# BEA WebLogic Integration™

## Using WebLogic Integration – Business Connect

Release 2.1
Document Date: January 2002

## Copyright

## Restricted Rights Legend

Information in this document is subject to change without notice and does not represent a commitment on the part of BEA Systems. THE SOFTWARE AND DOCUMENTATION ARE PROVIDED “AS IS” WITHOUT WARRANTY OF ANY KIND INCLUDING WITHOUT LIMITATION, ANY WARRANTY OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. FURTHER, BEA Systems DOES NOT WARRANT, GUARANTEE, OR MAKE ANY REPRESENTATIONS REGARDING THE USE, OR THE RESULTS OF THE USE, OF THE SOFTWARE OR WRITTEN MATERIAL IN TERMS OF CORRECTNESS, ACCURACY, RELIABILITY, OR OTHERWISE.

## Trademarks

All products and company names referred to in this documentation are the property of their respective trademark holders. A partial list is as follows:

BEA, Jolt, Tuxedo, and WebLogic are registered trademarks of BEA Systems, Inc. BEA Builder, BEA Campaign Manager for WebLogic, BEA eLink, BEA Manager, BEA WebLogic Commerce Server, BEA WebLogic E-Business Platform, BEA WebLogic Enterprise, BEA WebLogic Express, BEA WebLogic Integration, BEA WebLogic Personalization Server, BEA WebLogic Portal, BEA WebLogic Server and How Business Becomes E-Business are trademarks of BEA Systems, Inc.

AIX is a registered trademark of IBM Corporation

AS/400 and OS/400 are registered trademarks of IBM Corporation

BizTalk is a trademark of Microsoft Corporation

Client Access Express for Windows is a trademark of IBM Corporation

Digital ID and Digital ID+ are trademarks of VeriSign, Inc.

Data Universal Numbering System (D-U-N-S®) is a registered trademark of Dun & Bradstreet

Entrust is a registered trademark of Entrust Technologies Inc.

HP-UX is a trademark of the Hewlett-Packard Company

Java is a trademark of Sun Microsystems, Inc.

Pentium is a trademark of the Intel Corporation

Microsoft COM is a trademark of the Microsoft Corporation

Microsoft Exchange is a trademark of the Microsoft Corporation

## Acknowledgments

This Software includes the following third-party products:

Iaki.jar, © IAIK-Java Group

SQL Anywhere, © Sybase, Inc.

JDBC DB2 AIX, © HiT Software Inc.

Ldapjdk.jar file, © Netscape Communications Corporation

MSSQL Driver (JDBC 1.22), © i-net software

Solaris JRE, Win 95/98/NT/200 JRE, Sun JSSE, jms.jar and jndi.jar © Sun Microsystems, Inc.

AIX JRE, MQ Series Java Client and Linux JVM © International Business Machines

Apache XML Parser, xerces.jar, log4j.jar and org.apache.jasper.jar © The Apache Software Foundation

Jetty, © Mort Bay Consulting Pty.Ltd (Australia)

HPUX JRE, © Hewlett Packard Company

Jdom.jar, © JDOM Project

**Using WebLogic Integration – Business Connect**

| Part Number | Date | Software Version |
|---|---|---|
| N/A | January 2002 | 2.1 |

# Contents

## About This Document

## 1. Introduction

## 2. System Requirements

## 3. Installation and Configuration

## 4. Installation on Windows

## 5. Installation on UNIX

## 6. Getting Started

## 7. User Interface and Online Help

## 8. Overview of Profiles

## 9. Company Profiles

## 10. Using ebXML

## 11. Keys and Certificates

## 12. Partner Profiles

## 13. Tools

## 14. Application Security

## 15. Exporting and Importing Data

## 16. Document Generator

## 17. Tracker

## 18. Messages

## A. ISO Country Codes

## Index

# About This Document

This document describes WebLogic Integration – Business Connect and provides step-by-step procedures to install, configure, test, implement, and maintain your WebLogic Integration – Business Connect system.

## What You Need to Know

This document is intended for use by people who oversee installation, configuration, maintenance and use of WebLogic Integration – Business Connect. This book was written under the assumption that WebLogic Integration – Business Connect administrators have a working knowledge of:

- Your organization’s business hardware, software and practices
- Electronic data interchange (EDI) and electronic commerce
- A graphical user interface
- The Internet, including use of a browser

In addition, your network, systems or mail administrator might find parts of this document useful as a guide for installation and configuration.

This document can also serve as a reference for EDI department supervisors and technical personnel.

# e-docs Web Site

BEA product documentation is available on the BEA corporate Web site. From the BEA Home page, click on Product Documentation or go directly to the “e-docs” Product Documentation page at http://e-docs.bea.com.

# How to Print the Document

You can print a copy of this document from a Web browser, one file at a time, by using the File→Print option on your Web browser.

A PDF version of this document is available from the BEA WebLogic Integration documentation Home page, which is available on the documentation CD and on the e-docs Web site at http://e-docs.bea.com. You can open the PDF in Adobe Acrobat Reader and print the entire document, or a portion of it, in book format. To access the PDFs, open the BEA WebLogic Integration documentation Home page, click the PDF Files button, and select the document you want to print.

If you do not have the Adobe Acrobat Reader installed, you can download it for free from the Adobe Web site at http://www.adobe.com/.

# Contact Us!

Your feedback on the BEA WebLogic Integration documentation is important to us. Send us e-mail at **docsupport@bea.com** if you have questions or comments. Your comments will be reviewed directly by the BEA professionals who create and update the WebLogic Integration documentation.

In your e-mail message, please indicate that you are using the documentation for the BEA WebLogic Integration 2.1 Service Pack 1 release.

If you have any questions about this version of BEA WebLogic Integration, or if you have problems installing and running BEA WebLogic Integration – Business Connect, contact BEA Customer Support through BEA WebSupport at **www.bea.com**. You can also contact Customer Support by using the contact information provided on the Customer Support Card, which is included in the product package.

When contacting Customer Support, be prepared to provide the following information:

- Your name, e-mail address, phone number, and fax number
- Your company name and company address
- Your machine type and authorization codes
- The name and version of the product you are using
- A description of the problem and the content of pertinent error messages

# Documentation Conventions

The following documentation conventions are used throughout this document.

| Convention | Item |
|---|---|
| **boldface text** | Indicates terms defined in the glossary. |
| Ctrl+Tab | Indicates that you must press two or more keys simultaneously. |
| *italics* | Indicates emphasis or book titles. |

| Convention | Item |
|---|---|
| `monospace text` | Indicates code samples, commands and their options, data structures and their members, data types, directories, and file names and their extensions. Monospace text also indicates text that you must enter from the keyboard.<br>*Examples*:<br>`#include <iostream.h> void main ( ) the pointer psz`<br>`chmod u+w *`<br>`\tux\data\ap`<br>`.doc`<br>`tux.doc`<br>`BITMAP`<br>`float` |
| **`monospace boldface text`** | Identifies significant words in code.<br>*Example*:<br>`void` **`commit`** `( )` |
| *`monospace italic text`* | Identifies variables in code.<br>*Example*:<br>`String` *`expr`* |
| UPPERCASE TEXT | Indicates device names, environment variables, and logical operators.<br>*Example*s:<br>LPT1<br>SIGNON<br>OR |
| `{ }` | Indicates a set of choices in a syntax line. The braces themselves should never be typed. |
| `[ ]` | Indicates optional items in a syntax line. The brackets themselves should never be typed.<br>*Example*:<br>`buildobjclient [-v] [-o name ] [-f` *`file-list`*`]...`<br>`[-l` *`file-list`*`]...` |
| `\|` | Separates mutually exclusive choices in a syntax line. The symbol itself should never be typed. |

| Convention | Item |
|---|---|
| `...` | Indicates one of the following in a command line:<br>■ That an argument can be repeated several times in a command line<br>■ That the statement omits additional optional arguments<br>■ That you can enter additional parameters, values, or other information<br>The ellipsis itself should never be typed.<br>*Example*:<br>`buildobjclient [-v] [-o name ] [-f file-list]...`<br>`[-l file-list]...` |
| .<br>.<br>. | Indicates the omission of items from a code example or from a syntax line. The vertical ellipsis itself should never be typed. |

CHAPTER

# 1 Introduction

The following topics are provided to summarize the WebLogic Integration – Business Connect system.

**Concepts**

## System Overview

WebLogic Integration – Business Connect can enable you to securely exchange large volumes of documents with your trading partners. WebLogic Integration – Business Connect packages documents in secure envelopes that are transmitted among trading partners according to schedules.

The following table describes the system's major components.

**Table 1-1 System Components**

| Icon | Component Description |
|---|---|
| 👤 | *Administrator* enables you to configure and maintain your WebLogic Integration – Business Connect system for document exchanges. The parameters you set using the Administrator application are stored in the WebLogic Integration – Business Connect database. |
| ⏻ | *Server* performs the document transfers. Server reads the parameters from the WebLogic Integration – Business Connect database and uses them to process, send and receive documents over the Internet. Server is designed for continuous operation, 24 hours a day, seven days a week. |
| 🔍 | *Tracker* enables you to monitor your system by viewing the alerts, events, traffic, transactions, and archive logs. You can use this application to search for documents, retransmit documents to partners or resubmit documents for processing. |

# How the System Works

Figure 1-1 and Figure 1-2 present high-level views of how WebLogic Integration – Business Connect processes outbound and inbound documents. These graphics show typical document flows, although your organization's configuration might differ.

**Figure 1-1 Outbound Document Processing**

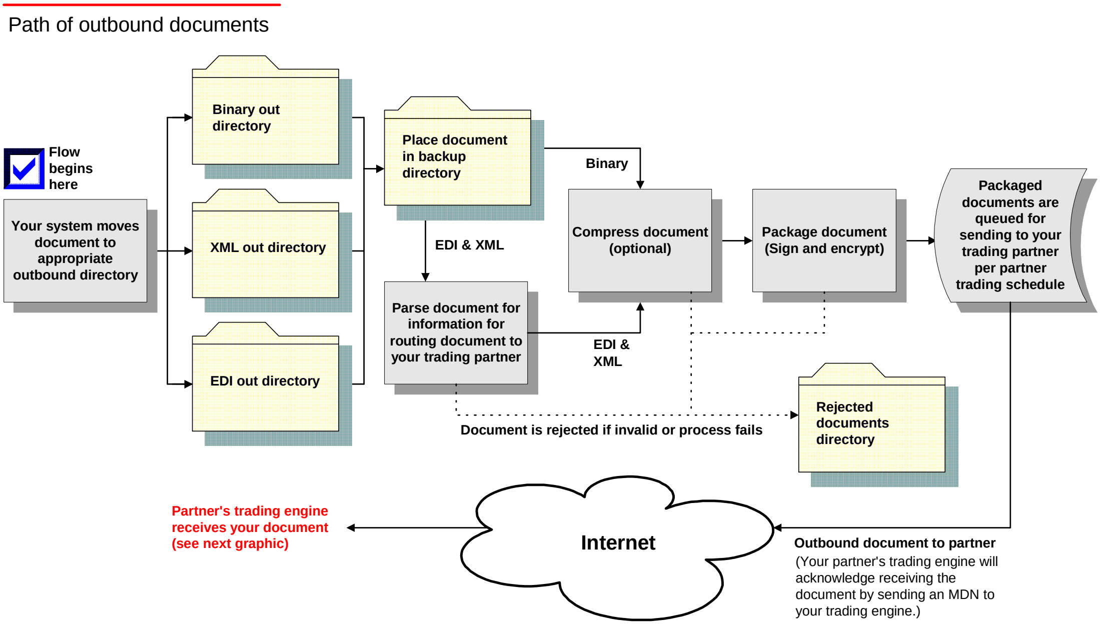
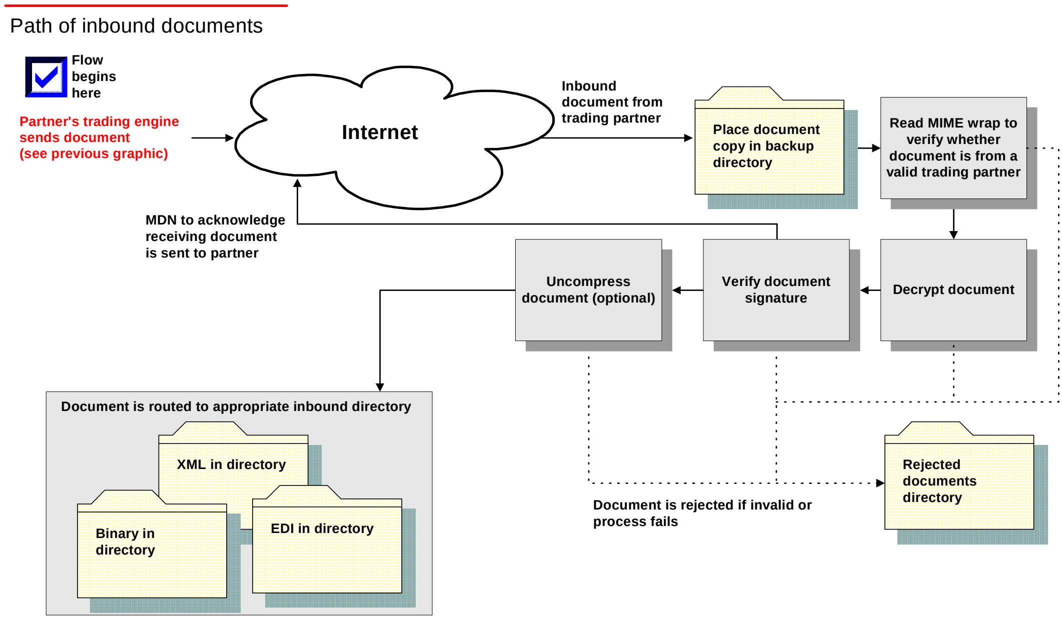

Path of outbound documents
Flow begins here
Your system moves document to appropriate outbound directory
Binary out directory
XML out directory
EDI out directory
Place document in backup directory
Binary
EDI & XML
Compress document (optional)
Package document (Sign and encrypt)
Packaged documents are queued for sending to your trading partner per partner trading schedule
Parse document for information for routing document to your trading partner
EDI & XML
Document is rejected if invalid or process fails
Rejected documents directory
Partner's trading engine receives your document (see next graphic)
Internet
Outbound document to partner
(Your partner's trading engine will acknowledge receiving the document by sending an MDN to your trading engine.)

**Figure 1-2 Inbound Document Processing**


Path of inbound documents
Flow begins here
Partner's trading engine sends document (see previous graphic)
Internet
Inbound document from trading partner
Place document copy in backup directory
Read MIME wrap to verify whether document is from a valid trading partner
MDN to acknowledge receiving document is sent to partner
Uncompress document (optional)
Verify document signature
Decrypt document
Document is routed to appropriate inbound directory
XML in directory
Binary in directory
EDI in directory
Rejected documents directory
Document is rejected if invalid or process fails

# What's New in 2.1

The following features are new to WebLogic Integration – Business Connect 2.1.

## Support for ebXML

Support for electronic business XML (ebXML) 1.0.

# Enhanced Certificate Authority Integration

Enhanced certificate authority integration includes the ability to acquire VeriSign XKMS certificates from within the Administrator application.

# Improved Reliability, Scalability, Performance

WebLogic Integration – Business Connect has enhanced synchronous support.

WebLogic Integration – Business Connect incorporates the latest Java 3 technology by using version 1.3.1 of the Java virtual machine.

# Enhanced Presentation and Usability

WebLogic Integration – Business Connect enables you to export company profiles and lets you import the backed-up profiles to a current or new installation of the application.

The addition of more keyboard commands lets you control the Administrator and Tracker applications without using a mouse.

WebLogic Integration – Business Connect generates alert messages to warn you when active company profile certificates are about to expire.

# Integration

WebLogic Integration – Business Connect has SOAP support, enhanced JMS integration and supports correlation IDs.

# Security

WebLogic Integration – Business Connect encrypts transport server passwords in the XML profiles you exchange with partners.

# System Administrator Duties

Your organization's WebLogic Integration – Business Connect system administrator is the focal point for setting up and managing the WebLogic Integration – Business Connect system. Some responsibilities include:

- Installing WebLogic Integration – Business Connect.
- Configuring WebLogic Integration – Business Connect and testing the interfaces between WebLogic Integration – Business Connect and your automated systems and between WebLogic Integration – Business Connect and the Internet.
- Controlling user access to the WebLogic Integration – Business Connect server and its processes.
- Exchanging partner profiles or certificates with your trading partners.
- Monitoring the WebLogic Integration – Business Connect system status.
- Receiving and responding to system alerts and notifications.
- Upgrading WebLogic Integration – Business Connect software to implement new releases.
- Overseeing system security to include managing certificates for you and your partners.
- Contacting technical support, if you have purchased support, to resolve WebLogic Integration – Business Connect issues. When working with technical support, it is recommended that your organization assign a single point of contact. This helps to identify and resolve issues.

CHAPTER

# 2 System Requirements

The following topics are provided regarding the hardware, software, communications, and interfaces required for installing WebLogic Integration – Business Connect.

**Concepts**

- "Windows Requirements" on page 2-1
- "UNIX Requirements" on page 2-3

**Note:** We strongly recommend that you read the release notes in the readme file on the installation CD for supplemental information about system requirements and installation.

## Windows Requirements

The following topics provide the hardware and software requirements for running WebLogic Integration – Business Connect on computers with Microsoft Windows operating systems.

- "Hardware on Windows"
- "Software on Windows" on page 2-2

# Hardware on Windows

A Windows computer must have the following minimum configuration.

- A Pentium-class processor running at 400 MHz or faster
- Random Access Memory (RAM)
  - 256MB recommended
  - 128MB minimum
- 250MB available hard drive space (see note)
- SVGA monitor
- CD-ROM drive (for installation)
- TCP/IP network interface
- Local area network (LAN) card and a persistent Internet connection is required.

**Note:** We recommend at least a 1 GB hard drive for both the application and the documents you exchange.

# Software on Windows

WebLogic Integration – Business Connect supports the following windows operating systems: Windows NT 4.0 and Windows 2000.

To use Windows NT 4.0, you also must have installed the domestic United States version of Service Pack 4 or later with the associated bug fixes.

**Note:** Apache as the mediated web server is not supported when configured on Windows NT or Windows 2000.

## Administrator Rights for Windows NT and 2000

For Windows NT or 2000, you must have administrator rights to successfully install the application. If you are not sure whether you have administrator rights for a machine, check with your system administrator.

### Recommended Software for Windows

You should have Internet Explorer version 4.01 or later or Netscape Navigator version 4.0 or later. You use a browser to read WebLogic Integration – Business Connect online help files and to obtain third-party certificates from certificate authorities such as VeriSign, Inc.

In addition, you need Adobe Acrobat Reader to view and print Using WebLogic Integration – Business Connect, which is provided in a portable document format (PDF) file named `buscon.pdf`. The PDF guide can also be found in the userdoc directory on the installation CD and in the doc subdirectory after you install the application. Acrobat Reader is available free from Adobe Systems Inc., www.adobe.com.

# UNIX Requirements

The following topics provide the hardware and software requirements for running WebLogic Integration – Business Connect on UNIX computers.

- “Hardware on UNIX”
- “Software on UNIX”

## Hardware on UNIX

Your computer must have the following minimum configuration to successfully install WebLogic Integration – Business Connect on a UNIX platform.

- Random Access Memory (RAM)
  - 256MB recommended
  - 128MB minimum
- 250MB available hard drive space (see note)
- CD-ROM drive

- TCP/IP network interface
- A persistent Internet connection.

**Note:** We recommend at least a 1 GB hard drive for both the application and the documents you exchange.

# Software on UNIX

This topic lists the operating systems and other software necessary to install and configure WebLogic Integration – Business Connect on UNIX platforms.

## X Windows and Operating Systems

Your system requires X Windows and any of the following UNIX operating systems:

- Hewlett-Packard HP-UX 11.0
- IBM AIX 4.3.3
- Sun Solaris 2.6, 2.7 or 2.8

## OS Patches

Patches for some operating systems are required to support the Java technology that WebLogic Integration – Business Connect uses. For a list of recommended patches, see the release notes in the readme file on the installation CD.

## Recommended Software for UNIX

You should have Internet Explorer version 4.01 or later or Netscape Navigator version 4.0 or later. You use a browser to read WebLogic Integration – Business Connect online help files and to obtain third-party certificates from certificate authorities such as VeriSign, Inc.

In addition, you need Adobe Acrobat Reader to view and print Using WebLogic Integration – Business Connect, which is provided in a portable document format (PDF) file named `buscon.pdf`. The PDF guide can also be found in the `userdoc` directory on the installation CD and in the doc subdirectory after you install the application. Acrobat Reader is available free from Adobe Systems Inc., www.adobe.com.

CHAPTER

# 3 Installation and Configuration

The following topics are provided for installing and configuring WebLogic Integration – Business Connect.

**Concepts**

- "Maintenance Considerations" on page 3-3

**Procedures**

- "Quick Reference Outline" on page 3-2

**Note:** We strongly recommend that you read the release notes in the readme file on the installation CD for supplemental information about system requirements and installation.

# Quick Reference Outline

The following is a quick reference outline of the steps for installing and configuring WebLogic Integration – Business Connect.

For a typical installation, it is strongly recommended you perform each of the following steps in order.

1. Make sure your organization has the required hardware and software to support WebLogic Integration – Business Connect.

   See:
   Chapter 2, "System Requirements"

2. Make sure your system's date and time settings are accurate. This can prevent problems in trading documents later.

3. Install WebLogic Integration – Business Connect.

   See:
   Chapter 4, "Installation on Windows"
   Chapter 5, "Installation on UNIX"

4. Start Administrator.

   See:
   "Starting Administrator or Tracker" on page 6-1

5. Set up your company profile.

   See:
   Chapter 9, "Company Profiles"

6. Generate or obtain a certificate for your company profile.

   See:
   Chapter 11, "Keys and Certificates"

7. Export your company profile to your trading partners.

   See:
   "Exporting a Company Profile to a File" on page 9-13

8. Import or create profiles for your trading partners.

   See:
   Chapter 12, “Partner Profiles”

9. Start the Server application to begin sending and receiving documents.

   See:
   “Starting the Server Application” on page 6-2

10. Start the Tracker application to view records of trading activity.

    See:
    Chapter 17, “Tracker”

# Maintenance Considerations

The following actions should be taken to maintain the WebLogic Integration – Business Connect system and its data:

- Back up all system directories and files as part of your normal backup schedule.
- Review the system logs at frequent intervals to detect potential problems.
- Check the specified e-mail accounts for alerts and notifications.
- Make sure there is enough disk space available for the system and the documents you exchange.
- Use the web browser server monitor to determine the status of Interchange Server. Select Tools→Launch Server Monitor in Administrator or Tracker.
- Use your available system tools to check memory usage.
- Check the archive logs.

CHAPTER

# 4 Installation on Windows

The following topics are provided for installing WebLogic Integration – Business Connect on computers with Microsoft Windows operating systems.

**Procedures**

- "Installing on Windows" on page 4-1
- "Configuring as a Windows Service" on page 4-3
- "Uninstalling on Windows" on page 4-8

## Installing on Windows

Use this procedure to install WebLogic Integration – Business Connect from the installation CD.

Before installing WebLogic Integration – Business Connect, see Chapter 2, "System Requirements," to ensure your hardware, software and communications are ready. In addition, see Chapter 3, "Installation and Configuration," before installing.

Optionally, we recommend that you create a Windows user ID and password to be used by all persons who work with WebLogic Integration – Business Connect. Use this user ID for all installation, configuration, maintenance or monitoring of the Administrator, Server and Tracker applications. See your systems administrator for information and assistance.

## Steps

1. Close any applications that might be running on your local machine.
2. Place the installation CD in the CD-ROM drive. When the CD menu appears, click Windows to launch the installation wizard.

   If the CD menu does not appear after you insert the CD in the CD-ROM drive, use Windows Explorer and double-click the `install.bat` file in the windows directory on the CD.
3. Follow the on-screen prompts for installing the application.

   When prompted to enter the registration number, type the registration number exactly as it appears on the CD jewel case. This entry is case sensitive.

   When prompted to type your company name, you can use any alphanumeric characters and spaces. You also can use the following characters: `/ \ : . _`. If your company name includes spaces, the application translates them as underscores.

   When prompted to select an installation directory, be advised that you cannot use a directory name that includes blank spaces.

   When you are prompted to click Next to install, a window appears that shows the progress of the installation. When the installation is completed, an installation summary window appears. Click Exit to exit the window.

   The installation process adds the WebLogic Integration – Business Connect program group to the Start menu. The icons are shown in the following table.

**Table 4-1 Program Icons**

| | | |
|---|---|---|
| Administrator | Start Server | Tracker |
| View Server Log | Stop Server | Document Generator |

There also are icons for opening the PDF file for *Using WebLogic Integration – Business Connect* and the help systems for Administrator and Tracker.

4. Select Start→Programs→BEA WebLogic Integration – Business Connect 2.1→Administrator to log on to Administrator. See “Starting Administrator or Tracker” on page 6-1.

# Configuring as a Windows Service

Running WebLogic Integration – Business Connect as a service in Windows NT or Windows 2000 provides the following functionality:

- Windows can start the Server application during the Windows system initialization process and stop the application when Windows is shut down.
- The Windows system administrator can use Windows services to manually start or stop the service from the local machine that hosts WebLogic Integration – Business Connect.

**Note:** While the Server application is set up as an Windows service, you should not start the application from the Start menu.

The following topics are provided for using WebLogic Integration – Business Connect as a Windows service.

- “Installing the ECEngine Utility to Support Configuration as a Windows Service” on page 4-4
- “Configuring as a Windows NT Service” on page 4-4
- “Configuring as a Windows 2000 Service” on page 4-5
- “Starting as a Service” on page 4-6
- “Removing from the List of Services” on page 4-6
- “Changing the NT Service Start-Up Options” on page 4-7

# Installing the ECEngine Utility to Support Configuration as a Windows Service

Use this procedure to install the ECEngine utility to enable you to configure WebLogic Integration – Business Connect as a service in Windows NT or Windows 2000.

## Steps

1. Click Start in Windows and then open an MS-DOS command prompt window.
2. Use the `cd` command to change the current directory to the following:

   ```
   installation_directory\util\NT Service
   ```

3. Then type the following:

   ```
   ECEngine.exe -i
   ```

4. Press Enter. Wait for the prompt to reappear.
5. Close the MS-DOS command prompt window.
6. Go to "Configuring as a Windows NT Service" or "Configuring as a Windows 2000 Service" on page 4-5.

# Configuring as a Windows NT Service

Use this procedure to configure WebLogic Integration – Business Connect as a service in Windows NT.

1. Install the ECEngine utility. See "Installing the ECEngine Utility to Support Configuration as a Windows Service" on page 4-4.
2. In the Windows NT Control Panel, double-click the Services icon. The Services dialog box opens.
3. In the Services dialog box, select ecengine and click the Startup button. The Service dialog box opens.

4. In the Logon As box, select the This Account option. Type `Administrator`, or select it from the list (click the More button to see the list). Type the Administrator's password in the fields.

   **Note:** Make sure the Interact with the desktop option is not selected.

5. Click OK.

   You can now start the Server application. If at some time Windows NT stops and is restarted, Server is also restarted and runs in the background. You also can reboot the Windows NT server to have the Server application run in the background.

   **Note:** The WebLogic Integration – Business Connect Windows NT service is set to Automatic mode as the default. If you want to start and stop the application manually, you should change the mode to Manual in the Windows NT Services panel. For more information see "Changing the NT Service Start-Up Options" on page 4-7.

## Configuring as a Windows 2000 Service

Use this procedure to configure WebLogic Integration – Business Connect as a service in Windows 2000.

1. Install the ECEngine utility. See "Installing the ECEngine Utility to Support Configuration as a Windows Service" on page 4-4.

2. Right-click on the My Computer icon on the desktop and select the Manage option. On the Computer Management window, expand the Services and Applications path and select Services.

3. Double-click the ECEngine service to open the ECEngine Properties window.

4. Select the Log On tab. Select the radio button for This account. In the field following This account, type `Administrator` or click Browse and select Administrator. Type the password for the Administrator user in the password and confirm password fields.

5. Make sure that `Automatic` displays in the Startup type field.

6. Click OK to save your changes and close the window.

7. Close the Computer Management window.

   The next time you start Windows, the WebLogic Integration – Business Connect Server application will start. You can use the Startup type field on the ECEngine Properties window to disable the service or change startup of the Server application from automatic to manual.

# Starting as a Service

After you have installed WebLogic Integration – Business Connect as a service on Windows NT or Windows 2000, the Server application starts every time you reboot the computer or after every system outage.

Because WebLogic Integration – Business Connect runs in the background, the Server Display window does not display as when you start the Server application from the Start menu. To view transactions and other events as the system writes them to the console log, open the View Server Log tool.

**Note:** You can stop the Server application in the current Windows session by selecting Programs→BEA WebLogic Integration – Business Connect 2.1→Stop Server on the Start menu. The next time you start Windows, the Server application starts again as a service.

# Removing from the List of Services

Use this procedure to remove WebLogic Integration – Business Connect from the list of services in Windows NT or Windows 2000.

## Steps

1. Click the Windows Start menu button and then open an MS-DOS command prompt window.

2. Use the `cd` command to change the current directory to the following:

   ```
   installation_directory\util\NTService
   ```

3. Then type the following:

   ```
   ECEngine.exe -u
   ```

4. Press Enter. The message “NT Service Uninstalled” appears.
5. Close the MS-DOS command prompt window.

# Changing the NT Service Start-Up Options

The WebLogic Integration – Business Connect installation process installs the application as a service with an automatic start-up option. This means that the service is automatically started during Windows NT initialization. You can change this option if necessary.

## Steps

1. In Windows click Start→Control Panel to open the Control Panel.
2. Double-click the Services icon. The Services dialog box appears.
3. Select WebLogic Integration – Business Connect in the Services box and then click the Setup button. The Service dialog box appears.
4. Select one of the following depending on your needs:
   - *Automatic*
     Select this option to have WebLogic Integration – Business Connect start when Windows NT starts.
   - *Manual*
     Select this option if you want to start WebLogic Integration – Business Connect manually from your desktop.
   - *Disabled*
     Select this option if you do not want to run WebLogic Integration – Business Connect manually or automatically. This option leaves the WebLogic Integration – Business Connect in the list of available NT services in a disabled state.

   **Note:** Make sure the Interact with the desktop option is not selected. This option is located at Start→Settings→Control Panel →Services→Startup.

5. Click OK on the Service dialog box and then click Close on the Services dialog box.

# Uninstalling on Windows

Use this procedure to remove WebLogic Integration – Business Connect from your Windows computer using the installation CD.

**Note:** To uninstall WebLogic Integration – Business Connect manually, delete the WebLogic Integration – Business Connect installation directory and the Start Programs menu shortcuts.

## Steps

1. Place the installation CD in the CD-ROM drive.
2. Click Start→Settings→Control Panel to open the Control Panel window.
3. Click the Add/Remove Programs icon to open the Add/Remove Programs Properties dialog box.
4. Select the WebLogic Integration – Business Connect program you want to remove and then click the Remove button.

   The uninstall program removes some of the application files and directories and deletes the folder containing the application shortcuts and the Start Programs menu shortcuts. You can remove the remaining components by deleting the WebLogic Integration – Business Connect installation directory.

CHAPTER

# 5 Installation on UNIX

The following topics are provided for installing WebLogic Integration – Business Connect on computers with UNIX operating systems.

**Concepts**

- “Initialization and Termination Scripts for UNIX” on page 5-1

**Procedures**

- “Installing on UNIX” on page 5-2
- “Uninstalling on UNIX” on page 5-8

## Initialization and Termination Scripts for UNIX

After you have installed the application on UNIX, tested it to your satisfaction and are ready to place it into production, you might want to run it automatically in the background.

Installed with the application is a System V initialization and termination script that enables you to start WebLogic Integration – Business Connect when you boot your system and close it when you shut your system down. We recommend that you get assistance from your UNIX system administrator if you want to implement this script.

The script is named `interchange` and is installed in the following location for each UNIX operating system:

*`installation_directory`*`/bin/interchange`

# Installing on UNIX

Use this procedure as the starting point for installing WebLogic Integration – Business Connect on the supported UNIX operating systems. They are:

- Hewlett-Packard HP-UX 11.0
- IBM AIX 4.3.3
- Sun Solaris 2.6, 2.7 or 2.8

The default installation process is text-based, but you can use an option that activates a graphical user interface during installation.

The following steps are common to all UNIX operating systems. Once you perform them, you are directed to the procedure for your particular operating system to complete the installation.

Before you install WebLogic Integration – Business Connect, see Chapter 2, "System Requirements," to ensure your hardware, software and communications are ready for installation of the application. In addition, see Chapter 3, "Installation and Configuration," before installing.

## Steps

1. Create a user account for WebLogic Integration – Business Connect (`connect`, for example) as the home directory for the application. For example, you can use one of the following as a home directory:

   ```
   /opt/connect
   ```

   ```
   /usr/local/connect
   ```

   **Note:** The directory *must not be automounted or on an automounted file system*. WebLogic Integration – Business Connect cannot run correctly on an automounted file system. This applies to volumes mounted using the automount utility and not to volumes that are automatically mounted at startup. WebLogic Integration – Business Connect cannot be installed on automounted volumes because of automatic unmounting of such drives.

2. Determine the device name of your CD-ROM drive.

   The installation CD has a standard ISO-9660 (High Sierra) file system with Rock Ridge extensions.

3. Determine how much RAM your server has. You need to enter this information during the installation routine.

4. See the installation procedure for your operating system:

   - "Installing on Hewlett-Packard HP-UX" on page 5-4
   - "Installing on IBM AIX" on page 5-5
   - "Installing on Sun Solaris" on page 5-6

   The following installation guidelines apply to all UNIX operating systems.

   You can use the following options with the `install.sh` command:

**Table 5-1 install.sh Options**

| Option | Description |
|---|---|
| `-g` | Uses a graphical user interface (GUI) for the installation routine. The default routine is text-based.<br>If you use this option, ensure you have X Windows connectivity to the server where you are going to install the application. This option tests for X Windows capability and, if the system passes, launches the GUI installation. |
| `-s` | Logs screen output to the file `*installation_directory*/logs/install.log` |
| `-x` | Prints all commands before they are executed. Used for debugging, this is a powerful tool when combined with the -s option. |

When using the default text-based installation, be aware of the following:

- Press Ctrl+C to cancel the installation at any time.
- When the license agreement text displays, press Enter to scroll through the text until you reach the accept agreement prompt or type `q` and press Enter to skip through the license and go directly to the accept agreement prompt.
- When the ready to install prompt appears, press Enter to install or type `2` and press Enter to cancel the installation.

When prompted to enter the registration number, type the registration number exactly as it appears on the CD jewel case. This entry is case sensitive.

When prompted to type your company name, you can use any alphanumeric characters and spaces. You also can use the following characters: `/ \ : . _`. If your company name includes spaces, the application translates them as underscores.

When prompted to select an installation directory, be advised that you cannot use a directory name that includes blank spaces.

When prompted to type the path where your HTML browser is located, you can skip this and specify a location later by selecting Tools→Preferences in Administrator. You use a browser to access the online help and obtain certificates from third-party certificate authorities. You will not be able to access the online help until you specify a browser.

Following installation, the Terminal window provides the command for starting Administrator. It also provides instructions for enabling group access to the application.

# Installing on Hewlett-Packard HP-UX

Use this procedure to install the application on your Hewlett-Packard HP-UX server.

## Steps

1. Log in as **root**.
2. Insert the WebLogic Integration – Business Connect CD into the CD-ROM drive.
3. If `/mnt` does not exist, create it with the following command:

   ```
   mkdir /mnt
   ```

4. Mount the WebLogic Integration – Business Connect CD with the following command:

   ```
   mount -o cdcase /dev/dsk/* /mnt
   ```

   where `/dev/dsk/*` is the device name of your CD-ROM.

5. Log out as root.

6. Log in to the account you created previously.

7. From the home directory, run the following command:

   ```
   /mnt/hpux/install.sh
   ```

8. Follow the instructions in the installation process.

9. Log out from the account.

10. Log in as root.

11. Unmount the WebLogic Integration – Business Connect CD by running the following command:

    ```
    umount /mnt
    ```

12. Eject the WebLogic Integration – Business Connect CD from the CD-ROM drive.

13. Log out as root.

# Installing on IBM AIX

Use this procedure to install the application on your IBM AIX server.

The Logical Volume Manager (LVM) enables the user to specify the physical sectors of the hard drive, or group of hard drives, to use when creating a volume on the AIX. The sectors closest to the center spindle of the disk generally give the fastest, most efficient, input and output reads and writes. The sectors towards the edge of the disk generally give the slowest input and output results. Once the LVM is used to create and mount a volume on the AIX, WebLogic Integration – Business Connect can be installed into a directory on that mount point just as it can with a non-LVM volume. The WebLogic Integration – Business Connect software itself is not aware of whether or not this is an LVM mount point.

## Steps

1. Insert the WebLogic Integration – Business Connect CD into the CD-ROM drive.
2. Log in as root
3. Run the command:

   ```
   mount -vcdrfs -r -p /dev/cd? /mnt
   ```

   where `/dev/cd?` is the device name of your CD-ROM. Possible values are `0` through `9`. If you have only one CD-ROM, its number is probably `0`.
4. Log out as root.
5. Log in to the account you created previously.
6. From the home directory, run the following command:

   ```
   /mnt/aix/install.sh
   ```
7. Follow the instructions in the installation process.
8. Log out from the account.
9. Log in as root.
10. Unmount the CD by running the following command:

    ```
    umount /mnt
    ```
11. Eject the CD from the CD-ROM drive.
12. Log out as root.

# Installing on Sun Solaris

Use this procedure to install the application on your Sun Solaris server. Note that separate procedures are provided, depending on whether you are running the automounter.

## Steps

**If you are running the automounter (the Solaris default):**

1. Log in to the account you created previously.
2. Insert the WebLogic Integration – Business Connect CD into the CD-ROM drive.
3. From the home directory, run the following command:

   ```
   /cdrom/solaris/install.sh
   ```

4. Follow the instructions in the installation process.
5. Eject the WebLogic Integration – Business Connect CD by running the following command:

   ```
   eject cdrom
   ```

**If you are not running the automounter:**

1. Insert the WebLogic Integration – Business Connect CD into the CD-ROM drive.
2. Log in as root.
3. Run the command:

   `mount` *`/dev/sr?`* `/mnt`

   where *`/dev/sr?`* is the device name of your CD-ROM. Possible values are `0` through `9`. If you have only one CD-ROM, its number is probably `0`.

4. Log out as root.
5. Log in to the account you created previously.
6. From the home directory, run the following command:

   ```
   /mnt/solaris/install.sh
   ```

7. Follow the instructions in the installation process.
8. Log out from the account.
9. Log in as root.

10. Unmount the WebLogic Integration – Business Connect CD by running the following command:

    ```
    umount /mnt
    ```

11. Eject the WebLogic Integration – Business Connect CD from the CD-ROM drive.

12. Log out as root.

# Uninstalling on UNIX

Use this procedure to remove WebLogic Integration – Business Connect from your UNIX computer.

## Steps

1. Log in to the account you created previously.

2. Shut down all WebLogic Integration – Business Connect applications.

3. Run the following command:

    ```
    rm -rf installation_directory
    ```

    All program files and documents are removed from your computer.

CHAPTER

# 6 Getting Started

The following topics are provided about using WebLogic Integration – Business Connect applications.

**Procedures**

## Starting Administrator or Tracker

Use this procedure to start the Administrator or Tracker application.

In a client-server configuration, start the Server application before you log on to Administrator or Tracker.

On some UNIX operating systems, occasional X windows scroll bar exceptions might occur in the normal use of the Administrator and Tracker X windows clients. These exceptions display in the terminal window where the clients were launched and are of no consequence. For example:

```
Warning:
 Name: HorScrollBar
 Class: XmScrollBar
 The specified scrollbar value is greater than the maximum
 scrollbar value minus the scrollbar slider size.
```

## Steps

1. Open the login dialog box with the default user, Administrator, in the user ID field.

   On the Windows Start menu, select Programs→Administrator or Tracker.

   On UNIX, ensure you have X Windows connectivity to the system where WebLogic Integration – Business Connect is installed. Log in to the account you created during the installation process. Run the following command:

   ```
   installation_directory/bin/admin
   ```

2. If you are starting the application for the first time, click OK. Do not type a user ID or a password. The default user ID is Administrator and the default password is blank.

# Starting the Server Application

The Server application must be running before you can exchange documents with your partners. Although you can start and stop Server at any time, we recommend you run the application continuously.

It is highly recommended that you have only one instance of WebLogic Integration – Business Connect on a computer. You should not have two or more instances installed at the same time on the same computer. The only exception is when you temporarily have two instances installed while upgrading the application. But even in that case, you should not run two applications at the same time on the same computer.

The Server application synchronizes with your system's time for time-stamping transactions. If you change the system time on the system where the Server application is running, you must re-start the Server application for the Server to recognize the change.

If you are already running WebLogic Integration – Business Connect Server as a Windows service, you should not start it from your desktop.

On UNIX computers you can set up the Server application as a system service. See "Initialization and Termination Scripts for UNIX" in "Installing on UNIX" in *Using WebLogic Integration – Business Connect*.

The following topics are provided:

- "Starting the Server on Windows" on page 6-3
- "Starting the Server on UNIX" on page 6-5

## Starting the Server on Windows

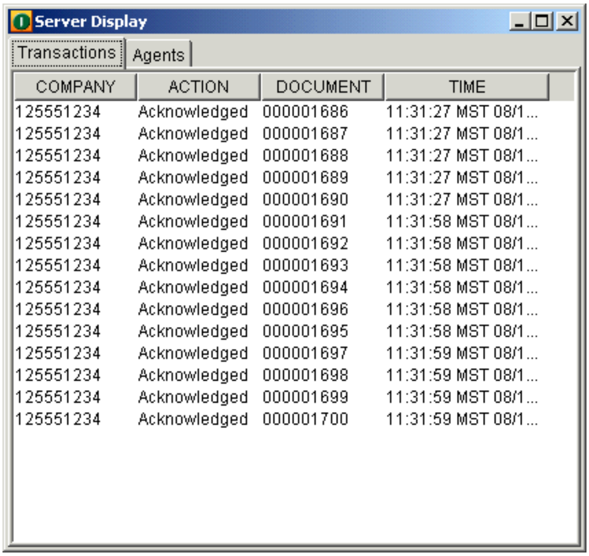
To start the Server application on Windows, select Start→Programs→BEA WebLogic Integration – Business Connect 2.1→Start Server. In addition to starting the server, the Server Display window opens. You can use a mouse to adjust the widths of the columns on the window.

On the Agents tab, the displays for outbound and inbound polling show three numbers following each active transport or document type. These are, in order, the document polling rate in seconds, the documents per cycle and the maximum threads. The polling rate is the interval when WebLogic Integration – Business Connect polls for inbound or outbound documents. The documents per cycle is the maximum number of documents the application can retrieve at each polling interval. The maximum threads are packaging threads for outbound documents and unpackaging threads for inbound documents.

Now you can:

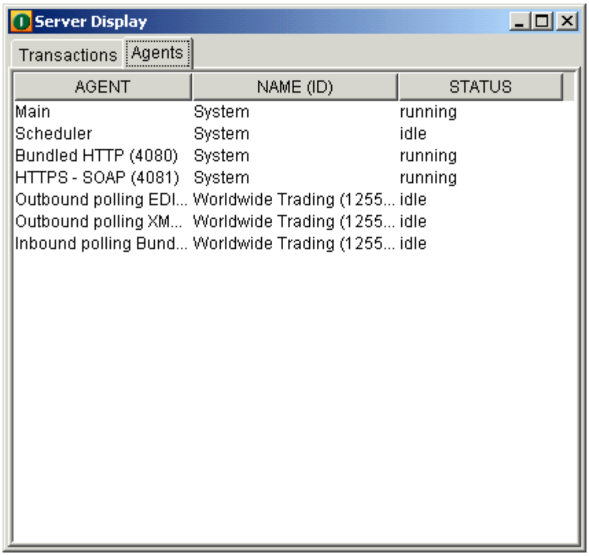
- Click the Transactions tab to observe document processing milestones.
- Click the Agents tab to observe which agents are running.
- Use the View Server Log utility to observe output to the console log. See "Monitoring the Server Application" on page 6-5.
- In Administrator or Tracker, select Tools→Launch Server Monitor to view server activity on a browser.

**Figure 6-1 Server Display Window Transactions Tab**



| COMPANY | ACTION | DOCUMENT | TIME |
|---|---|---|---|
| 125551234 | Acknowledged | 000001686 | 11:31:27 MST 08/1... |
| 125551234 | Acknowledged | 000001687 | 11:31:27 MST 08/1... |
| 125551234 | Acknowledged | 000001688 | 11:31:27 MST 08/1... |
| 125551234 | Acknowledged | 000001689 | 11:31:27 MST 08/1... |
| 125551234 | Acknowledged | 000001690 | 11:31:27 MST 08/1... |
| 125551234 | Acknowledged | 000001691 | 11:31:58 MST 08/1... |
| 125551234 | Acknowledged | 000001692 | 11:31:58 MST 08/1... |
| 125551234 | Acknowledged | 000001693 | 11:31:58 MST 08/1... |
| 125551234 | Acknowledged | 000001694 | 11:31:58 MST 08/1... |
| 125551234 | Acknowledged | 000001696 | 11:31:58 MST 08/1... |
| 125551234 | Acknowledged | 000001695 | 11:31:58 MST 08/1... |
| 125551234 | Acknowledged | 000001697 | 11:31:59 MST 08/1... |
| 125551234 | Acknowledged | 000001698 | 11:31:59 MST 08/1... |
| 125551234 | Acknowledged | 000001699 | 11:31:59 MST 08/1... |
| 125551234 | Acknowledged | 000001700 | 11:31:59 MST 08/1... |

**Figure 6-2 Server Display Window Agents Tab**



| AGENT | NAME (ID) | STATUS |
|---|---|---|
| Main | System | running |
| Scheduler | System | idle |
| Bundled HTTP (4080) | System | running |
| HTTPS - SOAP (4081) | System | running |
| Outbound polling EDI... | Worldwide Trading (1255... | idle |
| Outbound polling XM... | Worldwide Trading (1255... | idle |
| Inbound polling Bund... | Worldwide Trading (1255... | idle |

## Starting the Server on UNIX

To start the Server application on UNIX, ensure you have X Windows connectivity to the system where WebLogic Integration – Business Connect is installed. Log in to the account you created during the installation process. Run the following command:

```
installation_directory/bin/start_server
```

In Administrator or Tracker, select Tools→Launch Server Monitor to view server activity on a browser. Also, see "Monitoring the Server Application" on page 6-5 for information about using the `tail -f` command to view the console output. (A Server Display window is not available on UNIX as it is on Windows.)

# Monitoring the Server Application

The following topics are provided for monitoring activity on the Server application.

- Viewing the server.log File in Windows and UNIX
- Viewing Processes on UNIX
- Monitoring the Server with a Browser

## Viewing the server.log File in Windows and UNIX

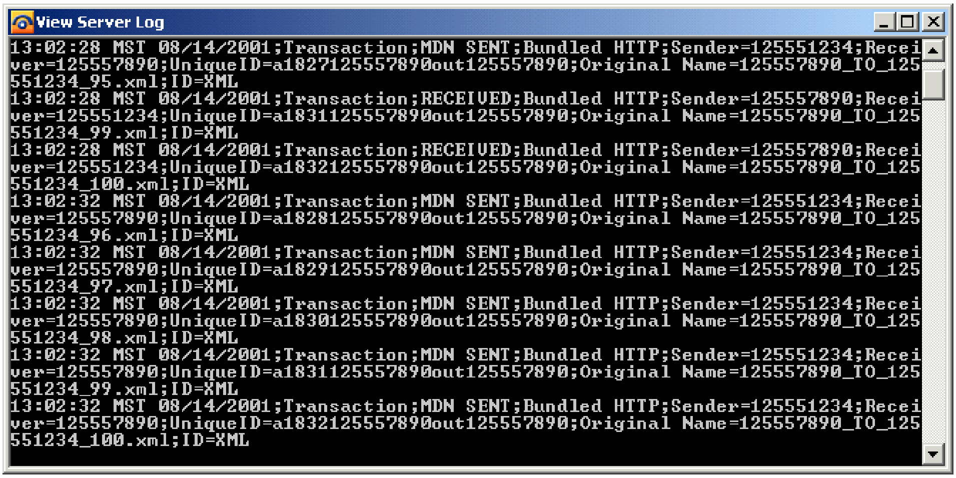
You can use the View Server Log utility to view real-time activity on the Server application. The activity you view is recorded in the `server.log` file in the logs subdirectory under the directory where WebLogic Integration – Business Connect is installed. You can use the View Server Log utility only on the computer where you have installed the Server application. All Server actions display as they occur.

