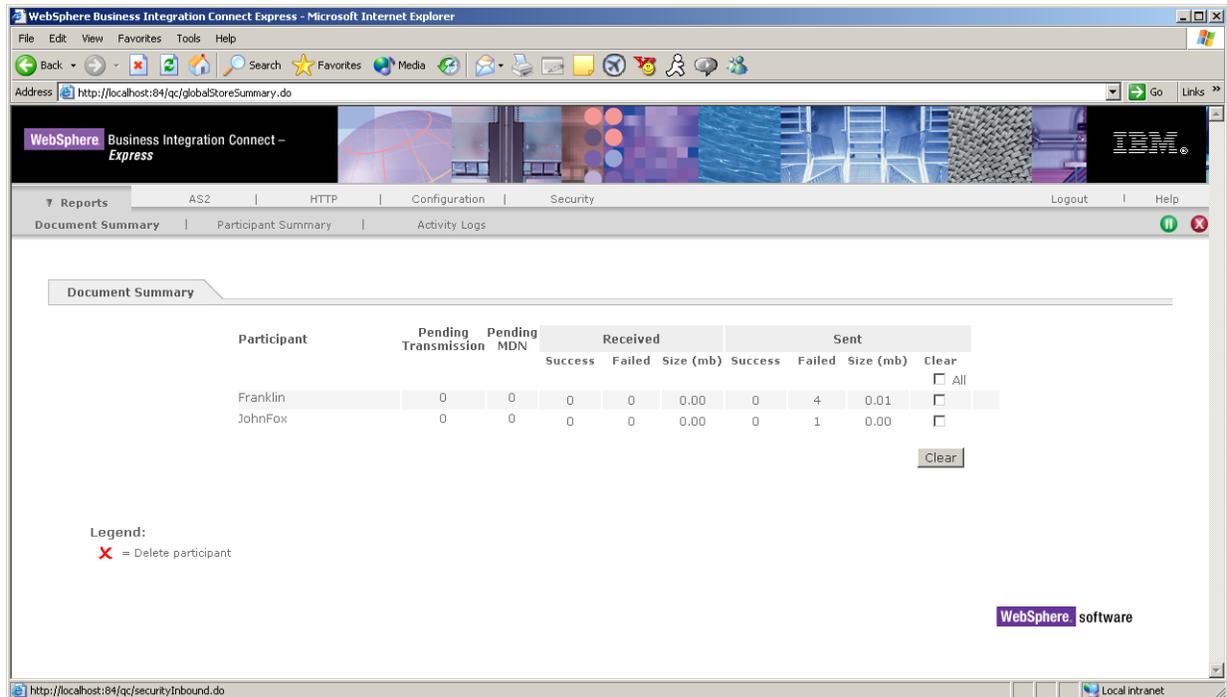


Figure 7-2. Document Summary Screen

If desired, you can clear sent items in the Document Summary screen 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).
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. Figure 7-3 shows an example of a Participant Summary report.