**Note:** If the View Server Log window is open when archiving occurs, the file you are viewing is archived and no further Server activity displays. When this occurs, the following line appears at the bottom of the window: Archiving console logs [date and time]. Open a new View Server Log window to continue monitoring activity.

## Windows

On the Windows Start menu select Programs→BEA WebLogic Integration – Business Connect 2.1→View Server Log to open a console window displaying server messages that are written to the `server.log` file. The `server.log` file is located in *`installation_directory`*`\logs`.

**Figure 6-3 View Server Log Window**



```
13:02:28 MST 08/14/2001;Transaction;MDN SENT;Bundled HTTP;Sender=125551234;Recei
ver=125557890;UniqueID=a1827125557890out125557890;Original Name=125557890_TO_125
551234_95.xml;ID=XML
13:02:28 MST 08/14/2001;Transaction;RECEIVED;Bundled HTTP;Sender=125557890;Recei
ver=125551234;UniqueID=a1831125557890out125557890;Original Name=125557890_TO_125
551234_99.xml;ID=XML
13:02:28 MST 08/14/2001;Transaction;RECEIVED;Bundled HTTP;Sender=125557890;Recei
ver=125551234;UniqueID=a1832125557890out125557890;Original Name=125557890_TO_125
551234_100.xml;ID=XML
13:02:32 MST 08/14/2001;Transaction;MDN SENT;Bundled HTTP;Sender=125551234;Recei
ver=125557890;UniqueID=a1828125557890out125557890;Original Name=125557890_TO_125
551234_96.xml;ID=XML
13:02:32 MST 08/14/2001;Transaction;MDN SENT;Bundled HTTP;Sender=125551234;Recei
ver=125557890;UniqueID=a1829125557890out125557890;Original Name=125557890_TO_125
551234_97.xml;ID=XML
13:02:32 MST 08/14/2001;Transaction;MDN SENT;Bundled HTTP;Sender=125551234;Recei
ver=125557890;UniqueID=a1830125557890out125557890;Original Name=125557890_TO_125
551234_98.xml;ID=XML
13:02:32 MST 08/14/2001;Transaction;MDN SENT;Bundled HTTP;Sender=125551234;Recei
ver=125557890;UniqueID=a1831125557890out125557890;Original Name=125557890_TO_125
551234_99.xml;ID=XML
13:02:32 MST 08/14/2001;Transaction;MDN SENT;Bundled HTTP;Sender=125551234;Recei
ver=125557890;UniqueID=a1832125557890out125557890;Original Name=125557890_TO_125
551234_100.xml;ID=XML
```

## UNIX

On UNIX, log in to the account you created during the installation process. Run the following command:

```
tail -f installation_directory/logs/server.log
```

# Viewing Processes on UNIX

To view a snapshot of all WebLogic Integration – Business Connect components, you can use the `processes` command. The output of this command identifies each WebLogic Integration – Business Connect process that is running. This can be helpful in troubleshooting the application. Run the following command:

```
installation_directory/bin/processes
```

For definitions of the column headings displayed with the processes command, use the `man ps` command.

# Monitoring the Server with a Browser

Use this procedure to view Server application activity on a web page. You access the page with a browser such as Internet Explorer or Netscape Navigator that is on the same computer as WebLogic Integration – Business Connect Server or on a client computer with access to the Server. The Server application must be running for activity to display on the web page. The web page by default refreshes once a minute, but you can change the refresh rate.

The web page provides summary-level information not available in Tracker, such as totals for documents packaged, sent and received. It also shows whether server agents are active or idle and reports recent activity for transactions and alerts.

The information on the web page is for the current session of the Server application. If you stop and restart Server, the page display resets. You also can use the reset button to restart the counters in the summary section without restarting the application.

## Steps

1. Select Tools→Launch Server Monitor in Administrator or Tracker to display the web page on your browser.

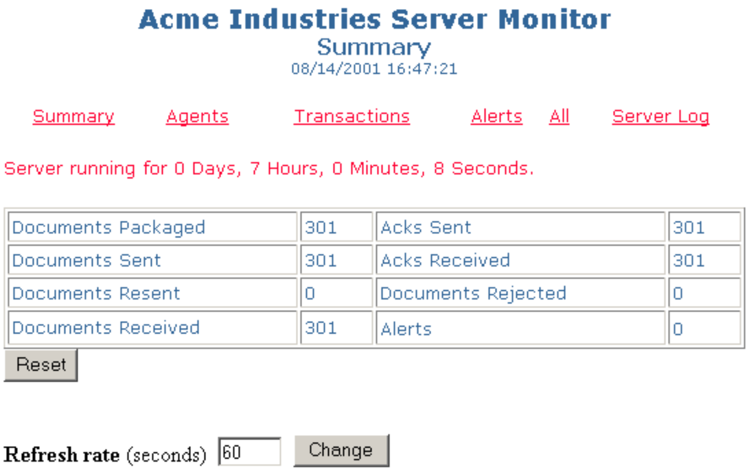
   Alternately, to access the web page outside of Administrator or Tracker, open a browser and type a URL in the following format:

   ```
   http://server_name:port_number/status/summary.html
   ```

Substitute the name of the computer running the Server application for `server_name`. The default `port_number` is 4080. If the computer name or port number has been changed, select Tools→Preferences in Administrator and check the host name and HTTP port fields on the General and Port tabs, respectively, of the Preferences window.

Press Enter to display the web page.

**Figure 6-4 Partial View of the Server Monitor Web Page**



Acme Industries Server Monitor

Summary

08/14/2001 16:47:21

Server running for 0 Days, 7 Hours, 0 Minutes, 8 Seconds.

| | | | |
|---|---|---|---|
| Documents Packaged | 301 | Acks Sent | 301 |
| Documents Sent | 301 | Acks Received | 301 |
| Documents Resent | 0 | Documents Rejected | 0 |
| Documents Received | 301 | Alerts | 0 |

**Refresh rate** (seconds) 60

2. Click the links at the top of the page to display different views of the page.

3. To reset the fields above the Reset button on the summary section of the page, click Reset.

4. To change the page refresh rate, scroll to the Refresh rate field, type the refresh rate you want in seconds and click Change.

## Description of Web Page

The follow list describes the information on the server monitor web page. To access the page, see "Steps" on page 6-7.

*[company name] Server Monitor*

The company name under which the application was installed identifies whose trading activity the server monitor page is tracking. This is the company name as it appears in the registered to field in Help →Product Information in Administrator or Tracker.

*Summary*

The following information is in the Summary section.

*Server running for [n] days, [n] hours, [n] minutes, [n] seconds*

The elapsed time that Server has been running. The web page displays activity for the current session only. If you restart Server, the counters reset to zero. For historical trading information use Tracker.

*Documents packaged*

The number of documents that have been packaged (encrypted and signed, as applicable) in the current session of Server. Packaging occurs before documents are sent to partners.

*Documents sent*

The number of documents sent to all trading partners in the current session of Server.

*Documents resent*

The number of documents resent in the current session of Server following unsuccessful attempts.

*Documents received*

The number of documents received from all trading partners in the current session of Server.

*Acks sent*

The number of message disposition notices (MDNs) sent to trading partners to acknowledge receiving documents from them in the current session of Server.

*Acks received*

The number of MDNs received from trading partners in the current session of Server. Your partners sent the MDNs to acknowledge receiving documents from you.

*Documents rejected*

The number of inbound or outbound documents that you or your trading partners have rejected in the current session of Server.

*Alerts*

The number of alert notices that Server has sent to you in the current session.

*Agents*

This area lists the active processes and inbound and outbound transport sessions in Server. The status of processes and transports are shown as running or idle.

*Transactions*

This area lists recent transactions in the current session of Server. For historical transaction information use Tracker.

*Alerts*

This area lists recent alert messages that have been generated in the current session of Server.

*RMI port*

The remote method invocation port that WebLogic Integration – Business Connect is using.

*Version*

The version and build numbers of the installed WebLogic Integration – Business Connect.

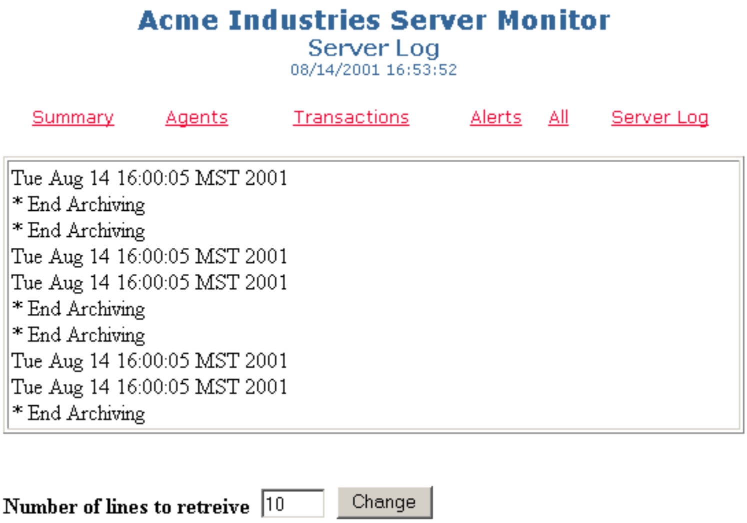
*Refresh rate*

The rate in seconds at which the web page refreshes.

*Server log*

This area lists the latest number of lines specified in the `server.log` file. To change the number of displayed lines, type the number in the number of lines to retrieve field and click Change.

**Figure 6-5 Server Log Area of Server Monitor Web Page**



Acme Industries Server Monitor

Server Log

08/14/2001 16:53:52

```
Tue Aug 14 16:00:05 MST 2001
* End Archiving
* End Archiving
Tue Aug 14 16:00:05 MST 2001
Tue Aug 14 16:00:05 MST 2001
* End Archiving
* End Archiving
Tue Aug 14 16:00:05 MST 2001
Tue Aug 14 16:00:05 MST 2001
* End Archiving
```

Number of lines to retreive 10

# Closing Applications

You can close and restart Administrator, Tracker and the Server application independently of each other.

You can close the Server application only on the computer where you have installed it and not from a client computer.

The following topics are provided.

- Closing the Server on Windows
- Closing the Server on UNIX
- Stopping All Processes on UNIX
- Closing Administrator or Tracker

## Closing the Server on Windows

To close the Server application on Windows, do one of the following:

- On the Start menu select Programs→BEA WebLogic Integration – Business Connect 2.1→Stop Server.
- If the Server Display window is displayed, click the Close button in the upper-right of the window.
- If you are running WebLogic Integration – Business Connect as a Windows service, use the Stop button in the Services dialog box. See “Configuring as a Windows Service” in “Installation on Windows” in *Using WebLogic Integration – Business Connect*.

## Closing the Server on UNIX

To close the Server application on UNIX, log in to the account you created during the installation process. Run the following command:

```
installation_directory/bin/stop_server
```

If shutdown is successful, the following messages are displayed:

```
$ bin/stop_server
starting shutdown process ...
found local registry
found server
shutting server down ...

Server successfully shutdown.
```

## Stopping All Processes on UNIX

Unlike the `stop_server` command, which only closes the Server application, the `kill_app` command on UNIX shuts down all WebLogic Integration – Business Connect processes. These include the Server, Administrator and Tracker applications.

You might want to use this command only after trying other steps to resolve issues such as not being able to close or open Administrator or Tracker or having multiple Java processes running.

To use the `kill_app` command, log in to the account you created during the installation process and run the following command:

```
installation_directory/bin/kill_app
```

## Closing Administrator or Tracker

Select File→Exit to close Administrator or Tracker.

# Printing Administrator Records

You can print a list of the records in the currently active information viewer by selecting File→Print or pressing Ctrl-P. Administrator prints to your system's default printer.

The application prints the data as displayed on the current information viewer, so maximizing the window size before you print yields longer horizontal printed records. Although the records print in landscape format, you might have to adjust the column widths in the information viewers to print the columns of data you want. This is necessary to account for differences in fonts and printers.

You can adjust column widths by placing the cursor over the lines between the columns to make a double-arrow appear. Click and hold the left button to adjust the column widths. You also can click and drag columns to change their locations.

CHAPTER

# 7 User Interface and Online Help

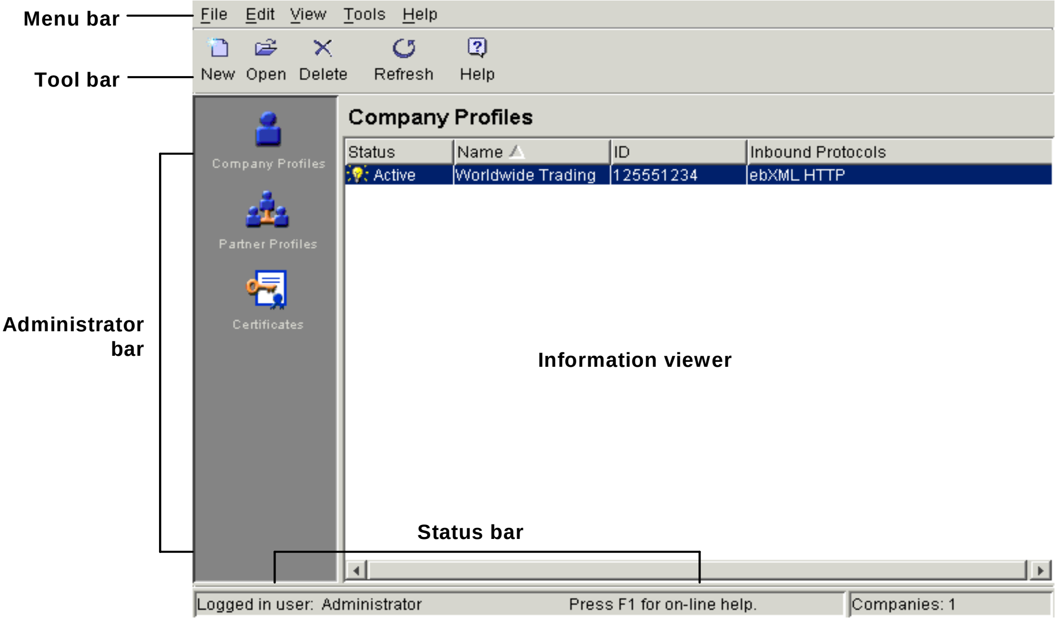
The following topics are provided for using the WebLogic Integration – Business Connect graphical user interface (GUI) and online help.

**Concepts**

- "Types of Windows" on page 7-2
- "Window Descriptions" on page 7-4
- "Navigating the Application" on page 7-6
- "Using Online Help" on page 7-8

Figure 7-1 identifies the components of a user interface window in Administrator. The components are similar in Tracker.

**Figure 7-1 User Interface**



Company Profiles

| Status | Name | ID | Inbound Protocols |
|---|---|---|---|
| Active | Worldwide Trading | 125551234 | ebXML HTTP |

Logged in user: Administrator Press F1 for on-line help. Companies: 1

# Types of Windows

In Administrator and Tracker, clicking the icons on the bar on the left side displays the primary windows you use for managing profiles and certificates and for viewing records of trading activity.

## Administrator

The following are the icons and related windows and functions in Administrator.

| Icon | Window | Function |
|---|---|---|
| 👤 | Company Profiles | This window enables you to manage company profiles. Company profiles contain information about your organization and specify the TCP/IP protocols your trading partners can use to send secure documents to you. |
| 👥 | Partner Profiles | This window enables you to manage partner profiles. Partner profiles contain information about your trading partners and specify the TCP/IP protocols you can use to send secure documents to them. |
| 🔑 | Certificates | This window enables you to manage digital certificates that ensure the security of the documents you and your partners exchange over the Internet. |

# Tracker

The following are the icons and related windows and functions in Tracker.

| Icon | Window | Function |
|---|---|---|
| ❗ | Alerts | This window enables you to view application events that might require user intervention to resolve. |
| 📥 | Inbound Traffic | This window enables you to view details about inbound documents. |
| 📤 | Outbound Traffic | This window enables you to view details about outbound documents. |
| 🚫 | Rejected Traffic | This window enables you to view details about rejected documents. |

| Icon | Window | Function |
|---|---|---|
| 🔍 | Transactions | This window enables you to view a reverse chronological listing of each milestone event in the processing of inbound and outbound documents. |

# Window Descriptions

The following table describes the various windows you encounter in the user interface.

**Table 7-1 User Inteface Windows**

| Type of window | Description |
|---|---|
| Information viewer | This window contains lists of records. You must first select a record before you can view, edit, copy, or delete it. To select the record, click on it and then press the button for the function you want to perform. Each record in the system appears on a separate line in the list. If there are more records than available space on this screen, a scrollbar appears on the right side of the screen. |
| Tab windows | Tab windows contain the detail behind each record. When you create or open a record, the tab windows appear. |
| Dialog boxes | Dialog boxes provide a working area where you can complete an action. They require you to make choices or enter data. Examples include the Certificate Profile or the Schedule-List of Dates dialog boxes. |
| Wizards | Wizards are series of linked dialog boxes that take you through a specific setup procedure from start to finish. Examples include the New Certificate and the Import Certificate wizards. |
| Message boxes | Message boxes provide feedback about actions. The box contains the message and an OK button for closing the box. |

# The Information Viewer

The user interface allows you to view or work with records for each of the configurable parts of the application by selecting an icon from the bar along the left side of the main Administrator and Tracker windows. You can use the information viewer to add, edit, or delete a record.

The commands you can use in the information viewer are available from the menu bar, the toolbar, or right-clicking the mouse. Commands or buttons that cannot be used in particular instances appear dimmed.

Right-clicking the mouse displays different pop-up menus on the various information viewer windows (Company Profiles, Partner Profiles and so on). For example, you can quickly change the status of a company profile by right-clicking the record in the Company Profiles information viewer and then left-clicking Change Status in the pop-up menu.

# Tab Windows and Dialog Boxes

The user interface is further organized into tab windows and dialog boxes to make maintenance logical and easy. From the information viewer, you can select and open a user, company profile or partner record to display an array of tab windows that contain the detailed information about that record.

You can complete or maintain these tabs in any order. If you click the Save button before you complete all required fields on all tabs, a message appears listing the fields you must complete.

## Symbols

The following symbols are used on windows in Administrator.

| **This symbol** | **Represents this status in the information viewer** |
|---|---|
| 💡 | A lit, yellow light bulb represents an active record. |
| 💡 | A dim, blue light bulb represents an inactive record. In the Certificates information viewer, this light bulb represents a valid certificate. |
| 💡 | A colorless light bulb represents a retired record (certificates only). |
| 💡 | A red light bulb represents a pending record (certificates only). |

# Navigating the Application

You can use a mouse to navigate the user interface or you can use keyboard commands for mouse-free navigation.

## Tool Bar Text

You can view the names of the tool bar icons by selecting View→Toolbar Text. This control toggles the names on and off. The default is to display toolbar text.

# Required Fields

An asterisk next to a field name on a window means it is a system-required field. The system prompts you to complete such fields if you leave them blank.

# Sorting Columns of Data

You can sort data in information viewers in Administrator and Tracker. Some of the Name columns in Administrator and the Date columns in Tracker can be sorted in ascending or descending order. Arrows pointing up or down indicate the columns you can sort. An up arrow indicates ascending order and a down arrow indicates descending order. You can click the column to toggle between ascending and descending order.

# Tab and Ctrl-Tab

In a window or dialog box, you can use the Tab key to move the focus from one field, button, option, or check box to the next. You can then use the spacebar to select an option or check box or to click a button. In some cases, such as tables, you must use Ctrl-Tab to move into or out of a table and use Tab to move from cell to cell.

## Ctrl Keys

The following keyboard commands, using the Ctrl key to execute functions, are available.

| Command | Description |
|---|---|
| Ctrl-A | Select all |
| Ctrl-F | Find |
| Ctrl-N | New |
| Ctrl-O | Open |
| Ctrl-P | Print |

## Alt Keys

WebLogic Integration – Business Connect follows the Windows convention of using Alt key commands to display toolbar menus. For example, Alt-F displays the File menu, Alt-E displays the Edit menu, Alt-V displays the View menu, and so on.

# Using Online Help

WebLogic Integration – Business Connect includes online help that is displayed in your Internet browser.

The online help is available from within Administrator and Tracker. Administrator contains help topics for all aspects of the application, with the exception of those for Tracker. Tracker has its own help system. Help topics for the Server application are included in the help for Administrator.

## Accessing Help

You can access online help by:

- Selecting Help→Help in Administrator or Tracker.
- Pressing the F1 key in Administrator or Tracker.
- Clicking Help on the toolbar in Administrator or Tracker.
- On the Windows Start menu, selecting Programs→BEA WebLogic Integration – Business Connect 2.1→Administrator Help or Tracker Help.

## Navigating Help

Using the online help is similar to navigating any web site. You can scroll through the table of contents in the left side of the help frameset and click on the topic you want. Help topics appear in the right frame. Icons on each help topic page let you jump to the home page, the previous topic, the next topic and the index.

## Searching for Help Topics

The online help has a key word search feature. On the search tab, type a word or phrase and click Search. The help system displays a list of topics that contain the word or phrase, if any matches are found. If you do not find the topic you want, try searching using other key words or look in the Contents or Index.

CHAPTER

# 8 Overview of Profiles

The following topics are provided about company and partner profiles and how they work together in WebLogic Integration – Business Connect.

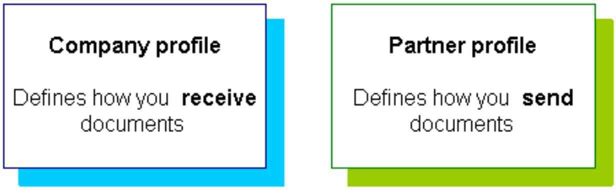
**Concepts**

- "How Profiles Work" on page 8-1
- "The Company and Partner Profile Relationship" on page 8-4
- "Document Sizes" on page 8-5

## How Profiles Work

WebLogic Integration – Business Connect organizes the information you need to exchange documents with your trading partners into company and partner profiles. This makes it easy to set up and maintain trading relationships. Company profiles define how you receive documents from your partners. Partner profiles define how you send documents to your partners.

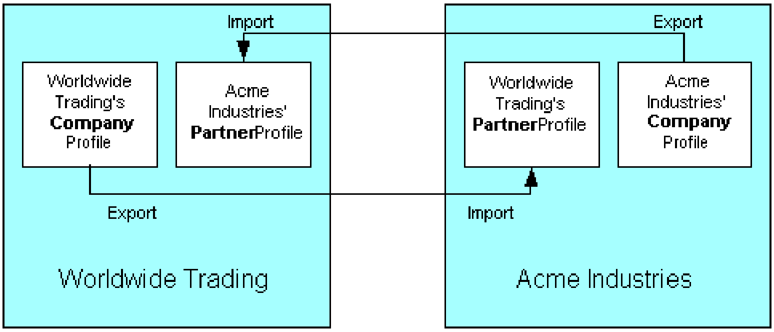
**Figure 8-1 Purpose of a Company and Partner Profile**


Company profile
Defines how you receive documents
Partner profile
Defines how you send documents

To establish a trading relationship, you create and export your company profile to your trading partner, who imports it to WebLogic Integration – Business Connect as your partner profile. Conversely, your partner creates and exports a company profile that you import as a partner profile on your system.

The following illustration shows the company-partner profile exchange within WebLogic Integration – Business Connect. This example uses Worldwide Trading as the local trading partner and Acme Industries as the remote trading partner.

**Figure 8-2 Example of Company-Partner Profile Exchange**


Import
Export
Worldwide Trading's **Company** Profile
Acme Industries' **Partner**Profile
Worldwide Trading's **Partner**Profile
Acme Industries' **Company** Profile
Export
Import
Worldwide Trading
Acme Industries

To understand how a company and a partner profile work together, let's examine half of the relationship at Worldwide Trading. Once we've reviewed this half, you will understand that the half at Acme Industries is the reverse, or the complement, of Worldwide Trading's.

# Company Profiles

At a high level, the company profile is a combination of local information to be used by your WebLogic Integration – Business Connect system and exportable information to be used by your trading partners. The local information is used by your WebLogic Integration – Business Connect system to set your document back-up options, tune the performance of your system, handle the files you receive from your translator, integrate with certain translators and manage your file system. While these settings are significant to you, they are not relevant for your trading partner. The local information includes most of the settings in the Preferences tab and all the information in the System Directories tab of the Company Profile window.

By contrast, the exportable information in the company profile is important to your trading partners and consists of what transports you want your partners to use when they send documents to you. The exportable information is contained in the Identity and Inbound Protocols tabs and the notification e-mail address field of the Preferences tab.

The Company Profile window organizes information into the following tabs:

- *Identity*
  In the Identity tab you specify the address of the company and provide information about your WebLogic Integration – Business Connect point of contact. You can also view the company profile name and ID.

- *Preferences*
  In the Preferences tab you indicate whether the profile is active or inactive. You also provide the e-mail addresses for alerts and notifications as well as the name or IP address of your SMTP server for receiving such messages. You can choose your inbound and outbound backup or archive options for documents.

- *Inbound Protocols*
  In the Inbound Protocols tab you enter the information about how you receive documents. You must supply all the information for at least one TCP/IP transport method.

- *XML*
  In the XML tab you enter XPath strings that locate sender and recipient information in your XML documents.

- *System Directories*
  In the System Directories tab you can specify where your WebLogic Integration – Business Connect-related files are to be stored. The file directories can be local or shared.

- *Integration*
  In the Integration tab you can integrate WebLogic Integration – Business Connect with an FTP server or IBM MQSeries or JMS systems. You also can set up post-processing for inbound documents.

- *Tuning*
  In the Tuning tab you can adjust polling rates and documents per cycle for outbound and inbound documents.

## Partner Profiles

Just as you send a company profile to your partner, your partner exports a company profile to a file and sends it to you. You import this file as the partner's profile on your system. When you open this partner profile, you again see a combination of imported and local information. The imported information consists of identifying information about your partner's company, such as the partner's contact information, and the transport methods your partner supports. This information is in the Identity and Outbound Protocol tabs of the Partner Profile window.

# The Company and Partner Profile Relationship

To describe how company and partner profiles work together, let's review the information in the transport tabs of the company and partner profiles.

When you or your partner sets up a company profile, you each decide what transport method or methods to make available to all of your trading partners. At a minimum, you must select one transport method by which your partners can send documents to you and complete all the fields for that method. If you choose to support additional transport methods, you fill in the appropriate information for them, too.

When you import your partner's profile and open the Partner Profile window Outbound Protocol tab, you see your partner's transport choices. You know that your partner is prepared to receive documents from you by way of any of the transport methods that your partner has indicated. Although your partner might have indicated two or more transports, you pick only the one you want to use to send documents to that partner. The one you pick to send documents to your partner does not have to match the one your partner picks to send documents to you. Obviously, you would not pick a transport method that your partner has not made available to you.

Your choice of transports also applies to the security you want to apply to the documents you exchange with this partner, except for one important advisory. When you change settings on the Partner Profile window Security tab, you must coordinate the changes with your trading partner.

You and your trading partners might want to change security settings based on what your systems can support. If you and your partner use WebLogic Integration – Business Connect, you need to ensure that each of your security settings are identical.

# Document Sizes

WebLogic Integration – Business Connect has no limitations on maximum sizes of documents, whether inbound or outbound. Limitations on document sizes rest solely on your and your partners' hardware resources and software configurations for various transport methods. A document that one organization considers to be large might be small by another organization's standards. Your organization might have to conduct its own capacity tests to determine the optimal transport for your trading situation.

CHAPTER

# 9 Company Profiles

The following topics are provided about managing company profiles in WebLogic Integration – Business Connect.

**Concepts**

- "Company Profile Overview" on page 9-2
- "The Difference Between the POP and SMTP Transports" on page 9-3
- "Inbound Fall-Off Algorithm" on page 9-4
- "Distributing Profiles to Partners" on page 9-4
- "Supported Formats for Profile IDs" on page 9-5
- "Transport Selection Considerations" on page 9-31

**Procedures**

- "Adding or Changing a Company Profile" on page 9-9
- "Exporting a Company Profile to a File" on page 9-13
- "Importing a Backed Up Company Profile" on page 9-16
- "Changing All System Directories at Once" on page 9-18
- "Deleting a Company Profile" on page 9-19
- "Adding an Inbound Protocol" on page 9-29
- "Editing an Inbound Protocol" on page 9-30
- "Removing an Inbound Protocol" on page 9-31

**Windows**

- "Company Profile Identity Tab" on page 9-19
- "Company Profile Preferences Tab" on page 9-22
- "Company Profile Inbound Protocols Tab" on page 9-27
- "Company Profile XML Tab" on page 9-38
- "Company Profile System Directories Tab" on page 9-40
- "Company Profile Integration Tab" on page 9-46
- "Company Profile Tuning Tab" on page 9-64

# Company Profile Overview

You can use the Company Profile information viewer to set up and maintain company profiles.

With a company profile, you can trade with different trading partners using:

- Any transport; you can use different transports with different partners. You do not have to use the same transport method as your trading partner.
- Any document type, including X12, EDIFACT, XML or binary documents such as those generated by legacy business applications, SAP, PeopleSoft or Oracle Financial.

You might find it necessary to set up more than one company profile. Each company profile you set up must have its own ID. Moreover, creating additional company profiles affects the performance of WebLogic Integration – Business Connect by adding to its processing overhead. You should not create multiple company profiles unless you need them.

One reason for creating more than one company profile is you might have more than one business unit, each of which uses a different EDI ID.

# The Difference Between the POP and SMTP Transports

WebLogic Integration – Business Connect has two e-mail transport methods: POP and SMTP. They are distinctly different transports.

POP, which sends documents via Post Office Protocol (POP), is a store-and-forward transport. WebLogic Integration – Business Connect sends packaged documents to your Simple Mail Transfer Protocol (SMTP) server, and your SMTP server sends them to your partner's POP3 server. If your trading partner's POP3 server is off line, your WebLogic Integration – Business Connect can still send the document, but will not get back an MDN acknowledging the document until the partner's POP3 server comes back on line.

SMTP can only occur when WebLogic Integration – Business Connect is running on both ends of the trading relationship. It is not a store-and-forward transport; it is more like bundled HTTP and HTTPS, in that it requires a direct connection with your trading partner's WebLogic Integration – Business Connect. If your partner's WebLogic Integration – Business Connect server is not running, you cannot send a document to the partner. In using SMTP, WebLogic Integration – Business Connect is its own (internal) SMTP server on both ends.

For details about configuring these transports, see “SMTP Inbound Transport” on page 9-32 and “POP Inbound Transport” on page 9-36.

# Inbound Fall-Off Algorithm

WebLogic Integration – Business Connect uses a fall-off algorithm for document polling retries in the event of a transport connection failure. The algorithm is based on the inbound polling rate plus a wait state of 10 seconds that doubles at each successive failure. For example, if the inbound polling rate is 30 seconds and a connection failure occurs, the wait state becomes active and the next polling interval is 40 seconds (polling rate of 30 seconds plus one wait state of 10 seconds). The wait state doubles for each successive failure, so the polling interval increases as follows: 50 seconds (30 seconds plus two wait states), 70 seconds (30 seconds plus four wait states), and so on until a plateau of 12 hours is reached and repeated at that interval.

Wait states are maintained by company profile for each transport type. The original polling rate returns when the transport connection is restored or when any part of the company profile is updated, on the presumption that the update resolves the connection problem. However, the fall-off algorithm restarts if the transport connection failure persists.

WebLogic Integration – Business Connect also uses a fall-off algorithm in attempting to resend outbound documents in the event of transport failures. For details see "Partner Profile Preferences Tab" on page 12-14.

# Distributing Profiles to Partners

Once you have created a company profile and have associated a certificate with it, you must distribute the profile to your trading partners. Your partners who use WebLogic Integration – Business Connect import your profile as a partner profile.

The first step in distributing a company profile is to save the profile information in a file. WebLogic Integration – Business Connect has an export feature that enables you to export a company profile as a partner profile saved in an XML or PFL file. See "Exporting a Company Profile to a File" on page 9-13.

After you export your company profile to a file, you distribute it to your partners on diskette, by e-mail or some other secure means. Although you can negotiate the exact details, distributing your company profile for the first time should be done with some care. It is recommended that you accomplish this first exchange by some means that ensures secure delivery. Examples of appropriate means include in-person, by way of the U.S. Postal Service or another delivery service such as Federal Express. After your partner has imported your profile and set up a trading profile for you, you can use e-mail or the Update Partner feature to send subsequent profiles and certificates.

When your partner receives your company profile file, the partner imports the data in the file to create a partner profile for you on the partner's WebLogic Integration – Business Connect system.

# Supported Formats for Profile IDs

You can use alphanumeric and non-alphanumeric characters as well as spaces in profile IDs. All alphanumeric characters are supported. Use of specific non-alphanumeric characters is supported, but results in the system creating names of data directories and processed files that use hex codes in place of the characters. Spaces in IDs are allowed within limitations. You also can create an ID in an electronic data interchange (EDI) format. The following topics are provided for supported profile ID formats:

- Alphanumeric Characters in Profile IDs
- Non-Alphanumeric Characters in Profile IDs
- EDI Format for Profile IDs
- Spaces in Profile IDs

## Alphanumeric Characters in Profile IDs

You can use any alphanumeric characters in profile IDs. These are the alphabetic characters a through z (upper and lower case) and the numerals 0 through 9.

# Non-Alphanumeric Characters in Profile IDs

WebLogic Integration – Business Connect supports specific non-alphanumeric characters in profile IDs. WebLogic Integration – Business Connect converts most of these characters to ASCII hex codes when it creates the names of document directories in the file system. The system creates directories for inbound and outbound documents for each company profile under the WebLogic Integration – Business Connect data directory. Profile IDs are used for the directory names. You can see examples of these directory names on the Company Profile window System Directories tab. The non-alphanumeric characters display as literals in the information viewers in Administrator, but as hex codes on the System Directories tab.

Not only data directory names, but the names that WebLogic Integration – Business Connect gives to processed documents are based on profile IDs. The non-alphanumeric characters in names of processed documents convert to hex codes in the WebLogic Integration – Business Connect data directories in the file system. In Tracker, if IDs contain non-alphanumeric characters, files names for processed documents also display with the hex codes.

The following table shows the non-alphanumeric characters that can be used in profile IDs. It also shows the hex code for the character that is used in document directory names and names of processed documents. Note that the underscore is the only character that is not converted to a hex code in names of data directories and processed files.

**Table 9-1 Non-Alphanumeric Character Usage**

| Character | Description | Hex code |
|---|---|---|
| ‘ | accent | %60 |
| ’ | apostrophe | %27 |
| @ | at symbol | %40 |
| / | back slash | %2f |
| ) | close parenthesis | %29 |
| : | colon | %3a |
| , | comma | %2c |

**Table 9-1 Non-Alphanumeric Character Usage (Continued)**

| Character | Description | Hex code |
|---|---|---|
| $ | dollar sign | %24 |
| = | equals sign | %3d |
| ! | exclamation point | %21 |
| \ | forward slash | %5c |
| - | hyphen | %2d |
| { | left brace | %7b |
| [ | left bracket | %5b |
| ( | open parenthesis | %28 |
| % | percent sign | %25 |
| + | plus sign | %2b |
| ? | question mark | %3f |
| } | right brace | %7d |
| ] | right bracket | %5d |
| ~ | tilde | %7e |
| _ | underscore | n/a |
| \| | vertical line | %7c |

# EDI Format for Profile IDs

You can set up a profile ID in a qualifier-EDI ID format. Under this format, a 2-character qualifier precedes the EDI ID as follows:

**Table 9-2 EDI ID Format**

| Qualifier | Description |
|---|---|
| 01 | Indicates that a Dun & Bradstreet Data Universal Numbering System (D-U-N-S®) number is used as the ID. |
| 08 | Indicates that the ID is user defined. |
| 12 | Indicates that a phone number is used as the ID. |

If you use a 2-character qualifier-EDI ID format, type the EDI ID immediately after the qualifier as one string with no spaces, hyphens or other separating characters. For a complete list of EDI qualifiers, see *ASC X12 Standards for EDI.*

# Spaces in Profile IDs

Spaces mostly are useful as placeholders for a 2-character qualifier for a profile ID in EDI format, but you can use them in any ID. The following table describes the allowable formats for using spaces in IDs. The character * represents a space and *n* represents an alphanumeric character.

**Table 9-3 Using Spaces in IDs**

| Proper ID format | Why you can use it |
|---|---|
| **nnnnnnnnnn* | Two spaces can be used in lieu of a 2-character qualifier. |
| *nnnnn*nnnnn* | A space can be used within the ID itself. The space cannot be in the third position or the last position of the ID. |
| **nnnnn*nnnnn* | Two spaces can be used in lieu of a 2-character qualifier and a space is used within the ID itself. |
| *nnnnnnnnnn* | One space can precede the first character of an ID. |

**Table 9-3 Using Spaces in IDs (Continued)**

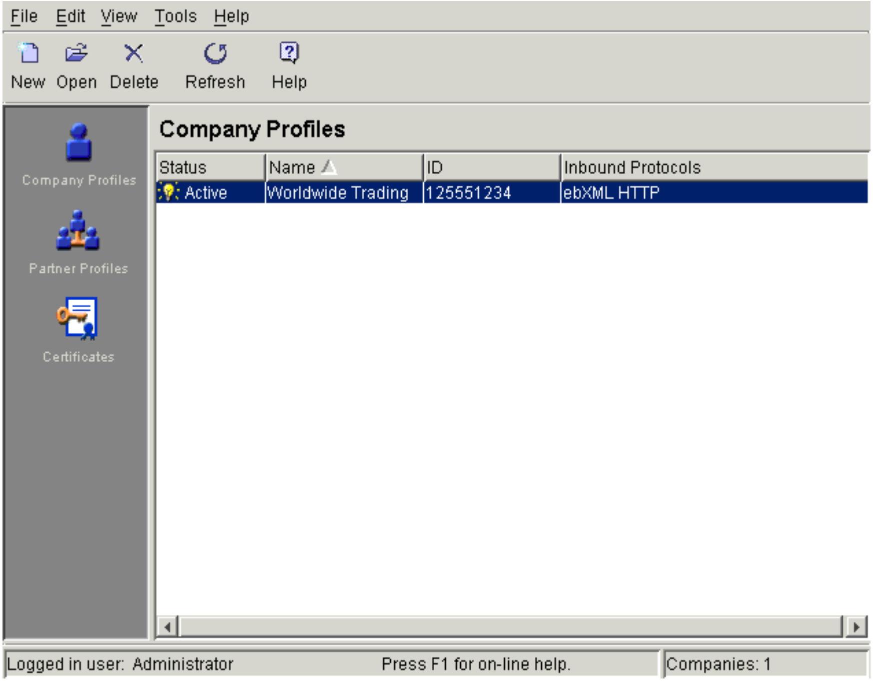
| Proper ID format | Why you can use it |
|---|---|
| *n*nnnnnnnnn* | A space can be used in the second position of an ID. |

The system displays an error message if you try to create an ID with an unsupported format.

# Adding or Changing a Company Profile

Use this procedure to add a new profile or change a profile.

**Figure 9-1 Company Profiles Information Viewer**



| Status | Name | ID | Inbound Protocols |
|---|---|---|---|
| Active | Worldwide Trading | 125551234 | ebXML HTTP |

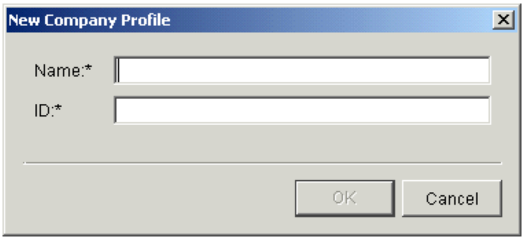
Logged in user: Administrator    Press F1 for on-line help.    Companies: 1

## Steps

1. Click Company Profiles on the Administrator bar to open the Company Profiles information viewer. The window displays any company profiles added earlier.
2. To change a company profile, double-click the profile's record line in the information viewer. Or, select the profile and click Open. The Company Profile window Identity tab opens. Go to step 4.

   To add a company profile, click New to open the New Company Profile dialog box.

   **Figure 9-2 New Company Profile Dialog Box**

3. Complete the following fields for a new company profile.
   - *Name*
     Type the profile name in this required field. You can edit this name after you have added and saved a profile. You can use any alphanumeric characters and the following characters: back slash (\), hyphen (-), forward slash (/), colon (:), underscore (_), comma (,), period (.). You can use spaces in your name; WebLogic Integration – Business Connect translates them to underscores. WebLogic Integration – Business Connect removes any other characters.

- *ID*
  Type an identification for the profile. You cannot change the ID after you have created a profile.

  You can use alphanumeric and non-alphanumeric characters as well as spaces in profile IDs. All alphanumeric characters are supported. Use of specific non-alphanumeric characters is supported, but results in the system creating names of data directories and processed files that use hex codes in place of the characters. Spaces in IDs are allowed within limitations. You also can create an ID in an electronic data interchange (EDI) format. For details see "Supported Formats for Profile IDs" on page 9-5.

  The system displays an error message if you try to create an ID with an unsupported format.

Click OK to open the Company Profile window Identity tab.

4. Add or change information on the Company Profile window tabs. You can complete a new profile or make changes to an existing one by choosing the tabs in any order you want.

   See the following topics for information about adding or changing information on the tabs:

**Table 9-4 Adding or Changing Profile Information**

| If you want to . . . | See . . . |
|---|---|
| Specify the address of the company and provide information about your WebLogic Integration – Business Connect point of contact. You can also view the company profile name and ID. | "Company Profile Identity Tab" on page 9-19 |
| Set up or change preferences information for a company profile, including: trading status, alert and notify e-mail addresses and SMTP server, and document backup options. | "Company Profile Preferences Tab" on page 9-22 |
| Set up or change information about the transport methods you allow trading partners to use to send documents to you. | "Company Profile Inbound Protocols Tab" on page 9-27 |
| Identify senders and receivers in Extensible Markup Language (XML) documents that you send to trading partners. | "Company Profile XML Tab" on page 9-38 |

**Table 9-4 Adding or Changing Profile Information (Continued)**

| If you want to . . . | See . . . |
|---|---|
| Change the directories where your document-related information is physically stored. Use this tab only if you want to use other than the default locations. | "Company Profile System Directories Tab" on page 9-40 |
| Send inbound or outbound documents to an FTP server, JMS or IBM MQSeries application. You also can set up post-processing commands for inbound documents. | "Company Profile Integration Tab" on page 9-46 |
| Adjust the polling rate and documents per cycle of inbound transports and outbound documents types. | "Company Profile Tuning Tab" on page 9-64 |

5. Click OK to save and close the new or changed profile or Cancel to exit without saving.

   If you changed a company profile and want to update your partners, see "Distributing Profiles to Partners" on page 9-4.

   If this is a new company profile, the system displays a message asking whether you want to set up a certificate for the profile. Go to the next step.

6. Decide whether you want to set up a digital certificate for the new profile. You can set up a certificate now or later. Review the certificate options and ways to procure them in Chapter 11, "Keys and Certificates". Click Yes to set up a certificate now or No if you do not want to.

7. Provide your new company profile to your trading partners by exporting it to a file and sending it to your partners on diskette or by some other secure means. See "Exporting a Company Profile to a File" on page 9-13.

# Exporting a Company Profile to a File

Use this procedure to export a company profile to a file. You can export your company profile as a partner profile that you can distribute to your partners, or you can export your company profile as a backup that you do not share with your partners. The following are some reasons for exporting a profile to a file:

- Distribute your company profile to trading partners who also use WebLogic Integration – Business Connect or can receive profile data in XML format. For details about distributing your profile to partners, see "Distributing Profiles to Partners" on page 9-4.
- Back up your company profile as an XML file.

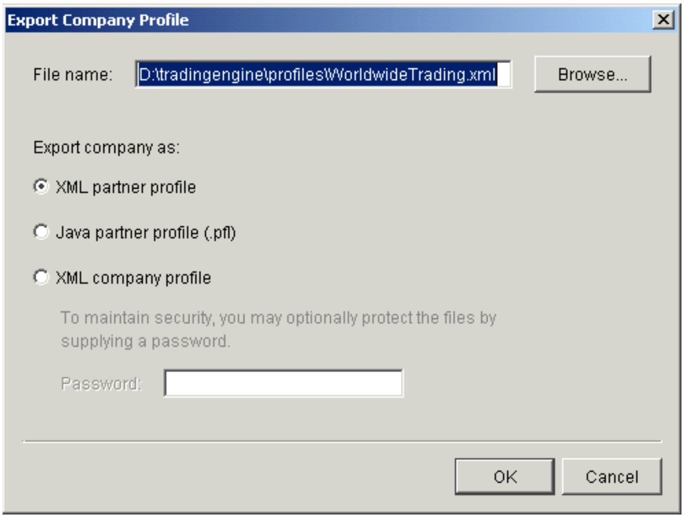
You can save an exported partner profile in an XML or PFL file. WebLogic Integration – Business Connect 2.1 can use partner profiles of either file type.

If you export your company profile as an XML file for backup purposes, you can later import the file as a company profile on any WebLogic Integration – Business Connect system version 2.1 or later. The exported company profile includes the associated certificate and public-private key pair. A company profile exported as a backup file cannot be imported as a partner profile; the system will not allow it.

## Steps

1. At the Company Profiles information viewer, select the company profile you want to export and select File→Export to open the Export Company Profile window.

**Figure 9-3 Export Company Profile Window**



Export Company Profile

File name: D:\tradingengine\profiles\WorldwideTrading.xml

Export company as:

● XML partner profile

○ Java partner profile (.pfl)

○ XML company profile

To maintain security, you may optionally protect the files by supplying a password.

Password:

2. Select the appropriate export option. Each option is described in the following table.

**Table 9-5 Export Options**

| Option | Description |
|---|---|
| XML partner profile | Select this option to export your company profile and associated certificate and public key to a file for manual distribution as a partner profile to partners who use WebLogic Integration – Business Connect 2.1 or later.<br>This option exports the profile in an XML file. Any transport server passwords in the profile are encrypted for security. |
| Java partner profile (`.pfl`) | Select this option to export your company profile and associated certificate and public key to a file for manual distribution as a partner profile to partners.<br>This option exports the profile in a PFL file. |

**Table 9-5 Export Options (Continued)**

| Option | Description |
|---|---|
| XML company profile | Select this option to export your company profile and associated certificate and public-private key pair to an XML file for backup purposes.<br>You can type a password that you must remember and use if you later import the profile. See "Importing a Backed Up Company Profile" on page 9-16. The password protects the private key in the certificate associated with the company profile. Although using a password is optional, we recommend that you do so. We also recommend that you store the XML file in a secure place. Do not share this file with a partner. |

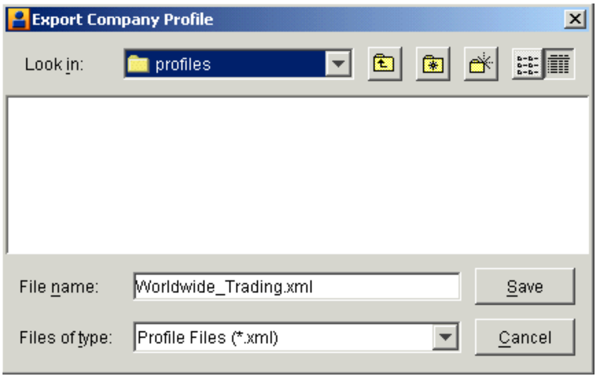
The default name of the file you are exporting depends on your selection, as the following table shows:

**Table 9-6 Export File Name Defaults**

| If you are exporting this profile: | The default file name is: |
|---|---|
| XML partner profile | `*ProfileName*.xml` |
| Java partner profile (`.pfl`) | `*ProfileName*.pfl` |
| XML company profile | `*ProfileName_company*.xml` |

You can click Browse to open the Export Company Profile dialog box and change the default path and file name. Click Save to close the dialog box and return to the Export Company Profile window. Clicking Save on the dialog box only sets the name of the file to be saved, but does not save the file.

**Figure 9-4 Export Company Profile Dialog Box**



Export Company Profile

Look in: profiles

File name: Worldwide_Trading.xml

Files of type: Profile Files (*.xml)

3. Click OK to save the profile to a file. Exported profile files are relatively small in size.

4. If you exported the profile as a partner profile, distribute it by some secure means to your partners.

   If you plan to send the profile file to a partner as an e-mail attachment, we recommend that you use a utility such as WinZip to package the file and then send the compressed file to your partner. This method is recommended to protect the profile file from possible corruption during transmission. Some SMTP servers append verbiage to e-mail attachments, which can harm the profile file.

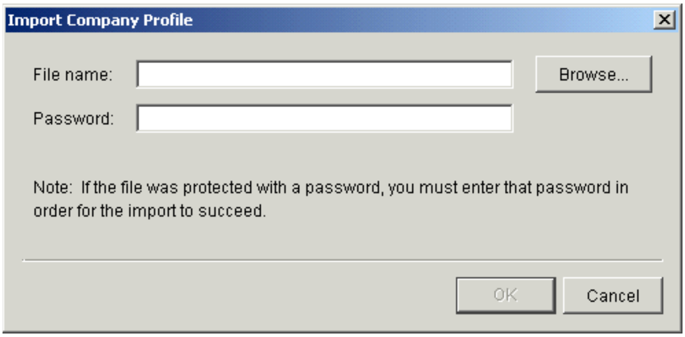
# Importing a Backed Up Company Profile

Use this procedure to import a company profile and associated certificate and public-private key pair that was earlier exported for backup purposes to an XML file. See "Exporting a Company Profile to a File" on page 9-13.

## Steps

1. At the Company Profiles information viewer, select File→Import to open the Import Company Profile window.

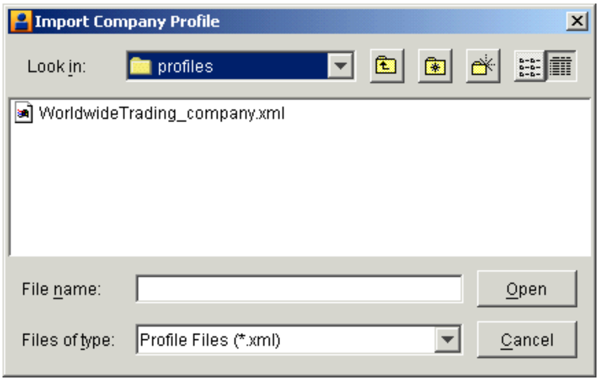
**Figure 9-5 Import Company Profile Window**



Note: If the file was protected with a password, you must enter that password in order for the import to succeed.

2. Click Browse to open the Import Company Profile dialog box. Find and select the company profile you want to import and click Open. The default names of company profile files are in the format `ProfileName_company.xml`.

**Figure 9-6 Import Company Profile Dialog Box**



Look in: profiles

WorldwideTrading_company.xml

Files of type: Profile Files (*.xml)

3. If the company profile was exported with a password, type the password and click OK. Otherwise, leave the password field blank and click OK.

4. Click OK to import the company profile file. A message displays when the company profile imports successfully.

   If the company profile you are importing already is in WebLogic Integration – Business Connect, a message displays asking whether you want the imported profile to overwrite the existing profile. Click Yes to overwrite the existing profile.

# Changing All System Directories at Once

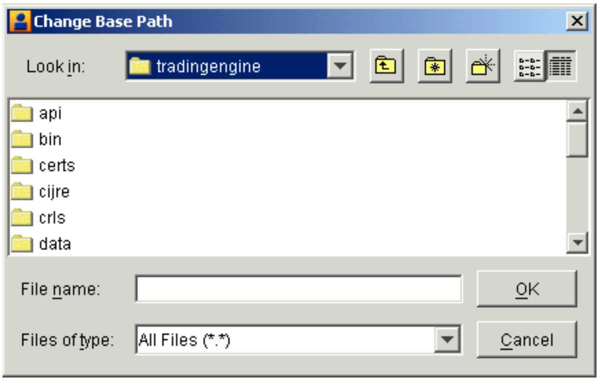
Use this procedure to change the locations of all system directories at the same time to conform to a desired root path. This procedure uses the Company Profile window System Directories tab. For descriptions of the fields on this tab, see "Company Profile System Directories Tab" on page 9-40.

## Steps

1. Open the Company Profile window System Directories tab for the company profile you want to change all system directories.
2. To change the location of all system directories at the same time, click Change Base Path. A message appears asking you to confirm whether you want to perform this action. Note that this change will not affect existing binary directories.

   The Change Base Path button is not available for client Administrator applications that are not installed on the same machine as the Server application.
3. Click Yes to confirm that you want to change the directory locations. The Change Base Path dialog box opens.

**Figure 9-7 Change Base Path Dialog Box**



4. Select the new directory for the base path of all system directories and click OK.

5. Click OK to save your changes and close the profile or Cancel to exit without saving your changes.

# Deleting a Company Profile

Use this procedure to delete a company profile that is no longer needed.

When you delete a company profile, it is no longer displayed in the Company Profiles or Certificates information viewers.

If you generated a self-signed certificate for this profile, it is not deleted; rather, it is retained in Retired status.

If, after you have deleted a company profile, you create another with the same ID, all the old profile's certificates are re-associated with this new profile.

**Note:** You cannot undo a company profile deletion.

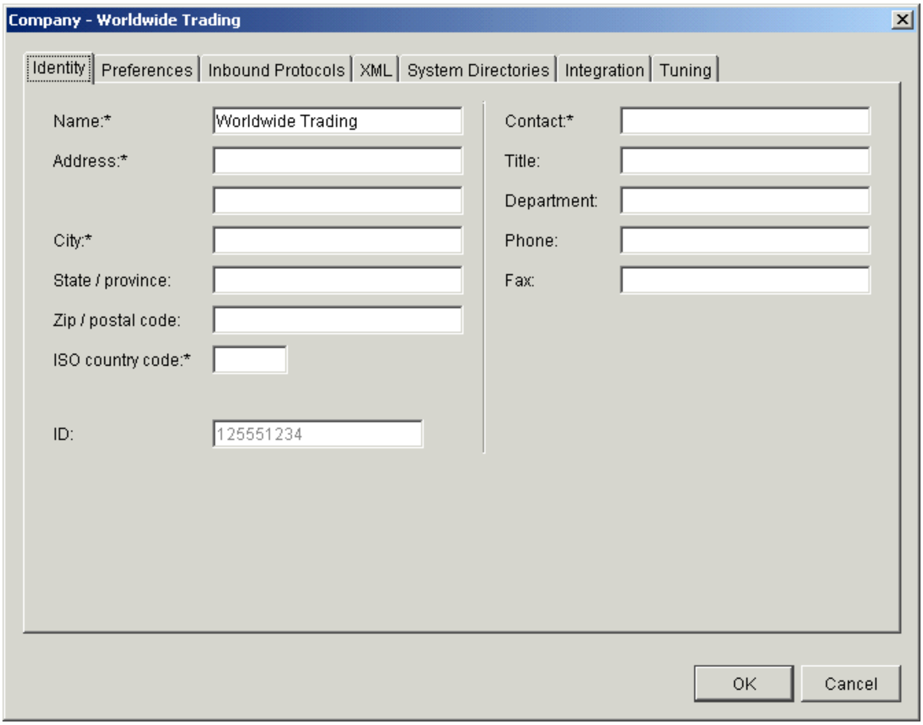
## Steps

1. At the Company Profiles information viewer, select the company profile you want to delete and click Delete.
2. Confirm the deletion in the dialog box that appears.

# Company Profile Identity Tab

Use the Company Profile window Identity tab to specify the address of the company and provide information about your WebLogic Integration – Business Connect point of contact. You can also view the company profile name and ID.

**Figure 9-8 Company Profile Identity Tab**



Name:* Worldwide Trading
Address:*
City:*
State / province:
Zip / postal code:
ISO country code:*
ID: 125551234
Contact:*
Title:
Department:
Phone:
Fax:

## Field Descriptions

The following describes the fields on the Company Profile window Identity tab. For procedure see "Adding or Changing a Company Profile" on page 9-9.

*Name*

Type the company profile name. This field is required. You can use any alphanumeric characters and the following characters: back slash, forward slash, colon, underscore, comma and period. The application removes any other characters.

You can use spaces in your company name; the application translates them to underscores.

*Address*

Type the mailing address for this company profile. The first line of this field is required; the second is optional.

*City*

Type the city where this company or business unit is located. This field is required.

*State/province*

Type the state or province where your company or business unit is located.

*Zip/postal code*

Type the ZIP or postal code for your company or business unit's address.

*ISO country code*

Type the two-letter ISO country code of the country where your company or business unit is located. The following are the ISO codes for selected countries. See Appendix A, "ISO Country Codes," for a complete list of the codes.

**Table 9-7 Selected Country Codes**

| Code | Country |
|---|---|
| ca | Canada |
| cn | China |
| fr | France |
| de | Germany |
| gb | Great Britan |
| it | Italy |
| jp | Japan |
| mx | Mexico |
| tw | Taiwan |
| us | United States |

*ID*

The ID or combined qualifier-EDI ID you entered when you created this company profile. This is a view-only field; you cannot change it.

*Contact*

Type the name of the person who is to receive WebLogic Integration – Business Connect alert messages. This field is required.

*Title*

Type the contact person’s job title. This field is optional.

*Department*

Type the contact person’s department. This field is optional.

*Phone*

Type the contact person’s phone number. This field is optional.

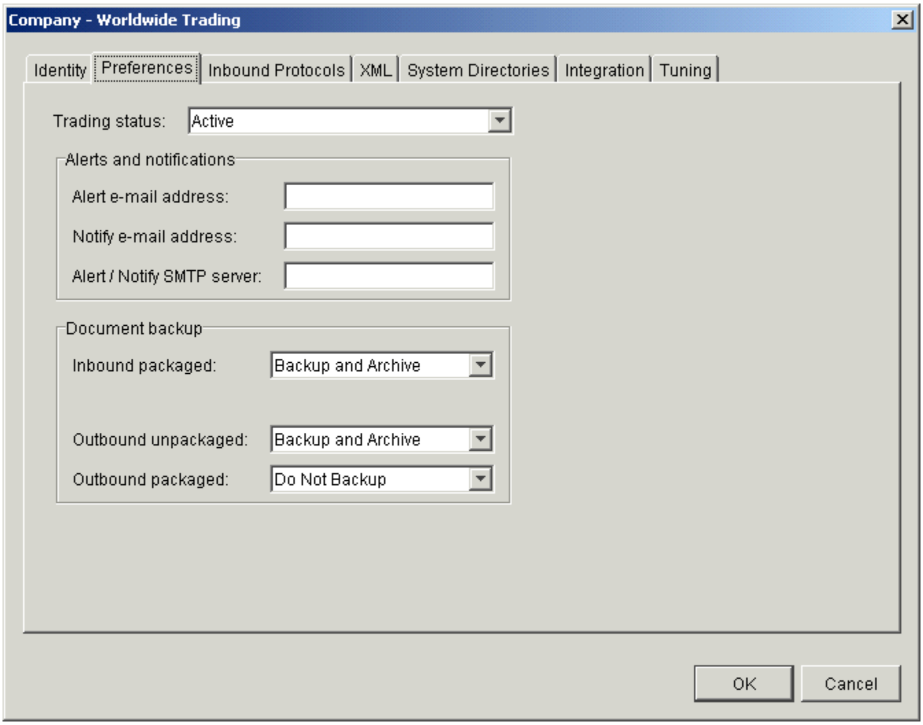
*Fax*

Type the contact person’s fax number. This field is optional.

# Company Profile Preferences Tab

Use the Company Profile window Preferences tab to set up or change preferences information for a company profile, including: trading status, alert and notify e-mail addresses and SMTP server, and document backup options.

**Figure 9-9 Company Profile Preferences Tab**



Trading status: Active

Alert e-mail address:

Notify e-mail address:

Alert / Notify SMTP server:

Inbound packaged: Backup and Archive

Outbound unpackaged: Backup and Archive

Outbound packaged: Do Not Backup

# Field Descriptions

The following describes the fields on the Company Profile window Identity tab. For procedure see “Adding or Changing a Company Profile” on page 9-9.

*Trading status*

Select Active if the company profile is active and is used to process documents. This is the default. Select Inactive if the company profile is not to be used to process documents.

You can quickly change the trading status by right-clicking the company profile in the Company Profiles information viewer and then left-clicking Change Status in the pop-up menu that appears.

*Alerts and notifications*

Use the following three fields to specify where the application sends alert and notification e-mail messages.

*Alert e-mail address*

Type the e-mail address of the person to receive alert messages generated by your WebLogic Integration – Business Connect system. This field is optional, but you do not receive alerts if you leave this field blank.

Type only one e-mail address. If you want more than one person to receive messages, use a group address.

Identified by the word *alert* in the subject line, alert messages are sent when WebLogic Integration – Business Connect detects a condition that might halt document exchange and require you to take action. An example of this situation is when WebLogic Integration – Business Connect cannot connect to the network or when there is a problem with the WebLogic Integration – Business Connect software.

If you plan to send your company profile to a partner, complete this field if you want the partner's WebLogic Integration – Business Connect to send notifications to you.

*Notify e-mail address*

Type the e-mail address of the person to receive notification messages from your WebLogic Integration – Business Connect system. This field is optional, but you do not receive notification messages if you leave this field blank.

Type only one e-mail address. If you want more than one person to receive messages, use a group address.

Identified by the word *notification* in the subject line, notification messages are informational and do not require you to take action. Document exchange continues. WebLogic Integration – Business Connect sends a notification, for example, when it rejects a document or when it receives a binary (non-EDI) document from a partner for which it does not have a partner profile.

*Alert/Notify SMTP server*

Type the fully qualified domain name or IP address of the Simple Mail Transfer Protocol (SMTP) mail server WebLogic Integration – Business Connect uses to send alerts and notifications. If you want to send alert or notification e-mail messages, you must complete this field, regardless of the transport method you use for trading documents.

*Document backup*

Use the following three fields for specifying backup options for inbound and outbound documents. For information about document archiving, see "Configure Archive Schedule Window" on page 13-13.

*Inbound packaged*

Select from the drop-down list one of the following backup options for inbound packaged documents. Inbound documents are backed up in the state they were received (that is, MIME-wrapped and, if applicable, encrypted and signed).

**Table 9-8 Backup Options**

| Option | Description |
|---|---|
| Backup and Archive | Select this option to have WebLogic Integration – Business Connect save copies of inbound packaged documents and MDNs (acknowledgments) of inbound documents in the backup directory. When the archive process runs, the documents and MDNs are moved to the archive directory. This is the default. |
| Do Not Backup | If you select this option, WebLogic Integration – Business Connect does not place copies of inbound packaged documents or acknowledgments in the backup directory. |
| Backup and Delete | Select this option to have WebLogic Integration – Business Connect save copies of inbound documents and MDNs (acknowledgments) of inbound documents in the backup directory. When the archive process runs, the documents are deleted from the backup directory. |

*Outbound unpackaged*

Select from the drop-down list one of the following options for backing up outbound documents in unpackaged or clear-text form:

**Table 9-9 Backup Options**

| Option | Description |
|---|---|
| Backup and Archive | Select this option to have WebLogic Integration – Business Connect save copies of unpackaged outbound documents in the backup directory. When the archive process runs, the documents are moved to the archive directory. This is the default. |
| Backup and Delete | Select this option to have WebLogic Integration – Business Connect save copies of unpackaged outbound documents in the backup directory. When the archive process runs, the documents are deleted from the backup directory. |

*Outbound packaged*

Select from the drop-down list one of the following options for backing up outbound packaged documents. Depending on your security settings, these are copies of the encrypted, signed and MIME-wrapped documents that WebLogic Integration – Business Connect has packaged for sending to your partners.

**Table 9-10 Backup Options**

| Option | Description |
|---|---|
| Do Not Backup | If you select this option, WebLogic Integration – Business Connect does not place copies of outbound packaged documents in the backup directory. This is the default. |
| Backup and Delete | Select this option to have WebLogic Integration – Business Connect save copies of outbound packaged documents in the backup directory. When the archive process runs, the documents are deleted from the backup directory. |
| Backup and Archive | Select this option to have WebLogic Integration – Business Connect save copies of outbound packaged documents in the backup directory. When the archive process runs, the documents are moved to the archive directory. |

# Company Profile Inbound Protocols Tab

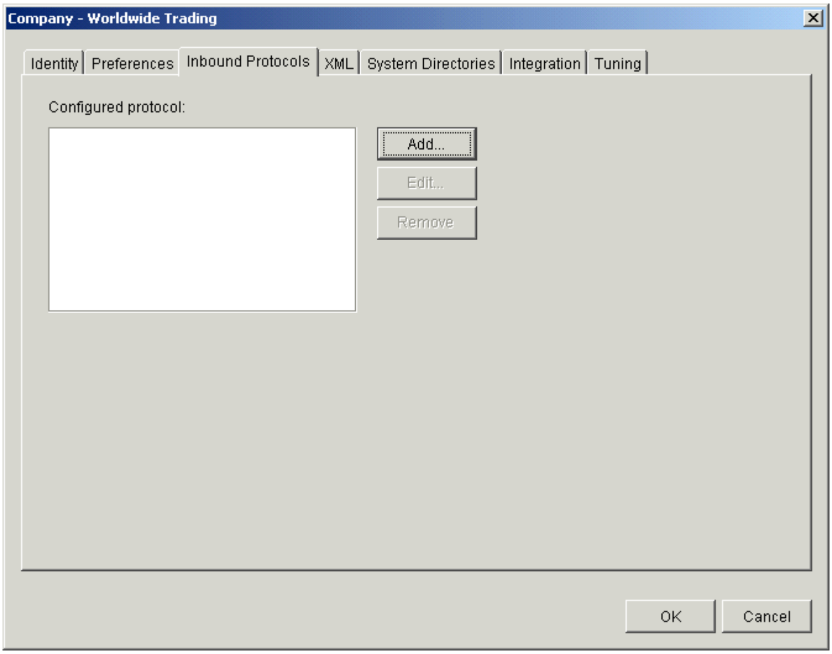
Use the Company Profile window Inbound Protocols tab to set up or change information about the protocols and transports you allow trading partners to use to send documents to you. It is recommended that you consult with your partners on your preferred protocols and transports for receiving documents.

A profile must have at least one fully configured protocol and transport. Regardless how many transports you might configure for a protocol, a partner who imports your profile uses only one to send documents to you.

The follow topics are discussed:

- Supported Protocols and Transports
- Adding, Editing, and Removing Inbound Protocols

**Figure 9-10 Company Profile Inbound Protocols Tab**



# Supported Protocols and Transports

WebLogic Integration – Business Connect supports the ebXML protocol and the following transports:

- POP
- SMTP
- HTTP
- HTTPS

**Note:** WebLogic Integration – Business Connect supports bundled transports for the HTTP and HTTPS servers that are built into the application. To make it clear that this does not constitute support for external HTTP and HTTPS web servers, the user documentation references these transports as bundled HTTP and bundled HTTPS.

# Adding, Editing, and Removing Inbound Protocols

The Inbound Protocols tab allows you to change your company profile in the following ways:

- Add a protocol that partners can use to send documents to you. The single protocol available in WebLogic Integration – Business Connect is specified by your software license.
- Edit the settings for a protocol’s inbound transport.
- Remove a protocol and transport combination from the configured protocol list for the profile.

The following topics explain each of these functions in detail:

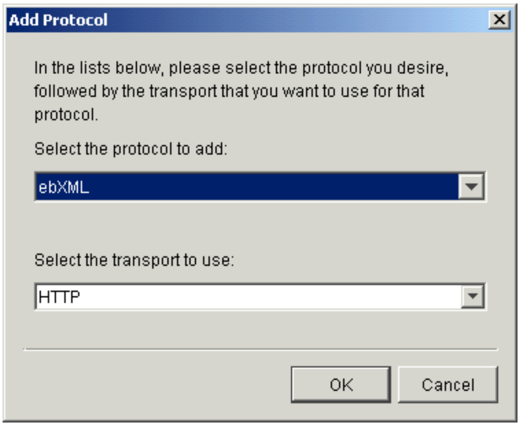
- “Adding an Inbound Protocol” on page 9-29
- “Editing an Inbound Protocol” on page 9-30
- “Removing an Inbound Protocol” on page 9-31

See "Adding or Changing a Company Profile" on page 9-9 for procedure about company profiles.

## Adding an Inbound Protocol

To add an inbound protocol to a company profile, click Add on the Company Profile window Inbound Protocols tab. This opens the Add Protocol window.

**Figure 9-11 Add Protocol Window**



In the lists below, please select the protocol you desire, followed by the transport that you want to use for that protocol.

Select the protocol to add: ebXML

Select the transport to use: HTTP

Select the protocol from the drop-down list. The default protocol for WebLogic Integration – Business Connect already is selected, and no other can be selected. Then select a transport from the transports drop-down list. A protocol has at least one transport from which to choose. If more than one transport is available, you must configure at least one, but you can later select another transport and configure it, too. See "Transport Selection Considerations" on page 9-31 for guidelines about selecting transports.

After you select a protocol and transport, click OK. A configuration window opens for the transport method you selected. See one of the following topics for information about configuring the transport:

- "SMTP Inbound Transport" on page 9-32
- "Bundled HTTP Inbound Transport" on page 9-33
- "Bundled HTTPS Inbound Transport" on page 9-34
- "POP Inbound Transport" on page 9-36

On the configuration window for the selected transport, complete the applicable fields and then click OK to save the transport information and close the window. Or, click Cancel to close the configuration window without saving your changes.

After you click OK, the transport method you added appears on the configured protocol list on the Inbound Protocols tab. The information appears in the following format: protocol transport.

If more than one transport is available for the protocol, you can click Add and repeat the process to configure another transport. If you are done, click OK on the Inbound Protocols tab to save your changes and close the profile. Or, click Cancel to close the profile without saving your changes.

The following are related topics: "Editing an Inbound Protocol" on page 9-30, "Removing an Inbound Protocol" on page 9-31, "Adding or Changing a Company Profile" on page 9-9.

## Editing an Inbound Protocol

To edit an inbound transport for a protocol that was configured earlier for a company profile, select the protocol and transport combination you want from the configured protocol list on the Company Profile window Inbound Protocols tab and then click Edit. This opens the configuration window for the transport. See one of the following topics for information about configuring the transport:

- "SMTP Inbound Transport" on page 9-32
- "Bundled HTTP Inbound Transport" on page 9-33
- "Bundled HTTPS Inbound Transport" on page 9-34
- "POP Inbound Transport" on page 9-36

On the configuration window for the selected transport, edit the applicable fields and then click OK to save the transport information and close the window. Or, click Cancel to close the configuration window without saving your changes. Then click OK on the Inbound Protocols tab to save your changes and close the profile. Or, click Cancel to close the profile without saving your changes.

The following are related topics: "Adding an Inbound Protocol" on page 9-29, "Removing an Inbound Protocol" on page 9-31, "Adding or Changing a Company Profile" on page 9-9.

## Removing an Inbound Protocol

To remove an inbound transport that was configured earlier for a company profile's protocol, select the protocol and transport combination you want from the configured protocol list on the Company Profile window Inbound Protocols tab and then click Remove. This removes the protocol and transport combination from the configured protocol list. Then click OK on the Inbound Protocols tab to save your changes and close the profile. Or, click Cancel to close the profile without saving your changes.

When you remove a transport and give your updated profile to your partners, the removed transport no longer is available for partners to send documents to you. However, on your system, removing a transport only removes the protocol and transport combination from the configured protocol list. It does not delete the configuration information for the transport. That information persists in your system. If you add a transport, later remove it and still later add it back, the earlier configuration information is saved and you do not have to re-enter it.

The following are related topics: "Adding an Inbound Protocol" on page 9-29, "Editing an Inbound Protocol" on page 9-30, "Adding or Changing a Company Profile" on page 9-9.

# Transport Selection Considerations

Keep the following points in mind while selecting transports for company or partner profiles. For more information, see "Company Profile Inbound Protocols Tab" on page 9-27 or "Partner Profile Outbound Protocol Tab" on page 12-19.

- You must select at least one transport method and complete all the fields for that method. You do not have to select or complete more than one transport method. Because WebLogic Integration – Business Connect polls each new server or directory that you add, we recommend that you add a transport method only when you need to use that method to communicate with a trading partner. Moreover, we recommend that you consult with your trading partner before selecting or changing a transport method. If you change transports, you should leave the old transport method open until all your trading partners have switched over to the new transport.

- WebLogic Integration – Business Connect uses one HTTP thread for as many company profiles as you create. For bundled HTTPS, however, you must configure a separate HTTPS port for each company profile that uses this transport method. Each HTTPS server thread needs its own certificate to authenticate connections.
- For documents sent via bundled HTTPS, double encrypting adds only marginally to data security at the cost of inhibiting performance. If you send documents by bundled HTTPS, you can turn off document encryption by clearing the encrypt documents check box on the Partner Profile window Security tab.

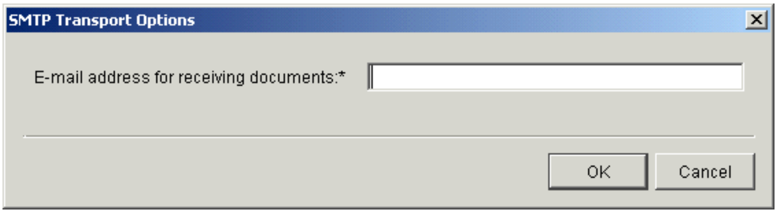
**Note:** Some operating systems throw socket exceptions when HTTPS server sockets are closed. These exceptions are written to the application console, but are of no consequence.

# SMTP Inbound Transport

The SMTP transport enables partners to send you documents via the SMTP server in WebLogic Integration – Business Connect. You configure this transport on the SMTP Transport Options window accessed from the Company Profile window Inbound Protocols tab.

For a comparison of the POP and SMTP inbound transports, see “The Difference Between the POP and SMTP Transports” on page 9-3.

**Figure 9-12 SMTP Transport Options Window**



## Field Description

E-mail address for receiving documents is the single field on the SMTP Transport Options window. Type the e-mail address your trading partners are to use to send documents to you. The e-mail address must be in the standard format of *`mailbox@server.domain`* (for example, `john@worldwide.com`).

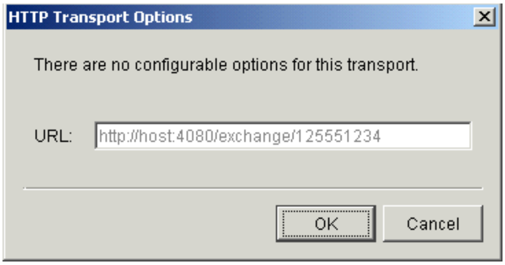
For procedure see the following topics: "Adding an Inbound Protocol" on page 9-29, "Editing an Inbound Protocol" on page 9-30, "Removing an Inbound Protocol" on page 9-31.

# Bundled HTTP Inbound Transport

The bundled HTTP transport enables partners to send you documents via the HTTP server in WebLogic Integration – Business Connect. You configure this transport on the HTTP Transport Options window accessed from the Company Profile window Inbound Protocols tab.

**Note:** This bundled transport is named simply HTTP on the user interface.

**Figure 9-13 HTTP Transport Options Window**



There are no configurable options for this transport.

URL: http://host:4080/exchange/125551234

## Field Description

URL is the single field on the HTTP Transport Options window. The field is system defined; you cannot change it. This field provides a URL alias for the HTTP server in WebLogic Integration – Business Connect. The alias is used for security for your system.

WebLogic Integration – Business Connect obtains the computer name in the URL from the host name field on the General tab in Tools→Preferences. The host name is the computer that is running the Server application.

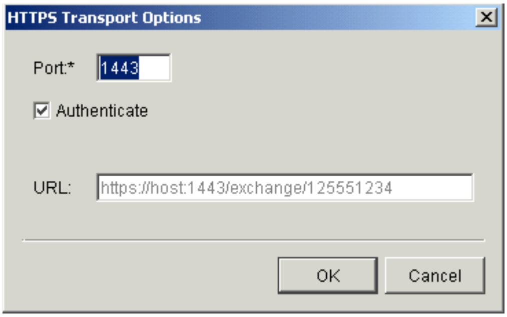
For procedure see the following topics: "Adding an Inbound Protocol" on page 9-29, "Editing an Inbound Protocol" on page 9-30, "Removing an Inbound Protocol" on page 9-31.

# Bundled HTTPS Inbound Transport

The bundled HTTPS transport enables partners to send you documents via the HTTPS server in WebLogic Integration – Business Connect. You configure this transport on the HTTPS Transport Options window accessed from the Company Profile window Inbound Protocols tab.

**Note:** This bundled transport is named simply HTTPS on the user interface.

**Figure 9-14 HTTPS Transport Options Window**



HTTPS Transport Options

Port:* 1443

☑ Authenticate

URL: https://host:1443/exchange/125551234

# Field Descriptions

The following describes the fields on the HTTPS Transport Options window. For procedure see the following topics: "Adding an Inbound Protocol" on page 9-29, "Editing an Inbound Protocol" on page 9-30, "Removing an Inbound Protocol" on page 9-31.

*Port*

If necessary, type the port where the WebLogic Integration – Business Connect HTTPS server is listening for inbound HTTPS documents. You must have a separate HTTPS port for each company profile that uses bundled HTTPS. The default port is `1443`.

*Authenticate*

Select this check box to indicate you require your partners' HTTPS clients to authenticate the SSL connection with you using their certificates. This is the default.

Clear this check box to indicate that you allow your partners' HTTPS clients to make anonymous SSL connections with you.

SSL authentication results in somewhat longer processing per connection for large-key certificates.

*URL*

A system-defined alias for the bundled HTTPS server in WebLogic Integration – Business Connect. You cannot change the value in the field. The alias is used for security for your system.

WebLogic Integration – Business Connect obtains the computer name in the URL from the host name field on the General tab in Tools→Preferences. The host name is the computer that is running the Server application.

# POP Inbound Transport

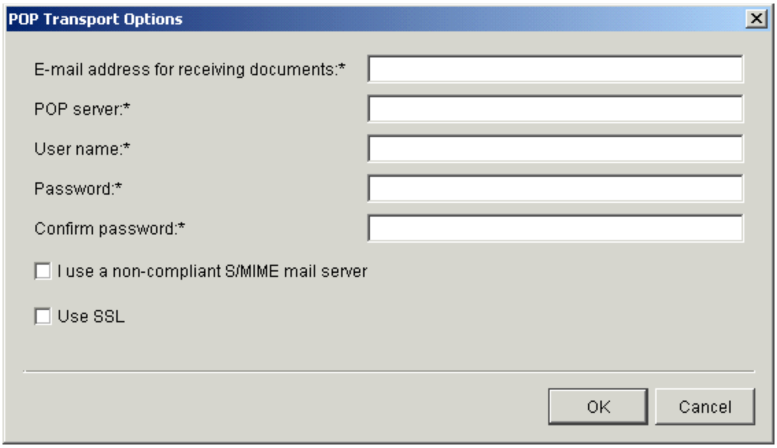
The POP transport enables you to retrieve documents from partners on a POP server. You configure this transport on the POP Transport Options window accessed from the Company Profile window Inbound Protocols tab.

In addition to completing the POP Transport Options window, you must complete the Outbound SMTP tab in Tools→Preferences in Administrator for the SMTP server your organization uses for outbound mail. Complete the server name, user name and password fields; there also is a check box if you use SSL. You must complete the tab before you give your partner your profile. Your SMTP server information is incorporated in your company profile. A partner who uses WebLogic Integration – Business Connect can view the SMTP information after importing your profile. See "Preferences Outbound SMTP Tab" on page 13-26.

If you intend to make POP available as a way for your trading partners to send documents to you, you first must have set up an account, user ID and password for your POP3 server where WebLogic Integration – Business Connect polls to retrieve inbound files.

For a comparison of the POP and SMTP inbound transports, see "The Difference Between the POP and SMTP Transports" on page 9-3.

**Figure 9-15 POP Transport Options Window**



POP Transport Options

E-mail address for receiving documents:*

POP server:*

User name:*

Password:*

Confirm password:*

☐ I use a non-compliant S/MIME mail server

☐ Use SSL

# Field Descriptions

The following describes the fields on the POP Transport Options window. For procedure see the following topics: "Adding an Inbound Protocol" on page 9-29, "Editing an Inbound Protocol" on page 9-30, "Removing an Inbound Protocol" on page 9-31.

*E-mail address for receiving documents*

Type the e-mail address your trading partners are to use to send documents to you. The e-mail address must be in the standard format of `mailbox@server.domain` (for example, `john@worldwide.com`).

*POP server*

Type the fully qualified domain name or IP address of the Post Office Protocol (POP) server where WebLogic Integration – Business Connect checks for inbound e-mail documents.

*User name*

Type the fully qualified domain name of the e-mail account where documents are received from the POP server. The user name you enter must match that of the e-mail account on the POP server. Depending on the POP server, the name might also be case sensitive.

*Password*

Type a password using any combination of letters and numbers. WebLogic Integration – Business Connect can support passwords of up to 50 characters. The field is masked to hide the password, so it is important to enter this information carefully. The password is case sensitive and must match the password of the POP server account. WebLogic Integration – Business Connect uses this password with the user name to retrieve inbound documents from the POP server.

*Confirm password*

Type the POP password again.

*Use SSL*

Check this box only if you want to use the Secure Sockets Layer protocol for inbound documents. If you select this check box, your server must support SSL. If you do not select this option your partners can make anonymous connections.

# Company Profile XML Tab

Use the Company Profile window XML tab to configure WebLogic Integration – Business Connect to identify senders and receivers in Extensible Markup Language (XML) documents that you send to trading partners.

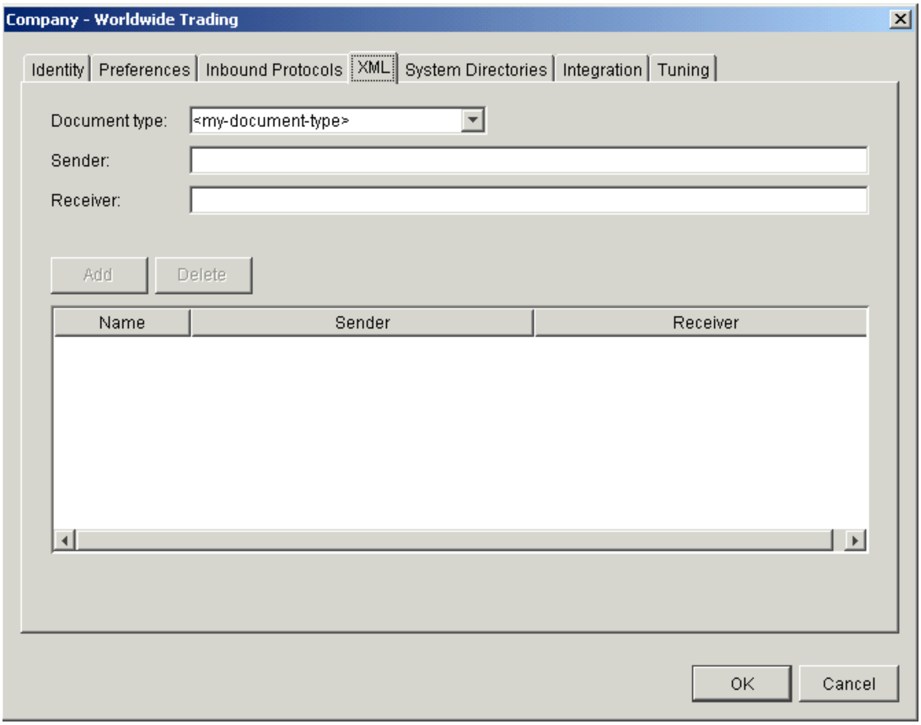
WebLogic Integration – Business Connect uses a specification called XPath to identify discrete elements within XML documents. Specifically, it uses XPath to find the sender and receiver addresses in XML documents polled from your XML out directory.

Selecting one or more XML document types on the XML tab affects outbound documents only. The settings on this tab do not affect inbound documents.

Your and your trading partners should decide beforehand which XML type to use. WebLogic Integration – Business Connect supports any XML document type.

**Note:** You must specify at least one XML type if you want to send XML documents. Otherwise, the system will not poll the XML-out directory for documents.

**Figure 9-16 Company Profile XML Tab**



Company - Worldwide Trading

Document type: <my-document-type>

Sender:

Receiver:

| Name | Sender | Receiver |
|---|---|---|

## Field Descriptions

The following describes the fields on the Company Profile window XML tab. For procedure see "Adding or Changing a Company Profile" on page 9-9.

*Document type*

Select from the drop-down list the XML document type you want. Click Add to add the document type and display it on the window. Repeat this step if you want to add another document type.

If you select ebXML Interface (MCD), see Chapter 10, "Using ebXML."

If you select <my document type>, type a name for the document type you are adding and then see the information for the Sender and Receiver fields.

To delete a document type, select one from the list of types added earlier and click Delete.

*Sender and Receiver*

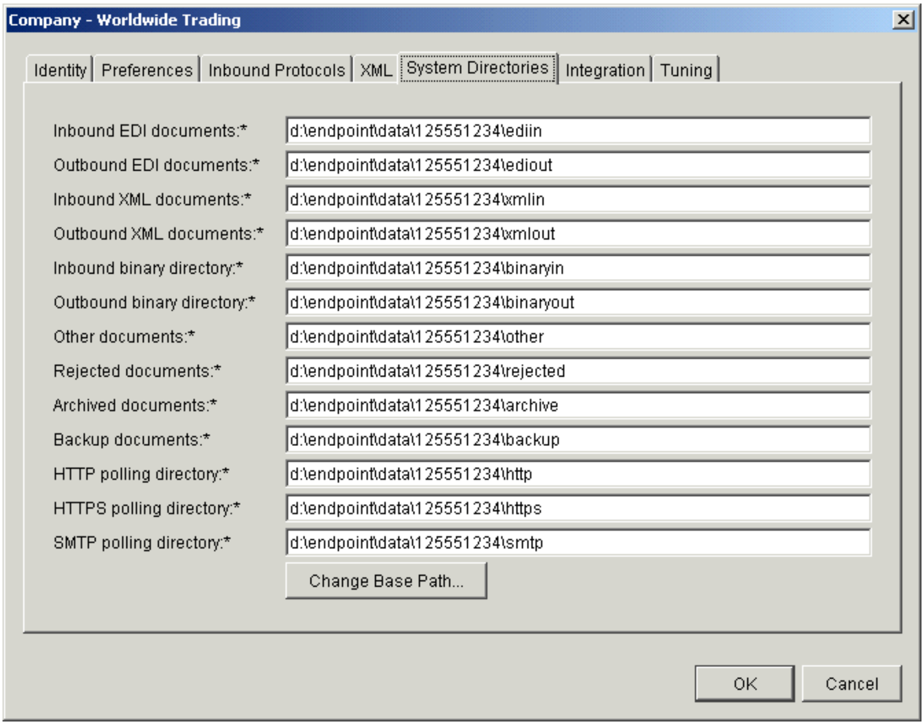
If you select <my document type>, type the XPath strings in these two fields. Click Add to add the document type and display it on the window.

# Company Profile System Directories Tab

Use the Company Profile window System Directories tab to change the directories where your document-related information is physically stored. Use this tab only if you want to use other than the default locations. If you want to use the default locations, you can bypass this tab.

Each path can point anywhere on your system. If the path is to a network drive, you must have it available whenever the Server application is running.

**Figure 9-17 Company Profile System Directories Tab**



| | |
|---|---|
| Inbound EDI documents:* | d:\endpoint\data\125551234\ediin |
| Outbound EDI documents:* | d:\endpoint\data\125551234\ediout |
| Inbound XML documents:* | d:\endpoint\data\125551234\xmlin |
| Outbound XML documents:* | d:\endpoint\data\125551234\xmlout |
| Inbound binary directory:* | d:\endpoint\data\125551234\binaryin |
| Outbound binary directory:* | d:\endpoint\data\125551234\binaryout |
| Other documents:* | d:\endpoint\data\125551234\other |
| Rejected documents:* | d:\endpoint\data\125551234\rejected |
| Archived documents:* | d:\endpoint\data\125551234\archive |
| Backup documents:* | d:\endpoint\data\125551234\backup |
| HTTP polling directory:* | d:\endpoint\data\125551234\http |
| HTTPS polling directory:* | d:\endpoint\data\125551234\https |
| SMTP polling directory:* | d:\endpoint\data\125551234\smtp |

Please consider the following points about system directories:

- If this is the first company profile you have set up, the system directories are not created until you start the Server application.
- If the Server application is already running, the system directories for a new company profile are not created until you save the profile.
- Changing the directory structure after WebLogic Integration – Business Connect has been operational must be done with care. This is because documents received previous to this change are not transferred to the new directory structure. WebLogic Integration – Business Connect does not delete the old directory structure.

# Field Descriptions

The following describes the fields on the Company Profile window System Directories tab. For procedure for using the Change Base Path button, see "Changing All System Directories at Once" on page 9-18. For procedure for setting up company profiles, see "Adding or Changing a Company Profile" on page 9-9.

*Inbound EDI documents*

The directory where WebLogic Integration – Business Connect places all processed inbound EDI files for pickup by your translator. The default directory is:

Windows:
`..\`*`installation_directory`*`\data\`*`company_profile_id`*`\ediin`

UNIX:
*`account`*`/data/`*`company_profile_id`*`/ediin`

*Outbound EDI documents*

The directory where your translator places all outbound EDI files for pickup and processing by WebLogic Integration – Business Connect. The default directory is:

Windows:
`..\`*`installation_directory`*`\data\`*`company_profile_id`*`\ediout`

UNIX:
*`account`*`/data/`*`company_profile_id`*`/ediout`

*Inbound XML documents*

The directory where WebLogic Integration – Business Connect places successfully processed documents from your trading partners for pick up by your XML application. The default directory is:

Windows:
`..\`*`installation_directory`*`\data\`*`company_profile_id`*`\xmlin`

UNIX:
*`account`*`/data/`*`company_profile_id`*`/xmlin`

*Outbound XML documents*

The directory where your XML application places XML documents for processing by WebLogic Integration – Business Connect and transmission across the Internet. The default directory is:

Windows:
`..\installation_directory\data\company_profile_id\xmlout`

UNIX:
`account/data/company_profile_id/xmlout`

*Inbound binary directory*

The directory where WebLogic Integration – Business Connect places successfully processed documents from your trading partners for pick up by your binary application. The default directory is:

Windows:
`..\installation_directory\data\company_profile_id\binaryin`

UNIX:
`account/data/company_profile_id/binaryin`

*Outbound binary directory*

The directory where your binary application places binary documents for processing by WebLogic Integration – Business Connect and transmission across the Internet. The default directory is:

Windows:
`..\installation_directory\data\company_profile_id\binaryout`

UNIX:
`account/data/company_profile_id/binaryout`

*Other documents*

The directory where WebLogic Integration – Business Connect stores inbound binary (non-EDI) documents when you receive a binary document from a partner for whom you have not enabled binary trading on the Partner Profile window Binary Directories tab. When this occurs, WebLogic Integration – Business Connect sends your contact person a notification message. The default directory is:

Windows:
`..\installation_directory\data\company_profile_id\other`

UNIX:
`account/data/company_profile_id/other`

*Rejected documents*

The directory where all rejected inbound or outbound documents are stored. Documents are rejected when, for example, WebLogic Integration – Business Connect:

* Cannot compress, encrypt, or sign outbound documents

* Cannot uncompress, decrypt, or verify inbound documents

* Cannot find a valid partner profile for an inbound or outbound document

* Receives a clear-text MIME document from a sender for whom you do not have a partner profile

When a file is placed in this directory, a notification message is sent to your company's WebLogic Integration – Business Connect point of contact. The notification is also sent to your partner's point of contact if you choose this option. The default directory is:

Windows:
`..\installation_directory\data\company_profile_id\rejected`

UNIX:
`account/data/company_profile_id/rejected`

*Archived documents*

If you choose the Backup and Archive option in the Company Profile window Preferences tab, WebLogic Integration – Business Connect moves completed documents from the inbound and outbound backup directories to the archive directory when the archive process runs.

This action deletes those archived files from the inbound and outbound backup directories. See "Configure Archive Schedule Window" on page 13-13 for information on how to set the interval for running the archive process. The default directory is:

Windows
`..\installation_directory\data\company_profile_id\archive`

UNIX:
`account/data/company_profile_id/archive`

*Backup documents*

The backup directory is where all backed-up files are stored. WebLogic Integration – Business Connect makes a backup copy before encrypting and signing outbound documents and (optionally) immediately after receiving inbound signed and encrypted documents. If you request them, the MDNs your partners send you in response to your outbound documents are also stored in this directory. The default directory is:

Windows:
`..\installation_directory\data\company_profile_id\backup`

UNIX:
`account/data/company_profile_id/backup`

*HTTP polling directory*

The directory WebLogic Integration – Business Connect polls to retrieve and process inbound documents sent via HTTP. The default directory is:

Windows
`..\installation_directory\data\company_profile_id\http`

UNIX:
`account/data/company_profile_id/http`

*HTTPS polling directory*

The directory WebLogic Integration – Business Connect polls to retrieve and process inbound documents sent via HTTPS. The default directory is:

Windows:
`..\installation_directory\data\company_profile_id\https`

UNIX:
`account/data/company_profile_id/https`

*SMTP polling directory*

If you configured the SMTP transport ("SMTP Inbound Transport" on page 9-32), the name of the directory WebLogic Integration – Business Connect polls for inbound documents. The default directory is:

Windows:
`..\installation_directory\data\company_profile_id\smtp`

UNIX:
`account/data/company_profile_id/smtp`

# Company Profile Integration Tab

Use the Company Profile window Integration tab to have WebLogic Integration – Business Connect send inbound or outbound documents to an FTP server, JMS interface or IBM MQSeries application. You also can set up post-processing commands for inbound documents.

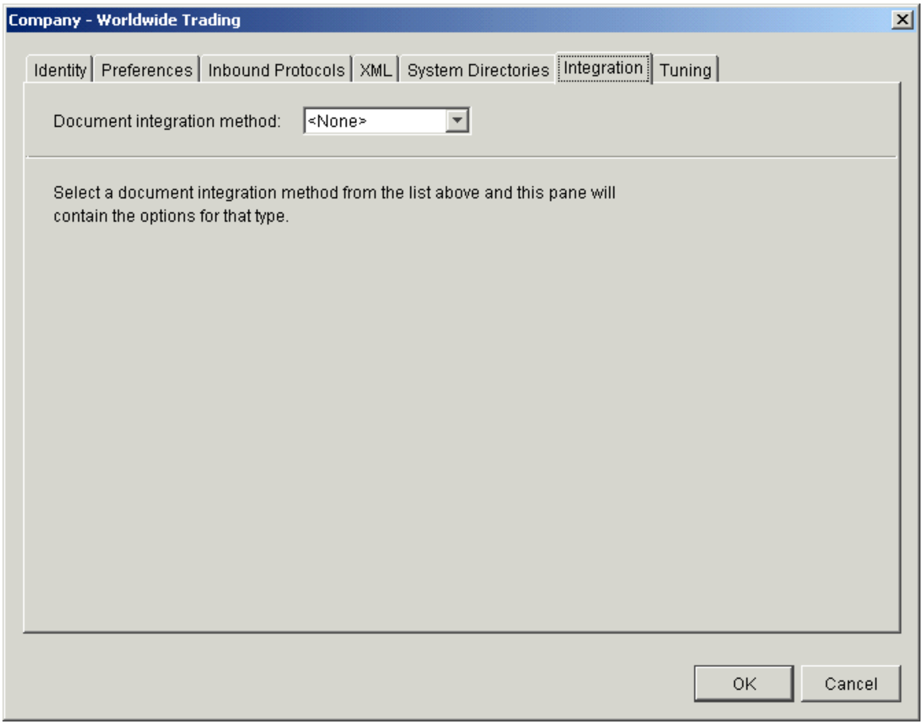
WebLogic Integration – Business Connect does not package any documents that are transferred by way of integration options.

The Integration tab enables you to set up integration for a single company profile. You can select any combination of document-type integration options for a single company profile. For example, for EDI documents you can integrate with MQSeries; for XML documents you can integrate with an FTP server; for binary documents you can set up post-processing for documents received from a specific partner.

When you select integration options on the Integration tab, other windows open for you to enter configuration information. The following topics are provided:

- "Integration Tab Field Descriptions" on page 9-48
- "IBM MQSeries Options Window" on page 9-50
- "FTP Options Window" on page 9-51
- "JMS Options Window" on page 9-54
- "Post-Processing Options Windows" on page 9-57
- "Post-Processing Configuration Details" on page 9-58

**Figure 9-18 Integration tab as Seen in Default View with <None> Selected**



Document integration method: <None>

Select a document integration method from the list above and this pane will contain the options for that type.