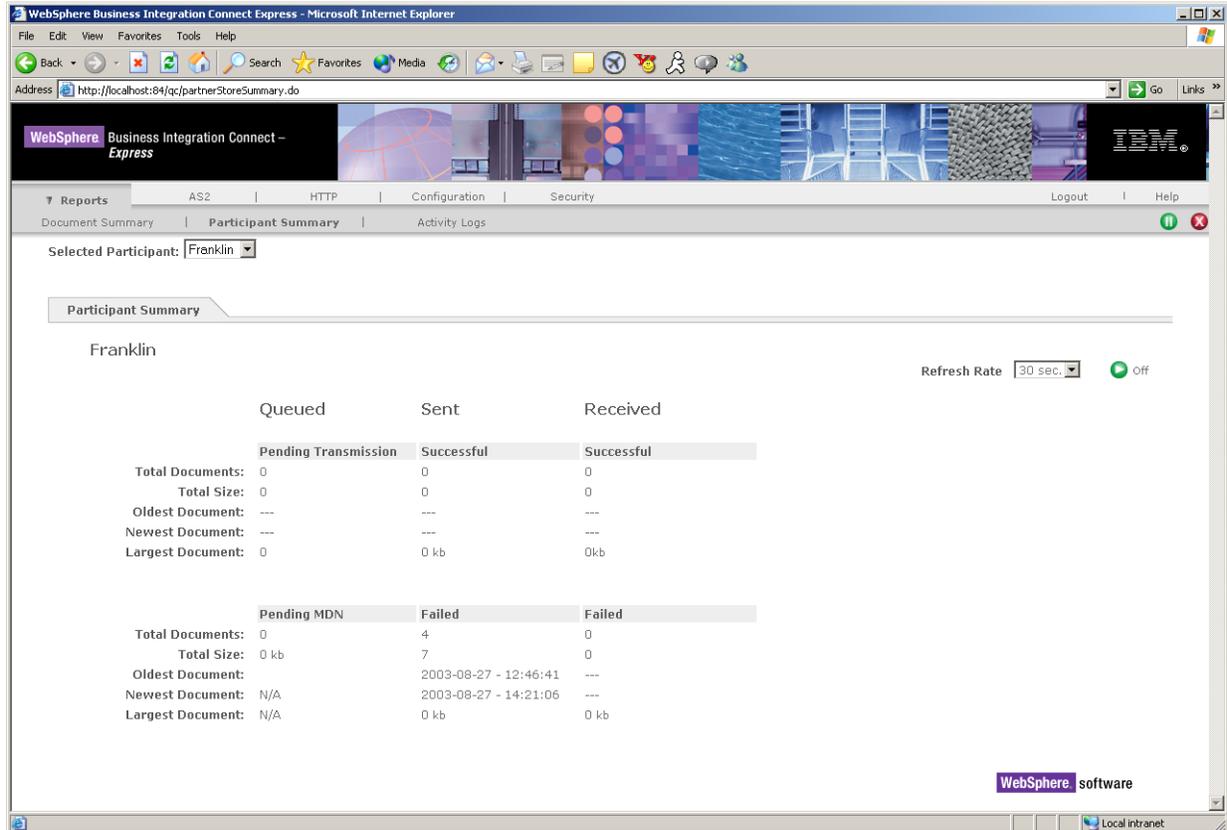


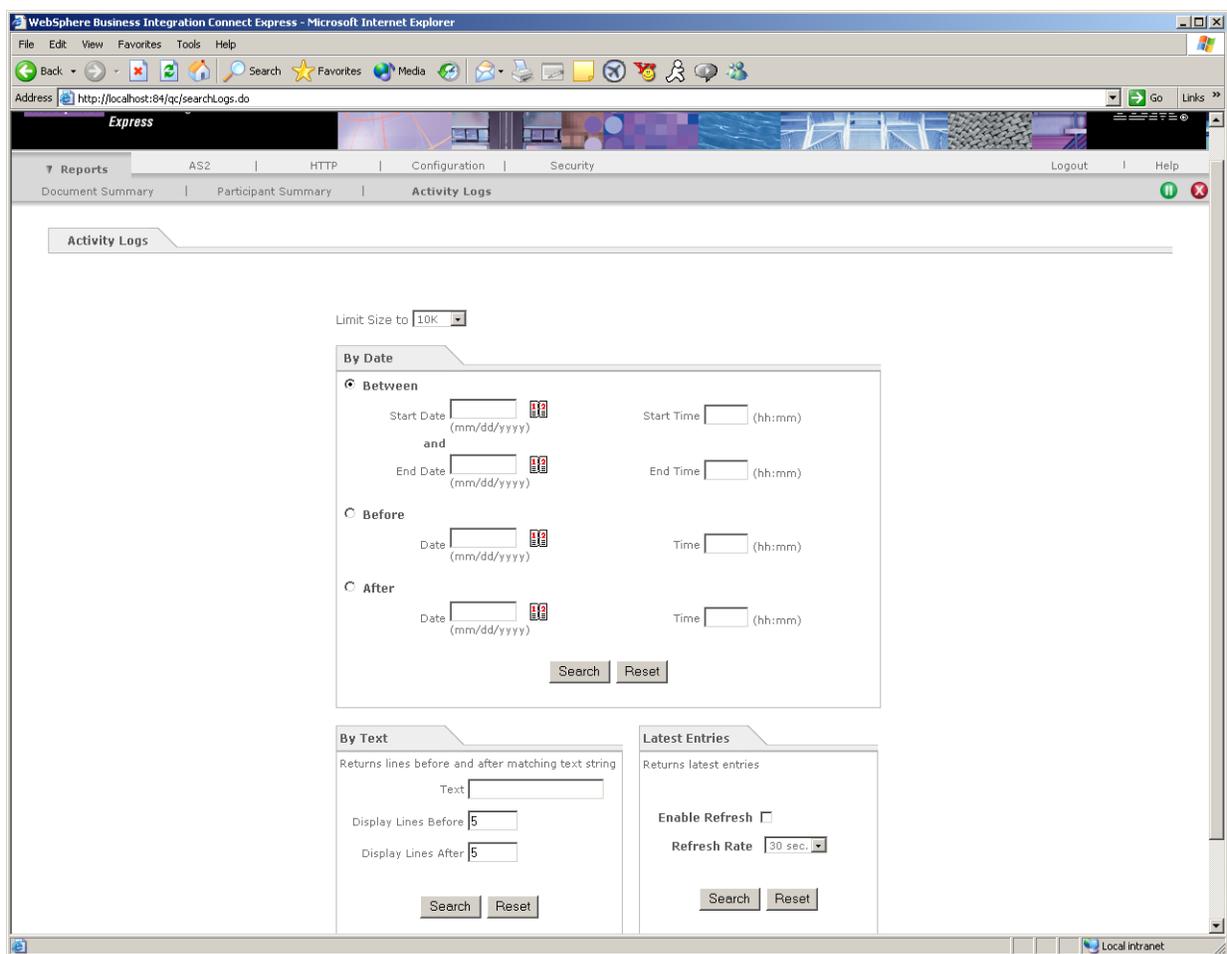
Figure 7-3. Participant Summary Report

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 screen where you enter search criteria, click the **Reports** menu, then click **Activity Logs** on the horizontal navigation bar. The screen in [Figure 7-3](#) appears. This screen lets you search for activity information by date, by text, or by latest entries.



The screenshot shows the 'Activity Logs' search interface in a Microsoft Internet Explorer browser window. The browser title is 'WebSphere Business Integration Connect Express - Microsoft Internet Explorer' and the address bar shows 'http://localhost:84/qc/searchLogs.do'. The application navigation bar includes 'Reports', 'AS2', 'HTTP', 'Configuration', 'Security', 'Logout', and 'Help'. The 'Activity Logs' section is active, showing a 'Limit Size to' dropdown set to '10K'. There are three main search criteria sections: 'By Date', 'By Text', and 'Latest Entries'. The 'By Date' section has radio buttons for 'Between', 'Before', and 'After', with corresponding date and time input fields. The 'By Text' section has a 'Text' input field and 'Display Lines Before' and 'Display Lines After' dropdowns set to '5'. The 'Latest Entries' section has an 'Enable Refresh' checkbox and a 'Refresh Rate' dropdown set to '30 sec.'. Each section has 'Search' and 'Reset' buttons. The browser status bar at the bottom indicates 'Local intranet'.

Figure 7-4. Screen for Entering Activity Log Criteria

To view the Activity Log, use the following procedure.

1. Click the **Reports** menu, then click **Activity Logs** in the horizontal navigation bar. The screen in [Figure 7-4 on page 118](#) appears.
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.

[Figure 7-5 on page 120](#) shows an example of an Activity Log.