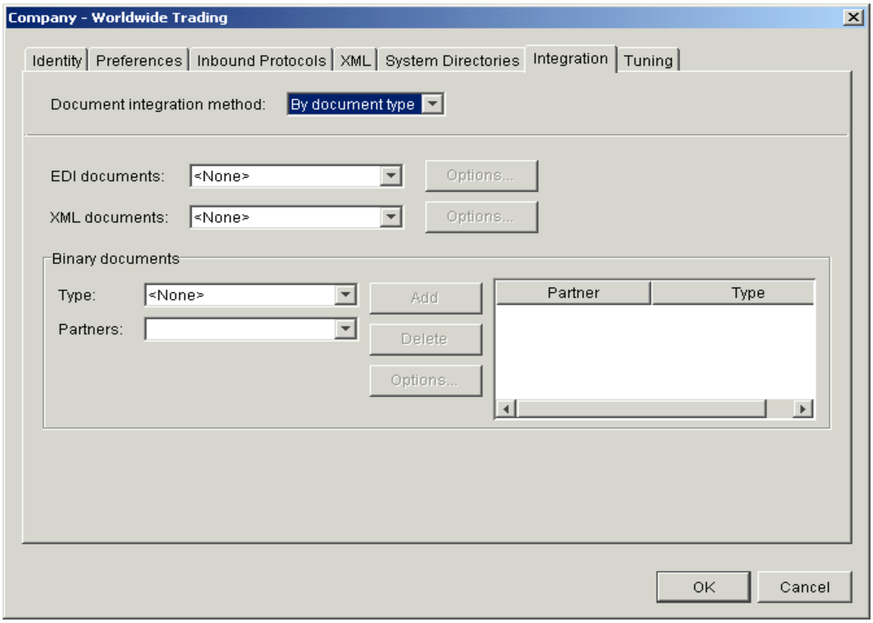
# Integration Tab Field Descriptions

The following describes the fields on the Company Profile window Integration tab. For procedure see "Adding or Changing a Company Profile" on page 9-9.

*Document integration method*

If you want document integration, select By document type from the drop-down list to display the integration options on the tab.

**Figure 9-19 Integration Tab as Seen with *By document type* Selected**



Document integration method: By document type

EDI documents: <None>

XML documents: <None>

Binary documents

Type: <None>

Partners:

| Partner | Type |
|---|---|

The steps are identical for setting up EDI and XML documents for integration. The steps for binary documents are somewhat different.

*EDI and XML documents*

In the fields for EDI documents or XML documents, select from the drop-down list one of the following options and click Options to open a configuration window:

IBM MQSeries

FTP

JMS

Inbound post-processing

*Binary documents*

Complete the following two fields for binary document integration.

*Type*

Select from the drop-down list one of the following options: IBM MQSeries, FTP, JMS, Inbound post-processing.

*Partners*

Select a partner from the drop-down list. Click Add and then click Options to open a configuration window.

You must import or create the partner profile before the partner's name appears on the drop-down list. Also, you must save your company profile and then set up your company for binary trading in the Partner Profile window Binary Directories tab for the partner you want. Otherwise, there are no partners to select.

You can add more than one partner. If you select inbound post-processing as the type, you can select All for all partners, rather than adding each partner individually.

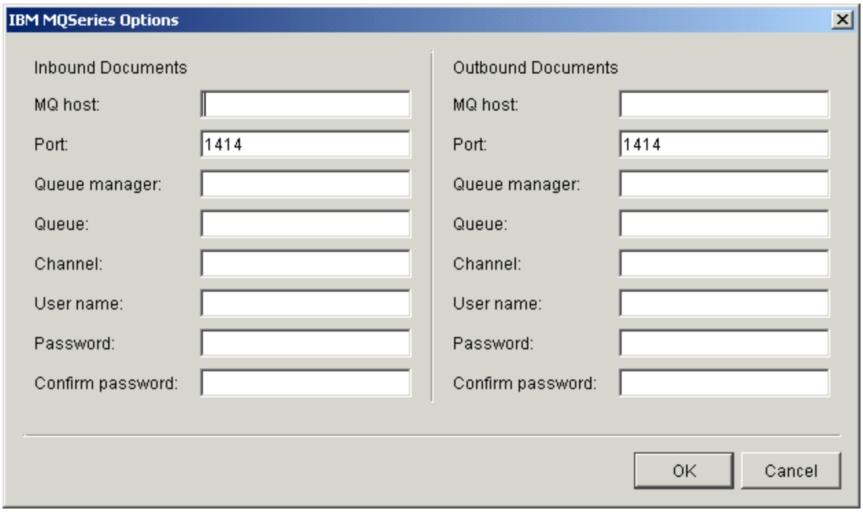
See the topic for the integration option you selected:

- "IBM MQSeries Options Window" (below)
- "FTP Options Window" on page 9-51
- "JMS Options Window" on page 9-54
- "Post-Processing Options Windows" on page 9-57

# IBM MQSeries Options Window

Use the IBM MQSeries Options window for configuring document integration with MQSeries. To access the window, select By document type as the integration method on the Company Profile window Integration tab, select an integration option for EDI, XML or binary documents and click Options. See "Company Profile Integration Tab" on page 9-46.

**Figure 9-20 IBM MQSeries Options Window**



Inbound Documents

MQ host:
Port: 1414
Queue manager:
Queue:
Channel:
User name:
Password:
Confirm password:

Outbound Documents

MQ host:
Port: 1414
Queue manager:
Queue:
Channel:
User name:
Password:
Confirm password:

## Field Descriptions

The following describes the fields on the IBM MQSeries Options window.

You might want to contact your organization's MQSeries administrator for help in establishing criteria for inbound and outbound documents. For inbound documents, the information you enter is used to hand off documents to your legacy system. For outbound documents, the information you enter is used to retrieve documents from your legacy system.

After retrieving documents from the MQSeries host, WebLogic Integration – Business Connect deletes the acquired files from the host. Inbound files passed to the MQSeries host are not deleted from the WebLogic Integration – Business Connect file system.

You can complete the fields for inbound documents or outbound documents or both, depending on your needs.

*MQ host*
Type the name or IP address of the MQ host for inbound or outbound documents.

*Port*
Type the port number if other than the default of `1414`.

*Queue manager*
Type the name of the MQSeries queue manager for inbound or outbound documents.

*Queue*
Type the name of the MQSeries queue for inbound or outbound documents.

*Channel*
Type the name of the communications channel for inbound or outbound documents.

*User name*
Type the name of the MQSeries user.

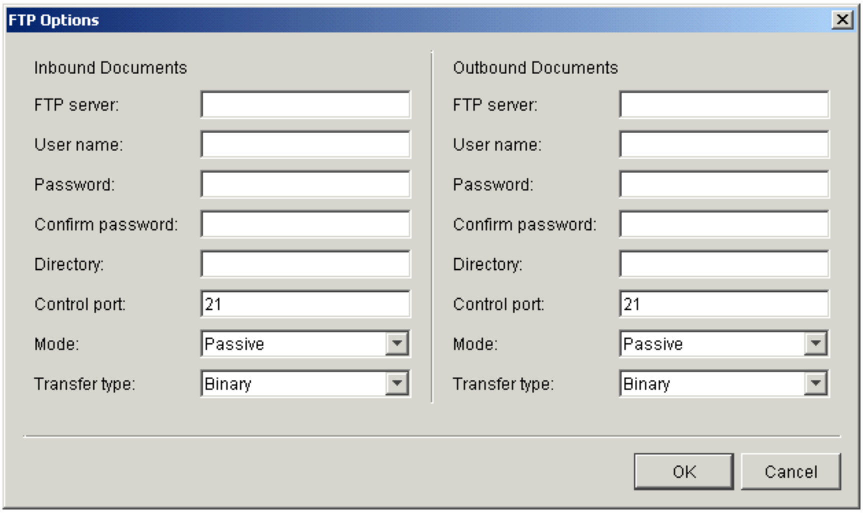
*Password*
Type the password of the MQSeries user.

*Confirm password*
Type the password again.

# FTP Options Window

Use the FTP Options window for configuring document integration with an FTP server. To access the window, select By document type as the integration method on the Company Profile window Integration tab, select an integration option for EDI, XML or binary documents and click Options. See “Company Profile Integration Tab” on page 9-46.

**Figure 9-21 FTP Options Window**



FTP Options

| | | | |
|---|---|---|---|
| Inbound Documents | | Outbound Documents | |
| FTP server: | | FTP server: | |
| User name: | | User name: | |
| Password: | | Password: | |
| Confirm password: | | Confirm password: | |
| Directory: | | Directory: | |
| Control port: | 21 | Control port: | 21 |
| Mode: | Passive | Mode: | Passive |
| Transfer type: | Binary | Transfer type: | Binary |

## Field Descriptions

The following describes the fields on the FTP Options window.

The fields are described once for inbound and outbound documents. You can complete the inbound or the outbound side of the window or both. You do not have to complete both sides.

The fields on the inbound side of the window are for routing to the FTP server documents that WebLogic Integration – Business Connect receives from partners. The fields on the outbound side of the window are for retrieving from the FTP server documents that WebLogic Integration – Business Connect sends to partners.

After acquiring documents from the FTP server, WebLogic Integration – Business Connect deletes the acquired files from the server. WebLogic Integration – Business Connect preserves the names of the files it acquires from the FTP server. Inbound files passed to the FTP server are not deleted from the WebLogic Integration – Business Connect file system.

*FTP server*

Type the fully qualified domain name or IP address of the FTP server.

You must set up your FTP account information outside WebLogic Integration – Business Connect. This set up must include establishing the FTP account, user ID, and password, and creating the directory where WebLogic Integration – Business Connect retrieves or sends documents.

*User name*

Type the user name for the FTP server.

*Password*

Type the password to be used with this FTP user name on the FTP server.

*Confirm password*

Type the password again.

*Directory*

Type the path of the directory on the FTP server where documents are retrieved or sent.

*Control port*

Type the port over which FTP sends commands. The default control port is `21`.

*Mode*

Select one of the following from the drop-down list.

Passive means the FTP server selects the data port for the FTP data transfer. Passive is the default.

Port means the FTP client selects the data port for the FTP data transfer.

*Transfer type*

Select one of the following from the drop-down list.

Binary means documents are transported as-is with no conversions. Binary is the default.

ASCII means documents are converted when appropriate from ASCII to extended binary coded decimal interchange code (EBCDIC) or from DOS text to UNIX text. Use the ASCII setting with caution because it might change the data being transported.

# JMS Options Window

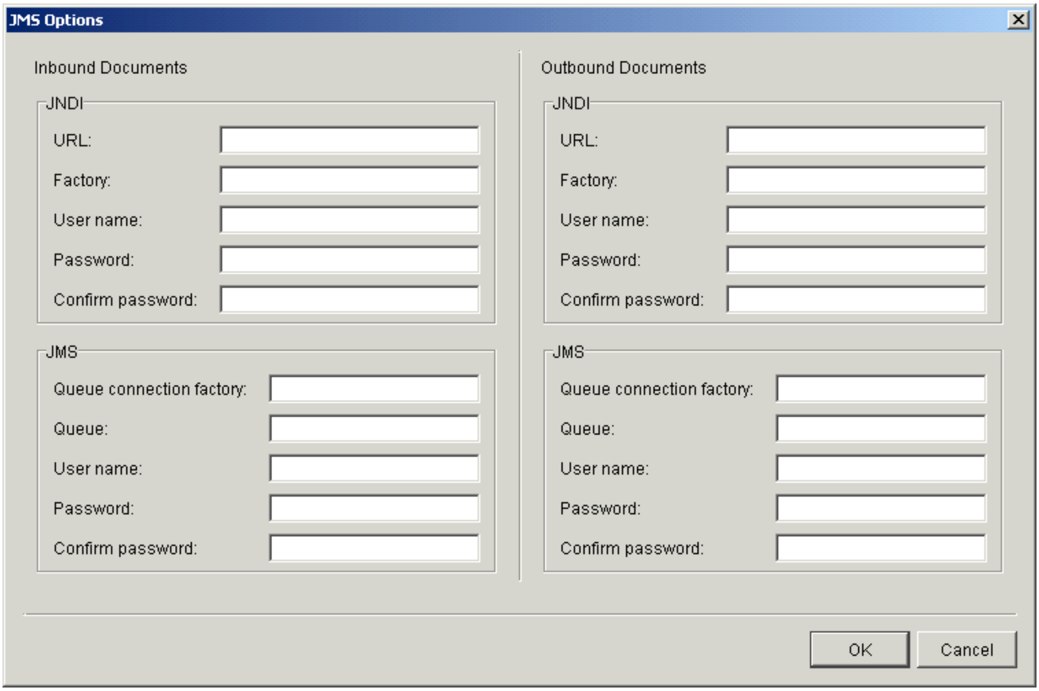
Use the JMS Options window for configuring document integration with a JMS queue. To access the window, select By document type as the integration method on the Company Profile window Integration tab, select an integration option for EDI, XML or binary documents and click Options. See "Company Profile Integration Tab" on page 9-46.

To use this tab your organization must have JMS experience and a working JMS messaging system. Also, see "JMS Integration Details" on page 13-4 for BytesMessage format requirements.

In addition to completing this tab, you must add the names of the JAR or class files or both in the `server.ini` or `server.bat` file in Windows or your environment file in UNIX so the Server application can locate the JMS and JNDI provider. The `server.ini` and `server.bat` files are located in the installation directory bin subdirectory. In some cases, you need to add the name of only one JAR file (for example, `swiftmq.jar`), but you might have to include a series of jars or paths.

This window is for configuring JMS document integration for a single company. To configure JMS document integration for all companies, see "JMS Global Integration for Documents" on page 13-3.

**Figure 9-22 JMS Options Window**



## Field Descriptions

The following describes the fields on the JMS Options window.

The fields are described once for inbound and outbound documents.

The Inbound Documents area is for configuring WebLogic Integration – Business Connect to poll a back-end JMS queue for documents that are to be retrieved, packaged and sent to partners.

The Outbound Documents area is for configuring WebLogic Integration – Business Connect to place documents that have been received from partners and unpackaged on a back-end JMS queue.

Except for the user name and password, you can obtain the information needed to complete the tab from the JMS or JNDI provider's documentation. The information will vary depending on the provider. If you have questions, contact your JMS or JNDI provider.

*JNDI*

Complete the following fields for the Java naming and directory interface (JNDI).

*URL*

Type the network URL that will be used to obtain access to the JNDI service provider for your JMS service. Example: `smqp://localhost:4001/timeout=10000`

*Factory*

Type the name for the JNDI service provider class. Example: `com.swiftmq.jndi.InitialContextFactoryImpl`

*User name*

Type a user name for the JNDI provider. This value could be blank and is typically provided for in the JNDI URL. However, this will depend on the JNDI provider and how it is configured.

*Password*

Type a password for the JNDI provider. This value could be blank and is typically provided for in the JNDI URL. However, this will depend on the JNDI provider and how it is configured.

*Confirm password*

Type the password again.

*JMS*

Complete the following fields for the Java messaging service (JMS).

*Queue connection factory*

Type the connection factory as defined within the JMS provider. This value can be either in the form *`factoryname@routername`* or the JNDI public symbol for the QueueConnectionFactory. Examples: `plainsocket@router1` or `QueueConnectionFactory22`. This would be dependent on your JMS provider and how it is configured.

*Queue*

Type the name of the queue in the form *`queuename@routername`*. Example: `XMLQueue@router1`

*User name*

Type a user name for the JMS provider. This can be the same as your JNDI user name. However, this will depend on how your JMS provider and how it is configured.

*Password*

Type a password for the JMS provider. This can be the same as your JNDI password. However, this will depend on how your JMS provider and how it is configured.

*Confirm password*

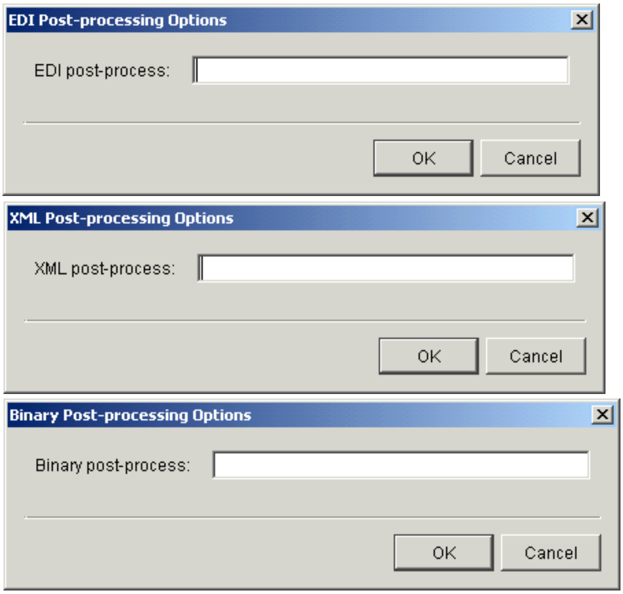
Type the password again.

# Post-Processing Options Windows

Use the Post-processing Options windows for configuring post-processing for inbound documents. To access the windows, select By document type as the integration method on the Company Profile window Integration tab, select an integration option for EDI, XML or binary documents and click Options. For more information see "Company Profile Integration Tab" on page 9-46.

**Note:** Under HP-UX, inbound post-processing fails when you use spaces in an EDI qualifier in a profile ID.

**Figure 9-23 Post-processing Options Windows**


EDI Post-processing Options
EDI post-process:
OK
Cancel
XML Post-processing Options
XML post-process:
OK
Cancel
Binary Post-processing Options
Binary post-process:
OK
Cancel

## Field Description

The following describes the field on the Post-processing Options windows. There are three variations of the window: one each for EDI, XML and binary inbound document types.

*EDI, XML or Binary post-process*

Type the fully qualified path and file name of the batch file, script or executable file. See "Post-Processing Configuration Details."

# Post-Processing Configuration Details

You can perform post-processing commands on each inbound document immediately after WebLogic Integration – Business Connect has received, processed and written it to the EDI-in, XML-in, or binary-in directory. WebLogic Integration – Business Connect can initiate any executable or batch file or script you specify. You can specify the same executable for each document type or a different one for each type.

The post-processing script must be on a drive that WebLogic Integration – Business Connect can access and has permission to execute.

WebLogic Integration – Business Connect passes 12 command-line parameters to the post process. Your script can use any or all of the parameters. The following table provides an example of the syntax of a command that is executed against an inbound document.

**Table 9-11 Example**

| | |
|---|---|
| Windows | `c:\directoryname\myfile.bat` |
| UNIX | `/directoryname/myscript.sh` |

The parameters are described in the following table. The parameter numbers are shown for Windows and UNIX.

**Table 9-12 Post-Processing Parameters**

| Windows | UNIX | Post-processing parameter | Description |
|---|---|---|---|
| %1 | $1 | Windows: `c:\directoryname\inboundfile`<br>UNIX: `/directoryname/inboundfile` | The fully qualified file name of the document for post processing. |
| %2 | $2 | SenderID | The partner ID of the sender of the document. |
| %3 | $3 | Transport | The transport method used to receive the document. The possible transports are:<br>Bundled HTTP<br>Bundled HTTPS<br>EMAIL<br>SMTP |
| %4 | $4 | TrueSenderID | This is the same as the sender ID. In the future this parameter might have other values. |
| %5 | $5 | ReceiverID | This is the partner ID of the receiver of the document. In a service provider configuration, this is the ID of the hub. |
| %6 | $6 | TrueReceiverID | This is the same as the receiver ID, except in a service provider configuration, where this is the partner ID of the partner who actually receives the document and not the partner ID of the intermediary hub. |
| %7 | $7 | ControlID | The control ID of an EDI document. Otherwise, the ID is XML or BINARY |
| %8 | $8 | UniqueID | The unique alphanumeric string WebLogic Integration – Business Connect assigns to the document. Appended to the value is the receiver’s ID. |

**Table 9-12 Post-Processing Parameters (Continued)**

| Windows | UNIX | Post-processing parameter | Description |
|---|---|---|---|
| %9 | $9 | OriginalName | The original name of the document if different from the document name specified in the document path. |
| shift command<br>%9 | shift command<br>$9 | DocumentType | Indicates whether the document is XML, binary, X12 or EDIFACT. |
| shift command<br>%9 | shift command<br>$9 | SequenceID | Indicates duplicate document names by appending file names with `_1`, `_2`, `_3` and so on. You only want to use this parameter when you have selected sequence duplicate file names on the Partner Profile window Preferences tab. |
| shift command<br>%9 | shift command<br>$9 | CorrelationID | The assigned correlation ID of the document. This ID relates documents that are parts of conversations between partners in an ebXML exchange. |

## Notes About Parameters

- You can type the name of only one executable per document type.
- The executable runs against each document that is written to the directory you specify. Documents do not accumulate for batch processing.
- Use the 10th, 11th and 12th parameters, DocumentType, SequenceID and CorrelationID, as shown in the table by using a shift command (not the keyboard shift key) following on the next line by %9 (Windows) or $9 (UNIX). Windows and UNIX only use single-digit parameters. The script will fail using %10 or $10 for the 10th parameter, %11 or $11 for the 11th parameter or %12 or $12 for the 12th parameter. See the script examples in the next section.
- If you do not use the 10th parameter, DocumentType, but do use the 11th parameter, SequenceID, you must use a shift command in place of the DocumentType parameter as a placeholder in the script. See the script examples in the next section.

- WebLogic Integration – Business Connect writes a message to the `server.log` file to indicate when a post-processing script is invoked. However, it does not display or log any messages from the post-process itself. WebLogic Integration – Business Connect writes details about receiving a document from a partner and another message that a document has been transferred and that post-processing has been invoked for it.

## Languages for Writing Scripts

You can use the following languages for writing post-processing scripts:

**Table 9-13 Script Languages**

| Operating system | Languages |
|---|---|
| Windows | Only compiled languages for security reasons. For example, Java, Visual BASIC, C++ or Delphi. |
| UNIX | Any language. For example, shell script, Java, C or Perl. |

We recommend using a compiled program for post-processing. Although a batch file often is adequate for this purpose, we recommend changing to a compiled program if problems occur.

## Script Examples for Windows

The following are examples of post-processing scripts for Windows. These scripts re-direct an inbound file to a local directory and write activity to an external log file. These examples are shown solely to illustrate the correct format for such scripts.

The first example includes the DocumentType parameter. The second example does not.

**Listing 9-1 Example 1 Windows Script**

```
@echo off
rem  WindowsPostprocess.bat to test post-processing.
rem  This batch file does two things. It moves the ediin, xmlin
rem  or binary-in file to another directory. Then it appends into
rem  a log file all the information that CI makes available about
rem  that file.

@echo off
move %1 d:\tmp
echo. >> d:\tmp\postprocess.log
echo -----newfile info----- >> d:\tmp\postprocess.log
date/t >> d:\tmp\postprocess.log
time/t >> d:\tmp\postprocess.log
echo The filename is %1 >> d:\tmp\postprocess.log
echo The SenderID is %2 >> d:\tmp\postprocess.log
echo The Transport is %3 >> d:\tmp\postprocess.log
echo The TrueSenderID is %4 >> d:\tmp\postprocess.log
echo The ReceiverID is %5 >> d:\tmp\postprocess.log
echo The TrueReceiverID is %6 >> d:\tmp\postprocess.log
echo The ControlID is %7 >> d:\tmp\postprocess.log
echo The UniqueID is %8 >> d:\tmp\postprocess.log
echo The OriginalName is %9 >> d:\tmp\postprocess.log
shift
echo The DocumentType is %9 >> d:\tmp\postprocess.log
shift
echo The SequenceID is %9 >> d:\tmp\postprocess.log
shift
echo The CorrelationID is %9 >> d:\tmp\postprocess.log
```

**Listing 9-2 Example 2 Windows Script**

```
@echo off
move %1 d:\tmp
echo. >> d:\tmp\postprocess.log
echo -----newfile info----- >> d:\tmp\postprocess.log
date/t >> d:\tmp\postprocess.log
time/t >> d:\tmp\postprocess.log
echo The filename is %1 >> d:\tmp\postprocess.log
echo The SenderID is %2 >> d:\tmp\postprocess.log
echo The Transport is %3 >> d:\tmp\postprocess.log
echo The TrueSenderID is %4 >> d:\tmp\postprocess.log
echo The ReceiverID is %5 >> d:\tmp\postprocess.log
echo The TrueReceiverID is %6 >> d:\tmp\postprocess.log
echo The ControlID is %7 >> d:\tmp\postprocess.log
echo The UniqueID is %8 >> d:\tmp\postprocess.log
echo The OriginalName is %9 >> d:\tmp\postprocess.log
shift
rem Skipping DocumentType
shift
echo The SequenceID is %9 >> d:\tmp\postprocess.log
shift
echo The CorrelationID is %9 >> d:\tmp\postprocess.log
```

## Script Example for UNIX

The following is an example of a post-processing script for UNIX. This script re-directs an inbound file to a local directory and writes activity to an external log file. This example is shown solely to illustrate the correct format for such scripts.

**Listing 9-3 Example 2 UNIX Script**

```
#!/bin/sh
# $Id: UNIXpostprocess.sh to test post-processing.
# This shell script does two things. It moves the ediin, xmlin,
# or binary-in file to another directory. Then it appends into
# a log file all the information that CI makes available about
# that file.

mv "$1" /home/wlibc/tmp
echo -----newfile info----- >> /home/wlibc/tmp/postprocess.log
date >> /home/wlibc/tmp/postprocess.log
echo The filename is "$1" >> /home/wlibc/tmp/postprocess.log
echo The SenderID is "$2" >> /home/wlibc/tmp/postprocess.log
echo The Transport is "$3" >> /home/wlibc/tmp/postprocess.log
echo The TrueSenderID is "$4" >> /home/wlibc/tmp/postprocess.log
echo The ReceiverID is "$5" >> /home/wlibc/tmp/postprocess.log
echo The TrueReceiverID is "$6" >> /home/wlibc/tmp/postprocess.log
echo The ControlID is "$7" >> /home/wlibc/tmp/postprocess.log
echo The UniqueID is "$8" >> /home/wlibc/tmp/postprocess.log
echo The OriginalName is "$9" >> /home/wlibc/tmp/postprocess.log
shift
echo The DocumentType is "$9" >> /home/wlibc/tmp/postprocess.log
shift
echo The SequenceID is "$9" >> /home/wlibc/tmp/postprocess.log
shift
echo The CorrelationID is "$9" >> /home/wlibc/tmp/postprocess.log
```

# Company Profile Tuning Tab

Use the Company Profile window Tuning tab to adjust the polling rate and documents per cycle of inbound transports and outbound documents by type. For some transports you can use synchronous unpackaging instead of inbound document polling.

The following topics are provided:

- "Tuning Tab Description"
- "Document Polling Rates" on page 9-68
- "Inbound Protocols Tuning" on page 9-69
- "Outbound Documents Tuning" on page 9-70
- "Tuning Guidelines" on page 9-70
- "Asynchronous and Synchronous Unpackaging" on page 9-71

Changing any values on this tab is optional and should be considered only if you need to improve system performance.

For procedure about company profiles see "Adding or Changing a Company Profile" on page 9-9.

## Tuning Tab Description

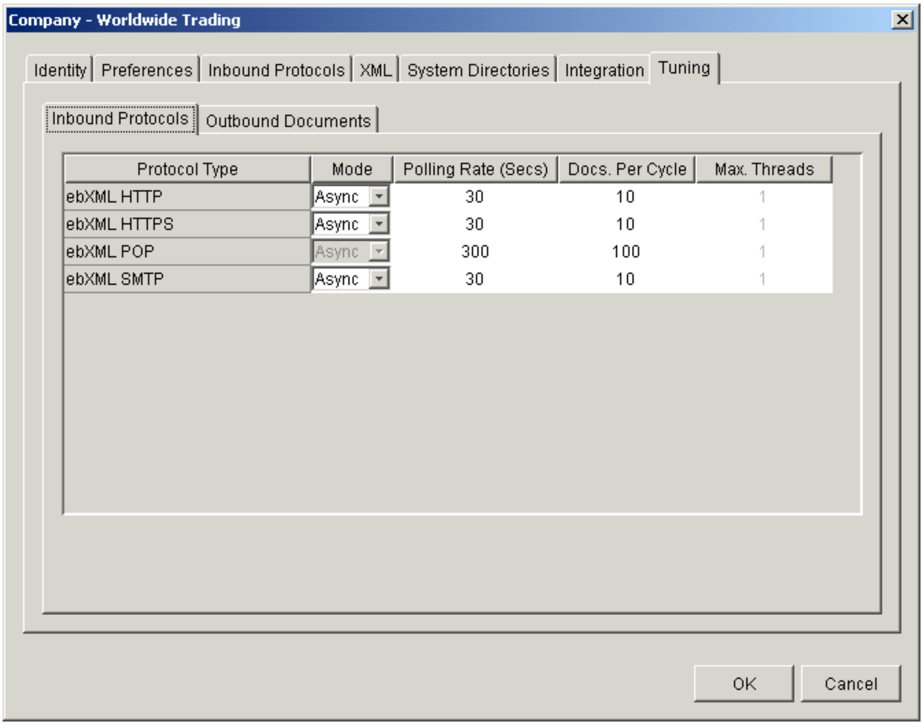
The Company Profile window Tuning tab is comprised of two sub-tabs: Inbound Protocols and Outbound Documents. You adjust settings for inbound and outbound documents on the sub-tabs.

The Inbound Protocols sub-tab only displays the inbound transport types you have configured in your company profile. If no transports are configured, no transport types are displayed. The Outbound Documents tab, however, always displays all three possible outbound document types: EDI, XML and binary.

To change values on these sub-tabs, double-click a field to enter edit mode. You can highlight the value, delete it and type a new value, or you can use the Backspace key to delete the value and type a new one. Press Enter or click another field to apply the change. Click OK to save the change and close the profile.

For navigating the sub-tabs without a mouse, use Ctrl-Tab to move into the table and then use the Tab key to move from cell to cell. Use Ctrl-Tab again to leave the table.

**Figure 9-24 Company Profile Tuning, Inbound Protocols Tab**



| Protocol Type | Mode | Polling Rate (Secs) | Docs. Per Cycle | Max. Threads |
|---|---|---|---|---|
| ebXML HTTP | Async | 30 | 10 | 1 |
| ebXML HTTPS | Async | 30 | 10 | 1 |
| ebXML POP | Async | 300 | 100 | 1 |
| ebXML SMTP | Async | 30 | 10 | 1 |

## Inbound Protocols Column Descriptions

The following describes the columns on the Tuning, Inbound Protocols tab. For more information see "Inbound Protocols Tuning" on page 9-69.

*Protocol Type*

The inbound transport types that have been configured in the company profile. Only configured transports are displayed.

*Mode*

If you have configured one or more bundled inbound transports, you can select synchronous unpackaging. This selection turns off the inbound polling enabled with the default asynchronous unpackaging. For more informations see "Asynchronous and Synchronous Unpackaging" on page 9-71.

*Polling Rate (Secs)*

The interval in seconds WebLogic Integration – Business Connect waits before polling directories and servers for inbound documents from your partners.

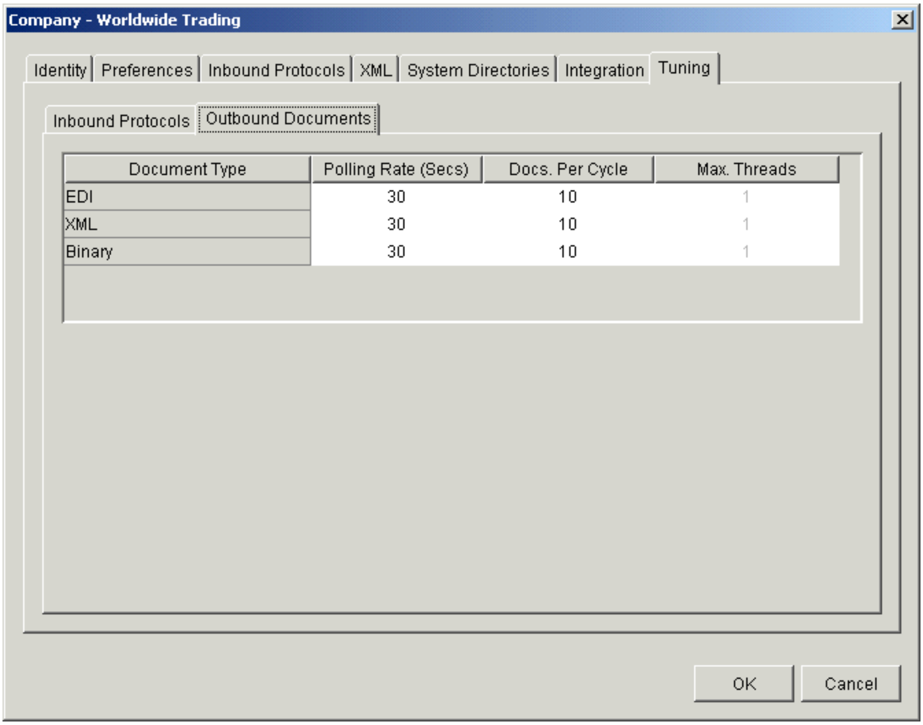
*Docs. Per Cycle*

The highest number of documents that WebLogic Integration – Business Connect can retrieve from a directory or server each time it polls for incoming documents. Your POP server might override this setting.

*Max. Threads*

The maximum number of threads the system can spawn to unpackage inbound documents. This value cannot be changed.

**Figure 9-25 Company Profile Tuning, Outbound Documents Tab**



| Document Type | Polling Rate (Secs) | Docs. Per Cycle | Max. Threads |
|---|---|---|---|
| EDI | 30 | 10 | 1 |
| XML | 30 | 10 | 1 |
| Binary | 30 | 10 | 1 |

## Outbound Documents Column Descriptions

The following describes the columns on the Tuning, Outbound Documents tab. For more information see "Outbound Documents Tuning" on page 9-70.

*Document Type*

The types of documents that the system can send to your partners: EDI, XML and binary.

*Polling Rate (Secs)*

The interval in seconds WebLogic Integration – Business Connect waits before polling the EDI-out, XML-out or binary-out directories for outbound documents to package and send to your partners.

*Docs. Per Cycle*

The highest number of documents that WebLogic Integration – Business Connect can retrieve from an outbound directory each time it polls for outbound documents.

*Max. Threads*

The maximum number of threads the system can spawn to package outbound documents. This value cannot be changed.

# Document Polling Rates

WebLogic Integration – Business Connect processes inbound and outbound documents according to polling rates in seconds and number of documents per cycle. Polling rates control the intervals when the system polls for outbound or inbound documents to process. Documents per cycle control the maximum number of documents the system can retrieve at each polling interval.

These settings, which are built into the application, ensure first-in, first-out (FIFO) document traffic (except e-mail).

The following table provides the default settings for polling rates and documents per cycle. These are set by transport for inbound documents and by document type for outbound documents.

**Table 9-14 Default Settings for Inbound Documents**

| Transport | Polling rate | Documents per cycle |
|---|---|---|
| Bundled HTTP | 30 | 10 |
| Bundled HTTPS | 30 | 10 |
| SMTP | 30 | 10 |
| POP | 300 | 100 |

**Table 9-15 Default Settings for Outbound Documents**

| Document type | Polling rate | Documents per cycle |
|---|---|---|
| Binary | 30 | 10 |
| EDI | 30 | 10 |
| XML | 30 | 10 |

For inbound documents, a polling rate of 300 seconds and 100 documents per cycle for the POP transport means the system will poll the POP server for inbound documents every 300 seconds. Finding any, the system will retrieve them, up to a maximum of 100 documents, and then unpackage them. If there are more than 100 documents waiting, they will be retrieved at the next polling interval.

For outbound documents, a polling rate of 30 seconds and 10 documents per cycle for EDI documents means the system will poll the EDI-out directory for outbound documents every 30 seconds. Finding any, the system will retrieve them, up to a maximum of 10 documents, and then package and send them to the addressed partners. If there are more than 10 documents waiting, they will be retrieved at the next polling interval.

To calculate the maximum number of inbound or outbound documents that can be processed per hour, use the following formula: (3600 / polling rate) * documents per cycle. 3600 is the number of seconds in an hour.

# Inbound Protocols Tuning

On the Tuning, Inbound Protocols tab, you can adjust polling rates and documents per cycle for inbound documents. Provided you choose to adjust any values at all, you can only change those for the transports you set up in your company profile.

Assume for a particular transport you have settings of 30 seconds for a polling rate, 10 documents per cycle and 1 thread. This means WebLogic Integration – Business Connect will poll the transport for inbound documents every 30 seconds. Finding any, it will retrieve them up to a maximum of 10 and then distribute the documents to the single unpackaging thread.

## Outbound Documents Tuning

On the Tuning, Outbound Documents tab, you can adjust polling rates and documents per cycle for the document types EDI, XML and binary.

Assume for a particular document type you have settings of 30 seconds for a polling rate, 10 documents per cycle and 1 thread. This means WebLogic Integration – Business Connect will poll the EDI-out, XML-out or binary-out directory for documents every 30 seconds. Finding any, it will retrieve them up to a maximum of 10 and then pass them to a single packaging thread.

## Tuning Guidelines

You can improve application performance by changing the settings on the Company Profile window Tuning tab. If are unsure whether to change some of the settings, you can safely bypass the tab and use the default values.

You might have to experiment to find the settings best for your trading environment. Factors to consider for your situation include:

- Average document size
- Documents processed per hour
- System resources
- The system's limit on the number of files that can be open at the same time

If your organization has a relatively low volume of document traffic or handles mostly small documents, you may not see an appreciable gain by adjusting polling rates or documents per cycle or a combination of these. On the other hand, a system with a high volume of traffic or that handles large-size documents may experience significant performance improvements.

With these tuning capabilities, it is possible to generate errors such as “out of memory” and “too many files open.” If such errors occur, adjust the polling rate or the number of inbound and outbound threads.

# Asynchronous and Synchronous Unpackaging

Asynchronous unpackaging of inbound documents is the default for all transport types. This means the system polls and processes inbound documents according to the polling rates, documents per cycle and unpackaging threads on the Tuning, Inbound Protocols tab.

Synchronous unpackaging of inbound documents is available for the three transport servers within WebLogic Integration – Business Connect: SMTP, bundled HTTP and bundled HTTPS. Synchronous unpackaging can significantly speed up document unpackaging and processing of acknowledgements. The benefits can be especially advantageous for organizations that handle a large volume of inbound documents. If you configure one or more bundled inbound transports in your company profile, you can enable synchronous unpackaging.

When synchronous unpackaging is active, the system does not poll for inbound documents. Instead, the transport server hands off inbound documents to unpackaging threads immediately upon receipt. When synchronous unpackaging is active, polling becomes inactive, and you cannot edit the tuning values on the Tuning, Inbound Protocols tab.

With synchronous unpackaging, the system spawns unpackaging threads on demand. The number of threads that can be active at one time is limited only by your system resources. It is possible that a large number of inbound documents arriving at the same time could overwhelm your system. However, this could be a high threshold not likely to be reached. We recommend that you monitor your system, both to gauge unpackaging performance and for possible pitfalls, when using synchronous unpackaging.

If you select synchronous unpackaging for a bundled inbound transport, the inbound polling agent for the transport appears just as it does for asynchronous unpackaging in Server monitor displays. Those include the agents area of the server monitor page that you view in a browser by selecting Tools→Launch Server Monitor and on the Server Display window, which is available on Windows systems.

CHAPTER

# 10 Using ebXML

The following topics are provided about the ebXML-based business protocol that WebLogic Integration – Business Connect supports.

**Concepts**

# Supported Transports

WebLogic Integration – Business Connect supports ebXML trading with the following transports:

- bundled HTTP
- bundled HTTPS
- SMTP
- POP

Your organization must have a thorough understanding and working knowledge of ebXML to successfully trade documents using this business protocol. For information about ebXML see www.ebxml.org.

# ebXML Overview

ebXML, sponsored by UN/CEFACT and OASIS, is a modular suite of specifications that enables a company located anywhere to conduct business over the Internet. ebXML embodies the definition and registration of processes for exchanging business messages, conducting trading relationships and communicating data in common terms.

WebLogic Integration – Business Connect supports version 1.0 of the ebXML Transport, Routing and Packaging (TRP) specification and a subset of version 1.0 of the ebXML Collaboration Protocol Agreement (CPA). WebLogic Integration – Business Connect supports packaging and transporting any document type according to the 1.0 TRP specification.

WebLogic Integration – Business Connect supports two methods for exchanging documents with the ebXML protocol. One method supports ebXML business processes and back-end system integration. The other does not, but enables partners to trade documents that are packaged as ebXML documents.

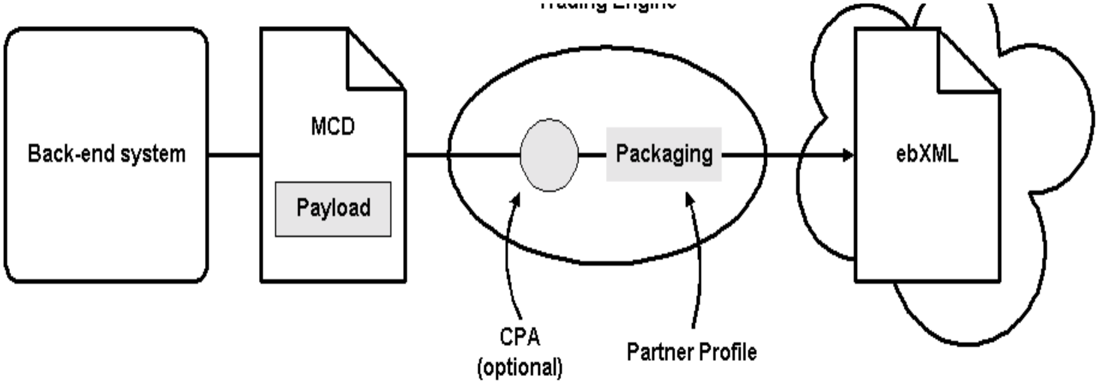
The following topics describe both of these methods:

- "ebXML with MCD Interface"
- "ebXML with File System Interface" on page 10-6

## ebXML with MCD Interface

WebLogic Integration – Business Connect supports ebXML business processes using Message Control Documents (MCDs) as the interface between it and a back-end system. The MCDs are XML documents that contain an arbitrary payload and information that WebLogic Integration – Business Connect uses to process outbound and inbound ebXML documents. Figure 10-1 and Figure 10-2 show high-level views of ebXML processing with the MCD interface in WebLogic Integration – Business Connect.

**Figure 10-1 ebXML with MCD Interface Outbound Processing**

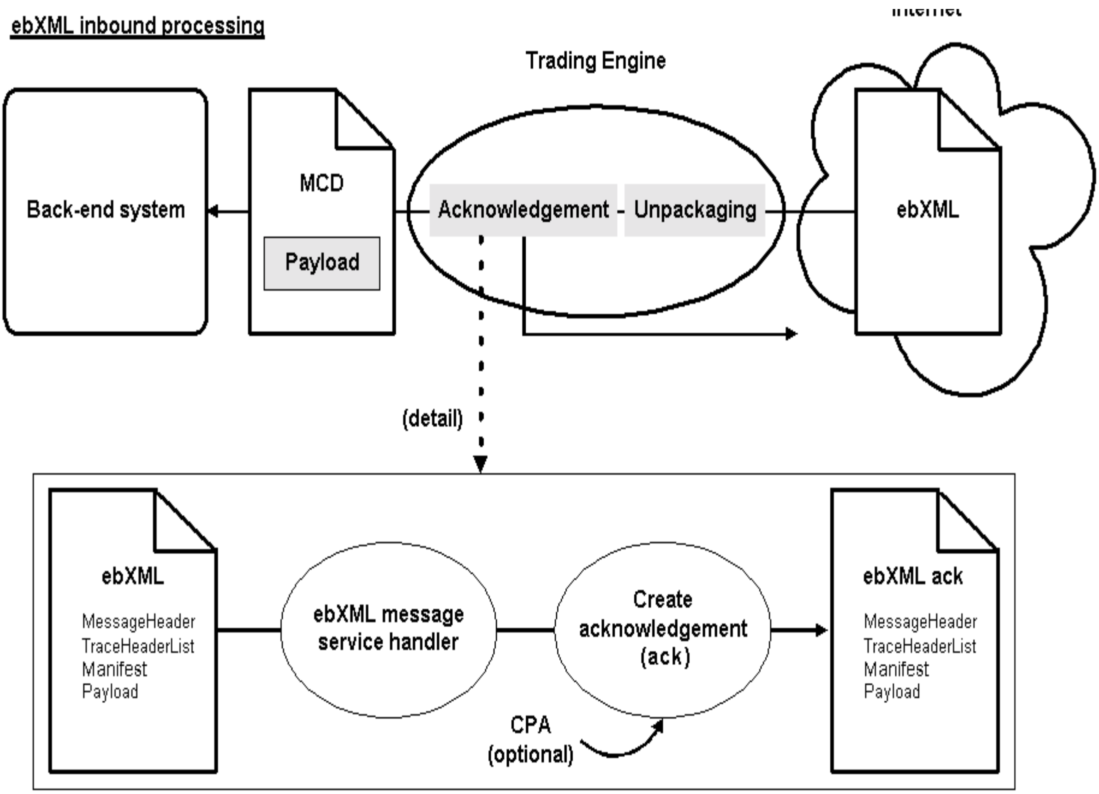


For outbound processing, WebLogic Integration – Business Connect does the following:

- Retrieves the MCD from the XML-out directory.
- Validates the incoming MCD against an MCD schema that resides on the Internet.
- Uses the SenderId and ReceiverId of the MCD to look up a CPA document.

- If there is a CPA, loads the file and extracts document packaging information.
- If there is no CPA, uses information from the MCD and partner profile for packaging.
- Packages the ebXML document.
- Sends the ebXML document to the partner.

**Figure 10-2 ebXML with MCD Interface Inbound Processing**



For inbound processing, WebLogic Integration – Business Connect does the following:

- Receives an ebXML document or acknowledgment.

- Unpackages the document or acknowledgment and sends it to the ebXML Message Service Handler (MSH).
- Uses the CPAId of the inbound ebXML document to look up a CPA document.
- If there is a CPA, loads the file and extracts information which for reliable messaging parameters.
- For an inbound document, the MSH queries the CPA, if present, or the inbound document itself for whether an acknowledgement document is to be created and sent back to the sender.
- Wraps the inbound document, if the destination is the back-end system and not the MSH in an MCD.
- Puts the MCD in the XML-in directory.

WebLogic Integration – Business Connect supports the use of CPAs with the MCD interface. A CPA is an agreement between two or more parties that specifies the transport, messaging and security protocols to use in trading. WebLogic Integration – Business Connect supports file system-based lookups of CPA documents.

WebLogic Integration – Business Connect supports a subset of the CPA document, including security and reliable messaging settings for a specific DeliveryChannel. Parsing based on CollaborationRole is not supported. If there is more than one CollaborationRole element in a CPA, WebLogic Integration – Business Connect extracts the first one and uses it to resolve the specific DeliveryChannel to use. There is no automated support for creating or importing CPAs. You must provide pre-defined CPA documents.

You must edit the `CpaRegistry.xml` file for each CPA you use. This file is in the WebLogic Integration – Business Connect `mcd\ebxml\config` directory. The value for the CPA element must be a valid URL that references the location of the CPA document. A sample CPA document is in the WebLogic Integration – Business Connect `mcd\ebxml\cpas` directory. We recommend this directory as the location for your CPAs.

# ebXML with File System Interface

WebLogic Integration – Business Connect can retrieve any type of document from the EDI-out, XML-out or binary-out directory. Documents also can be retrieved from an API client or integration points. This method does not support ebXML business processes, but enables partners to exchange documents that are packaged as ebXML documents.

An ebXML protocol-enabled WebLogic Integration – Business Connect can use the the MCD interface after editing certain values in the `MCDHandlerConfig.xml` file in the WebLogic Integration – Business Connect MCD directory.

In the following two properties, change `false` to `true`. False, which is the default for both, enables the file system interface. True enables the MCD interface.

```
<mcdconfig:Property name="requireOutboundMcd">false</mcdconfig:Property>

<mcdconfig:Property name="generateInboundMcd">false</mcdconfig:Property>
```

In the following two properties, type your own values for *`service`* and *`action`*. These can be any values you choose.

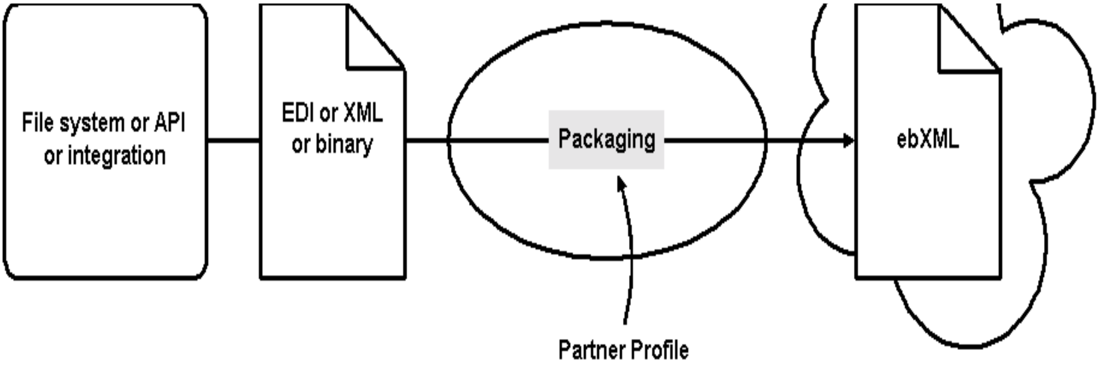
**Note:** When trading with a WebLogic Integration trading partner, the value of *`service`* must match the name of the conversation definition defined in WebLogic Integration. There are no WebLogic Integration requirements for the value of the *`action`*.

```
<mcdconfig:Property name="defaultService">service</mcdconfig:Property>

<mcdconfig:Property name="defaultAction">action</mcdconfig:Property>
```

Figure 10-3 and Figure 10-4 show high-level views of ebXML processing with the file system interface in WebLogic Integration – Business Connect.