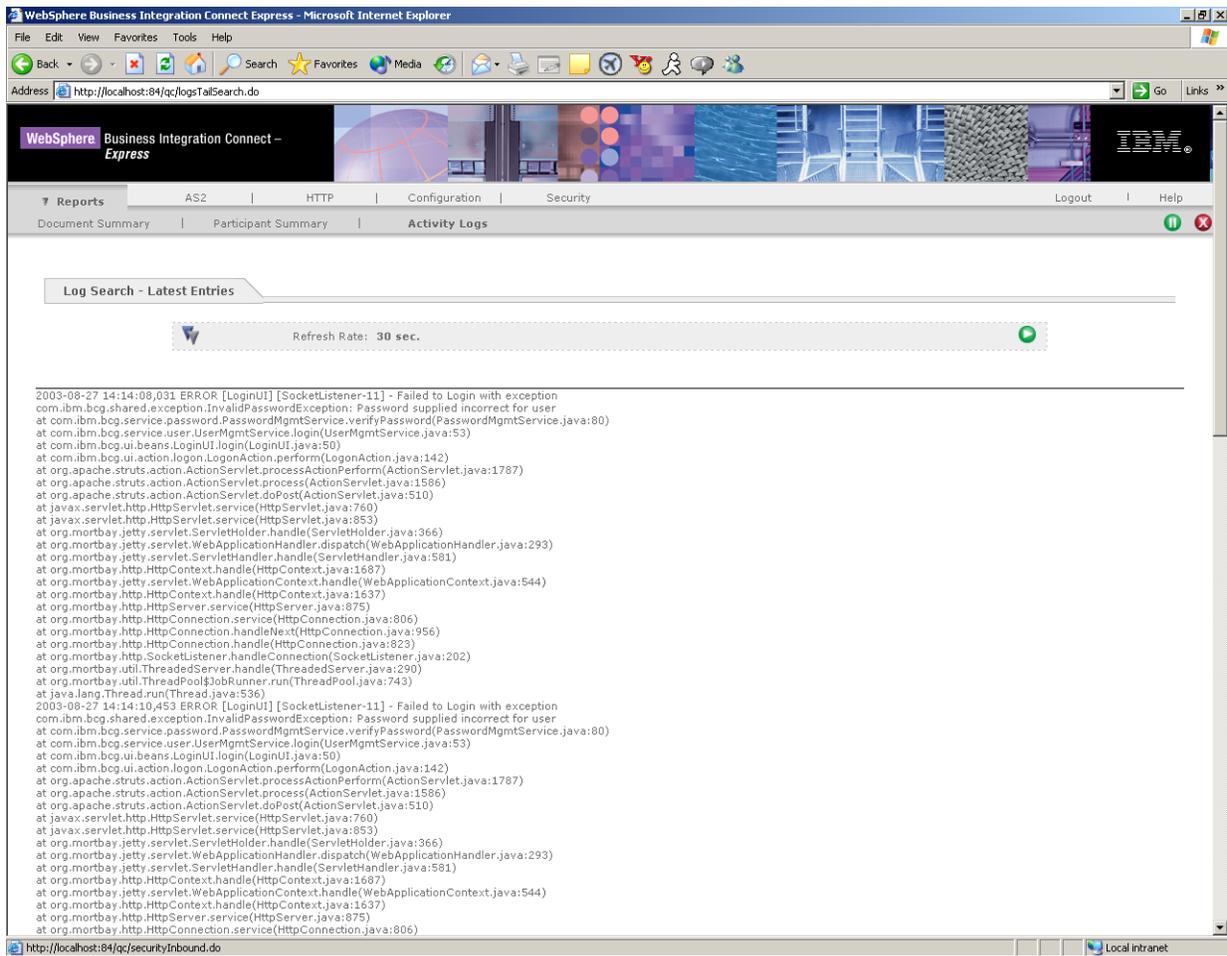


Figure 7-5. Example of an Activity Log

Appendix A. Error Messages

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

Table A-1. 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.



bin

Contains batch and shell script files for executing programs associated with WebSphere Business Integration Connect – Express.