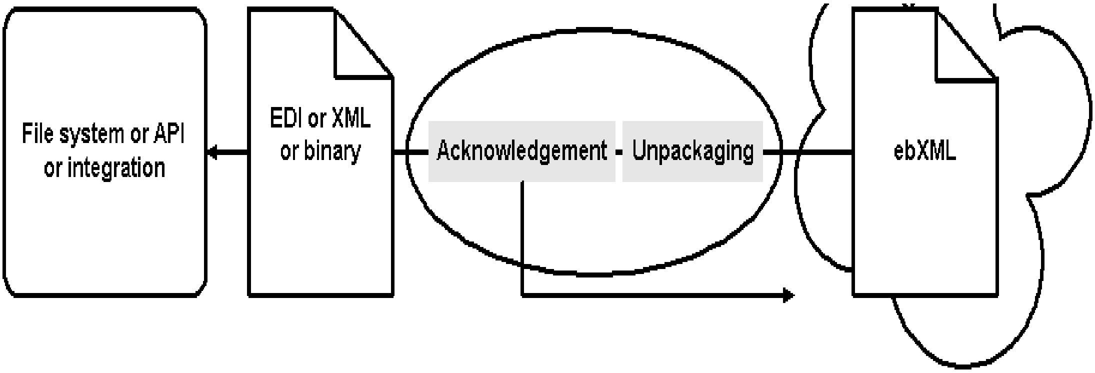
**Figure 10-3 ebXML with File System Interface Outbound Processing**



For outbound processing, WebLogic Integration – Business Connect does the following:

- Retrieves the document from the EDI-out, XML-out or binary-out directory or from the API or integration points.
- Uses information from the partner profile for packaging.
- Packages the document as an ebXML document.
- Sends the ebXML document to the partner.

**Figure 10-4 ebXML with File System Interface Inbound Processing**



For inbound processing, WebLogic Integration – Business Connect does the following:

- Receives an ebXML document or acknowledgment.
- Unpackages the document or acknowledgment.
- For an inbound document, an acknowledgement is created and sent back to the sender.
- Puts the document in the EDI-in, XML-in or binary-in directory or sends to the document API or integration points.

# Using Message Control Documents

A Message Control Document (MCD) is an XML document that is used in the WebLogic Integration – Business Connect implementation of the ebXML business protocol. An MCD is an interface between a back-end system and WebLogic Integration – Business Connect for processing business messages.

The following topics explain more about the use of MCDs:

- "MCDs for ebXML" on page 10-8
- "MCD Element Descriptions" on page 10-9
- "Optional ebXML MessageAgentInfo Elements" on page 10-12
- "MCD Example for ebXML" on page 10-14

## MCDs for ebXML

For ebXML, an MCD is an interface between a back-end business application and the WebLogic Integration – Business Connect ebXML engine. MCDs support ebXML 1.0.

MCDs are used to:

- Send outgoing business documents from the back-end system to WebLogic Integration – Business Connect
- Send incoming business documents from WebLogic Integration – Business Connect to the back-end system

For ebXML processing, MCDs are used to:

- Send outgoing ebXML business documents from the back-end system to the ebXML engine.
- Send incoming ebXML business documents from the ebXML engine to the back-end system.

# MCD Element Descriptions

Table 10-2 lists the information elements used in an MCD to send business documents between a back-end system and WebLogic Integration – Business Connect. The definitions of the letters in the Usage column are summarized in  Table 10-1.

**Table 10-1 Key**

| **This letter . . .** | **In this column . . .** | **Indicates that the element is . . .** |
|---|---|---|
| R | Usage | Required in the MCD produced by the back-end system. |
| O | Usage | Optional in the MCD produced by the back-end system. |
| C | Usage | Optional only when a CPA is present. |

Also see the following topic,  "Optional ebXML MessageAgentInfo Elements" on page 10-12.

**Table 10-2 MCD Information Elements**

| MCD element | Description | Usage |
|---|---|---|
| PackagingProtocol | | |
| Standard | Contains a value, ebXML, indicating the protocol in which the outbound message or acknowledgement is to be packaged or the packaging protocol used by the inbound message or acknowledgement. The MCD supports CIDX and ebXML packaging standards. | R |
| Version | Contains a value indicating the version, 01.10, 02.00 or 01.00, of the packaging protocol. | R |
| Service | Back-end system service name (ebXML BPSS Service). If a CPA is present this is an optional element, otherwise it is required. | C |
| Type | If Service value is not a valid URI then use the type attribute to indicate the format of the Service value. | O |
| Action | Back-end system document action name. | R |
| TimeStamp | The creation time of the MCD. | O |
| CorrelationId | An identifier that matches multiple documents to the same process flow. | R |

**Table 10-2 MCD Information Elements (Continued)**

| MCD element | Description | Usage |
|---|---|---|
| RoutingInfo | | |
| SenderID | A unique business identifier for the sender of a message. | R |
| ReceiverID | A unique business identifier for the receiver of a message. | R |
| TransportInfo | | |
| SessionID | A unique identifier for a specfic transport session. This identifier is used when sending multiple message using the same transport instance.<br>If the SessionID is present on an inbound message, it must be copied to the outbound response MCD. | O |
| MaxRetrys | The maximun number of times to retry sending a message at the message level. | O |
| RetryInterval | The time to wait for an acknowledgement before resending a document. | O |
| MessageAgentInfo | An optional element for attaching protocol-specific information.<br>See "Optional ebXML MessageAgentInfo Elements" on page 10-12. | O |
| ManifestInfo | | |
| MessageContentInfo | Contains a back-end system business payload. | |
| MIME Content ID | A unique identifier for this part of the message. | R |
| MIME Content Type | The MIME content type of the payload. | R |
| Description | A string describing the payload. | O |
| URI | An optional pointer to the actual data.<br>URI or Body, but not both, must be specified. | R |
| Body | The actual data for this section of the message.<br>URI or Body, but not both, must be specified. | R |

**Table 10-2 MCD Information Elements (Continued)**

| MCD element | Description | Usage |
|---|---|---|
| StatusInfo | The status information container. | O |
| StatusType | The type of status message,  acknowledgement or exception. | O |
| ExceptionInfo | Exception Info if Status Type = Exception. | O |
| Error Description | A description of the error. | O |
| Error Classification | The classification of the error. | O |
| Offending Message Component | The section of the message that generated the error. | O |
| Exception Type | The type of exception received. | O |
| DigestInfo | | |
| DigestValue | A base64 encoded digest value. | O |
| DigestAlgorithm | The algorithm used in computing the digest. | O |

# Optional ebXML MessageAgentInfo Elements

The following table lists the optional MessageAgentInfo elements for ebXML. These elements are optional only when a CPA is present.

**Table 10-3 Optional MessageAgentInfo Elements**

| MessageAgentInfo element | Description |
|---|---|
| ebXML | An MCD extension element for ebXML-specific options. |
| ebXMLBinding | |
| ReliableMessaging | Contains ebXML Reliable Messaging specific data. |
| Retries | The maximum number of times to retry sending a message at the message level. Overrides the MCD MaxRetries element. |

**Table 10-3 Optional MessageAgentInfo Elements (Continued)**

| MessageAgentInfo element | Description |
|---|---|
| RetryInterval | The time to wait for an acknowledgement before resending a document. |
| PersistDuration | n/a |
| Acknowledgement | The ackRequested attribute specifies if the ebXML engine should request an acknowledgement. Values are Signed, Unsigned and None. |
| DeliveryReceipt | The deliveryReceiptRequested attribute specifies if the ebXML engine should request a DeliveryReceipt. Values are Signed, Unsigned and None. |
| Envelope | Security related values for the ebXML header envelope. |
| NonRepudiation | Non-repudiation specific values. |
| Protocol | The non-repudiation protocol to use for the ebXML envelope. Only XMLDSIG is supported. Value is `http://www.w3.org/2000/09/xmldsig#`. |
| HashFunction | The hash function to use for XMLDSIG non-repudiation protocol. Only SHA1 is supported. Value is `http://www.w3.org/2000/09/xmldsig#sha1`. |
| DigitalEnvelope | Encryption specific values. Currently, ebXML header envelope encryption is not supported. |
| Protocol | The encryption protocol to use for the ebXML envelope. |
| EncryptionAlgorithm | The encryption algorithm to use. |
| ManifestInfo | Security related values for the ebXML payloads. |
| NonRepudiation | Non-repudiation specific values. |
| Protocol | The non-repudiation protocol to use for the ebXML payloads. Only S/MIME is supported. Value is S/MIME. |
| HashFuntion | The hash function to use for the S/MIME non-repudiation protocol. |
| DigitalEnvelope | Encryption specific values. |

**Table 10-3 Optional MessageAgentInfo Elements (Continued)**

| MessageAgentInfo element | Description |
|---|---|
| Protocol | The encryption protocol to use for the ebXML envelope. Only S/MIME is supported. Value is S/MIME. |
| EncryptionAlgorithm | The encryption algorithm to use. |

# MCD Example for ebXML

The following is an example of an MCD for an ebXML document.

**Listing 10-1 MCD for an ebXML Document**

```
  <?xml version="1.0" encoding="UTF-8" ?>
- <mcd:MessageControlDocument
 xmlns:mcd="http://www.cyclonecommerce.com/Schemas/2001/08/mcd"
 xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
 version="2.0" xsi:schemaLocation=
"http://www.cyclonecommerce.com/Schemas/2001/08/mcd
http://www.cyclonecommerce.com/Schemas/2001/08/MCD_v2_0.xsd">
- <mcd:PackagingProtocol>
  <mcd:Standard>ebXML</mcd:Standard>
  <mcd:Version>1.0</mcd:Version>
  </mcd:PackagingProtocol>
  <mcd:MessageId />
  <mcd:Service>FileTransfer</mcd:Service>
  <mcd:Action>Request</mcd:Action>
  <mcd:TimeStamp>2001-10-04T15:48:01.813Z</mcd:TimeStamp>
- <mcd:RoutingInfo>
  <mcd:SenderId type="Name">Worldwide</mcd:SenderId>
  <mcd:ReceiverId type="Name">ACME</mcd:ReceiverId>
  <mcd:MarketPlace />
  </mcd:RoutingInfo>
- <mcd:TransportInfo sessionId="">
  <mcd:MaxRetry>0</mcd:MaxRetry>
  <mcd:RetryInterval>0</mcd:RetryInterval>
  </mcd:TransportInfo>
- <mcd:TrackingInfo>

<mcd:RefToMessageId>906d1c3f5590f139:723d7c:e959e6dbc5:-8111</mcd:R
```

```
efToMessageId>

<mcd:CorrelationId>906d1c3f5590f139:723d7c:e959e6dbc5:-8000</mcd:Co
rrelationId>
  </mcd:TrackingInfo>
- <mcd:MessagingAgentInfo>
- <mcd-ext:ebXML
xmlns:mcd-ext="http://www.cyclonecommerce.com/Schemas/2001/10/mcd-e
xt-ebXML"


xmlns:ds="http://www.w3.org/2000/09/xmldsig#"


xsi:schemaLocation="http://www.cyclonecommerce.com/Schemas/2001/10/
mcd-ext-ebXML


http://www.cyclonecommerce.com/Schemas/2001/10/MCD_Extension_ebXML_
v1_0.xsd">
- <mcd-ext:ebXMLBinding version="1.0">
- <mcd-ext:ReliableMessaging deliverySemantics="OnceAndOnlyOnce"

messageOrderSemantics="NotGuaranteed">
  <mcd-ext:Retries>0</mcd-ext:Retries>
  <mcd-ext:RetryInterval>0</mcd-ext:RetryInterval>
  <mcd-ext:PersistDuration>0</mcd-ext:PersistDuration>
  <mcd-ext:Acknowledgement ackRequested="Signed" />
  </mcd-ext:ReliableMessaging>
  <mcd-ext:DeliveryReceipt deliveryReceiptRequested="None" />
- <mcd-ext:Envelope>
- <mcd-ext:NonRepudiation>
  <mcd-ext:Protocol
version="">http://www.w3.org/2000/09/xmldsig#</mcd-ext:Protocol>

<mcd-ext:HashFunction>http://www.w3.org/2000/09/xmldsig#sha1</mcd-e
xt:HashFunction>
  </mcd-ext:NonRepudiation>
- <mcd-ext:DigitalEnvelope>
  <mcd-ext:Protocol version="" />
  <mcd-ext:EncryptionAlgorithm />
  </mcd-ext:DigitalEnvelope>
  </mcd-ext:Envelope>
- <mcd-ext:ManifestInfo>
- <mcd-ext:NonRepudiation>
  <mcd-ext:Protocol version="2.0">S/MIME</mcd-ext:Protocol>
  <mcd-ext:HashFunction>SHA1</mcd-ext:HashFunction>
  </mcd-ext:NonRepudiation>
- <mcd-ext:DigitalEnvelope>
  <mcd-ext:Protocol version="2.0">S/MIME</mcd-ext:Protocol>
```

```
<mcd-ext:EncryptionAlgorithm>DES-CBC</mcd-ext:EncryptionAlgorithm>
  </mcd-ext:DigitalEnvelope>
  </mcd-ext:ManifestInfo>
  </mcd-ext:ebXMLBinding>
  </mcd-ext:ebXML>
  </mcd:MessagingAgentInfo>
- <mcd:StatusInfo type="">
  <mcd:Description />
- <mcd:ExceptionInfo type="">
  <mcd:ErrorDescription />
  <mcd:ErrorClassification />
  <mcd:OffendingMessageComponent />
  </mcd:ExceptionInfo>
- <mcd:DigestInfo>
  <mcd:DigestValue />
  <mcd:DigestAlgorithm />
  </mcd:DigestInfo>
  </mcd:StatusInfo>
- <mcd:ManifestInfo>
- <mcd:MessageContentInfo id="723d7c:e959e6dbc5:-7fff">
  <mcd:MIMEContentId>PurchaseOrder</mcd:MIMEContentId>

<mcd:MIMEContentType>application/octet-stream</mcd:MIMEContentType>
  <mcd:Description>Word document</mcd:Description>
- <mcd:Body bodyEncoding="base64">
- <![CDATA[
(payload here)

  ]]>
  </mcd:Body>
  </mcd:MessageContentInfo>
  </mcd:ManifestInfo>
  </mcd:MessageControlDocument>
```

CHAPTER

# 11 Keys and Certificates

WebLogic Integration – Business Connect offers true security by providing privacy, authentication, integrity and non-repudiation of documents. WebLogic Integration – Business Connect uses state-of-the-art cryptography to ensure the security of the documents you exchange over the public Internet. The following topics are provided.

**Concepts**

**Windows**

**Procedures**

- "Setting Up Certificates for Your Company Profile" on page 11-23
- "Importing a Partner's Certificate" on page 11-37
- "Exporting Your Certificate for Backup or Distribution" on page 11-40
- "Deleting Certificates" on page 11-43
- "Viewing Certificate Information" on page 11-46
- "Viewing the Certificate Path" on page 11-47
- "Activating a Pending or Valid Certificate" on page 11-48
- "Retiring a Certificate" on page 11-49
- "Un-Retiring Certificate" on page 11-50
- "Viewing, Editing or Importing Trusted Roots" on page 11-52
- "Using Certificate Revocation Lists" on page 11-54

These topics provide the information you need to:

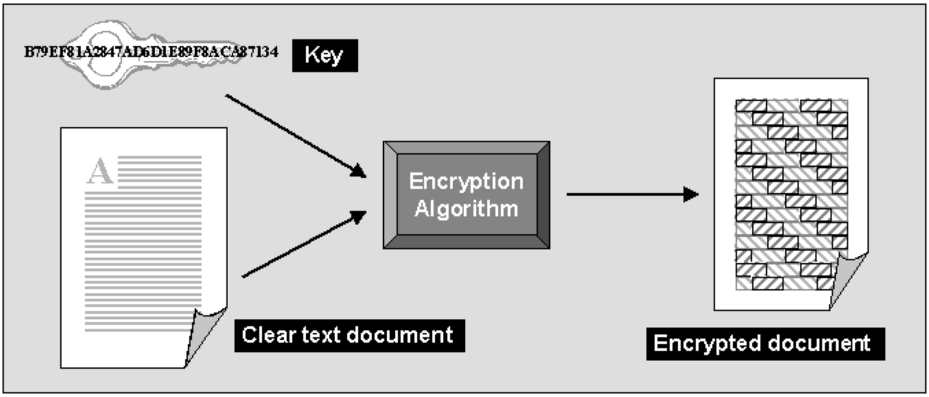
- Understand the basics of encrypting and signing documents. You use this information when you and your trading partners agree upon and select the security settings in your partner profiles.
- Complete preparations to use certificates.
- Create and manage certificates for your company profile.
- Manage the certificates for your partner profiles.

# Why Use Encryption and Digital Signatures

Encrypting and digitally signing documents by using certificates provides WebLogic Integration – Business Connect users with the following assurances about each of their document transmissions:

- Only the addressee can read the message and not any unauthorized people. Encryption provides this assurance.
- The message cannot be tampered with. That is, data cannot be changed, added or deleted without you knowing it. A document's digital signature provides this assurance.
- Partners who send you documents are genuinely who they claim to be. Likewise, when partners receive documents signed by you, they can be confident the documents came from you. A document's digital signature provides this assurance.
- The partners who send you documents cannot claim they did not send them. This is referred to as non-repudiation of origin. A document's digital signature provides this assurance.
- Partners to whom you send documents cannot claim they did not receive them. This is referred to as non-repudiation of receipt. A signed document acknowledgment provides this assurance.

**Figure 11-1 Encrypting a Document Using a Key**



# WebLogic Integration – Business Connect Encryption Method

WebLogic Integration – Business Connect uses a combination of public-private key encryption, which is also known as asymmetric encryption, and symmetric key encryption. This hybrid system uses the best characteristics of each method and minimizes the shortcomings of each. It follows the widely adopted S/MIME standard for securing messages.

The advantage of symmetric key encryption is that it performs the encryption task more quickly than asymmetric encryption. The advantage of asymmetric encryption is that it allows you to send an encrypted message to a partner who does not hold your secret key.

To use the best of both, WebLogic Integration – Business Connect uses the faster symmetric key to encrypt the document, such as a lengthy EDI transaction set, and the asymmetric key for the smaller task of encrypting the one-time session key. The session key can then be securely included with the message for transmission and allows your partner to decrypt the contents without sharing your secret key.

**Note:** As noted in "Transport Selection Considerations" on page 9-31, if you send documents using the HTTPS transport, double encrypting adds only marginally to data security. You can turn off document encryption by clearing the encrypt documents check box on the Partner Profile window Security tab.

## Symmetric Key Encryption Algorithms

WebLogic Integration – Business Connect supports RC2, ARC4, DES, and Triple DES encryption algorithms. The encryption algorithm is used in conjunction with a randomly generated session key to encrypt your document. When you set up a partner profile with WebLogic Integration – Business Connect, you must choose one of these encryption algorithms. WebLogic Integration – Business Connect provides you a full range of choices so that you are capable of trading with whatever algorithm your partner might require. However, when you choose an algorithm, you need to be careful to choose one your trading partner can support.

## Symmetric Key Lengths

WebLogic Integration – Business Connect supports several key lengths for the symmetric key you choose. The choice you make depends on which encryption algorithm you choose. If you choose the RC2 or ARC4 algorithm, you can select 40-, 64-, or 128-bit key length. If you choose DES, the default key length is 56 bits. Triple DES, as the name implies, uses a 168-bit key length. As with algorithms, you need to be careful to choose a key length your trading partner can support.

**Note:** ARC4 is an independently developed algorithm that is interoperable with RSA RC4.

## Public-Private (Asymmetric) Key Algorithms

WebLogic Integration – Business Connect uses the RSA cryptosystem for asymmetric encryption and the digital signatures provided by using certificates.

You can use two types of asymmetric RSA keys:

- Keys issued to you, typically by a certificate authority, and subsequently imported into WebLogic Integration – Business Connect. Such keys are sometimes called managed keys.
- Keys generated by you in WebLogic Integration – Business Connect. Such keys are called self-signed keys.

## Public-Private (Asymmetric) Key Lengths

WebLogic Integration – Business Connect supports encryption key lengths of 512, 1024, and 2048 bits for the public-private key. You must choose one of these key lengths when you generate or obtain your certificate. You do not need to choose the same key length as your trading partner.

# Summary of Algorithms and Key Lengths

To use strong encryption you must ensure that the partner's software supports such strong encryption algorithms and key lengths. The following table summarizes algorithms and key lengths for symmetric and asymmetric keys.

**Table 11-1 Algorithms and Key Lengths**

| **Symmetric algorithm for document encryption** | |
|---|---|
| RC2<br>ARC4 | The default is 40 bits. You can use this length for trading partners located in the U.S. and internationally.<br>You can also choose stronger key lengths of 64 or 128 bits. Longer key lengths require more processing time to encrypt and decrypt, but provide more protection against cryptographic attacks. |
| DES<br>Triple DES | The key length is 56 bits.<br>The key length is 168. |
| **Asymmetric algorithm for authentication** | |
| RSA | The default key length is 512 bits when generating a self-signed certificate. You can also choose a key length of 1024 or 2048. The length of imported RSA keys is determined outside of WebLogic Integration – Business Connect. |

# Support for Dual Keys

WebLogic Integration – Business Connect supports single- and dual-key certificates. You do not need to do anything different to trade documents with a partner who uses dual keys.

When you import the certificates from a partner who uses two keys, both are displayed in the Certificates information viewer. The Usage heading in the Certificates information viewer describes each key as follows:

- *Encryption*
  The key in the certificate is used for encryption purposes.
- *Signature*
  The key in the certificate is used for digital signature purposes.
- *Signature and Encryption*
  The key in the certificate is used for encryption and digital signature purposes.

# Encryption and Signing Summary

Described in the simplest terms, WebLogic Integration – Business Connect exchanges encrypted and signed documents in S/MIME format.

WebLogic Integration – Business Connect is certified S/MIME-compliant by RSA Data Security, Inc.

## Outbound Documents

The document contains the data that needs to be protected. The encryption and signing processes take place for every document that WebLogic Integration – Business Connect sends over the Internet.

WebLogic Integration – Business Connect encrypts and signs each document by building three parts: the encrypted document, the encrypted session key and the digital signature. The following is the process for an outbound document.

1. A hashing routine (MD5 or SHA-1) creates a digital digest of the document. This digest is a number. If the data in the transaction are changed, added to or subtracted from, reapplying the hashing routine will produce an entirely different digest. This characteristic of hashing routines makes it easy for a partner to verify the integrity of an inbound document.

2. The digital digest is encrypted using your private key. This encrypted digest is the digital signature for this document. It ensures that the data in the document were not changed and that the document came from you and only you.
3. WebLogic Integration – Business Connect generates a one-time session key. This is the symmetric key part of WebLogic Integration – Business Connect’s hybrid encryption method.
4. The session key is used to encrypt the document.
5. Your partner’s public key is provided in the certificate inside the profile your partner gave you. It is used to encrypt the session key for transmission. Thus, the key to decrypting the document has itself been encrypted by your partner’s public key and can be decrypted only by your partner’s private key.
6. The document is then sent using whatever transport method you chose for this partner.

## Inbound Documents

When a document is received by your trading partner, the process is reversed according to the following steps.

1. Upon receiving the document, your partner’s WebLogic Integration – Business Connect begins security processing.
2. Your partner uses his or her private key (the matching half to the asymmetric public key you used to encrypt it) to decrypt your symmetric key.
3. The one-time key that was just decrypted is used, in turn, to decrypt the document. Your partner now has your message in clear text.
4. With the public half of your public-private key pair that you sent your trading partner in your certificate (inside your company profile), your trading partner decrypts the digital signature.
5. Your partner uses the same hashing routine (MD5 or SHA-1) to create a digital digest of the document. This is called rehashing. Your trading partner then compares this to the digest in the digital signature you sent. If the two are identical, your partner has proof that the contents of the document were not altered and that it came from you and only you.

6. The document is now ready to be read into and used by your partner's business application.

   **Note:** Any documents that cannot be successfully processed are placed in the Rejected directory, and a notification message is sent to your WebLogic Integration – Business Connect point of contact.

# Certificate Basics

A certificate contains the public half of your public-private key pair along with other identifying information about your WebLogic Integration – Business Connect company profile and point of contact. WebLogic Integration – Business Connect uses certificates to distribute your public key and those of your partners. You use the public key in your partner's certificate to encrypt a document for transmission over the Internet. Your partner uses the public key in your certificate to verify the digital signature of a document received from you.

The following is some basic information about how WebLogic Integration – Business Connect uses certificates:

- Every company profile used to exchange secure documents must have a certificate. WebLogic Integration – Business Connect can generate the certificate or it can be generated externally.
- Every partner profile for partners with whom you exchange signed and encrypted documents must have a certificate.
- A company or partner profile can have only one active certificate at a time. Or, in the case of dual certificates, one active pair of certificates (one for signature, one for encryption).
- A company or partner profile must have an active certificate to successfully exchange signed and encrypted documents.
- A company or partner profile can have multiple valid or retired certificates.
- Certificates can be used to sign documents you transmit by all transport methods.

- You can delete a certificate from the Certificates information viewer, but it remains on the system in Retired status. WebLogic Integration – Business Connect does not use the keys in retired certificates to encrypt, decrypt, sign or verify documents.
- The key length for a certificate does not have to be the same as that for a partner’s certificate.

# How Certificates and Keys Are Stored

WebLogic Integration – Business Connect stores certificates and keys in two files: `ConfigDB.db` and `keys.db`. The `ConfigDB.db` file is in the root application directory. The `keys.db` file is in the keys subdirectory. The contents of these files are encrypted to ensure security. The following describes the roles of these two files.

## ConfigDB.db

Your partners’ certificates and root certificates of major third-party certificate authorities are stored in `ConfigDB.db`. Certificates that you choose to trust are copied to keys.db.

## keys.db

The keys for your certificates are stored in `keys.db`, because you implicitly trust your own certificates. Your partners’ keys also are copied from `ConfigDB.db` to `keys.db`, because you trust their certificates as well.

Moreover, when you install WebLogic Integration – Business Connect, CA root certificates are installed. Because WebLogic Integration – Business Connect implicitly trusts these root certificates, the certificate keys are copied from `ConfigDB.db` to `keys.db`. For more information on CA root certificates, see “Trusted Roots” on page 11-51.

## ConfigDB.db and keys.db Troubleshooting

The `ConfigDB.db` and `keys.db` files are safe and secure. In the slim event of either file becoming corrupted or lost, the most expedient solution is to re-install the application and then import or generate your own and your partners' certificates.

# Certificate Status

WebLogic Integration – Business Connect manages certificates by using the following status categories.

## Active Certificate (Yellow Bulb) 💡

The certificate identified with a yellow bulb is the active certificate for your company profile or for your trading partner's partner profile.

You distribute your public key to your trading partners in your certificate. Your trading partners use this key to verify the digital signature of documents they receive from you.

You receive your trading partner's public key in his or her certificate. You use your partner's public key to encrypt documents for transmission over the Internet.

There can be only one active certificate for signature and encryption or one active pair (one for signature, one for encryption) on your system. The active certificate on your system is also the active certificate on your partners' systems.

When you create or obtain a new certificate for your company profile, you can choose to activate it immediately or to save it in Pending status. If you choose to activate it immediately, WebLogic Integration – Business Connect places the active certificate for your profile in Valid status.

If you import your partner's certificate, WebLogic Integration – Business Connect activates it and places the active certificate for that profile in Valid status.

## Valid or Inactive Certificate (Blue Bulb)

The certificate identified with a blue bulb is one in Valid or Inactive status.

A valid certificate is one that was formerly active on your computer. You can have multiple valid certificates on your system.

If WebLogic Integration – Business Connect fails to verify an inbound document using the public key in the active certificate, the application tries again with each of the valid keys. If one of these succeeds, processing proceeds normally and no alert is sent.

An inactive certificate is one that is valid but is not used to verify signatures or to encrypt messages to a partner.

## Pending Certificate (Red Bulb)

The certificate identified with a red bulb is one in Pending status.

- A new certificate you created or imported for one of your company profiles. At the time of creation, you answered No to the question, "Do you want to activate this certificate?" which caused the certificate to be placed in Pending status rather than to replace an existing, active certificate.
- An untrusted certificate that WebLogic Integration – Business Connect receives electronically from one of your trading partners is automatically imported in Pending status. Before you activate this certificate, you should contact the partner from whom you received the unsigned certificate and verify the certificate's fingerprint.

In either of the preceding cases, you must use the Certificate Profile window to activate a pending certificate. See "Activating a Pending or Valid Certificate" on page 11-48.

## Retired Certificate (Clear Bulb)

A retired certificate is one which was formerly active or valid. You can have multiple retired certificates on your system.

WebLogic Integration – Business Connect does not use the keys associated with retired certificates to sign, verify, encrypt or decrypt documents.

# Exchanging Company Profiles and Certificates

Before you can exchange encrypted and signed documents with a trading partner, each of you must obtain the other's public key. You do this after you have created your company profile. Each of you generates a self-signed certificate or obtains one from a certificate authority (CA). Either way, the process creates a public-private key pair for your company profile. The private half of this key pair always remains on your computer. The public half is exported to a file and distributed to your trading partners on diskette by a secure means.

The following describes how to exchange profiles and certificates with your WebLogic Integration trading partners. In all cases, it is recommended that you confirm the certificate fingerprint with your trading partner before exchanging documents.

## Exchanging Certificate Information with WebLogic Integration Trading Partners

If you are using the Bundled HTTPS transport to exchange messages with a WebLogic Integration trading partner, the certificate information is exchanged as follows:

- Certificate information will not be included in the partner profile your WebLogic Integration trading partner provides. Instead, your WebLogic Integration trading partner must provide the certificate information in a file which you import, as described in "Importing a Partner's Certificate" on page 11-37.
- When your WebLogic Integration trading partner imports your company profile, the certificate information will not be imported. You must export the certificate information to a separate file, as described in "Exporting Your Certificate for Backup or Distribution" on page 11-40.

When you update the certificate associated with your company profile, it is important to coordinate the update process with your trading partners. For guidelines, see "Obtaining New and Replacement Certificates" on page 11-16.

# Self-Signed or CA Certificates

You and your trading partners should decide whether to use WebLogic Integration – Business Connect self-signed X.509 certificates or X.509 certificates from a third-party certificate authority (CA).

If your organization has an Entrust/PKI server and administrator and will use Entrust certificates, see "Entrust Certificates" on page 11-15.

Consider the following in deciding whether to generate a self-signed certificate or obtain one from a CA:

- WebLogic Integration – Business Connect self-signed certificates are easily created. Their primary disadvantage is that they are not verified by a trusted third party. If you decide to use self-signed certificates, see "Setting Up Certificates for Your Company Profile" on page 11-23.
- The primary advantage of using certificates from a CA is that the identity of the certificate holder is verified by a trusted third party. Disadvantages include the extra cost and administrative effort.
- A CA provides a centralized source for posting and obtaining information about certificates, including information about revoked certificates.

# Entrust Certificates

WebLogic Integration – Business Connect fulfills a client role in supporting the certificate management tasks of an Entrust server. The prerequisites for this client-server relationship are your Entrust server and a person who is designated as your organization's Entrust administrator. Lacking these two requirements, your organization cannot use Entrust certificates in exchanging documents with your trading partners through WebLogic Integration – Business Connect.

WebLogic Integration – Business Connect enables an organization with an Entrust/PKI server to:

- Create Entrust X.509 certificates
- Re-initialize Entrust certificates when replacements are needed
- Update Entrust certificates before they expire

WebLogic Integration – Business Connect does not support Entrust certificate revocation or recovery.

WebLogic Integration – Business Connect supports Entrust versions 4 and 5.

The following describes the certificate-generation process involving WebLogic Integration – Business Connect and the Entrust server.

After WebLogic Integration – Business Connect creates the key pair for signing documents, the application hands the public key to the Entrust server. The Entrust server creates the signing certificate and passes the certificate to WebLogic Integration – Business Connect. The public key is within the certificate. WebLogic Integration – Business Connect retains the private signing key. The private signing key is not disclosed to the Entrust server; the private key remains secure within WebLogic Integration – Business Connect. This guarantees security integrity.

Meanwhile, the Entrust server creates the encryption key pair and creates an encryption certificate, which includes the public key. The Entrust server passes to WebLogic Integration – Business Connect the encryption key pair and the encryption certificate.

# Obtaining New and Replacement Certificates

You can generate or obtain new certificates when:

- You know or suspect a certificate has been compromised.
- You need to replace a certificate that is about to expire.
- You want to change your encryption key at planned intervals just as you would change a password.
- You need to set up an additional company profile.

Also, by using the Certificates information viewer, you can make sure you and your trading partners keep your certificates current.

**Note:** WebLogic Integration – Business Connect notifies you when an active certificate associated with an active company profile is about to expire. See "Preferences General Tab" on page 13-19.

The procedure used depends on whether you are generating or loading a certificate for your company profile, or importing certificate information for one of your partners. See "Setting Up Certificates for Your Company Profile" on page 11-23 or "Importing a Partner's Certificate" on page 11-37.

When you generate or load a new certificate for your company profile, you must export the certificate information (your public key) to a file for distribution to your partners. See "Exporting Your Certificate for Backup or Distribution" on page 11-40.

When you generate a new certificate for your company profile because it has expired, become defective or corrupted, or cannot be used for any other reason, we recommend that you distribute it to your trading partners on diskette by a secure means. Recommended secure means include in-person, U.S. mail or private delivery service.

When you generate or load a new certificate for your company profile, you can choose to have WebLogic Integration – Business Connect activate the certificate, or save the certificate in Pending status until a later date. To avoid rejection of documents it is important that you coordinate the process of distributing and activating a replacement certificate. The following topics provide guidelines:

- Replacing a Certificate for non-HTTPS Encryption
- Replacing a Certificate for Bundled HTTPS with Authentication

## Replacing a Certificate for non-HTTPS Encryption

When you update a non-HTTPS certificate for your company profile (that is, one used to encrypt documents exchanged), you must carefully coordinate the timing of the update with your partners. If possible, you should perform such updates when your server is not processing outbound documents. By observing this precaution you can avoid documents being rejected by your trading partners.

If you create and activate a new certificate while WebLogic Integration – Business Connect is encrypting and signing outbound documents, documents that are signed by the private key associated with the new certificate will be rejected by your trading partners, if they have not yet received and activated the new certificate.

The update process for a non-HTTPS certificate does not affect inbound documents because your WebLogic Integration – Business Connect can decrypt and verify them with the last valid certificate.

## Replacing a Certificate for Bundled HTTPS with Authentication

If you have enabled the bundled HTTPS inbound transport, with the authenticate check box selected, you should exercise care when you create and distribute a new certificate. We recommend that you:

- Save the new certificate in pending status.
- Export and distribute the certificate to your partners.
- Coordinate the activation of the certificate with the trading partners who use bundled HTTPS. Ideally, choose a time when no documents are being exchanged in either direction.

It is important to coordinate the update with each partner ahead of time so they avoid sending you any documents until the new certificate has been activated on their system. The reason you must exercise this care is that your bundled HTTPS server can use only the active certificate to authenticate the SSL connection. Likewise, each partner must also hold your current certificate to authenticate the connection with you.

To minimize the number of errors during the process of certificate update, you and your partners should activate the new certificate nearly simultaneously, at a pre-designated time when traffic is at a minimum.

If you implement a new certificate while you are trading documents, your trading partners will not be able to establish the SSL connection required to communicate with you. During this time, your trading partners receive alerts stating that their system cannot connect with you. This situation clears itself up after your partners receive and begin using your new certificate to authenticate the SSL connection.

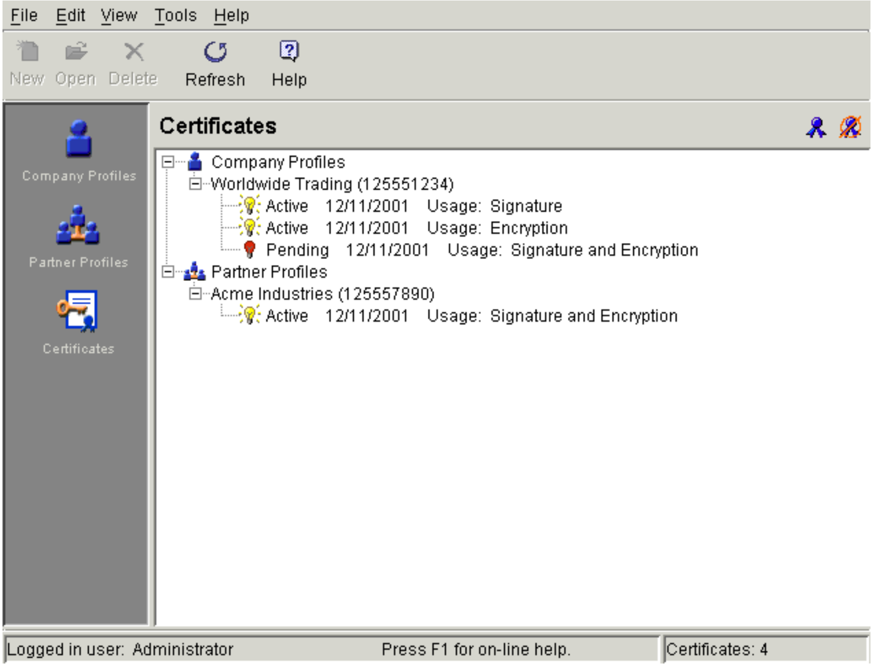
# Certificates Information Viewer

The Certificates information viewer in Administrator enables you to manage certificates for your company and partner profiles. Open the viewer by selecting Certificates on the Administrator bar. To expand or collapse the certificate tree, click the plus or minus signs.

Using the viewer you can:

- View a list of all active, valid and pending certificates for company and partner profiles on your system.
- Open and view the details about active, valid and pending certificates.
- Access the New Certificate wizard to generate or import a key pair and certificate for a company profile.
- Export an active certificate to a file for transmittal to your trading partners.
- Import a trading partner's certificate.
- Retire a certificate.
- Open the Certificate Profile window, where you can view details about certificates and the chain of trust for certificates. Here you can activate a valid or pending certificate. You can also view your retired certificates and bring one of these out of retirement. See "Certificate Profile Window" on page 11-45.

**Figure 11-2 Certificates Information Viewer**



```
Company Profiles
  Worldwide Trading (125551234)
    Active    12/11/2001   Usage:  Signature
    Active    12/11/2001   Usage:  Encryption
    Pending   12/11/2001   Usage:  Signature and Encryption
Partner Profiles
  Acme Industries (125557890)
    Active    12/11/2001   Usage:  Signature and Encryption
```

Logged in user: Administrator | Press F1 for on-line help. | Certificates: 4

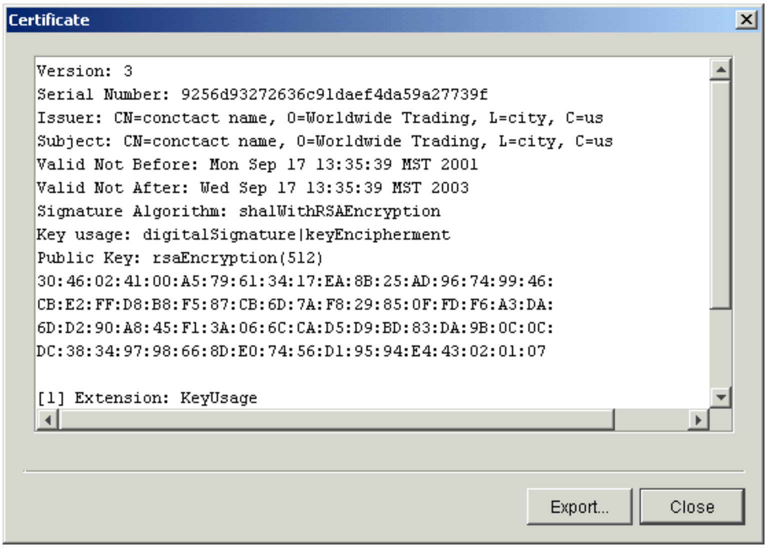
# Certificate Window

Use the Certificate window to view information about a certificate for a company or partner profile. You also can export a certificate to a file.

To open the window, display the Certificates information viewer. Select the certificate you want and double-click it or click Open.

When you finish viewing the certificate information, click Close. To export the certificate, click Export to display the Export Certificate window. See "Exporting Your Certificate for Backup or Distribution" on page 11-40.

**Figure 11-3 Certificate Window for a Self-Signed Certificate**



```
Version: 3
Serial Number: 9256d93272636c91daef4da59a27739f
Issuer: CN=conctact name, O=Worldwide Trading, L=city, C=us
Subject: CN=conctact name, O=Worldwide Trading, L=city, C=us
Valid Not Before: Mon Sep 17 13:35:39 MST 2001
Valid Not After: Wed Sep 17 13:35:39 MST 2003
Signature Algorithm: sha1WithRSAEncryption
Key usage: digitalSignature|keyEncipherment
Public Key: rsaEncryption(512)
30:46:02:41:00:A5:79:61:34:17:EA:8B:25:AD:96:74:99:46:
CB:E2:FF:D8:B8:F5:87:CB:6D:7A:F8:29:85:0F:FD:F6:A3:DA:
6D:D2:90:A8:45:F1:3A:06:6C:CA:D5:D9:BD:83:DA:9B:0C:0C:
DC:38:34:97:98:66:8D:E0:74:56:D1:95:94:E4:43:02:01:07

[1] Extension: KeyUsage
```

# Field Descriptions

The following describes the fields on the Certificate window The information displayed on the window is defined by the X.509 standard.

*Version*

The version of the X.509 standard that applies to the certificate.

*Serial Number*

The serial number uniquely identifies the certificate. The CA or entity that issued the certificate assigned this number. If the issuer revokes a certificate, it can place the serial number on a certificate revocation (CRL) list.

*Issuer and Subject*

The issuer is the X.500 distinguished name of the CA or entity that signed the certificate. In cases of a self-signed certificate, the issuer and subject are the same. Using the certificate implies trusting the signer.

The subject is the X.500 distinguished name of the entity whose public key the certificate identifies.

A distinguished name has the following parts:

| | |
|---|---|
| C | Two-letter ISO country code. See Appendix A, "ISO Country Codes." |
| L | City or locality name |
| O | Organization name |
| OU | Organizational unit. |
| CN | Common name of a person |

*Valid Not Before*
The date the certificate became valid.

*Valid Not After*
The date the certificate expires, provided it is not compromised or revoked before that date.

*Signature Algorithm*
The algorithm the CA used to sign the certificate.

*Key Usage*
Identifies the purpose of the key in the certificate, such as encipherment, digital signature or certificate signing.

*Public Key*
An algorithm identifier that specifies the public key crypto system this key belongs to and any associated key parameters, such as key length.

*Extension*
Optional information present in version 3 certificates. Extensions can be key and policy information, certificate subject and issuer attributes, certificate path constraints, distribution points for certificate revocation lists (CRLs) and private extensions.

For a CA-issued certificate, the CRL distribution point information is present in the form of a URL. This is one place you can find a CA's distribution point for a CRL if you want to configure WebLogic Integration – Business Connect to use CRLs. See "Using Certificate Revocation Lists" on page 11-54. A self-signed certificate does not have CRL distribution point information.

*Fingerprint*

The fingerprints are a way to verify the source of a certificate. After you import or export a certificate, you should contact your partner and ensure that the fingerprints at both ends are identical. You should do this before you attempt to exchange documents. If the fingerprints do not match, one of the certificates might be corrupted or out of date.

# Setting Up Certificates for Your Company Profile

Use this procedure to create new, self-signed certificates for your company profile or to load a new, third-party certificate for your company profile.

If you want to use a certificate from a third-party CA such as VeriSign, you must obtain that certificate using your Internet browser and export it to a file before you begin this procedure. You must export the certificate to a file that contains the private key and the entire chain of trust. You will need the password used to export the file from your browser to load the certificate into WebLogic Integration – Business Connect.

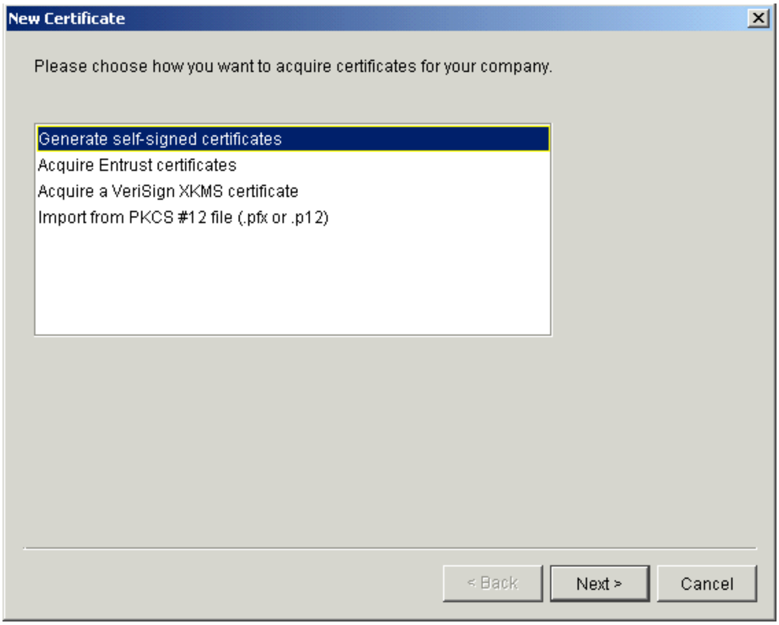
This is not the procedure to use for importing a partner's certificate. See "Importing a Partner's Certificate" on page 11-37.

## Steps

1. When you save a new company profile, the system prompts you to associate a certificate with the profile. Click Yes on the dialog box prompt to start the New Certificate wizard.

   If you want to associate a certificate with an existing company profile, click Certificates on the Administrator bar to display the Certificates information viewer. Select the company you want and click New to start the New Certificate wizard.

**Figure 11-4 New Certificate Wizard, Select Certificate Type Window**


New Certificate
Please choose how you want to acquire certificates for your company.
Generate self-signed certificates
Acquire Entrust certificates
Acquire a VeriSign XKMS certificate
Import from PKCS #12 file (.pfx or .p12)
< Back
Next >
Cancel

2. Select the appropriate certificate option, as described in the following table.

**Table 11-2 Certificate Options**

| Option | Description |
|---|---|
| Generate self-signed certificates | Click if you want WebLogic Integration – Business Connect to generate one self-signed certificate, for both signature and encryption, or two self-signed certificates, one for signature and one for encryption. Go to "Generating Self-Signed Certificates" on page 11-25. |
| Acquire Entrust certificates | Click if your organization has an Entrust Technologies server and administrator and plans to use Entrust certificates. Go to "Importing Entrust Certificates" on page 11-28. |
| Acquire a VeriSign XKMS certificate | Click to import a new VeriSign XML Key Management Specification (XKMS) certificate. Go to "Importing a VeriSign XKMS Certificate" on page 11-31 |

**Table 11-2 Certificate Options (Continued)**

| Option | Description |
|---|---|
| Import from PKCS #12 file (.pfx or .p12) | Click if you want to use a third-party certificate. Go to "Importing a Third-Party CA Certificate" on page 11-34. |

## Generating Self-Signed Certificates

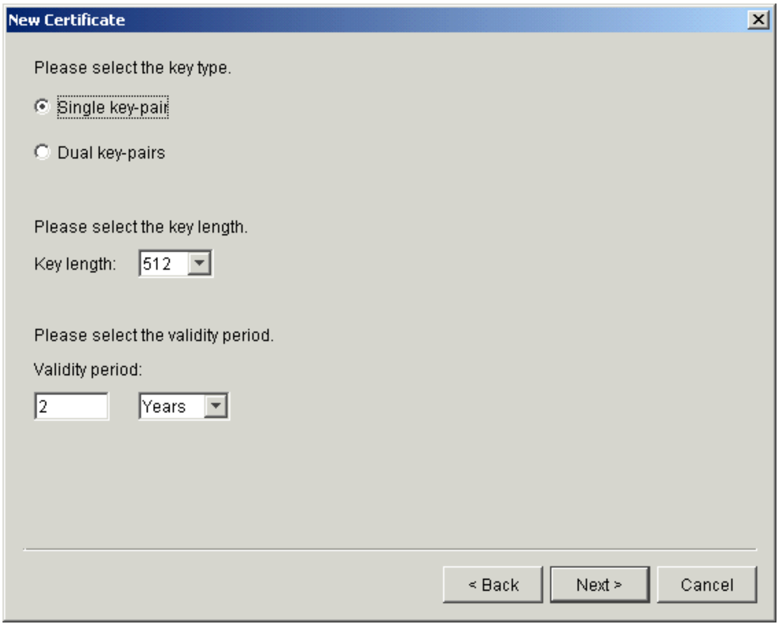
Use this procedure if you selected generate self-signed certificates in step 2 of "Setting Up Certificates for Your Company Profile" on page 11-23.

The following are the steps for generating and associating with a company profile either a single self-signed certificate for both encrypting and signing documents or two self-signed certificates, one for encrypting and one for signing.

## Steps

1. On the first New Certificate wizard window, click Next to display the New Certificate select key type window.

**Figure 11-5 New Certificate Wizard, Select Key Type Window**



New Certificate

Please select the key type.

● Single key-pair

○ Dual key-pairs

Please select the key length.

Key length: 512

Please select the validity period.

Validity period:

2 Years

2. Click single key if you want one certificate for both signing and encrypting documents. Click dual key if you want two certificates, one for signing documents and another for encrypting documents.

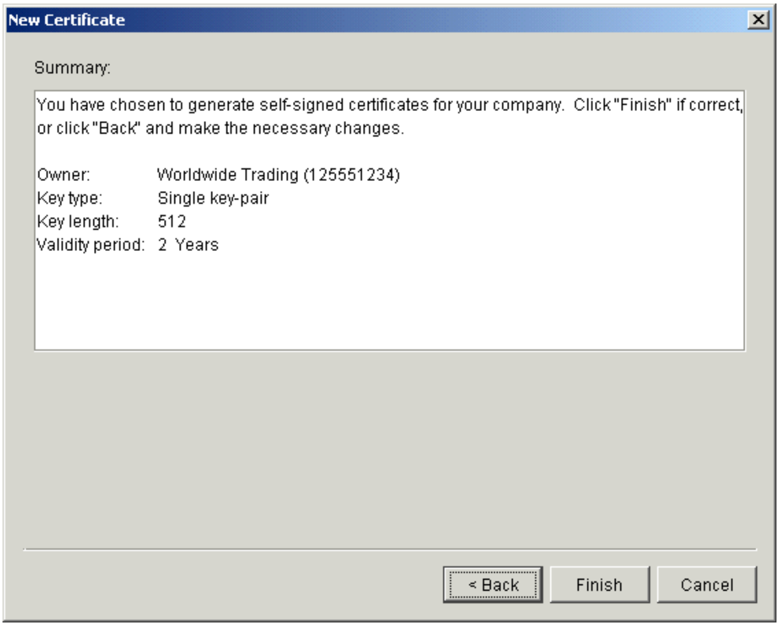
3. Select the one of the following encryption key lengths from the key length drop-down list:

| | |
|---|---|
| 512 | Standard encryption. For highly sensitive or valuable information, stronger encryption is recommended. |
| 1024 | Strong encryption. |
| 2048 | Very strong encryption. |

4. For the validity period, if you want other than the default value of 2 years, type the length of time you want the certificate to be valid in the validity period field. Select days, months or years from the drop-down list.

5. Click Next to display the New Certificate summary window.

**Figure 11-6 New Certificate Wizard, Summary Window**



You have chosen to generate self-signed certificates for your company. Click "Finish" if correct, or click "Back" and make the necessary changes.

| | |
|---|---|
| Owner: | Worldwide Trading (125551234) |
| Key type: | Single key-pair |
| Key length: | 512 |
| Validity period: | 2 Years |

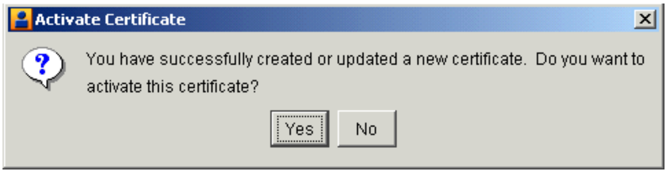
6. Review the information in the window. Click Back to change any information or click Finish to generate the certificate.

   When you click Finish, a dialog box appears with a message that the certificates are being generated and might take a few minutes to complete.

   If there are no other certificates for this company profile, the new certificate is placed in Active status.

   If a certificate already exists for this company profile, a dialog box appears asking whether you want to activate the new certificate.

**Figure 11-7 Activate Certificate Dialog Box**



Activate Certificate

You have successfully created or updated a new certificate. Do you want to activate this certificate?

When this message appears, click Yes or No as follows:

| | |
|---|---|
| Yes | Places the new certificate in Active status and any earlier certificate in Valid status. |
| No | Places the new certificate in Pending status. |

After the certificate is generated, the Company Profile or Certificates information viewer reappears, depending on whether you imported a certificate for a new or existing company profile. The new certificate appears on the Certificates information viewer.

7. Whether you are adding a certificate to new company profile, or replacing the certificate for an existing company profile, you must distribute the new certificate to partners on diskette or by some secure means. To export certificate information to a file for distribution, see "Exporting Your Certificate for Backup or Distribution" on page 11-40. For guidelines on coordinating the update of your certificate, see "Obtaining New and Replacement Certificates" on page 11-16.

**Note:** Before you attempt to exchange encrypted and signed documents, you should contact each partner with whom you exchanged certificates and confirm that the fingerprints in both your certificates are identical. For more information see "Certificate Window" on page 11-20.

# Importing Entrust Certificates

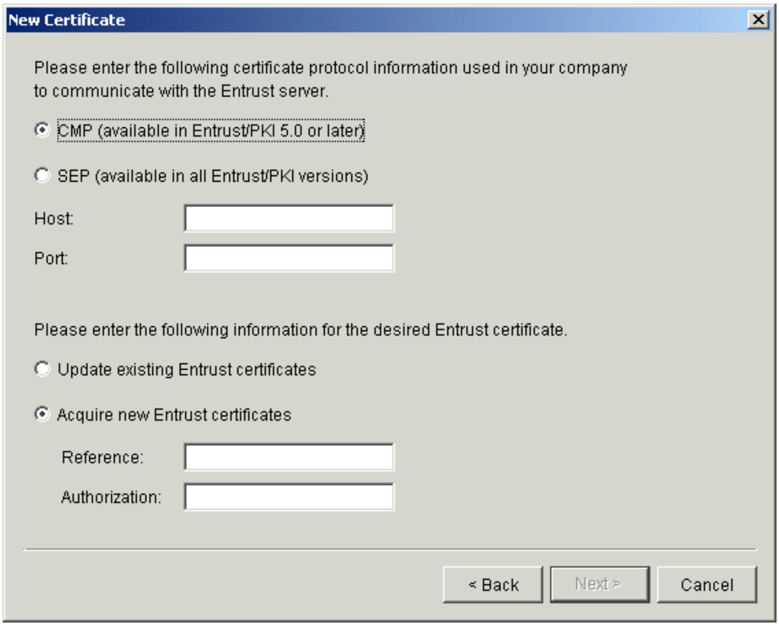
Use this procedure if you selected acquire Entrust certificates in step 2 of "Setting Up Certificates for Your Company Profile" on page 11-23.

The following are the steps for importing a new Entrust certificate into WebLogic Integration – Business Connect or for updating an Entrust certificate that is already associated with a company profile. Before you can use this procedure, you must consult with your organization’s Entrust administrator about the information required to connect with the Entrust/PKI server and import a new or updated certificate for your company profile.

## Steps

1. On the first New Certificate wizard window, click Next to display the Entrust server information window.

**Figure 11-8 New Certificate Wizard, Entrust Server Information Window**



New Certificate

Please enter the following certificate protocol information used in your company to communicate with the Entrust server.

● CMP (available in Entrust/PKI 5.0 or later)

○ SEP (available in all Entrust/PKI versions)

Host:

Port:

Please enter the following information for the desired Entrust certificate.

○ Update existing Entrust certificates

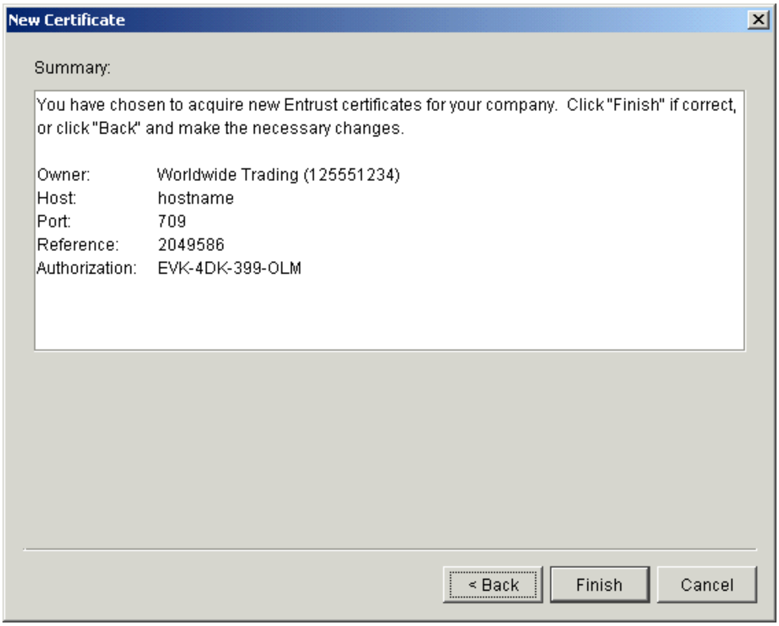
● Acquire new Entrust certificates

Reference:

Authorization:

2. Consult with your Entrust administrator on whether to select CMP or SEP.
3. Have your Entrust administrator provide the information for completing the host and port fields.
4. Click whether you want to update or acquire certificates. For acquiring certificates, have your Entrust administrator provide the information for the reference and authorization fields.
5. Click Next to display the New Certificate summary window.

**Figure 11-9 New Certificate Wizard, Summary Window**



New Certificate

Summary:

You have chosen to acquire new Entrust certificates for your company. Click "Finish" if correct, or click "Back" and make the necessary changes.

| | |
|---|---|
| Owner: | Worldwide Trading (125551234) |
| Host: | hostname |
| Port: | 709 |
| Reference: | 2049586 |
| Authorization: | EVK-4DK-399-OLM |

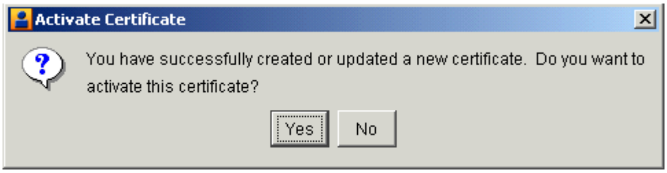
The window displays applicable summary information depending on the option you specified in step 4.

6. Review the information in the window. Click Back to change any information or click Finish to acquire or update a certificate.

   If there are no other certificates for this company profile, the new certificate is placed in Active status.

   If a certificate already exists for this company profile, a dialog box appears asking whether you want to activate the new certificate.

**Figure 11-10 Activate Certificate Dialog Box**



Activate Certificate

You have successfully created or updated a new certificate. Do you want to activate this certificate?

When this message appears, click Yes or No as follows:

| | |
|---|---|
| Yes | Places the new certificate in Active status and any earlier certificate in Valid status. |
| No | Places the new certificate in Pending status. |

After the certificate is generated, the Company Profile or Certificates information viewer reappears, depending on whether you imported a certificate for a new or existing company profile. The new certificate appears on the Certificates information viewer.

7. Whether you are adding a certificate to new company profile, or replacing the certificate for an existing company profile, you must distribute the new certificate to partners on diskette or by some secure means. To export certificate information to a file for distribution, see "Exporting Your Certificate for Backup or Distribution" on page 11-40. For guidelines on coordinating the update of your certificate, see "Obtaining New and Replacement Certificates" on page 11-16.

**Note:** Before you attempt to exchange encrypted and signed documents, you should contact each partner with whom you exchanged certificates and confirm that the fingerprints in both your certificates are identical. For more information see "Certificate Window" on page 11-20.

# Importing a VeriSign XKMS Certificate

Use this procedure if you selected acquire a VeriSign XKMS certificate in step 2 of "Setting Up Certificates for Your Company Profile" on page 11-23.

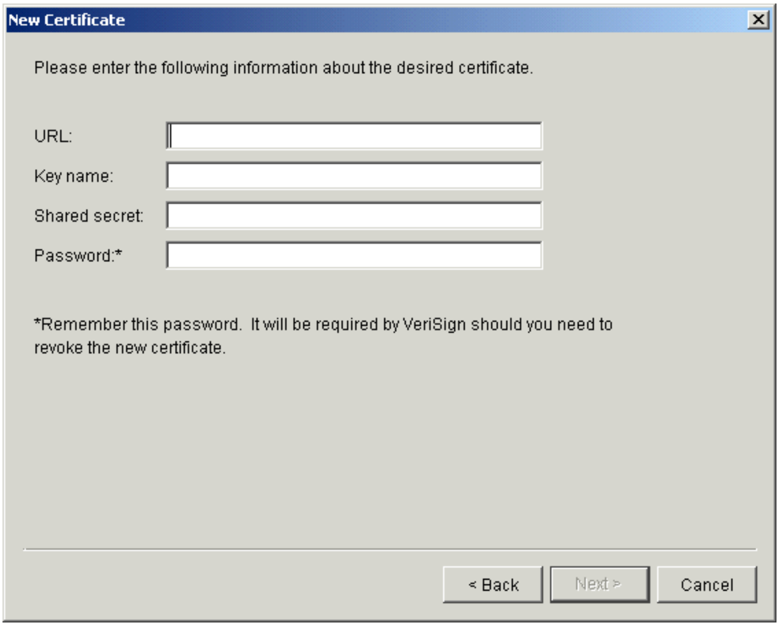
The following are the steps for importing a new XML Key Management Specification (XKMS) certificate into WebLogic Integration – Business Connect and associating it with a company profile. Before you can use this procedure, you must register for a new XKMS certificate from VeriSign. When the new certificate is ready, you will receive an e-mail containing the information needed to connect to a server and import the certificate for your company profile.

XKMS was designed in an effort to combine the interoperability afforded by Extensible Markup Language (XML) in business-to-business electronic commerce with secure and easy to use public key infrastructure (PKI). For information about XKMS see http://xmltrustcenter.org/index.htm.

## Steps

1. On the first New Certificate wizard window, click Next to display the VeriSign XKMS certificate window.

**Figure 11-11 New Certificate Wizard, VeriSign XKMS Certificate Window**



New Certificate

Please enter the following information about the desired certificate.

URL:

Key name:

Shared secret:

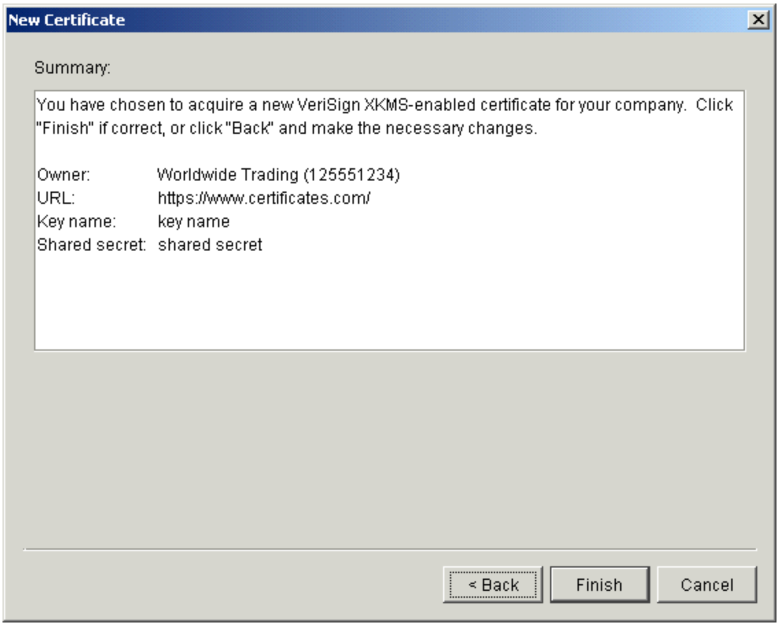
Password:*

*Remember this password. It will be required by VeriSign should you need to revoke the new certificate.

2. Using the information provided to you, complete the fields for importing the certificate. Type this information in the URL, key name and shared secret fields. In the password field, type a password that you can remember. You will need this password if you later ask VeriSign to revoke the certificate.

3. Click Next to display the New Certificate summary window.

**Figure 11-12 New Certificate Wizard, Summary Window**



You have chosen to acquire a new VeriSign XKMS-enabled certificate for your company. Click "Finish" if correct, or click "Back" and make the necessary changes.

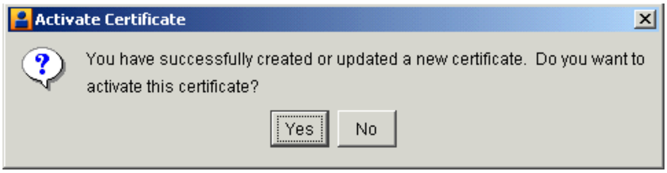
Owner: Worldwide Trading (125551234)
URL: https://www.certificates.com/
Key name: key name
Shared secret: shared secret

4. Review the information in the window. Click Back to change any information or click Finish to import the certificate.

   If there are no other certificates for this company profile, the new certificate is placed in Active status.

   If a certificate already exists for this company profile, a dialog box appears asking whether you want to activate the new certificate.

**Figure 11-13 Activate Certificate Dialog Box**



You have successfully created or updated a new certificate. Do you want to activate this certificate?

When this message appears, click Yes or No as follows:

| | |
|---|---|
| Yes | Places the new certificate in Active status and any earlier certificate in Valid status. |
| No | Places the new certificate in Pending status. |

After the certificate is generated, the Company Profile or Certificates information viewer reappears, depending on whether you imported a certificate for a new or existing company profile. The new certificate appears on the Certificates information viewer.

5. Whether you are adding a certificate to new company profile, or replacing the certificate for an existing company profile, you must distribute the new certificate to partners on diskette or by some secure means. To export certificate information to a file for distribution, see “Exporting Your Certificate for Backup or Distribution” on page 11-40. For guidelines on coordinating the update of your certificate, see “Obtaining New and Replacement Certificates” on page 11-16.

**Note:** Before you attempt to exchange encrypted and signed documents, you should contact each partner with whom you exchanged certificates and confirm that the fingerprints in both your certificates are identical. For more information see “Certificate Window” on page 11-20.

# Importing a Third-Party CA Certificate

Use this procedure if you selected to import from PKCS #12 file in step 2 of “Setting Up Certificates for Your Company Profile.”

The following are the steps for importing a third-party CA certificate into WebLogic Integration – Business Connect and associating it with a company profile. Such a certificate file contains both the public and private keys. Before you can use this procedure, you must perform the following tasks:

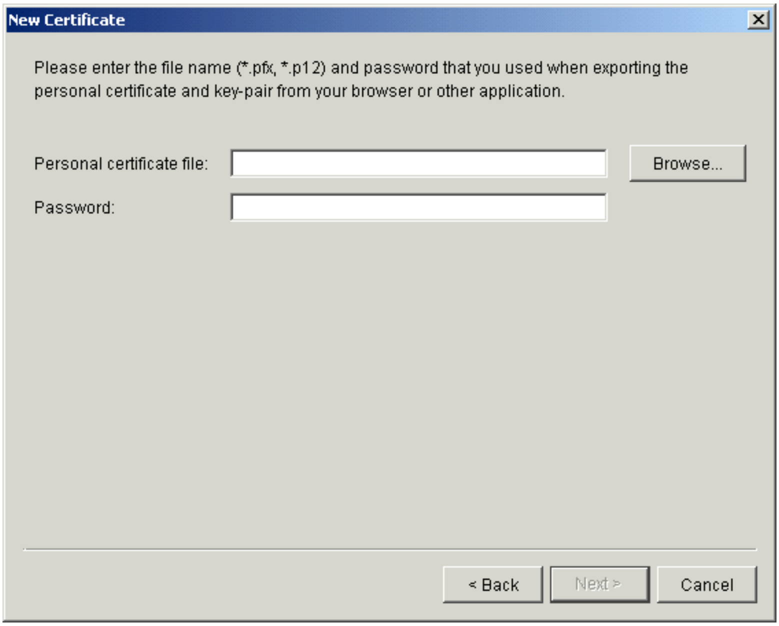
- Obtain a certificate from a certificate authority such as VeriSign.
- Export the certificate from a browser or mail client to a file. Assign a password when exporting the file; you will need this same password upon importing the file.

- Export both the public and private keys with the certificate. A certificate file with both keys is a P12 or PFX file.
- If you export the certificate from Microsoft Outlook or Internet Explorer, select the check box for “include all certificates in the certification path if possible.” You want the exported file to include the entire chain of trust.

## Steps

1. On the first New Certificate wizard window, click Next to display the New Certificate third-party certificate window.

**Figure 11-14 New Certificate Wizard, Third-Party Certificate Window**



New Certificate

Please enter the file name (*.pfx, *.p12) and password that you used when exporting the personal certificate and key-pair from your browser or other application.

Personal certificate file:

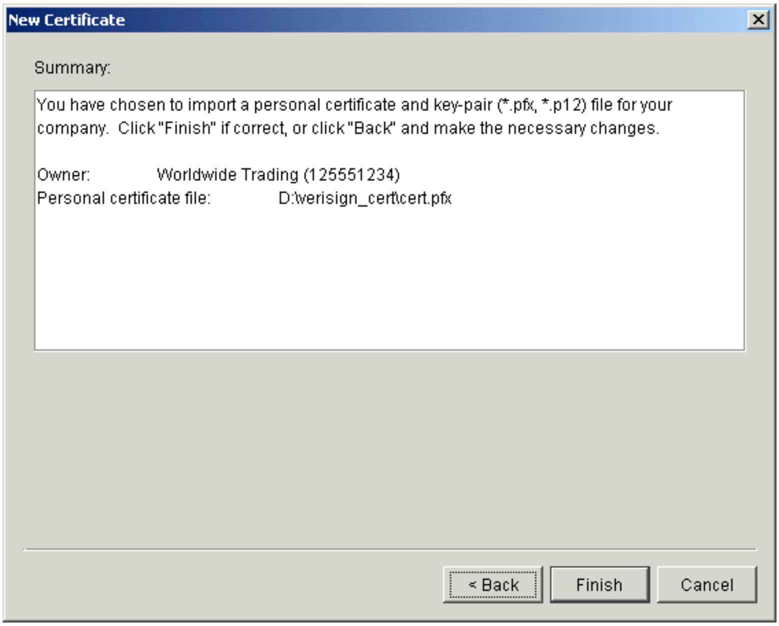
Password:

2. To locate the PKCS#12 file containing your certificate, click Browse to display the Browse dialog box.
3. Locate and select the certificate file. The file must have an extension of `.pfx` or `.p12`. Click Open and the New Certificate third-party certificate window reappears.

4. Type the same password you used when you exported the certificate file from a browser or mail client.

5. Click Next to display the New Certificate summary window.

**Figure 11-15 New Certificate Wizard, Summary Window**



New Certificate

Summary:

You have chosen to import a personal certificate and key-pair (*.pfx, *.p12) file for your company.  Click "Finish" if correct, or click "Back" and make the necessary changes.

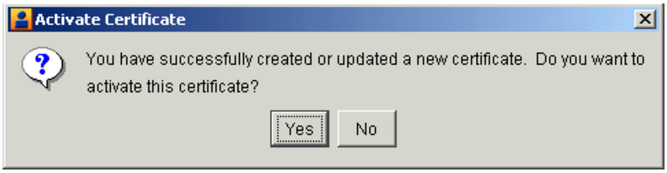
Owner: Worldwide Trading (125551234)
Personal certificate file: D:\verisign_cert\cert.pfx

6. Review the certificate information in the window. Click Back to change any information or click Finish to import the certificate.

   If there are no other certificates for this company profile, the new certificate is placed in Active status.

   If a certificate already exists for this company profile, a dialog box appears asking whether you want to activate the new certificate.

**Figure 11-16 Activate Certificate Dialog Box**



Activate Certificate

You have successfully created or updated a new certificate.  Do you want to activate this certificate?

When this message appears, click Yes or No as follows:

| | |
|---|---|
| Yes | Places the new certificate in Active status and any earlier certificate in Valid status. |
| No | Places the new certificate in Pending status. |

After the certificate is generated, the Company Profile or Certificates information viewer reappears, depending on whether you imported a certificate for a new or existing company profile. The new certificate appears on the Certificates information viewer.

7. Whether you are adding a certificate to new company profile, or replacing the certificate for an existing company profile, you must distribute the new certificate to partners on diskette or by some secure means. To export certificate information to a file for distribution, see “Exporting Your Certificate for Backup or Distribution” on page 11-40. For guidelines on coordinating the update of your certificate, see “Obtaining New and Replacement Certificates” on page 11-16.

**Note:** Before you attempt to exchange encrypted and signed documents, you should contact each partner with whom you exchanged certificates and confirm that the fingerprints in both your certificates are identical. For more information see “Certificate Window” on page 11-20.

# Importing a Partner’s Certificate

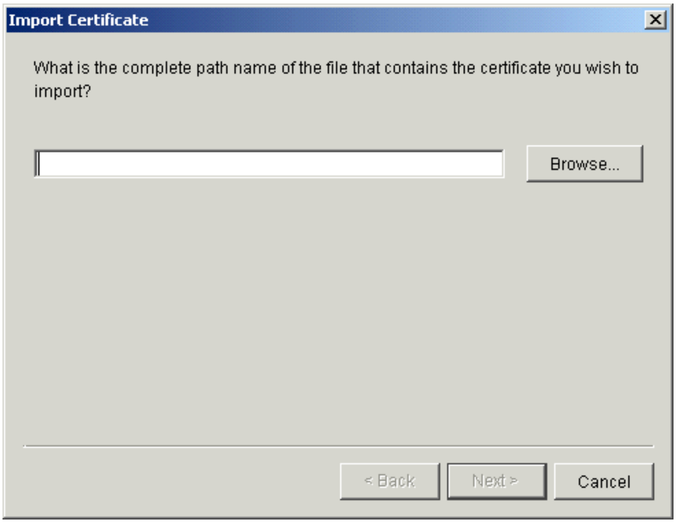
When your trading partner provides a new or updated certificate in a file, use this procedure to import the certificate.

**Note:** WebLogic Integration – Business Connect automatically places any existing partner certificate in Valid status when it imports a new one. The new certificate is automatically set to Active status.

## Steps

1. Make sure you can access on your system the replacement certificate file that your partner sent you.
2. From the Certificates information viewer, select the partner you want and select File→Import to open the Import Certificate window.

**Figure 11-17 Import Certificate Window**

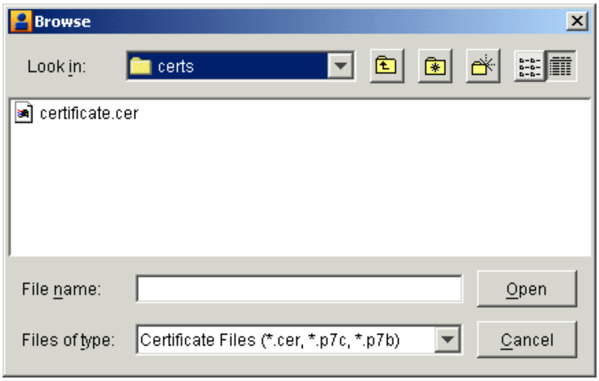


Import Certificate

What is the complete path name of the file that contains the certificate you wish to import?

3. Click Browse to open the Browse dialog box.

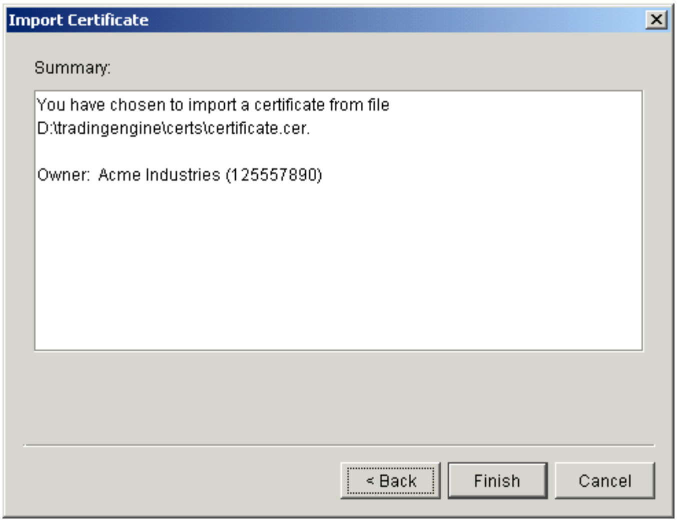
**Figure 11-18 Browse Dialog Box**



4. Select the certificate file you want to import and click Open to redisplay the Import Certificate window.

5. Click Next to display the Import Certificate summary window.

**Figure 11-19 Import Certificate Summary Window**



You have chosen to import a certificate from file D:\tradingengine\certs\certificate.cer.

Owner: Acme Industries (125557890)

6. Review the certificate information in the window. Click Back to change any information or click Finish to import the certificate. When you click Finish a dialog box appears with the message that the active certificate already associated with the profile will be set to valid so the new certificate can be set to active.

7. Click OK. The Certificates information viewer is redisplayed with the new certificate you imported. The certificate you just imported has a status of active. The replaced certificate has a status of valid.

**Note:** Before you attempt to exchange encrypted and signed documents, you should contact the partner from whom you imported the certificate and confirm that the fingerprints in both your certificates are identical. For more information see “Certificate Window” on page 11-20.

# Exporting Your Certificate for Backup or Distribution

Use this procedure to export a certificate to a file.

When exporting your certificate for distribution to your partners, only export your public key. Never give your partner a certificate that contains your private key.

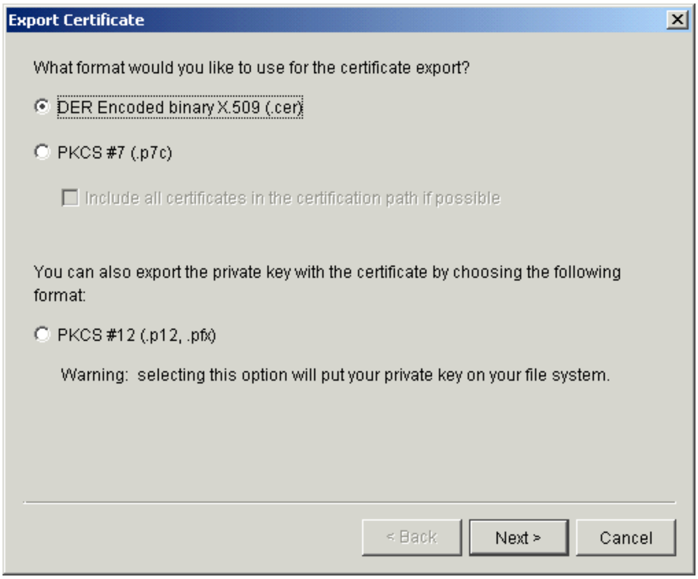
When exporting your certificate for backup purposes, you can export a certificate that contains your private key. If you do so, keep this certificate in a secure place and never give it to anyone.

After you export a certificate with a public key for distribution to your trading partners, you can send the file to your trading partners by e-mail or on diskette. This is one way to save a certificate to a file. For another way to export a certificate see “Viewing Certificate Information” on page 11-46.

## Steps

1. On the Certificates information viewer, select the certificate you want to export and select File→Export to open the Export Certificate selection window.

**Figure 11-20 Export Certificate Selection Window**



Export Certificate

What format would you like to use for the certificate export?

● DER Encoded binary X.509 (.cer)

○ PKCS #7 (.p7c)

□ Include all certificates in the certification path if possible

You can also export the private key with the certificate by choosing the following format:

○ PKCS #12 (.p12, .pfx)

Warning: selecting this option will put your private key on your file system.

2. Select an export option.

**Table 11-3 Export Options**

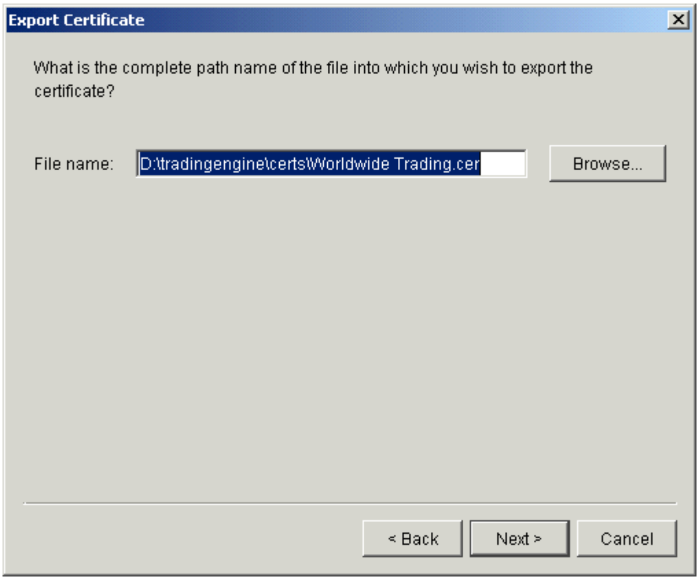
| Export option | Description |
|---|---|
| DER encoded binary X.509 (.cer) | Select this option to export a certificate containing a public key.<br>**Note:** If you are exporting a certificate for distribution to a WebLogic Integration trading partner, you must select this option. |
| PKCS #7 (.p7c) | Select this option to export a certificate containing a public key. |
| Include all certificates in the certification path if possible | If you select PKCS #7 (.p7c), select this option to include all certificates in the chain of trust for the certificate. This is applicable for third-party certificates, but not for self-signed certificates. |

**Table 11-3 Export Options (Continued)**

| Export option | Description |
|---|---|
| PKCS #12 (.p12, .pfx) | Select this option to export a certificate containing your private key. You should do this only if you can keep the certificate in a highly secure place.<br>This option is only available for exporting one of your certificates and not one of your partner's certificates. Your partner would not send you a certificate that contains a private key. |

3. Click Next to display the Export Certificate file name and path window.

**Figure 11-21 Export Certificate File Name and Path Window**



Export Certificate

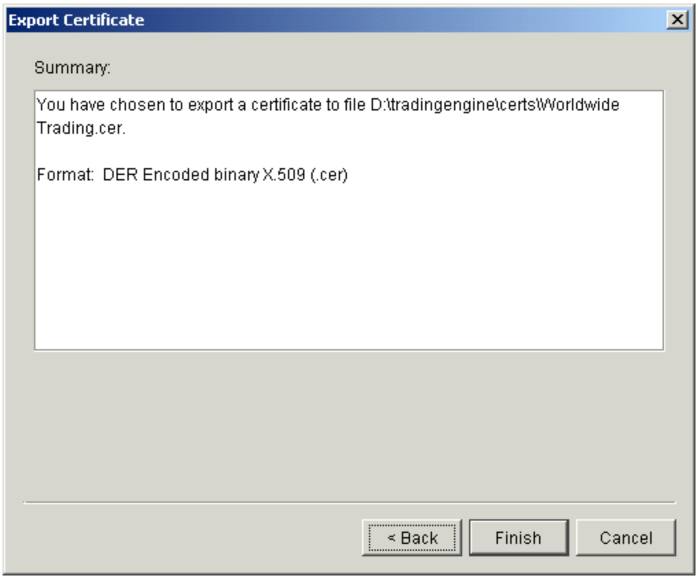
What is the complete path name of the file into which you wish to export the certificate?

File name: D:\tradingengine\certs\Worldwide Trading.cer

4. Review the file name and path for the file you are exporting. If you want to change the path or name, type your changes or click Browse to open a Browse window.

5. Click Next to display the Export Certificate summary window.

**Figure 11-22 Export Certificate Summary Window**



Export Certificate

Summary:

You have chosen to export a certificate to file D:\tradingengine\certs\Worldwide Trading.cer.

Format: DER Encoded binary X.509 (.cer)

6. Review the certificate information in the window. Click Back to change any information or click Finish to export the certificate. When you click Finish a dialog box appears with the message that the export succeeded. Click OK.

7. If you exported the certificate for a partner, send the certificate file to the partner by a secure means.

# Deleting Certificates

Use this procedure to retire certificates that you or your partners no longer use for verifying signatures or encrypting messages.

Retiring a certificate is a pseudo-deleting process that results in its removal from the Certificates information viewer. However, the certificate remains in the system as a dormant entity that can be reactivated if need be. Allowing a certificate to be retired but not deleted is a safeguard for the future in the event a signature must be re-validated or a secure message decrypted again.

This is one way to retire certificates. You also can use the Certificate Profile window for a selected company or partner profile. See “Retiring a Certificate” on page 11-49.

For the steps to reactivate a certificate, see “Un-Retiring Certificate” on page 11-50.

You can view a details window for retired certificates after you have withdrawn them.

## Steps

1. At the Certificates information viewer, select the certificate you want to retire and click Delete. A dialog box appears with a message asking whether you want to retire the certificate.
2. Click Yes to retire the certificate or No to cancel the operation.

   If you click Yes, the certificate no longer appears on the Certificates information viewer.

   If you want to verify that the certificate has been retired, select the profile associated with the retired certificate and click Open to open the Certificate Profile window. Select the Retired Certificates tab. The certificate you retired appears on the tab. To view details of the retired certificate, click View Certificate.

# Certificate Profile Window

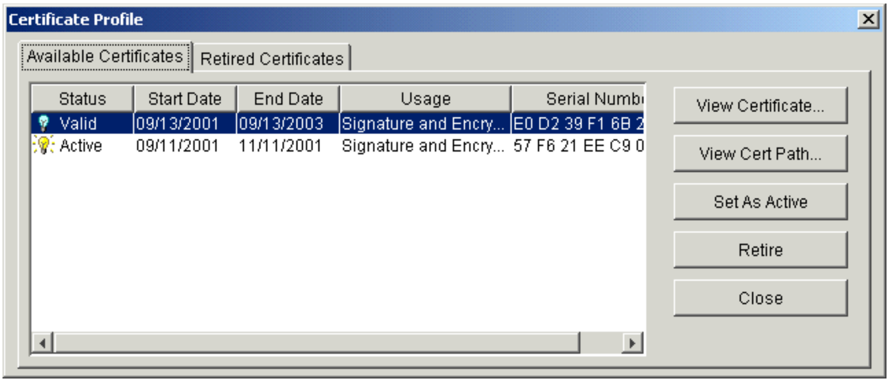
The Certificate Profile window can be opened from the Certificates information viewer. You can use the Certificate Profile window to manage the certificates associated with company and partner profiles. The following topics are provided for using the window.

- "Viewing Certificate Information" on page 11-46
- "Viewing the Certificate Path" on page 11-47
- "Activating a Pending or Valid Certificate" on page 11-48
- "Retiring a Certificate" on page 11-49
- "Un-Retiring Certificate" on page 11-50

To open the window from the Certificates information viewer, select the name of the company or partner with the certificates you want and click Open.

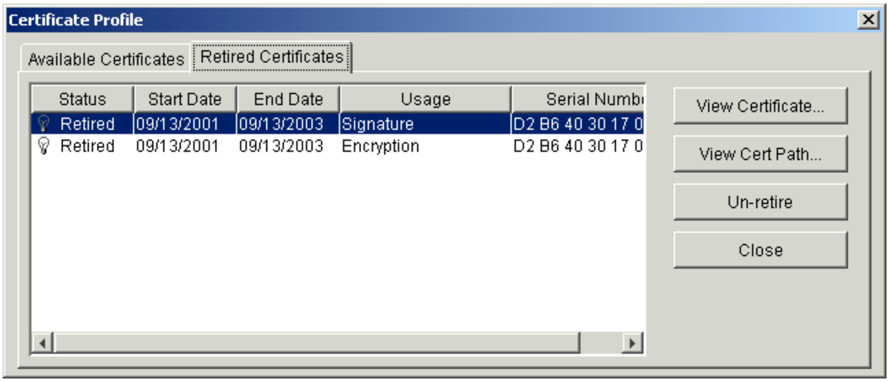
The window has two tabs: Available Certificates and Retired Certificates.

**Figure 11-23 Certificate Profile Window, Available Certificates Tab**



| Status | Start Date | End Date | Usage | Serial Numb |
|---|---|---|---|---|
| Valid | 09/13/2001 | 09/13/2003 | Signature and Encry... | E0 D2 39 F1 6B 2 |
| Active | 09/11/2001 | 11/11/2001 | Signature and Encry... | 57 F6 21 EE C9 0 |

**Figure 11-24 Certificate Profile Window, Retired Certificates Tab**



| Status | Start Date | End Date | Usage | Serial Numb |
|---|---|---|---|---|
| Retired | 09/13/2001 | 09/13/2003 | Signature | D2 B6 40 30 17 0 |
| Retired | 09/13/2001 | 09/13/2003 | Encryption | D2 B6 40 30 17 0 |

# Viewing Certificate Information

Use this procedure to view information about a certificate for a company or partner profile. You also can export a certificate to a file.

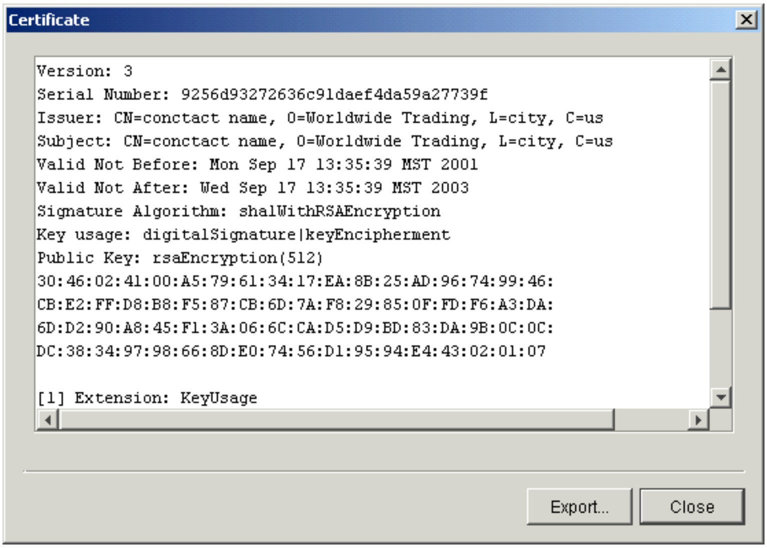
This procedure uses the Certificate window, which is the same one described in "Certificate Window" on page 11-20, but here you access the window through the Certificate Profile window. See "Certificate Profile Window" on page 11-45 for details about the window.

## Steps

1. At the Certificates information viewer, select the name of the company or partner with the certificates you want. Click Open to open the Certificate Profile window with the Available Certificates tab selected.

2. Select the certificate you want to view and click View Certificate to open the Certificate window.

**Figure 11-25 Certificate Window for a Self-Signed Certificate**



```
Version: 3
Serial Number: 9256d93272636c91daef4da59a27739f
Issuer: CN=conctact name, O=Worldwide Trading, L=city, C=us
Subject: CN=conctact name, O=Worldwide Trading, L=city, C=us
Valid Not Before: Mon Sep 17 13:35:39 MST 2001
Valid Not After: Wed Sep 17 13:35:39 MST 2003
Signature Algorithm: sha1WithRSAEncryption
Key usage: digitalSignature|keyEncipherment
Public Key: rsaEncryption(512)
30:46:02:41:00:A5:79:61:34:17:EA:8B:25:AD:96:74:99:46:
CB:E2:FF:D8:B8:F5:87:CB:6D:7A:F8:29:85:0F:FD:F6:A3:DA:
6D:D2:90:A8:45:F1:3A:06:6C:CA:D5:D9:BD:83:DA:9B:0C:0C:
DC:38:34:97:98:66:8D:E0:74:56:D1:95:94:E4:43:02:01:07

[1] Extension: KeyUsage
```

See “Certificate Window” on page 11-20 for a description of the fields.

If you want to export the certificate, click Export. See “Exporting Your Certificate for Backup or Distribution” on page 11-40.

3. When you finish viewing the certificate information, click Close to return to the Certificate Profile window.

# Viewing the Certificate Path

Use this procedure to view information about a certificate’s chain of trust. You also can export a certificate or its trusted roots to a file.

This procedure uses the Certificate Profile window. See “Certificate Profile Window” on page 11-45 for details about the window.

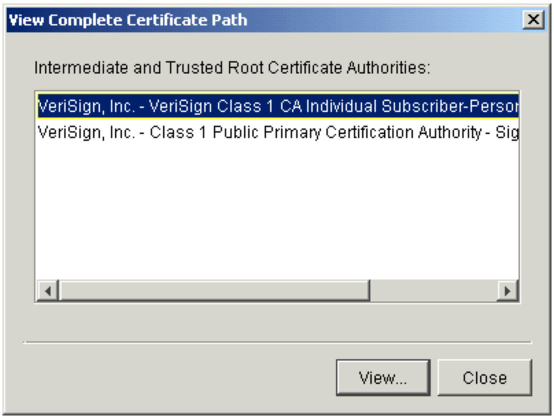
A chain of trust or certificate chain is an ordered list of certificates that includes the certificate of the end-user and certificates of the issuing CA. A trusted root is a public key that is verified as belonging to an issuing CA, which is called a trusted third party.

## Steps

1. At the Certificates information viewer, select the name of the company or partner with the certificates you want. Click Open to open the Certificate Profile window with the Available Certificates tab selected.

2. Select the certificate you want to view and click View Cert Path to open the View Complete Certificate Path window.

**Figure 11-26 View Complete Certificate Path Window**



View Complete Certificate Path

Intermediate and Trusted Root Certificate Authorities:

VeriSign, Inc. - VeriSign Class 1 CA Individual Subscriber-Persor
VeriSign, Inc. - Class 1 Public Primary Certification Authority - Sig

3. To view details about a certificate in the chain, select the certificate and click View to open the Certificate window. See "Certificate Window" on page 11-20 for a description of the fields.

4. To export a certificate in the chain, click Export on the Certificate window to display the Export Certificate window. You have the option to export a certificate file with an extension of `.cer` or `.p7c`. For procedure see "Exporting Your Certificate for Backup or Distribution" on page 11-40.

5. Click Close to return to the Certificate Profile window.

# Activating a Pending or Valid Certificate

Use this procedure to change the status of pending or valid certificates to active. A profile can have many certificates, but only one active certificate at a time. The active certificate is the one used for document trading.

This procedure uses the Certificate Profile window. See "Certificate Profile Window" on page 11-45 for details about the window.

## Steps

1. At the Certificates information viewer, select the name of the company or partner with the certificates you want. Click Open to open the Certificate Profile window with the Available Certificates tab selected.
2. Select the certificate with the pending or valid status that you want to set as the active certificate and click Set As Active. A dialog box appears asking you to confirm that you want to activate the certificate.
3. Click Yes to activate the certificate or No to cancel the activation. If you click Yes, the Available Certificates tab shows the status of the certificate as active. If there was an existing active certificate, its status is changed to valid.

   **Note:** WebLogic Integration – Business Connect does not automatically distribute the certificate to your trading partners. You must use some method to distribute the certificate.

# Retiring a Certificate

Use this procedure to retire a certificate. This procedure uses the Certificate Profile window and is one way to retire or delete a certificate. For details about inactivating certificates see "Deleting Certificates" on page 11-43.

For the steps to reactivate a certificate, see "Un-Retiring Certificate" on page 11-50.

See "Certificate Profile Window" on page 11-45 for details about the window.

1. At the Certificates information viewer, select the name of the company or partner with the certificates you want. Click Open to open the Certificate Profile window with the Available Certificates tab selected.
2. Select the certificate to retire and click Retire.
3. Click Yes to confirm you want to retire the certificate.

# Un-Retiring Certificate

Use this procedure to change the status of a retired certificate to valid or active.

As explained in "Deleting Certificates" on page 11-43, certificates you have retired from use are maintained in the system in a dormant state in the event they are needed again. When you un-retire a certificate, its status changes to valid and it appears once more on the Certificates information viewer. After changing the status to valid, you can make the certificate active if you want.

This procedure uses the Certificate Profile window. See "Certificate Profile Window" on page 11-45 for details about the window.

## Steps

1. At the Certificates information viewer, select the name of the company or partner with the certificates you want. Click Open to open the Certificate Profile window with the Available Certificates tab selected.