config

Contains property and system-configuration files, as well as generated and uploaded certificates.



error

Contains subfolders with documents that failed transmission. Each subfolder is date- and time-stamped.



jre

Contains the Java runtime environment.



lib

Contains library files supporting WebSphere Business Integration Connect – Express.



logs

Contains an activity log that summarizes each document sent and received. This folder also contains a trace log that can be used for troubleshooting.



received

Contains subfolders with documents received from the Community Manager or other Partners. Each subfolder is date- and time-stamped.



rec_err

Contains subfolders with received documents that could not be processed by WebSphere Business Integration Connect – Express. Each subfolder is date- and time-stamped.



send

Contains the documents that will be picked up by WebSphere Business Integration Connect – Express for transmission to the Community Manager or other Partners. You must copy or move documents into this folder for the documents to be sent.



sent

Contains subfolders with documents sent successfully to the Community Manager or other Partners. Each subfolder is date- and time-stamped.



webapps

Contains the WebSphere Business Integration Connect – Express user interface.

Appendix C. Uninstalling WebSphere Business Integration Connect – Express

If you no longer wish to use WebSphere Business Integration Connect – Express, use the following procedure to uninstall it from your PC.

1. Stop the gateway.
2. Once the gateway is stopped, go to the Windows Control Panel.
3. Double-click the **Add/Remove Programs** icon. The Add/Remove Programs dialog box appears.
4. Scroll down the list to find WebSphere Business Integration Connect – Express. Then click it.
5. Click **Change/Remove**.
6. Follow the prompts to uninstall the application.

Index

A

- Accessing the console [20](#)
- Activity Log [118](#)
- Adding a certificate to a truststore [56](#)
- Adding certificates from certifying authorities [76](#)
- Adding CRLs [78](#)
- Adding participants [34](#)
- AS2 documents
 - pending [93](#)
 - pending MDNs [95](#)
 - received [97](#)
 - resending [84](#)
 - sending [82](#)
 - sent [86](#)
- AS2 parameters [40](#)

C

- Certificate Revocation List
 - defined [49](#)
- Certificates
 - adding [76](#)
 - deleting [77](#)
- Changing the default login password [22](#)
- Client authentication, defined [48](#)
- Company Website [4](#)
- Configuration [31](#)
 - adding participants [34](#)
 - AS2 parameters [40](#)
 - deleting participants [36](#)
 - editing participants [35](#)
 - HTTP parameters [43](#)
 - my profile [37](#)
- Configuration menu [31](#)
- Configuring
 - participants [33](#)
- Console access [20](#)
- Creating participants [24](#)

- CRLs [79](#)
 - adding [78](#)
- Customer Service [4](#)

D

- Decryption, defined [48](#)
- Default login passwords, changing [22](#)
- Deleting
 - certificates [77](#)
 - CRLs [79](#)
 - document signing keypair [75](#)
 - encryption public certificate [71](#)
 - keypair for decryption [63](#)
 - SSL keystore [55](#)
 - truststore for client authentication [59](#)
- Deleting a keypair for client authentication [68](#)
- Deleting participants [36](#)
- Digital certificates, defined [48](#)
- Digital signatures, defined [48](#)
- Document Summary report [116](#)
- Downloading
 - client certificate for client authentication [68](#)
 - document signing public certificate [75](#)
 - encryption public certificate [71](#)
 - public certificate for decryption [63](#)
 - SSL keystore [54](#)

E

- Editing participants [35](#)
- Encryption, defined [48](#)

F

- Features
 - general [5](#)
- Folders [121, 123](#)

G

- General features [5](#)
- Generating
 - self-signed document decryption keypair [60](#)
 - self-signed document signing keypair [72](#)

self-signed SSL client certificate keypair [64](#)

self-signed SSL keystore [50](#)

Generating an options file [18](#)

Getting Help [4](#)

H

Help [4](#)

HTTP documents

pending [110](#)

received [112](#)

resending [101](#)

sending [100](#)

sent [103](#)