2. Select the Retired Certificates tab to view a list of the retired certificates, if any, associated with the profile.

3. Select the certificate you want to bring out of retirement and click Un-retire. A dialog box opens with a message asking whether you want to bring the certificate out of retirement.

4. Click Yes to un-retire the certificate or No to cancel the operation.

   If you click Yes, the certificate disappears from the Retired Certificates tab. The certificate status changes from retired to valid. The certificate now appears on the Available Certificates tab and the Certificates information viewer.

5. To change the status of the un-retired certificate from valid to active, see "Activating a Pending or Valid Certificate" on page 11-48.

# Trusted Roots

Trusted roots are the foundation upon which chains of trust are built in certificates. Underlying a certificate issued by a certificate authority is a root, self-signed certificate. In WebLogic Integration – Business Connect trusting a CA root means you trust all certificates issued by that CA. Conversely, if you elect not to trust a CA root, WebLogic Integration – Business Connect will not trust any certificates issued by that CA. Document trading fails in WebLogic Integration – Business Connect when a non-trusted certificate is used.

The self-signed certificates you can generate in WebLogic Integration – Business Connect are root certificates. This is because you are, in effect, your own CA when you generate a self-signed certificate.

WebLogic Integration – Business Connect by default trusts your and your partners' self-signed certificates that were generated by WebLogic Integration – Business Connect. WebLogic Integration – Business Connect also by default trusts the roots of many CA-issued certificates. You can, however, specify whether WebLogic Integration – Business Connect should not trust all or some certificates issued by a specific CA. You also can explicitly not trust a partner's self-signed certificate.

The Trusted Roots window displays trusted roots for various certificate authorities. It also displays the self-signed certificates of your partners and the certificates used by the WebLogic Integration – Business Connect SOAP-RPC HTTPS server and API HTTPS server (see Chapter 14, "Application Security").

Importing a trusted root is a task that rarely, if ever, must be performed. You might have to import a trusted root if, for example, your partner sends you a CA-issued certificate and your system does not have the trusted root for it. In such a case, document trading would fail. As a solution, you would need to import the root underlying the certificate and trust it.

WebLogic Integration – Business Connect can import trusted roots contained in files with the following extensions: `.cer`, `.p7c` and `.p7b`. There are various ways you can obtain such trusted root files:

- You can use WebLogic Integration – Business Connect to export a certificate file with an extension of `.p7c`. See "Viewing the Certificate Path" on page 11-47.
- You can check whether trusted root files are available for download on the web site of the public CA that issued the certificate.

- If the certificate was issued by an in-house CA such as Entrust, you can ask the CA administrator for a trusted root file.
- If the certificate is present in a browser, you can use the application's trusted roots option to export the trusted root to a file.

When you import a trusted root for a certificate to WebLogic Integration – Business Connect, we recommend that you compare the MD5 fingerprints in both the trusted root and the certificate to verify that they match.

# Viewing, Editing or Importing Trusted Roots

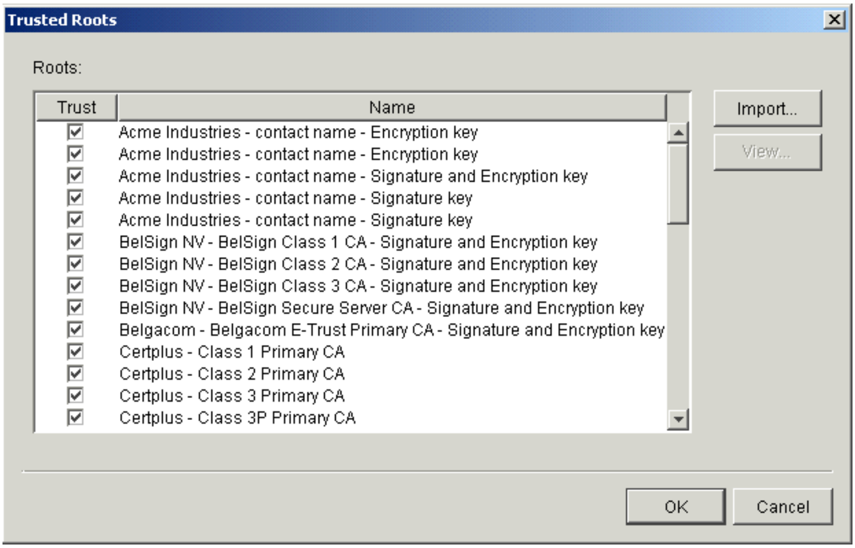
Use this procedure to specify whether to trust roots, view root details or import trusted roots. For details about trusted roots, see “Trusted Roots” on page 11-51.

## Steps

1. In Administrator select Tools→Certificates→Trusted Roots to open the Trusted Roots window. The window displays a list of CA roots and self-signed certificates your partners have sent you.

   Self-signed certificates that you have generated in WebLogic Integration – Business Connect for document trading do not display on the window. This is because you must trust your own self-signed certificates created for document trading; you cannot elect not to trust them. However, the self-signed certificates for the SOAP-RPC HTTPS server and API HTTPS server are listed on the window and are trusted by default. See “Certificate Tool (certloader)” on page 14-14.

**Figure 11-27 Trusted Roots Window**



Trusted Roots

Roots:

| Trust | Name |
|---|---|
| ☑ | Acme Industries - contact name - Encryption key |
| ☑ | Acme Industries - contact name - Encryption key |
| ☑ | Acme Industries - contact name - Signature and Encryption key |
| ☑ | Acme Industries - contact name - Signature key |
| ☑ | Acme Industries - contact name - Signature key |
| ☑ | BelSign NV - BelSign Class 1 CA - Signature and Encryption key |
| ☑ | BelSign NV - BelSign Class 2 CA - Signature and Encryption key |
| ☑ | BelSign NV - BelSign Class 3 CA - Signature and Encryption key |
| ☑ | BelSign NV - BelSign Secure Server CA - Signature and Encryption key |
| ☑ | Belgacom - Belgacom E-Trust Primary CA - Signature and Encryption key |
| ☑ | Certplus - Class 1 Primary CA |
| ☑ | Certplus - Class 2 Primary CA |
| ☑ | Certplus - Class 3 Primary CA |
| ☑ | Certplus - Class 3P Primary CA |

2. Check or clear the trust check boxes to indicate whether to trust certain CA roots or self-signed certificates.

   There are multiple lines for each CA because each has multiple roots, each with unique fingerprints under which it issues certificates.

3. To view the fingerprints, select a root and click View to open the Certificate window. By comparing fingerprints you can choose to trust or not trust some but not all of a CA's certificates. See "Certificate Window" on page 11-20 for a description of the fields on the window.

4. To import a trusted root, click Import on the Trusted Roots window to open the Import Certificate dialog box. Select the certificate file to import and click Open. You can import a file with an extension of `.cer`, `.p7c` or `.p7b`.

5. Click OK to save your changes and close the Trusted Roots window or Cancel to cancel the operation and close the window.

# Using Certificate Revocation Lists

Use this procedure to configure WebLogic Integration – Business Connect to compare your partners' certificates against lists of invalid certificates that are maintained by the issuing certificate authorities.

A certificate revocation list (CRL) is a list of third-party certificates that are no longer valid. Certificate authorities maintain such lists of certificates they issued, but later invalidated for one reason or another. CRLs are accessible on the Internet, and you need an Internet connection for WebLogic Integration – Business Connect to use them.

WebLogic Integration – Business Connect enables you to check your partners' certificates against CRLs. When you direct WebLogic Integration – Business Connect to use CRLs, your partners' certificates are checked each time documents are exchanged. For example, when a partner sends you an encrypted document, WebLogic Integration – Business Connect checks the certificate associated with the inbound document against the CRL. If the certificate is on the CRL, WebLogic Integration – Business Connect rejects the inbound document.

Although using CRLs can enhance security, the checking process can result in longer processing times. Consequently, your decision whether to use CRLs should weigh the security advantage against the performance handicap.

You can configure WebLogic Integration – Business Connect to check certificates against the CRLs of one or more certificate authorities. However, WebLogic Integration – Business Connect checks a specific certificate only against the appropriate CRL. For example, if you configure WebLogic Integration – Business Connect to use CRLs maintained by VeriSign, Inc. and GlobalSign and an inbound document is associated with a VeriSign certificate, the system checks only against the VeriSign CRL and not the GlobalSign CRL.

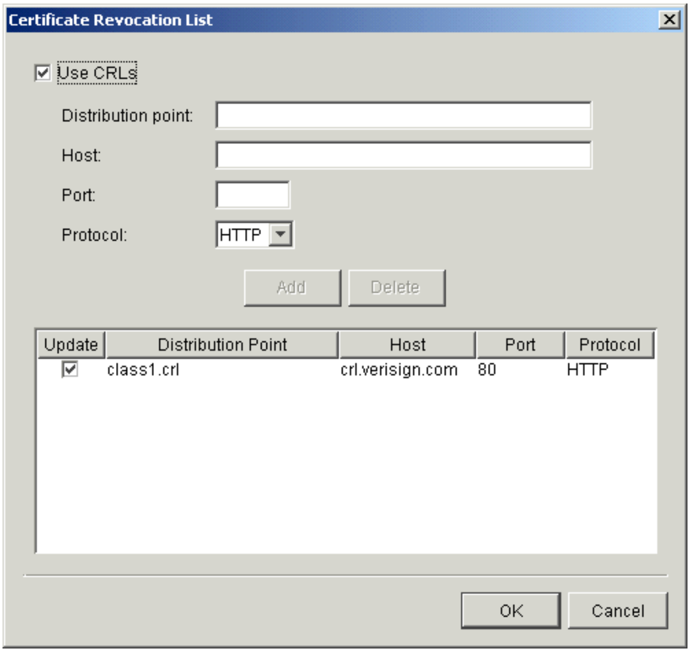
You are responsible for obtaining from the certificate authority the information required for accessing the CRL. WebLogic Integration – Business Connect downloads the latest CRL in performing certificate checks. It also downloads updates of the CRL, based on the update interval in the previously downloaded CRL.

# Steps

1. In Administrator, select Tools→Certificates→Cert. Revocation List to open the Certificate Revocation List window. Go to one of the following:

   - "Adding CRLs" on page 11-56
   - "Deleting CRLs" on page 11-57
   - "Turning CRL Checking On and Off" on page 11-58

**Figure 11-28 Certificate Revocation List Window**



☑ Use CRLs

Distribution point:

Host:

Port:

Protocol: HTTP

| Update | Distribution Point | Host | Port | Protocol |
|---|---|---|---|---|
| ☑ | class1.crl | crl.verisign.com | 80 | HTTP |

# Adding CRLs

Do the following on the Certificate Revocation List window to configure WebLogic Integration – Business Connect to use one or more CRLs.

1. Select the Use CRLs check box.

2. Obtain the information required to access the CA's CRL. This includes the CRL distribution point, the host name, port number and the TCP/IP protocol. Type the CRL access information in the appropriate fields.

   The protocols are hypertext transfer protocol (HTTP) and lightweight directory access protocol (LDAP). For example, VeriSign CRLs are accessed via HTTP and Entrust CRLs are accessed via LDAP.

   You can obtain the CRL information by viewing the details of a CA-issued certificate. See "Certificate Window" on page 11-20. The information, if present, is in the extensions section and is labeled as CRL distribution point.

   As an example, the following is the CRL distribution point within a VeriSign certificate. This is a URL as follows:

   ```
   http://crl.verisign.com/class1.crl
   ```

   This URL corresponds to the fields on the Certificate Revocation List window as described in the following table.

   **Table 11-4 URL Components**

   | | |
   |---|---|
   | `http:` | Select http from the protocol drop-down list. |
   | `[port number]` | When a port number does not follow http:, the port number is 80 for HTTP only. Type `80` in the port field. If the port is other than `80`, the URL will specify the port number. |
   | `crl.verisign.com` | This is the value for the host field. |
   | `class1.crl` | This is the value for the distribution point field. |

3. Click Add to add to the CRL and display it on the window. By default the Update check box next to the new CRL is selected. The Update check box must be selected for WebLogic Integration – Business Connect to initially download and subsequently perform update downloads of the CRL.

4. Repeat the previous steps to add another CRL.
5. Click OK to complete the configuration.

   After you add one or more CRLs and if the Server application is running, the system downloads the CRLs into the crls directory under the WebLogic Integration – Business Connect installation directory. There might be a delay of up to one hour before Server downloads a CRL the first time. This is because the application polls for new CRLs once an hour.

   Each CRL contains a refresh date that indicates when the CA updates the list. WebLogic Integration – Business Connect downloads the updated CRL after each refresh date, provided the Update check box next to the CRL is selected.

   The Update check boxes next to the CRLs tell WebLogic Integration – Business Connect whether to monitor the refresh dates within the CRLs and download updated CRLs from CAs at the appropriate times. When the Update check boxes are selected, WebLogic Integration – Business Connect downloads the latest available CRLs.

## Deleting CRLs

Do the following on the Certificate Revocation List window to delete CRLs.

1. Make sure the Use CRLs check box is selected.
2. Select the CRL you want to delete and click Delete. Repeat to delete another CRL.
3. Click OK for the deletions to become effective.

# Turning CRL Checking On and Off

Do the following on the Certificate Revocation List window to turn CRL checking on and off.

1. If you want WebLogic Integration – Business Connect to check your partners' certificates against CRLs, select the Use CRLs check box. If you want to turn off CRL checking, clear the Use CRLs check box.

   The Use CRLs check box controls whether all CRL checking is turned on or off. You cannot turn on or off checking for a particular CRL by selecting or clearing the Update check box next to a CRL.

2. Click OK for the selection to become effective.

CHAPTER

# 12 Partner Profiles

The following topics are provided for using the Partner Profile information viewer for setting up and maintaining partner profiles.

**Concepts**

- “Firewall Details” on page 12-36

**Procedures**

- “Importing a Profile from a Partner Who Uses WebLogic Integration” on page 12-2
- “Adding or Changing a Partner Profile” on page 12-5
- “Selecting an Active Outbound Protocol” on page 12-21
- “Adding an Outbound Protocol” on page 12-22
- “Editing an Outbound Protocol” on page 12-23
- “Removing an Outbound Protocol” on page 12-24
- “Delete a Partner Profile” on page 12-49

**Windows**

- “Partner Profile Identity Tab” on page 12-8
- “Partner Profile Preferences Tab” on page 12-14
- “Partner Profile Outbound Protocol Tab” on page 12-19
- “Partner Profile Firewall Tab” on page 12-31
- “Partner Profile Security Tab” on page 12-43
- “Partner Profile Binary Directories Tab” on page 12-46

# Importing a Profile from a Partner Who Uses WebLogic Integration

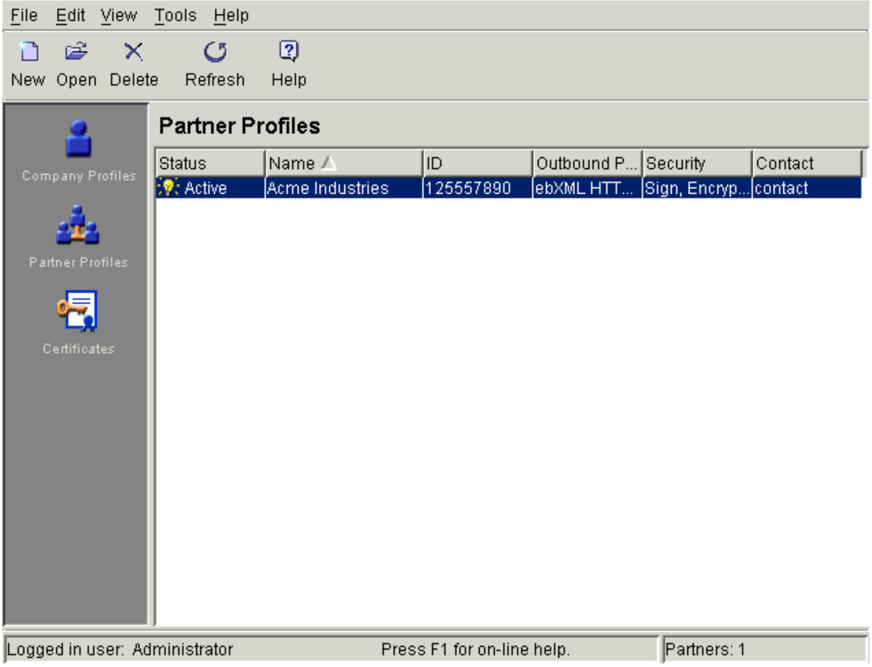
Use this procedure to import a company profile file that was sent to you by a trading partner who also uses WebLogic Integration. When imported, the profile, which contains your partner's identity and transport information, becomes a partner profile on your system.

Importing a profile from a partner who uses WebLogic Integration is a simple direct method of adding a new partner profile to your system. You must manually create partner profiles for your partners who use a trading engine other than WebLogic Integration. See "Adding or Changing a Partner Profile" on page 12-5.

## Steps

1. Have your trading partner send you by secure means the XML company profile file your partner created in WebLogic Integration.
2. Click Partner Profiles on the Administrator bar to open the Partner Profiles information viewer. The window displays any partner profiles added earlier.

**Figure 12-1 Partner Profiles Information Viewer**



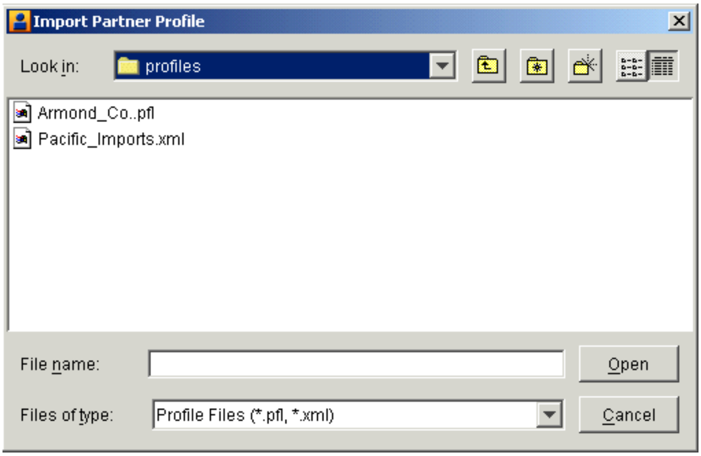
Partner Profiles

| Status | Name | ID | Outbound P... | Security | Contact |
|---|---|---|---|---|---|
| Active | Acme Industries | 125557890 | ebXML HTT... | Sign, Encryp... | contact |

Logged in user: Administrator Press F1 for on-line help. Partners: 1

3. Select File→Import to open the Import Partner Profile dialog box.

**Figure 12-2 Import Partner Profile Dialog Box**



Look in: profiles

Armond_Co..pfl
Pacific_Imports.xml

File name:

Files of type: Profile Files (*.pfl, *.xml)

4. Find and select the partner profile file you want to import and click Open. The file is located on your floppy disk drive or wherever your e-mail attachments are stored.

   Partner profiles files are relatively small in size. The files are in the format `*ProfileName*.pfl` or `*ProfileName*.xml`.

   **Note:** Partner profile generated in WebLogic Integration are XML files.

   If you are importing a profile for a partner already on your system, you are asked to confirm that you want the imported data to overwrite the existing data.

   If the profile includes more than one configured transport, the system reminds you to choose one active transport for the partner. Click OK to open the Partner Profile window Outbound Protocol tab. Select a configured transport as the active transport. See “Partner Profile Outbound Protocol Tab” on page 12-19.

   You can import a profile that has incomplete information for one or more outbound transports. If you import a profile with a single outbound transport and the configuration information for the transport is incomplete, the system displays a message informing you of the missing information. If you import a profile with two or more outbound transports, however, the system does not display a message if one or more of the transports is incompletely configured. Instead, the system opens the Partner Profile window Outbound Protocol tab for you to select the transport. Incompletely configured transports appear in red in the configured protocols area of the tab. Contact your partner to obtain the missing information or have your partner resend the profile.

5. Select the Security tab and review the settings. To successfully exchange documents, you must coordinate with your trading partner to confirm that both of you have made identical security selections.

   Make sure that your partner’s profile on your system and your profile on your partner’s system have identical settings. For more information see “Partner Profile Security Tab” on page 12-43.

6. If you intend to exchange binary documents with this partner, select the Binary Directories tab.

   Select your company profile from the Companies drop-down list and click Add. The application sets up default paths names for the binary-in and binary-out directories. You can change these paths by clicking on the directories and typing your changes.

These are the directories WebLogic Integration – Business Connect polls for binary (non-EDI) documents. You create unique binary-in and binary-out directories for each partner so the system knows the addressee for the outbound documents and can store inbound documents in partner-specific directories. For more information see “Partner Profile Binary Directories Tab” on page 12-46.

7. Click OK to save and close the profile.
8. If you are exchanging signed and encrypted data, open the Certificates information viewer and ensure that an active certificate exists for this partner profile. For more information see “Certificate Window” on page 11-20.

# Adding or Changing a Partner Profile

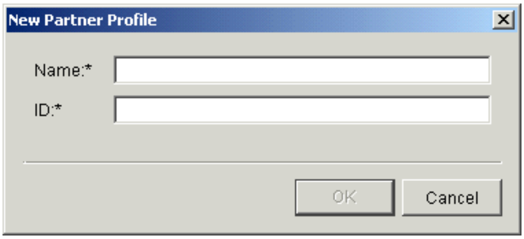
Use this procedure to add a new partner profile when you cannot import a partner’s profile file. You also can change an existing profile.

Before you create a partner profile, consult with your partner on the ID to use and other details involving the outbound transport and firewall and security issues.

## Steps

1. Click Partner Profiles on the Administrator bar to open the Partner Profiles information viewer. The window displays any partner profiles added earlier.
2. To add a new partner profile, click New to open the New Partner Profile dialog box.

**Figure 12-3 New Partner Profile Dialog Box**



3. Complete the following fields.

   - *Name*
     Type the profile name in this required field. You can edit this name after you have added and saved a profile. You can use any alphanumeric characters and the following characters: back slash (\), hyphen (-), forward slash (/), colon (:), underscore (_), comma (,), period (.). You can use spaces in your name; WebLogic Integration – Business Connect translates them to underscores. WebLogic Integration – Business Connect removes any other characters.

   - *ID*
     Type an identification for the profile. You cannot change the ID after you have created a profile.

     You can use alphanumeric and non-alphanumeric characters as well as spaces in profile IDs. All alphanumeric characters are supported. Use of specific non-alphanumeric characters is supported, but results in the system creating names of data directories and processed files that use hex codes in place of the characters. Spaces in IDs are allowed within limitations. You also can create an ID in an electronic data interchange (EDI) format. For details see "Supported Formats for Profile IDs" on page 9-5.

     The system displays an error message if you try to create an ID with an unsupported format.

4. Click OK to open the Partner Profile window Identity tab.

5. Add information on the Partner Profile window tabs. You can complete a new profile by choosing the tabs in any order you want.

   See the following topics for information about adding or changing information on the tabs:

**Table 12-1 Adding or Changing Partner Profile Information**

| If you want to . . . | See . . . |
|---|---|
| Review or change partner name and location data and secondary IDs. | "Partner Profile Identity Tab" on page 12-8 |
| Add or change partner preferences for document handling and processing for a partner profile. | "Partner Profile Preferences Tab" on page 12-14 |
| Select, add or change the protocol and transport for sending documents to a partner. | "Partner Profile Outbound Protocol Tab" on page 12-19 |
| Set the parameters WebLogic Integration – Business Connect uses to exchange data through a partner's firewall. | "Partner Profile Firewall Tab" on page 12-31 |
| Select or change the security settings for a partner profile. These are the parameters WebLogic Integration – Business Connect uses to sign, encrypt and acknowledge receipt of documents you send to a partner. | "Partner Profile Security Tab" on page 12-43 |
| Set up partner-specific inbound and outbound directories for sending and receiving binary documents. | "Partner Profile Binary Directories Tab" on page 12-46 |

6. Click OK to save the new partner profile or Cancel to close without adding the profile.

7. If you exchange encrypted or signed documents, you must import this partner's certificate in your Certificates information viewer. You should also confirm with your partner that the fingerprints in both certificates are identical.

# Partner Profile Identity Tab

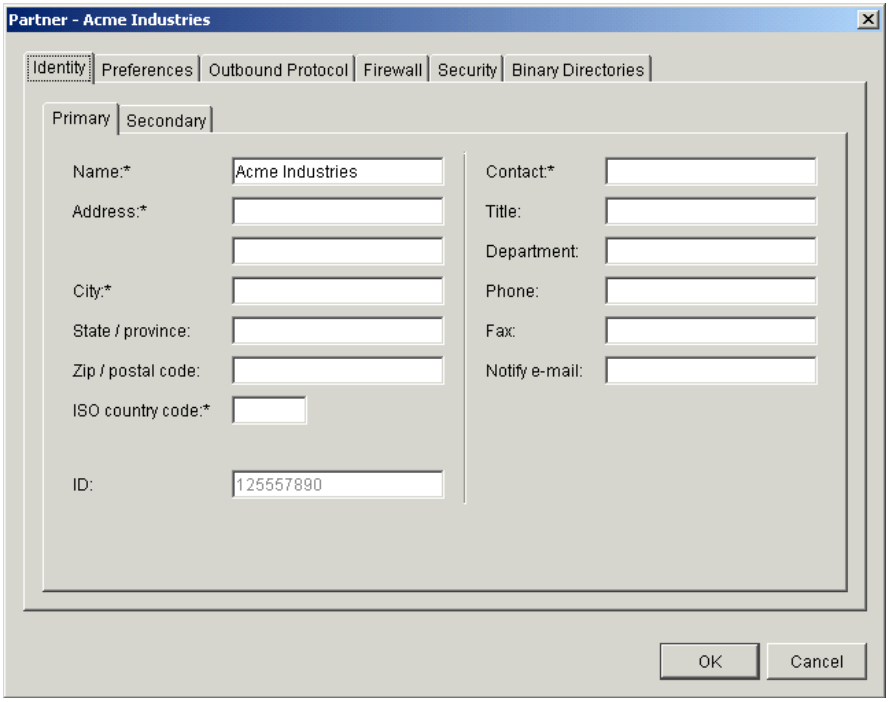
Use the Partner Profile window Identity tab to review or change partner name and location data and secondary IDs. The tab has two parts:

- "Identity, Primary Tab"
- "Identity, Secondary Tab" on page 12-12

## Identity, Primary Tab

Use the Partner Profile window Identity, Primary tab to view or change the name, location and contact information about your partner. You also can view the profile ID, but you cannot change it.

**Figure 12-4 Partner Profile Identity, Primary Tab**



Name:* Acme Industries

ID: 125557890

## Field Descriptions

The following describes the fields on the Partner Profile window Identity, Primary tab. For procedure see “Adding or Changing a Partner Profile” on page 12-5 or “Importing a Profile from a Partner Who Uses WebLogic Integration” on page 12-2.

*Name*

This field contains the company name of the trading partner. You can edit this name after you have added and saved a profile. You can use any alphanumeric characters and the following characters: back slash (\), forward slash (/), colon (:), underscore (_), comma (,), period (.). You can use spaces in your name; the system translates them to underscores. The system removes any other characters.

*Address*

If you imported this profile, this field contains the trading partner's street address. If you are manually adding this profile, type the trading partner's street address. The first line of the address is required. The second line is optional.

*City*

If you imported this profile, this field contains the city where the trading partner is located. If you are manually adding this profile, type your trading partner's city. This field is required.

*State/province*

If you imported this profile, this field contains the name of the state or province where the trading partner is located. If you are manually adding this profile, type the state or province where the trading partner is located.

*Zip/postal code*

If you imported this profile, this field contains the trading partner's zip or postal code. If you are manually adding this profile, type the trading partner's zip or postal code.

*ISO country code*

If you imported this profile, this field contains the partner's two-letter ISO country code. If you are manually adding this profile, type the partner's country code; `us` is United States. The following are the ISO codes for selected countries. See Appendix A, "ISO Country Codes," for a complete list of the codes.

**Table 12-2 Selected ISO Country Codes**

| Code | Country |
|---|---|
| ca | Canada |
| cn | China |
| fr | France |
| de | Germany |
| gb | Great Britain |
| it | Italy |
| jp | Japan |

**Table 12-2 Selected ISO Country Codes (Continued)**

| Code | Country |
|---|---|
| mx | Mexico |
| tw | Taiwan |

*ID*

The ID for this trading partner. You cannot edit this field.

*Contact*

If you imported this profile, this field contains the name of the trading partner's contact person. If you are manually adding this profile, type the name of the trading partner's contact person.

*Title*

If you imported this profile, this field contains the job title of the trading partner's contact person. If you are manually adding this profile, type the title of the trading partner's contact person.

*Department*

If you imported this profile, this field contains the department where the trading partner's contact person works. If you are manually adding this profile, type the name of the department where the trading partner's contact person works.

*Phone*

If you imported this profile, this field contains the phone number for the trading partner's contact person. If you are manually adding this profile, type the phone number of the trading partner's contact person.

*Fax*

If you imported this profile, this field contains the fax number for the trading partner's contact person. If you are manually adding this profile, type the fax number of the trading partner's contact person.

*Notify e-mail*

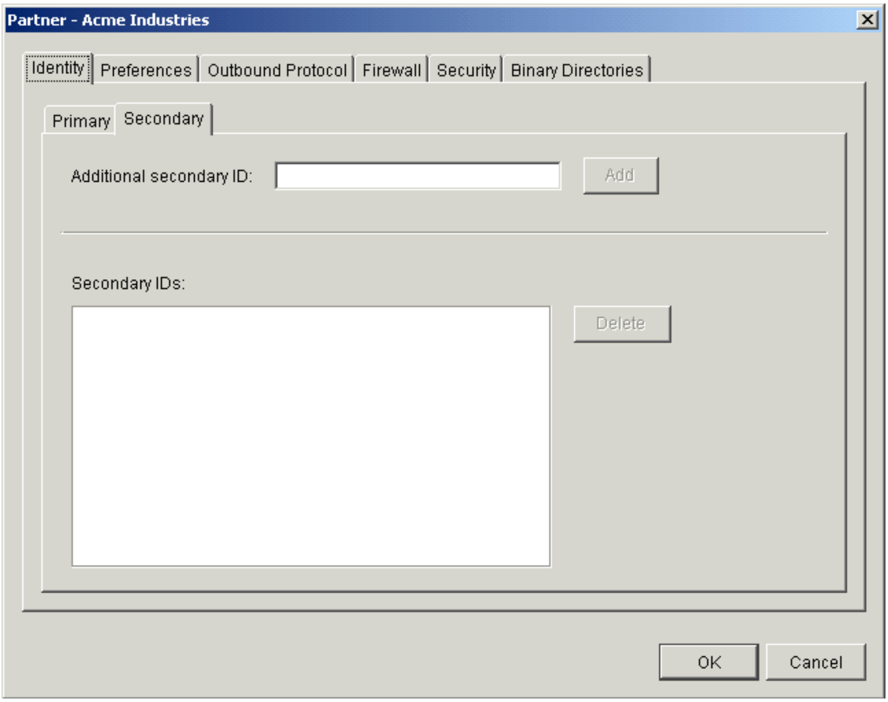
If you imported this profile, this field contains the e-mail address where your partner receives notifications from you. When an error occurs that concerns traffic with this partner, you and your partner receive the notification message. If you are adding this profile manually, type the e-mail address of the trading partner's contact person. This address cannot be the same as the one you enter in the e-mail address field on the outbound transport SMTP Transport Options window or POP Transport Options window.

# Identity, Secondary Tab

Use the Partner Profile window Identity, Secondary tab to add or change secondary IDs for partners.

You can use secondary IDs to designate partners other than the current partner as the ultimate intended recipients of documents. Your current partner receives your document and routes it to the partner designated by the secondary ID. Using a secondary ID is useful when trading in a service provider environment. You can send EDI, XML and binary documents to a partner by routing them through a service provider.

**Figure 12-5 Partner Profile Identity, Secondary Tab**



## Field Descriptions

The following describes the fields on the Partner Profile window Identity, Secondary tab. For procedure see "Adding or Changing a Partner Profile" on page 12-5 or "Importing a Profile from a Partner Who Uses WebLogic Integration" on page 12-2.

*Additional secondary ID*

Type the secondary partner's ID. Do not enter the ID of a partner that already exists on your system or an ID that is already a secondary ID in another partner profile on your system. Secondary IDs are case sensitive; type IDs precisely.

**Note:** WebLogic Integration – Business Connect rejects outbound documents without valid IDs. However, you can force the application to send such documents by using the wildcard character * (asterisk) as a secondary ID for the intermediary partner to whom you want such documents directed. This works for EDI and XML documents, but not binary documents. The wildcard secondary ID forces WebLogic Integration – Business Connect to process outbound documents it otherwise would reject.

Click Add. Repeat this step to add another secondary ID or click OK to save and close the profile.

*Secondary IDs*

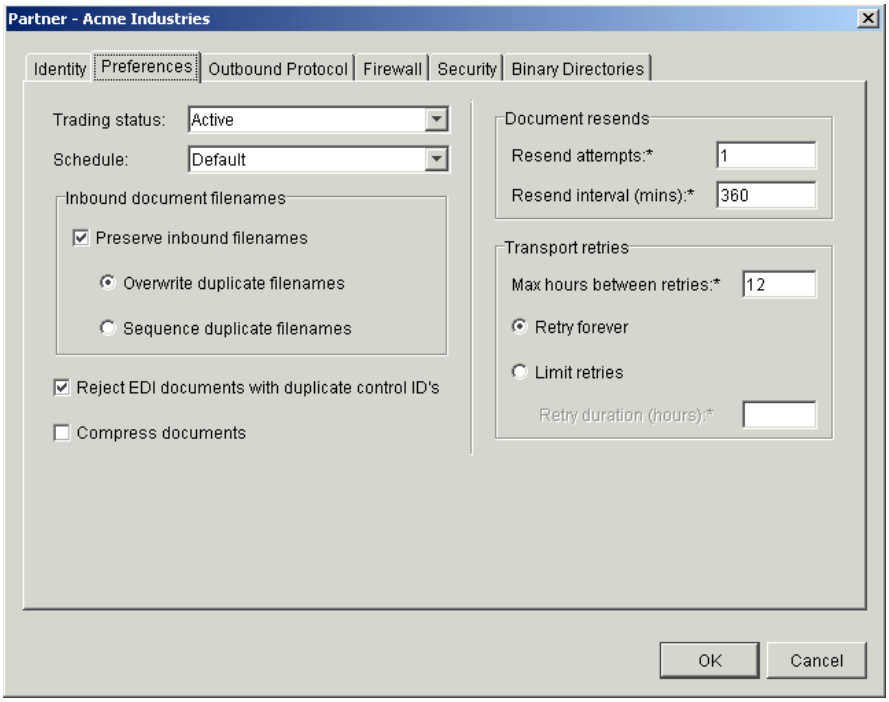
This window displays the secondary IDs associated with the partner profile.

To delete a secondary ID, select the ID you want to delete and click Delete. Repeat this step to delete another secondary ID or click OK to save and close the profile.

# Partner Profile Preferences Tab

Use the Partner Profile window Preferences tab to add or change partner preferences for document handling and processing for a partner profile.

**Figure 12-6 Partner Profile Preferences Tab**



Trading status: Active

Schedule: Default

Inbound document filenames

☑ Preserve inbound filenames

● Overwrite duplicate filenames

○ Sequence duplicate filenames

☑ Reject EDI documents with duplicate control ID's

□ Compress documents

Document resends

Resend attempts:* 1

Resend interval (mins):* 360

Transport retries

Max hours between retries:* 12

● Retry forever

○ Limit retries

Retry duration (hours):*

# Field Descriptions

The following describes the fields on the Partner Profile window Preferences tab. For procedure see “Adding or Changing a Partner Profile” on page 12-5 or “Importing a Profile from a Partner Who Uses WebLogic Integration” on page 12-2.

*Trading status*

Select Active from the drop-down list to indicate that the system is to process transactions to and from this trading partner. This is the default.

Select Inactive to indicate that the system is not to process transactions to and from this trading partner. Any attempt to exchange documents with this partner generates an alert.

**Note:** You can quickly change the trading status by right-clicking the partner profile in the Partner Profiles information viewer and then left-clicking Change Status in the pop-up menu that appears.

*Schedule*

Select from the drop-down list the document send schedule you want to use with this partner profile. WebLogic Integration – Business Connect must use the default schedule.

*Inbound document filenames*

The following fields control file names of inbound documents from this partner.

*Preserve inbound file names*

Select this check box to have the system write inbound documents to the binary-in, EDI-in or XML-in directory using the documents' original file names assigned by the remote partner. This is the default.

Clear this check box to have WebLogic Integration – Business Connect write inbound documents to the binary-in, EDI-in or XML-in directory using unique names.

If you clear this option, WebLogic Integration – Business Connect, upon receiving a binary document, assigns it a unique file name that does not provide any clues as to the content. It is recommended, therefore, that you accept the default option to have WebLogic Integration – Business Connect preserve inbound file names. This allows you to identify the documents more easily. It also allows your business application to process inbound binary documents based on their file names.

*Overwrite duplicate filenames*

If you select preserve inbound file names, select this radio button to have WebLogic Integration – Business Connect overwrite the first file if it later receives a document with the same name. This is the default.

*Sequence duplicate filenames*

If you select preserve inbound file names, select this radio button to have WebLogic Integration – Business Connect sequence the names of files it later receives that have the same name rather than overwriting the files.

*Reject EDI documents with duplicate control IDs*

Select this check box to have WebLogic Integration – Business Connect place inbound EDI documents with duplicate transaction control numbers in the rejected directory. This is the default.

Clear the check box to indicate that WebLogic Integration – Business Connect is to place all inbound EDI documents in the EDI-in directory without checking for possible duplicate transaction control numbers. You might choose this option if your translator performs the duplicate-checking function.

*Compress documents*

Select this check box to have WebLogic Integration – Business Connect compress the documents you transmit. The application uses GZIP to compress documents.

Compressing data before sending it enables you to increase your document throughput. You can use compression if:

* Your partner uses WebLogic Integration – Business Connect, which can uncompress the document as part of normal processing. You and your partner can choose compression independent of one another.

* Your partner uses an Internet document exchange software product that supports GZIP compression.

* Your partner agrees to compress and uncompress the documents as pre- and post-processing steps.

Clear this check box to send documents uncompressed. This is the default.

*Document resends*

The following fields control how the system will attempt to resend documents following failed attempts.

*Resend attempts*

Type the number of times you want WebLogic Integration – Business Connect to resend a document for which it does not receive an expected acknowledgment. After the specified number of retries have failed, WebLogic Integration – Business Connect sends you an alert. The default is 1 time. Increasing this number increases the risk of swamping your trading partner with re-sent documents.

This option applies only if you also select the request acknowledgment of documents check box in the Partner Profile window Security tab.

*Resend interval (mins)*

Type the number of minutes WebLogic Integration – Business Connect is to wait before it tries to re-send a document. The range is from 1 to 9999 minutes. The default is 360 minutes.

You can shorten or lengthen this period for each partner based on such factors as distance, time of day, known partner system down times and historical patterns. Shortening this interval increases the risk of swamping your trading partner with re-sent documents.

*Transport retries*

The following fields control the system's persistence in trying again to send documents in the event of a transport failure.

*Max hours between retries*

Type a number for the longest interval in hours between attempts to re-send a packaged document that did not send because of a transport failure. The default is 12 hours, which also is the highest allowed value. This is the maximum hours between re-send attempts, which is an interval the system can reach only after many retries. Attempts to re-send outbound documents is based on a fall-off algorithm. This is how it works:

When a document fails to send the first time, the document enters a wait state of 10 seconds, after which the system tries again to send the document. If it fails again, the wait state doubles to 20 seconds, then doubles again 40 seconds, then doubles again to 80 seconds, and so on until it doubles to the number of hours in this field. When the longest retry interval is reached, the system keeps trying each time the interval elapses, limited only by whether you have selected retry forever or limit retries.

The wait state resets to zero when the partner profile is updated. This is because the update might resolve the connection problem. However, the fall-off algorithm restarts if the transport failure persists.

This field does not apply to transport failures for inbound documents. That also is based on a fall-off algorithm, but uses a doubling factor in conjunction with the inbound polling rate that plateaus at 12 hours. For details see "Inbound Fall-Off Algorithm" on page 9-4.

*Retry forever*

Select this radio button for the system to keep re-trying without limit to resend documents to a partner. This is the default setting. It is strongly recommended that you use this setting unless you have a special situation or on the advice of technical support.

*Limit retries*

Select this radio button to limit retries for the maximum hours you type in the retry duration field.

*Retry duration (hours)*

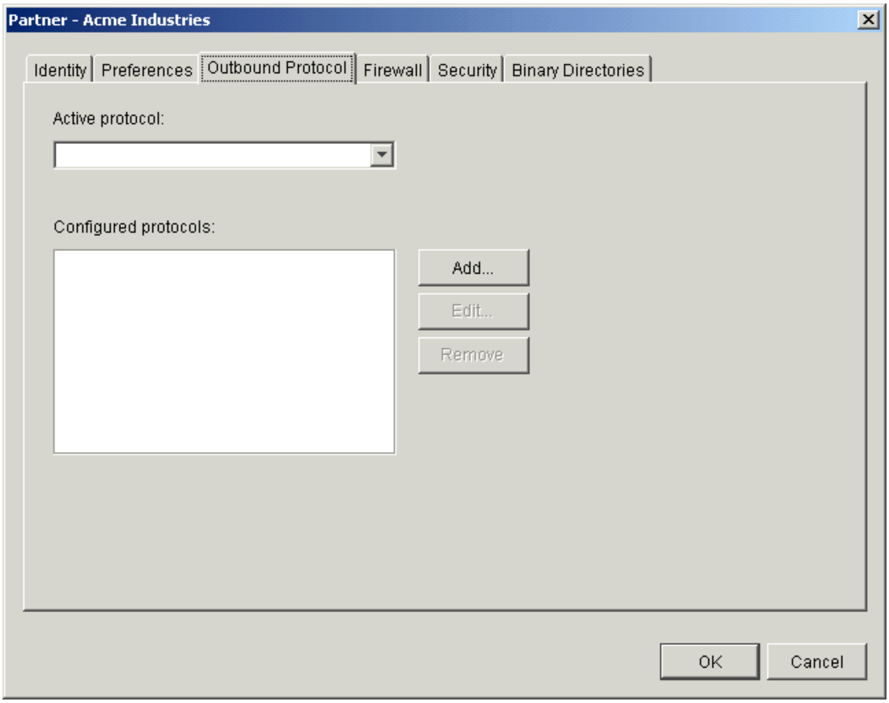
If you select limit retries, type the number of hours after which the system will stop re-trying to send documents. You can use numbers between 0 and 60.

# Partner Profile Outbound Protocol Tab

Use the Partner Profile window Outbound Protocol tab to select, add or change the protocol and transport for sending documents to a partner. A profile must have at least one fully configured protocol and transport.

If you import a partner profile, your partner might have configured two or more transport methods for a single protocol. However, you can choose only one active transport in the partner profile. It is recommended that you consult with your partners about preferred transports.

**Figure 12-7 Outbound Protocol Tab**



Partner - Acme Industries

Active protocol:

Configured protocols:

If you imported a profile from a user of WebLogic Integration – Business Connect, it should contain information about the protocol and transport methods your partner wants you to use for sending documents. If not, you must complete the fields yourself for the protocol and transport, based on information your partner provides.

For a list of supported protocols and transports, see "Supported Protocols and Transports" on page 9-28.

The Outbound Protocol tab allows you to change a partner profile in the following ways:

- Select a configured protocol and transport combination as the active method for sending documents to partners.
- Add a transport that you can use to send documents to a partner.
- Edit the settings for a configured protocol and transport combination.
- Remove a protocol and transport combination from the list of configured protocols for the profile.

The following topics explain each of these functions in detail:

- "Selecting an Active Outbound Protocol"
- "Adding an Outbound Protocol" on page 12-22
- "Editing an Outbound Protocol" on page 12-23
- "Removing an Outbound Protocol" on page 12-24

## Selecting an Active Outbound Protocol

To select an active outbound protocol and transport combination, click the drop-down list next to the active protocol field on the Partner Profile window Outbound Protocol tab. This displays a list of all configured protocol and transport combinations for the profile. Select the one to use for sending documents to the partner. Then click OK on the Outbound Protocol tab to save your changes and close the profile. Or, click Cancel to close the profile without saving your changes.

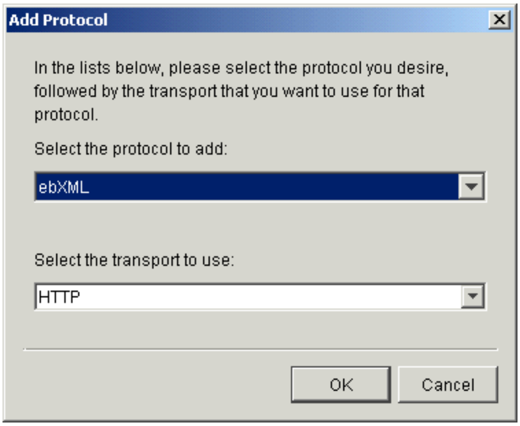
The following are related topics:

- "Adding an Outbound Protocol" on page 12-22
- "Editing an Outbound Protocol" on page 12-23
- "Removing an Outbound Protocol" on page 12-24
- "Adding or Changing a Partner Profile" on page 12-5
- "Importing a Profile from a Partner Who Uses WebLogic Integration" on page 12-2

# Adding an Outbound Protocol

To add a configured protocol to a partner profile, click Add on the Partner Profile window Outbound Protocol tab. This opens the Add Protocol window.

**Figure 12-8 Add Protocol Window**



Add Protocol

In the lists below, please select the protocol you desire, followed by the transport that you want to use for that protocol.

Select the protocol to add: ebXML

Select the transport to use: HTTP

Select the protocol from the drop-down list. The default protocol for WebLogic Integration – Business Connect already is selected, and no other can be selected. Then select a transport from the transports drop-down list. A protocol has at least one transport from which to choose. If more than one transport is available, you must configure at least one, but you can later select another transport and configure it, too. See "Transport Selection Considerations" on page 9-31 for guidelines about selecting transports.

After you select a protocol and transport, click OK. A configuration window opens for the transport method you selected. See one of the following topics for information about configuring the transport:

- "SMTP Outbound Transport" on page 12-25
- "Bundled HTTP Outbound Transport" on page 12-26
- "Bundled HTTPS Outbound Transport" on page 12-28
- "POP Outbound Transport" on page 12-29

On the configuration window for the selected transport, complete the applicable fields and then click OK to save the transport information and close the window. Or, click Cancel to close the configuration window without saving your changes.

After you click OK, the transport method you added appears on the list of configured protocols on the Outbound Protocol tab. The information appears in the following format: protocol transport.

If more than one transport is available for the protocol, you can click Add and repeat the process to configure another transport. If you are done, click OK on the Outbound Protocol tab to save your changes and close the profile. Or, click Cancel to close the profile without saving your changes.

The following are related topics:

- “Selecting an Active Outbound Protocol” on page 12-21
- “Editing an Outbound Protocol” on page 12-23
- “Removing an Outbound Protocol” on page 12-24
- “Adding or Changing a Partner Profile” on page 12-5
- “Importing a Profile from a Partner Who Uses WebLogic Integration” on page 12-2

# Editing an Outbound Protocol

To edit an outbound transport for a protocol that was configured earlier for a partner profile, select the protocol and transport combination you want from the configured protocol list on the Partner Profile window Outbound Protocol tab and then click Edit. This opens the configuration window for the transport. See one of the following topics for information about configuring the transport:

- “SMTP Outbound Transport” on page 12-25
- “Bundled HTTP Outbound Transport” on page 12-26
- “Bundled HTTPS Outbound Transport” on page 12-28
- “POP Outbound Transport” on page 12-29

On the configuration window for the selected transport, edit the applicable fields and then click OK to save the transport information and close the window. Or, click Cancel to close the configuration window without saving your changes. Then click OK on the Outbound Protocol tab to save your changes and close the profile. Or, click Cancel to close the profile without saving your changes.

The following are related topics:

- "Selecting an Active Outbound Protocol" on page 12-21
- "Adding an Outbound Protocol" on page 12-22
- "Removing an Outbound Protocol" on page 12-24
- "Adding or Changing a Partner Profile" on page 12-5
- "Importing a Profile from a Partner Who Uses WebLogic Integration" on page 12-2

# Removing an Outbound Protocol

To remove an outbound transport that was configured earlier for a partner profile's protocol, select the protocol and transport combination you want from the configured protocol list on the Partner Profile window Outbound Protocol tab and then click Remove. This removes the protocol and transport combination from the configured protocol list. Then click OK on the Outbound Protocol tab to save your changes and close the profile. Or, click Cancel to close the profile without saving your changes.