HTTP parameters [43](#)

I

Inbound transactions, securing [50](#)

Installation

generating an options file [18](#)

GUI method [9](#)

silent method [17](#)

K

Keypair

deleting [63, 68, 75](#)

generating [64](#)

generating self-signed [60, 72](#)

uploading [61, 67, 73](#)

keytool [56](#)

adding a certificate to a truststore [56](#)

listing certificates in a truststore [56](#)

removing a certificate from a truststore [57](#)

L

Listing certificates in a truststore [56](#)

Logging in [27](#)

Logging in for the first time [22](#)

changing the default login passwords [22](#)

creating a participant [24](#)

Login passwords

changing default [22](#)

updating [30](#)

M

Managing

AS2 documents [81](#)

encryption certificates [69](#)

HTTP documents [99](#)

keypairs for client authentication [64](#)

keypairs for decryption [60](#)

keypairs for digital signatures [72](#)

keystores for an SSL connection [50](#)

truststores for client authentication [56](#)

Menus

Configuration [31](#)

Reports [115](#)

Security [49](#)

Minimum installation requirements [9](#)

My Profile [37](#)

O

Online Help [4](#)

Options file [18](#)

Outbound transactions, securing [64](#)

P

Participant Summary report [117](#)

Participants

adding [34](#)

configuring [33](#)

creating at initial login [24](#)

deleting [36](#)

editing [35](#)

Public certificate

deleting [71](#)

downloading [71](#)

uploading [69](#)

R

Removing a certificate from a truststore [57](#)

Reports

Activity Log [118](#)

Document Summary [116](#)

Participant Summary [117](#)

Reports menu [115](#)

Requirements for installing WebSphere Business Integration Connect – Express [9](#)

Resending

AS2 documents [84](#)

HTTP documents [101](#)

S

Securing

inbound transactions [50](#)

outbound transactions [64](#)

Security

managing keypairs for decryption [60](#)

managing keystores for an SSL connection [50](#)

managing truststores for client authentication [56](#)

terms and concepts [47](#)

Security menu [49](#)

Sending

AS2 documents [82](#)

HTTP documents [100](#)

Silent installation [17](#)

SSL keystore

deleting [55](#)

downloading [54](#)

generating self-signed [50](#)

uploading [52](#)

SSL protocol, defined [47](#)

Starting WebSphere Business Integration Connect – Express [19](#)

T

Terms [4](#)

Testing WebSphere Business Integration Connect – Express [46](#)

Truststore

adding a certificate using keytool [56](#)

deleting [59](#)

listing certificates using keytool [56](#)

removing a certificate using keytool [57](#)

uploading [57](#)

U

Uninstalling WebSphere Business Integration Connect - Express [125](#)

Updating login password [30](#)

Uploading

client authentication keypair [67](#)

decryption keypair [61](#)

document signing keypair [73](#)

encryption public certificate [69](#)

SSL keystore [52](#)

truststore for client authentication [57](#)

User interface [28](#)

user interface [28](#)

V

Viewing

AS2 documents pending MDNs [95](#)

pending AS2 documents [93](#)

pending HTTP documents [110](#)

received AS2 documents [97](#)

received HTTP documents [112](#)

sent AS2 documents [86](#)

sent HTTP documents [103](#)

W

WebSphere Business Integration Connect - Express
uninstalling [125](#)

WebSphere Business Integration Connect – Express

configuring [31](#)

console [20](#)

document history [81, 115](#)

first-time login [22](#)

folders [121, 123](#)

general features [5](#)

history of documents [81, 115](#)

logging in [27](#)

minimum requirements for installing [9](#)

overview [5](#)

starting [19](#)

Notices and Trademarks

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 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 contains 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 contains 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. 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 IBM's application programming interfaces.

Programming interface information

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

IBM
the IBM logo
CrossWorlds
DB2
DB2 Universal Database
MQSeries
Passport Advantage
WebSphere

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

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

Solaris, 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.