When you remove a protocol and transport combination, it no longer is available for sending documents. However, removing a transport only removes the transport from the list of configured protocols. It does not delete the configuration information for the transport. That information persists in your system. If you add a transport, later remove it and still later add it back, the earlier configuration information is saved and you do not have to re-enter it.

The following are related topics:

- "Selecting an Active Outbound Protocol" on page 12-21
- "Adding an Outbound Protocol" on page 12-22
- "Editing an Outbound Protocol" on page 12-23

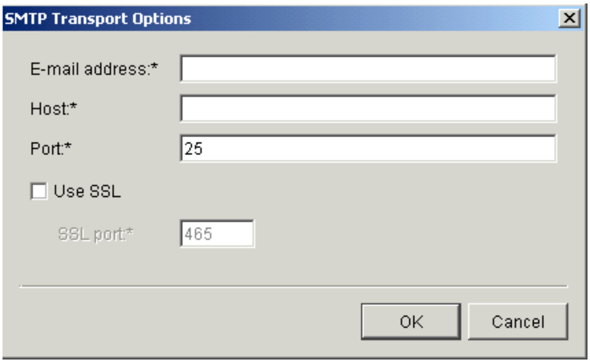
- "Adding or Changing a Partner Profile" on page 12-5
- "Importing a Profile from a Partner Who Uses WebLogic Integration" on page 12-2

# SMTP Outbound Transport

The SMTP transport enables you to send documents from the SMTP server in your WebLogic Integration – Business Connect system to the SMTP server in your partner's WebLogic Integration – Business Connect system. You configure this transport on the SMTP Transport Options window accessed from the Partner Profile window Outbound Protocol tab.

If you imported this profile, configuration information about this transport should be present if your partner wants you to send documents by this method.

**Figure 12-9 SMTP Transport Options Window**



SMTP Transport Options

E-mail address:*

Host:*

Port:* 25

□ Use SSL

SSL port:* 465

## Field Descriptions

The following describes the fields on the SMTP Transport Options window. For procedure see the following topics: "Adding an Outbound Protocol" on page 12-22, "Editing an Outbound Protocol" on page 12-23, "Removing an Outbound Protocol" on page 12-24.

*E-mail address*

The e-mail address where you send documents to your partner. If you are adding this profile manually, type this value.

The e-mail address must be in the standard format of mailbox@server.domain (for example, john@worldwide.com).

*Host*

The fully qualified domain name of the partner’s system where WebLogic Integration – Business Connect is installed.

If you imported the profile and there is a value in this field, it should be a FQDN. You can use this FQDN or obtain another FQDN or an IP address from your partner and enter that value.

*Port*

The host port. If you imported the profile, this value is from the SMTP port field on the Ports tab in Tools→Preferences in your partner’s Administrator application. If you are creating the profile, the default port is 25.

*Use SSL*

Select this radio button to have WebLogic Integration – Business Connect send documents over Secure Sockets Layer (SSL) protocol.

*SSL port*

The host SSL port. If you imported the profile, this value is from the SMTP SSL port field on the Ports tab in Tools→Preferences in your partner’s Administrator application. If you are creating the profile, the default port is `465`.

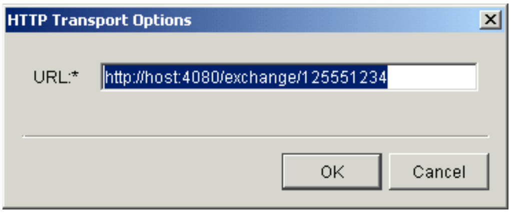
# Bundled HTTP Outbound Transport

The bundled HTTP transport enables you to send documents to the HTTP server in your partner’s WebLogic Integration – Business Connect system. You configure this transport on the HTTP Transport Options window accessed from the Partner Profile window Outbound Protocol tab.

If you imported this profile, configuration information about this transport should be present if your partner wants you to send documents by this method.

**Note:** This bundled transport is named simply HTTP on the user interface.

**Figure 12-10 HTTP Transport Options Window**



URL:* http://host:4080/exchange/125551234

# Field Description

URL is the single field on the HTTP Transport Options window. If you imported this profile and your partner wants you to use this transport, this field contains the URL for sending documents to your partner's HTTP server, which is bundled in the partner's WebLogic Integration – Business Connect system. For your partner's security, the URL is an alias in the following format:

```
http://partner_host_name:4080/exchange/partner_ID
```

The word `exchange` in the URL is an alias for the directory on your partner's server where you send documents. The number `4080` is the default port where your partner's WebLogic Integration – Business Connect HTTP server is listening for inbound documents from you.

If you want to request synchronous acknowledgments (MDNs) from your partner, see "Field Descriptions on the Security Tab" on page 12-44.

For procedure see the following topics: "Adding an Outbound Protocol" on page 12-22, "Editing an Outbound Protocol" on page 12-23, "Removing an Outbound Protocol" on page 12-24.

# Bundled HTTPS Outbound Transport

The bundled HTTPS transport enables you to send documents to the HTTPS server in your partner's WebLogic Integration – Business Connect system. You configure this transport on the HTTPS Transport Options window accessed from the Partner Profile window Outbound Protocol tab.

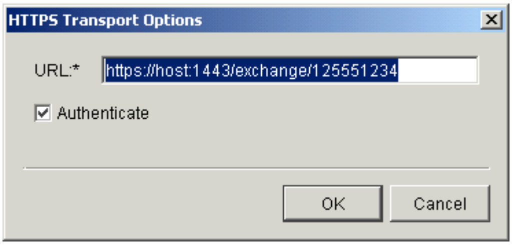
If you imported this profile, configuration information about this transport should be present if your partner wants you to send documents by this method.

If you use bundled HTTPS to send documents, we recommend that you make sure the sign documents check box is selected and the encrypt documents check box is not selected on the Partner Profile window Security tab.

Large-key certificates result in slower HTTPS processing.

**Note:** This bundled transport is named simply HTTPS on the user interface.

**Figure 12-11 HTTPS Transport Options Window**


HTTPS Transport Options

URL:* https://host:1443/exchange/125551234

☑ Authenticate

## Field Descriptions

The following describes the fields on the HTTPS Transport Options window. If you want to request synchronous acknowledgments (MDNs) from your partner, see "Field Descriptions on the Security Tab" on page 12-44.

For procedure see the following topics: "Adding an Outbound Protocol" on page 12-22, "Editing an Outbound Protocol" on page 12-23, "Removing an Outbound Protocol" on page 12-24.

*URL*

If you imported this profile and your partner wants you to use this transport, this field contains the URL for sending documents to your partner's HTTPS server, which is bundled in the partner's WebLogic Integration – Business Connect system. For your partner's security, the URL is an alias in the following format: `https://`*`partner_host_name`*`:1443/exchange/`*`partner_ID`*

The word `exchange` in the URL is an alias for the directory on your partner's server where you send documents. The number 1443 is the default port where your partner's WebLogic Integration – Business Connect HTTPS server is listening for inbound documents from you.

*Authenticate*

If you imported this profile and your partner wants you to use this transport, this check box can be either:

* Selected if your trading partner requires that you authenticate the SSL connection with your certificate.

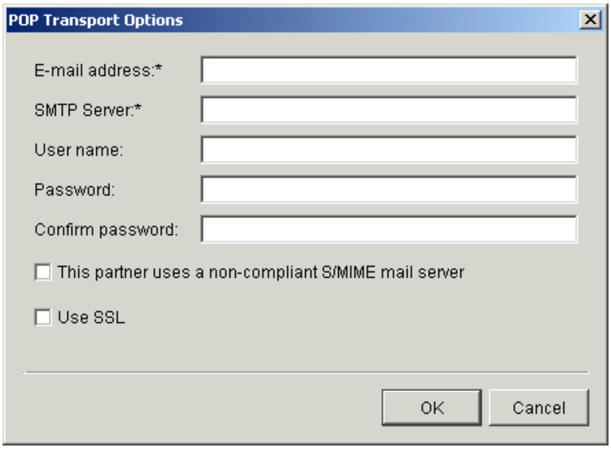
* Clear if your trading partner allows anonymous SSL connections.

# POP Outbound Transport

The POP transport enables you to send documents to an SMTP server and your partner to retrieve them from a POP server. You configure this transport on the POP Transport Options window accessed from the Partner Profile window Outbound Protocol tab.

If you imported this profile, configuration information about this transport should be present if your partner wants you to send documents by this method.

Figure 12-12 POP Transport Options Window



# Field Descriptions

The following describes the fields on the POP Transport Options window. For procedure see the following topics: "Adding an Outbound Protocol" on page 12-22, "Editing an Outbound Protocol" on page 12-23, "Removing an Outbound Protocol" on page 12-24.

*E-mail address*

The e-mail address where you send documents to your partner. If you are adding this profile manually, type this value.
The e-mail address must be in the standard format of `mailbox@server.domain` (for example, `john@worldwide.com`).

*SMTP server*

The fully qualified domain name (FQDN) or IP address of the SMTP server your organization uses for sending documents. Your WebLogic Integration – Business Connect system provides this value or you must type it. If a value is already present, it comes from the Outbound SMTP tab in Tools→Preferences, if you completed that tab. If you imported the profile and this field is blank, or if you are manually creating a profile, you must enter your SMTP server. For more information see "Preferences Outbound SMTP Tab" on page 13-26.

*User name*

The user name for the server. If you are adding this profile manually, type this value.

*Password*

The password for this user name. If you imported the profile, the password appears as asterisks. If you are adding this profile manually, type this value.

*Confirm password*

The password for this user name. If you imported the profile, the password appears as asterisks. If you are adding this profile manually, type this value.

*Use SSL*

If this check box is selected, documents will be sent via Secure Sockets Layer protocol. If you imported this profile, do not change the value in this check box without consulting with your partner.

# Partner Profile Firewall Tab

Use the Partner Profile window Firewall tab to set the parameters WebLogic Integration – Business Connect uses to exchange data through a partner's firewall. For more information see "Firewall Details" on page 12-36.

Currently, WebLogic Integration – Business Connect does not support outbound routing through your company's firewall.

The following topics are provided:

- "Supported Firewall Methods"
- "Getting Your Partner's Firewall Information" on page 12-32
- "Field Descriptions on the Firewall Tab" on page 12-34

# Supported Firewall Methods

Many organizations have installed firewalls to prevent unauthorized access to their computer systems. A firewall is a server that an organization places outside its network. It intercepts all inbound connections from the Internet, and by use of one of several schemes allows only authorized users to connect to a server on the organization's network. Three such schemes that WebLogic Integration – Business Connect supports are listed in the following table.

**Table 12-3 Supported Firewall Methods**

| Transport | Firewall support method |
|---|---|
| FTP | Native FTP routing |
| HTTP | HTTP proxy routing |
| HTTPS | SSL tunneling |

Because details about firewalls are kept confidential and because separate user IDs and passwords need to be set up for each partner, firewall information is not distributed in a company's profile. This is why you do not see this information in the Firewall tab when you import your partner's profile.

# Getting Your Partner's Firewall Information

To get your partner's firewall information, contact your partner and determine the following:

1. Ask whether your partner's organization has a firewall and whether it will require you to send documents through the firewall. Not all organizations with firewalls require that you use them.

2. If your partner requires you to send documents through a firewall, ask your partner for the following information:

   - What is the name or IP address and port number of the firewall for each protocol you intend to use?
   - Does the partner’s firewall require authentication?
   - If the firewall requires authentication, determine what authentication the partner uses. That is, user ID and password authentication or S/KEY.

3. If your partner’s firewall requires authentication, ask for the user name or user ID and secret password your partner wants your WebLogic Integration – Business Connect to use when establishing a connection with the partner’s firewall.

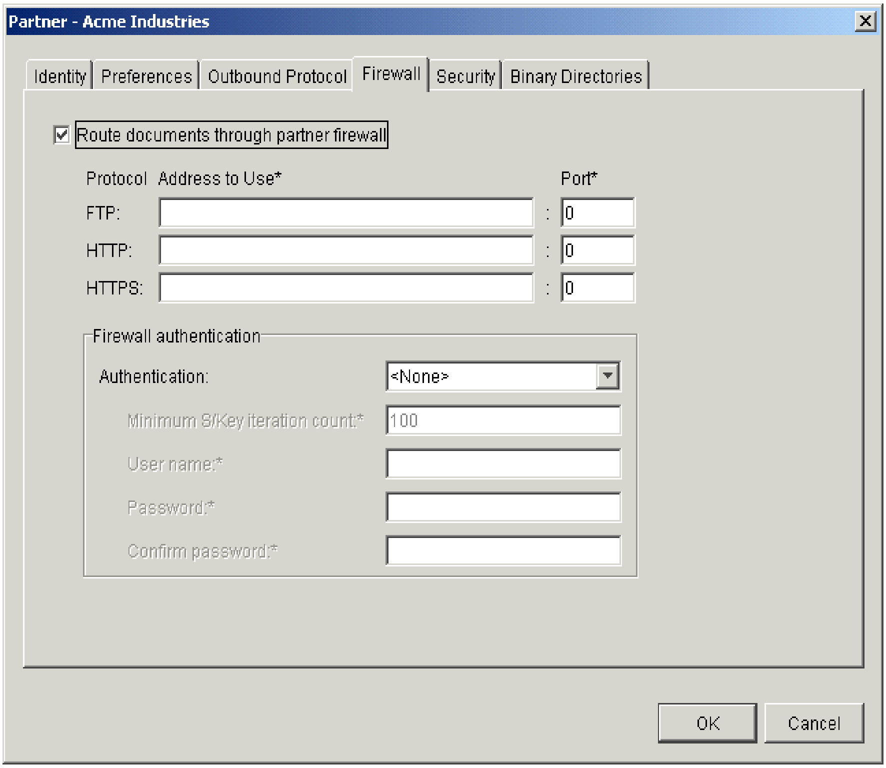
4. If your partner uses S/KEY, ask the partner to recommend a minimum iteration count. This number depends on how often you need to connect to your partner’s firewall to exchange documents. The iteration count functions as a reminder for you to obtain a new password from your partner. It is set each time your partner issues you a password. This setting is kept on your partner's system.

   Depending on how your partner sets this up, one use of a key might last for a predetermined period of time, so that several transactions might be passed during the time it is valid.

   Each use of this key decrements the iteration count by one. When the number reaches the limit you entered, WebLogic Integration – Business Connect issues a notification message reminding you to contact your partner for a new password. WebLogic Integration – Business Connect continues to send you notifications until your partner sends you a new password and resets your iteration count on the partner’s system. During the time when the iteration count is below the minimum, your password will continue to function, and message traffic will flow uninterrupted. If the iteration count falls to zero or below, authentication might fail.

After you get the preceding information, you are ready to enter information in the Partner Profile window Firewall tab.

**Figure 12-13 Partner Profile Firewall Tab**



☑ Route documents through partner firewall

| Protocol | Address to Use* | | Port* |
|---|---|---|---|
| FTP: | | : | 0 |
| HTTP: | | : | 0 |
| HTTPS: | | : | 0 |

Firewall authentication

Authentication: <None>

Minimum S/Key iteration count:* 100

User name:*

Password:*

Confirm password:*

# Field Descriptions on the Firewall Tab

The following describes the fields on the Partner Profile window Firewall tab. For procedure see "Adding or Changing a Partner Profile" on page 12-5 or "Importing a Profile from a Partner Who Uses WebLogic Integration" on page 12-2.

*Route documents through partner firewall*

If your partner requires that you route documents through a firewall, select this check box.

*Protocol address to use*

For the transport method you plan to use to send documents to this partner, type the name or IP address of the firewall host to which WebLogic Integration – Business Connect logs on when it sends documents to this partner. Your partner provides this information.

If your partner requires you to route documents through the partner's firewall but does not use authentication, you still must complete this field.

*Port*

In the port field for the transport method you plan to use to send documents to this partner, type the port number of your partner's firewall host. Your partner provides this information.

If your partner requires you to route documents through the partner's firewall but does not use authentication, you still must complete this field.

If you enter an address and port for the FTP transport protocol, WebLogic Integration – Business Connect uses them to establish the connection with the partner's firewall. The firewall then directs the connection to the partner's FTP server used by the partner's WebLogic Integration – Business Connect system. In this case, the values you enter in the control port field on the FTP Transport Options window are not used.

*Firewall authentication*

Skip this area if your partner does not require authentication. If your partner uses clear text or S/Key authentication, complete the following fields as applicable. Your partner must provide this information.

*Authentication*

If you select S/Key, complete the minimum S/Key iteration count, user name and password fields. If you select clear text, complete the user name and password fields. If your partner uses clear text authentication, your user name and password are sent to the partner's firewall in unencrypted form.

*Minimum S/Key iteration count*

If you select S/Key authentication, type the minimum iteration count you and your partner agreed upon. This field is active only if you select S/Key authentication.

When the number of iterations remaining on your current S/Key equals this number you enter, a notification is sent to you with each additional use of your key. In this way, it serves as a reminder that you need to ask your partner for a new key. For more information about how S/Key works see "Firewall Details" on page 12-36.

*User name*

If your partner uses clear text or S/Key authentication, type user name that WebLogic Integration – Business Connect uses when it logs on to your partner's firewall. Your partner must provide this information.

*Password*

If your partner uses clear text or S/Key authentication, type the password that WebLogic Integration – Business Connect uses when it logs on to your partner's firewall. If you authenticate with an S/Key-enabled firewall, your secret password is never sent in clear-text form. Your partner must provide this information.

# Firewall Details

The following topics are provided about sending documents to partners who use firewalls:

- "HTTP and HTTPS for Firewalls and Proxy Servers"
- "Commands Sent to Firewalls" on page 12-38
- "Firewall Authentication Methods" on page 12-39

# HTTP and HTTPS for Firewalls and Proxy Servers

You can configure WebLogic Integration – Business Connect to communicate using the HTTP or HTTPS transport through firewall and proxy servers without compromising the security of your network.

To do this, you can use one of two alternatives:

- *Network Address Translation (NAT)*
  This method translates a valid address from outside your firewall to an address behind your firewall. This is the recommended solution because it provides you the most flexibility in assigning port addresses.

- *Windows Sockets (Winsock)*
  This method creates a secure channel or tunnel to your proxy server. You can use this alternative if your server does not support NAT. You can use this alternative on proxy servers that support sockets.

## Using Network Address Translation

See your firewall software documentation for instructions on implementing this solution.

## Using Winsock

1. In Interchange Administrator select Tools→Preferences to open the Preferences window. Type `8080` in the HTTP port field. In your Company Profile Transport tab, HTTP/HTTPS subtab, type `4443` in the Port field.

2. Using your favorite text editor, create the `wspcfg.ini` file. The following is an example of the contents of this file:

   ```
   [jre]
   ServerBindTcpPorts=8080,4443
   Persistent=1
   KillOldSession=1
   ```

3. Save the file in installation directory\bin and close the text editor.

4. Re-initialize your server. The proxy server computer does not overwrite the `wspcfg.ini` file you created; rather it reads the file and binds the needed ports to WebLogic Integration – Business Connect when that application is started. Consequently, you can make configuration settings in this file that apply only to WebLogic Integration – Business Connect on a specific client computer.

# Commands Sent to Firewalls

The following describes how WebLogic Integration – Business Connect sends documents through a trading partner's firewall using FTP and HTTP. Listed are the commands WebLogic Integration – Business Connect sends to the partner firewall for each transport.

## Native FTP Authentication

```
User PROXYUSER@FTPUSER@DESTINATION

Password PROXYPASSWORD@FTPPASSWORD
```

## HTTP Proxy

```
POST http://destinationhost:port/uri

Authenticate: FIREWALLUSER:FIREWALLPSWD
```

## HTTPS Tunnelling

```
CONNECT http://destinationhost:port/

Authenticate: FIREWALLUSER:FIREWALLPSWD
```

# Firewall Authentication Methods

The following describes how WebLogic Integration – Business Connect authenticates with firewalls that use various authentication methods.

Organizations deploy firewalls to prevent unauthorized users from gaining access to the corporate data that resides on their networks or in their computer centers. Although most organizations use either clear text or S/KEY authentication methods, you might encounter partners who use other strategies. WebLogic Integration – Business Connect supports the following:

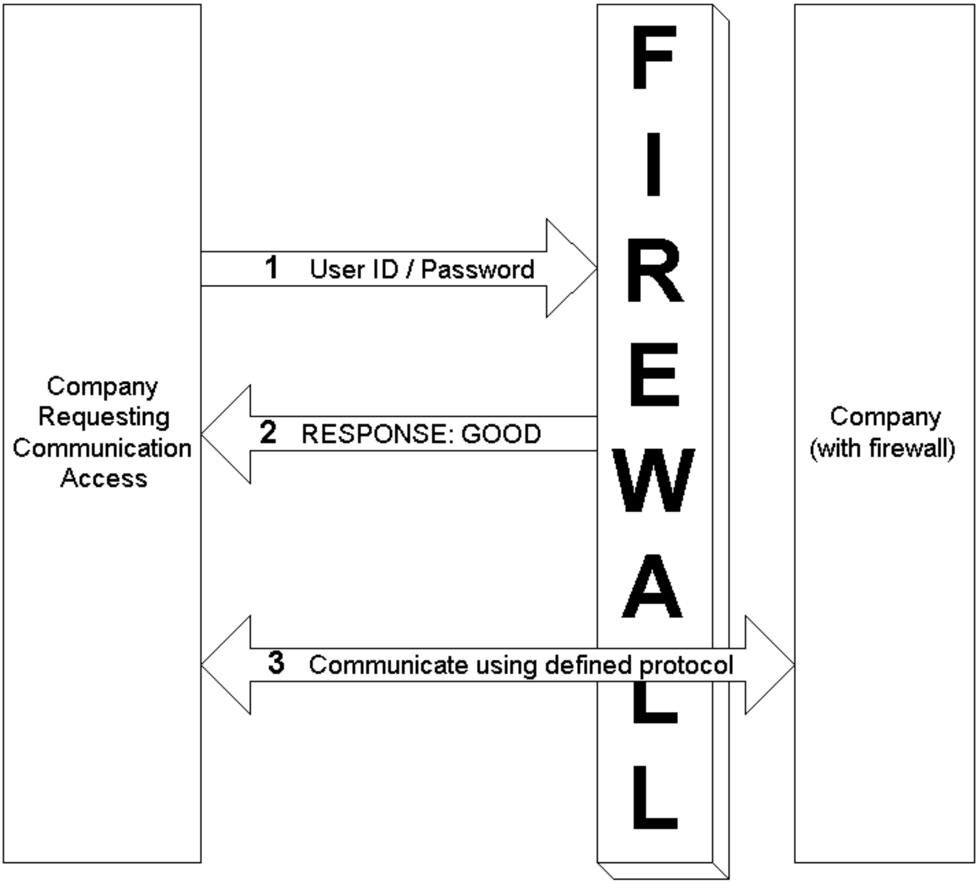
- *No authentication*
  If your partner uses this strategy, your WebLogic Integration – Business Connect server log on to your partners firewall but does not need to authenticate using a user ID or password.

- *IP authentication*
  The firewall checks the IP address of the sender against a known list of authorized senders. It blocks unauthorized addresses while allowing authorized senders to exchange data through the firewall. You do not need to use the WebLogic Integration – Business Connect firewall tab to navigate the firewall of a partner who uses this authentication method.

- *Clear-text authentication*
  If your partner's firewall requires clear text authentication you use the WebLogic Integration – Business Connect partner firewall tab. In this tab you provide the IP address of your partners firewall host along with the port he/she wants you to use. You also use the user ID and password which your partner has provided you.

- *S/KEY authentication*
  If your partner's firewall uses S/KEY authentication, you must supply the IP address and the port of the firewall host and a user ID and password which you would use for a series of challenge and response authentications.

**Figure 12-14 User ID/Password Challenge-Response**


Company Requesting Communication Access
1 User ID / Password
2 RESPONSE: GOOD
3 Communicate using defined protocol
FIREWALL
Company (with firewall)

## Support for the S/KEY One-Time Password System

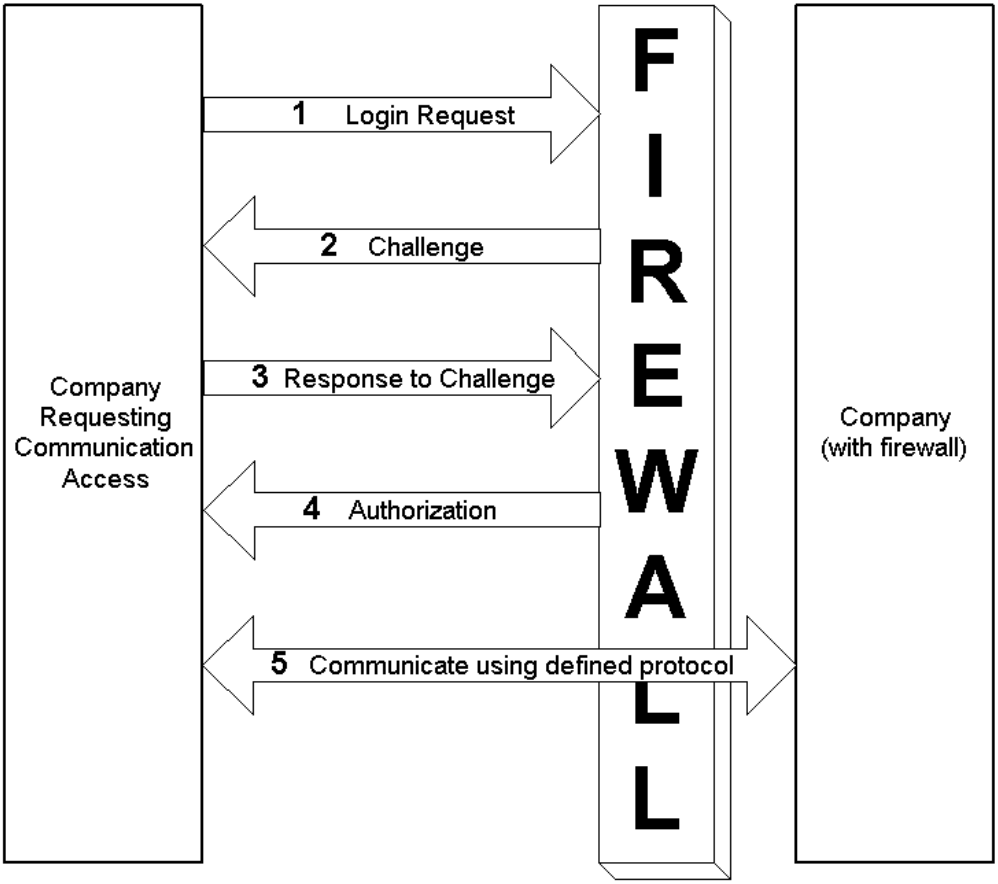
This section provides details about how WebLogic Integration – Business Connect uses the S/KEY One-time Password System (S/KEY) to navigate your partner's firewall. This information is for use by system administrators and other interested users. Because WebLogic Integration – Business Connect hides the complexity, a user need not understand it fully to successfully use the S/KEY.

S/KEY is used to prevent what is known as a replay attack on an organization's network. In a replay attack, an unauthorized person outside an organization's network eavesdrops on that network's connections to obtain the login IDs and passwords of legitimate users. At some later time, the unauthorized intruder replays the log-ins and passwords to gain access to the network. S/KEY foils these attacks by exchanging a series of challenge and responses with the user who is requesting access.

The S/KEY is documented by RFC 1760. You can see this RFC along with a list of others posted by the Internet Engineering Task Force (IETF) at the following web site: http://www.ietf.org/home.html

See "Partner Profile Firewall Tab" on page 12-31 for information on setting up WebLogic Integration – Business Connect to navigate an S/KEY-enabled firewall.

**Figure 12-15 S/KEY Challenge-Response**



A typical exchange between your WebLogic Integration – Business Connect and a partner with an S/KEY-enabled firewall occurs as follows (See Figure 12-15.):

1. Your WebLogic Integration – Business Connect server sends a login request to connect to your partner's firewall using a user name or user ID from the user name field in the firewall tab.

2. In response, your partner’s S/KEY-enabled firewall sends you a challenge. This challenge consists of the latest iteration count and a seed value.

3. Upon receipt of this challenge, your WebLogic Integration – Business Connect computes a new password by hashing the seed value, the iteration count from the challenge response, and the password from the firewall tab. More specifically, WebLogic Integration – Business Connect iteratively hashes the result of the previous hash up to the number specified in the iteration count that came with the challenge response. The new computed password consists of six English words. WebLogic Integration – Business Connect then sends this new, computed, multi-word password and your user ID to your partner.

4. Your partner verifies this new password and sends an approval or rejection back to your WebLogic Integration – Business Connect.

5. If the response is valid, your WebLogic Integration – Business Connect server then passes documents through the firewall to your partner's WebLogic Integration – Business Connect.

# Partner Profile Security Tab

Use the Partner Profile window Security tab to select or change the security settings for a partner profile. These are the parameters WebLogic Integration – Business Connect uses to sign, encrypt, and acknowledge receipt of documents you send to a partner.

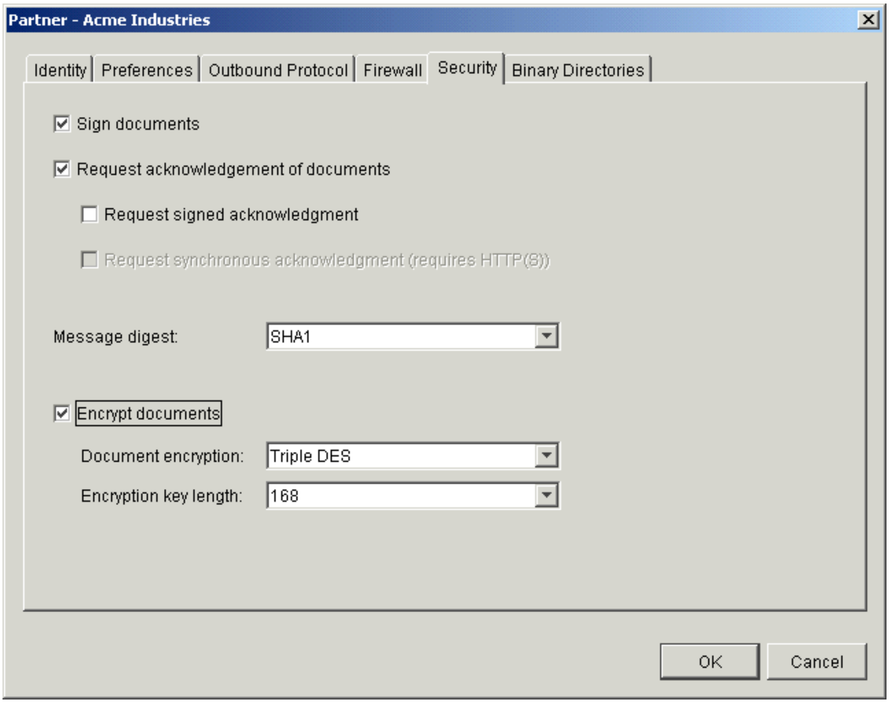
The following topics are provided:

- "Bundled HTTPS Guideline" on page 12-43
- "Field Descriptions on the Security Tab" on page 12-44

## Bundled HTTPS Guideline

If you use bundled HTTPS to send documents to partners, we recommend that you select the sign documents check box and that you do not select the encrypt documents check box on the Partner Profile window Security tab.

**Figure 12-16 Partner Profile Security Tab**



☑ Sign documents

☑ Request acknowledgement of documents

□ Request signed acknowledgment

□ Request synchronous acknowledgment (requires HTTP(S))

Message digest: SHA1

☑ Encrypt documents

Document encryption: Triple DES

Encryption key length: 168

# Field Descriptions on the Security Tab

The following describes the fields on the Partner Profile window Security tab. For procedure see "Adding or Changing a Partner Profile" on page 12-5 or "Importing a Profile from a Partner Who Uses WebLogic Integration" on page 12-2.

*Sign documents*

Select this check box to have WebLogic Integration – Business Connect sign the documents you transmit. This is the default.

Clear this check box to send documents without a digital signature.

*Request acknowledgment of documents*

Select this check box to have your partner send message disposition notification (MDN) acknowledgments to you upon receipt of your documents. The MDNs are signed or unsigned depending on your selection in the sign documents check box.

WebLogic Integration – Business Connect supports the use of MDNs for S/MIME documents as follows:

* sends MDNs to those partners who request them for their S/MIME documents.

* If you receive an unsigned MDN from a trading partner who uses S/MIME, WebLogic Integration – Business Connect considers the document to have been acknowledged, but logs the MDN as *Received, Generic* in Tracker. The selected check box is the default.

Clear the check box to indicate that you do not want your trading partners to send you acknowledgments for the documents you send them.

WebLogic Integration – Business Connect appends file names of received MDNs with `_ack`.

*Request signed acknowledgment*

Select this check box to have your partner sign the MDNs the partner sends to you. This is the default when you import a profile with a certificate from a partner who uses WebLogic Integration – Business Connect.

Clear this check box to have your partner send you unsigned MDNs.

*Request synchronous acknowledgment (requires bundled HTTP(S))*

If you use the bundled HTTP or HTTPS transport, select this check box if you want synchronous MDNs.

*Message digest*

The algorithm that WebLogic Integration – Business Connect uses to create a hash of the unencrypted document. This hash is a number which is encrypted with the sender’s private key. It is decrypted by the recipient using the sender’s public key. The recipient rehashes the decrypted document and compares the result with the hash that came with the document. If the two are identical, it ensures that the contents have not been altered.

You can choose from the algorithms MD5 and SHA1 (the default).

*Encrypt documents*

Select this check box to have WebLogic Integration – Business Connect encrypt the documents you transmit. This is the default when you import a profile with a certificate from a partner who uses WebLogic Integration – Business Connect.

Clear this check box to send unencrypted documents.

*Document encryption*

If you select encrypt documents, select one of the following from the drop-down list to indicate which algorithm WebLogic Integration – Business Connect is to use to encrypt the documents you send: RC2, ARC4, DES or Triple DES, the default.

*Encryption key length*

If you select encrypt documents, select the key length appropriate for the encryption algorithm you chose:

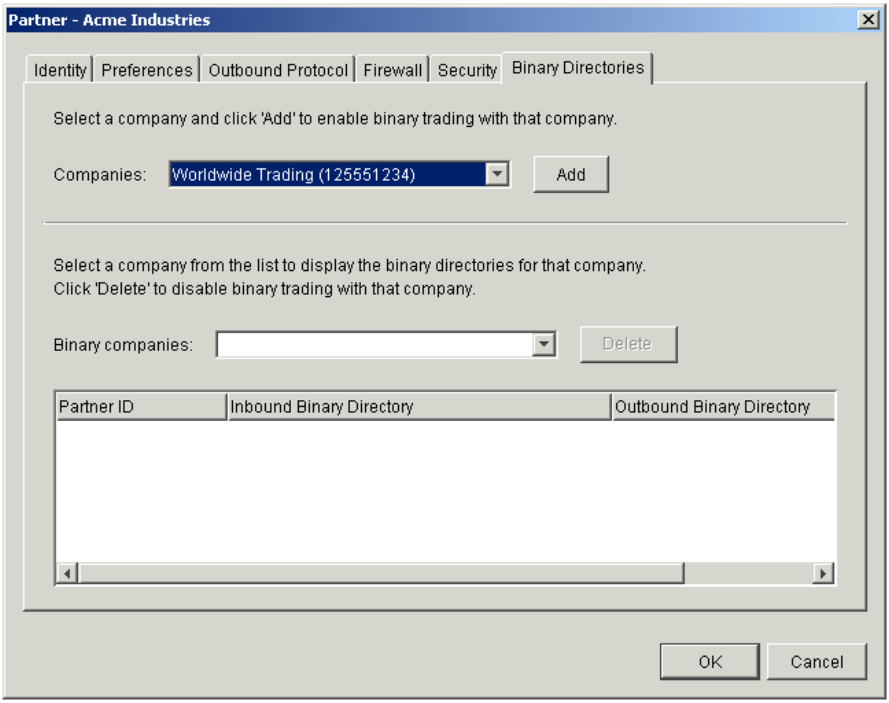
| | |
|---|---|
| 40 | Normal encryption. |
| 56 | Strong encryption. If you select DES, this key length is assigned. |
| 64 | Strong encryption. You can select this for the RC2 or ARC4 encryption algorithm. |
| 128 | Very strong encryption. You can select this for the RC2 or ARC4 encryption algorithm. |
| 168 | Very strong encryption. If you select Triple DES, this key length is assigned. |

# Partner Profile Binary Directories Tab

Use the Partner Profile window Binary Directories tab if you plan to exchange binary documents with a partner. This tab lets you set up partner-specific inbound and outbound directories for sending and receiving binary documents.

WebLogic Integration – Business Connect uses a unique binary-out directory for each partner so that it knows the correct addressee for the outbound binary documents. Conversely, the system uses a unique binary-in directory for each partner so that documents placed in it can be correctly processed by your business application.

**Figure 12-17 Partner Profile Binary Directories Tab**



Partner - Acme Industries

Select a company and click 'Add' to enable binary trading with that company.

Companies: Worldwide Trading (125551234)

Select a company from the list to display the binary directories for that company.
Click 'Delete' to disable binary trading with that company.

Binary companies:

| Partner ID | Inbound Binary Directory | Outbound Binary Directory |
|---|---|---|

# Field Descriptions

The following describes the fields on the Partner Profile window Binary Directories tab. For procedure see "Adding or Changing a Partner Profile" on page 12-5 or "Importing a Profile from a Partner Who Uses WebLogic Integration" on page 12-2.

*Companies*

If you intend to exchange binary documents with this partner, select your company profile from the drop-down list and click Add.

If you set up a secondary ID for another trading partner on the Partner Profile window Identity tab for this partner, the system sets up binary directories on this tab for the secondary ID partner.

**Note:** Your partner must also make a similar selection in your partner profile on the partner's WebLogic Integration – Business Connect system.

*Binary companies*

Select a company from the drop-down list to display the binary directories for the company. Click Delete if you want to disable binary trading with the company.

At your discretion, you can type new paths and directory names in the inbound and outbound binary directory fields. Outbound directories must be unique across the whole application; inbound directories need not be unique.

# Delete a Partner Profile

Use this procedure to delete a partner profile that is no longer needed. When you delete a partner profile:

- You cannot undo it.
- The record for this partner is no longer displayed in the Certificates information viewer. Although not displayed, any certificates for this partner are retired, not deleted.
- The system directories that WebLogic Integration – Business Connect created for this partner are not deleted.
- Documents received for a partner that has been deleted are placed in the rejected documents directory.

## Steps

1. At the Partner Profiles information viewer, select the partner profile you want to delete and click Delete.
2. Confirm the deletion in the dialog box that appears.

CHAPTER

# 13 Tools

The following topics describe some of the tools on the Tools menu in Administrator.

**Windows**

- "API Authentication Window" on page 13-2
- "JMS Global Integration for Documents" on page 13-3
- "JMS Integration for Events" on page 13-9
- "Change Password Window" on page 13-12
- "Configure Archive Schedule Window" on page 13-13
- "Configure Send Schedule Window" on page 13-16
- "Remove Record Locks Window" on page 13-17
- "Preferences General Tab" on page 13-19
- "Preferences Ports Tab" on page 13-23
- "Preferences Outbound SMTP Tab" on page 13-26
- "Preferences Monitoring Tab" on page 13-28

For other functions on the Tools menu, see the following topics:

- Certificates→Trusted Roots. See "Trusted Roots" on page 11-51
- Certificates→Cert Revocation List. See "Using Certificate Revocation Lists" on page 11-54
- Launch Server Monitor. See "Monitoring the Server with a Browser" on page 6-7

# API Authentication Window

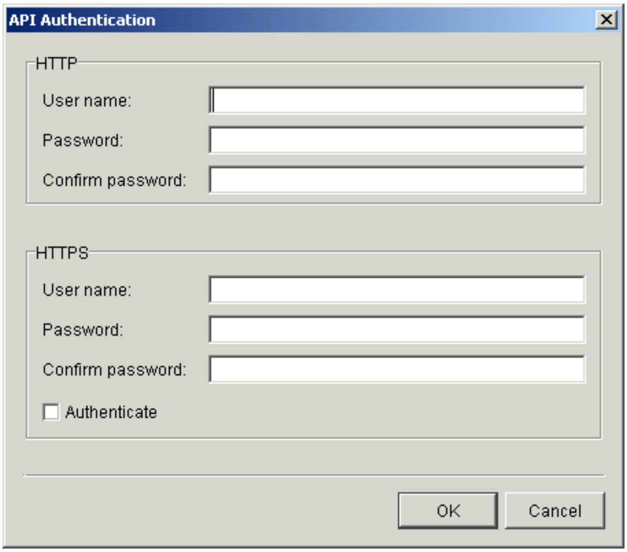
Use the API Authentication window to set a user name and password for the HTTP or HTTPS server that is built into WebLogic Integration – Business Connect for communicating with an API client.

Select Tools→API→Authentication in Administrator to open the API Authentication window.

To set HTTP or HTTPS ports for communications with an API client, see “Preferences Ports Tab” on page 13-23.

If you use the API HTTPS port for integration, you must generate or load a certificate for the HTTPS server using the certloader tool. See “Certificate Tool (certloader)” on page 14-14.

**Figure 13-1 API Authentication Window**



## Field Descriptions

The following describes the fields on the Preferences window API tab. The fields are described once for both HTTP and HTTPS.

*User name*

The user name that you specify for the API HTTP or HTTPS server. The API client uses this to access the server.

*Password*

The password that you specify for the API HTTP or HTTPS server. The API client uses this to access the server.

*Confirm password*

Type the password again.

*Authenticate (HTTPS)*

Select this check box only if the API HTTPS server will authenticate the client certificate. See "Configuring the API Server to Authenticate an API Client" on page 14-13.

# JMS Global Integration for Documents

Use the JMS Integration window Documents tab to configure WebLogic Integration – Business Connect to retrieve outbound documents from or direct inbound documents to a JMS queue. This affects inbound and outbound documents for all active company profiles, all partners and all document types: EDI, XML and binary.

The global treatment of all documents distinguishes this tab from JMS document integration that can be configured for a single company using the Company Profile window Integration tab. For more information see "JMS Options Window" on page 9-54.

To use the JMS Integration window Documents tab your organization must have JMS experience and a working JMS messaging system.

In addition to completing this tab, you must add the names of the JAR or class files or both in the `server.ini` or `server.bat` file in Windows or your environment file in UNIX so the Server application can locate the JMS and JNDI provider. The `server.ini` and `server.bat` files are located in the installation directory bin subdirectory. In some cases, you need to add the name of only one JAR file (for example, `swiftmq.jar`), but you might have to include a series of jars or paths.

To display the JMS Integration window Documents tab, select Tools→API→JMS and click the Documents tab.

The following are related topics:

- JMS Integration Details
- Field Descriptions for JMS Integration Documents Tab

# JMS Integration Details

This API is an input and output source for documents. This is how it works: WebLogic Integration – Business Connect registers as a listener with the JMS server for the designated inbound queue. This means that any JMSMessage placed in the queue by another process is passed to WebLogic Integration – Business Connect, which verifies that it is a BytesMessage (a type of JMSMessage). If verified, WebLogic Integration – Business Connect packages and sends it to the partner. Likewise, every document WebLogic Integration – Business Connect receives from a partner is unpackaged, converted to a BytesMessage and placed on the designated outbound queue.

The API requires that the JMS messages be in the format BytesMessage. WebLogic Integration – Business Connect does not process any other type of JMS Message (such as ObjectMessage). WebLogic Integration – Business Connect performs routing decisions based on JMS message string parameters that must be appended to each BytesMessage sent to it. If the required parameters are omitted, WebLogic Integration – Business Connect does not process the message. WebLogic Integration – Business Connect also places the same parameters on each message that it sends to the outbound queue. The parameters WebLogic Integration – Business Connect uses are described in the following table.

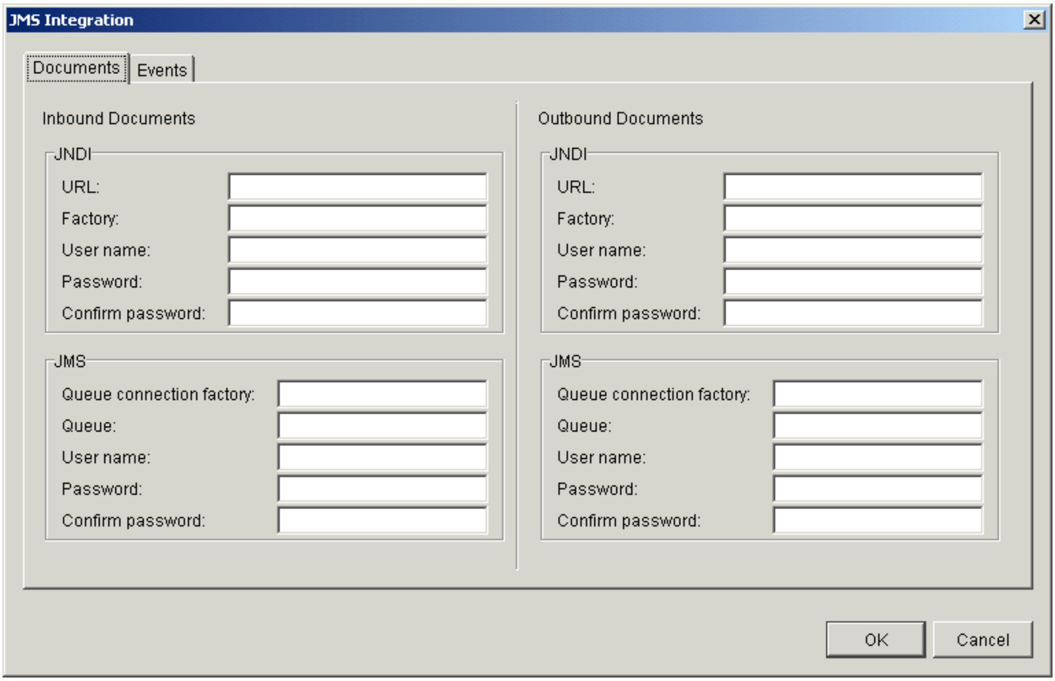
**Table 13-1 JMS Message String Parameters**

| Parameter | Description |
|---|---|
| SenderRoutingId | The ID of the document sender. This parameter is required. |
| TrueSenderId | The ID of the document sender. This is for document re-routing. This parameter is optional. |
| ReceiverRoutingId | The ID of the document receiver. This parameter is required. |
| TrueReceiverId | The ID of ultimate receiver of the document. This is for document re-routing. This parameter is optional. |
| DocumentType | Indicates whether the document is XML, binary, X12 or EDIFACT. This parameter is required. |
| DocumentSubType | The sub type of the message. This is used for EDI documents. This parameter is optional. |
| Path | The current path of the document. WebLogic Integration – Business Connect sets this value. |
| OriginalFileName | The original name of the file. This parameter is required. |
| CorrelationId | The assigned correlation ID of the document. This ID relates documents that are parts of conversations between partners in ebXML exchanges. This parameter is optional. |
| RefToMessageId | The assigned reference message ID of the document. This ID relates the current document to another document. This parameter is optional. |
| SequenceId | Indicates duplicate document names by appending file names with _1, _2, _3 and so on. You only want to use this parameter when you have selected sequence duplicate file names on the Partner Profile window Preferences tab. WebLogic Integration – Business Connect sets this value. |
| DocumentId | The unique alphanumeric string WebLogic Integration – Business Connect assigns to the document. Appended to the value is the receiver’s ID. WebLogic Integration – Business Connect sets this value. |

**Table 13-1 JMS Message String Parameters (Continued)**

| Parameter | Description |
|---|---|
| ControlId | The control ID of an EDI document. Otherwise, the ID is XML or BINARY. WebLogic Integration – Business Connect sets this value. |
| Transport | The transport method used to receive the document. WebLogic Integration – Business Connect sets this value. The possible transports are:<br>Bundled HTTP<br>Bundled HTTPS<br>EMAIL<br>SMTP |
| ebXmlAction | Identifies an ebXML process within a service that processes the message. For example, `NewOrder`.<br>If you are using the file system ebXML protocol method, the user sets this for outbound documents. WebLogic Integration – Business Connect sets this value for inbound documents. |
| ebXmlService | Identifies an ebXML business process. For example, a purchase order.<br>If you are using the file system ebXML protocol method, the user sets this for outbound documents. WebLogic Integration – Business Connect sets this value for inbound documents. |
| PackagingType | If you are using the file system ebXML protocol method, set to ebXML for outbound documents. WebLogic Integration – Business Connect sets this value for inbound documents. |
| PackagingVersion | If you are using the file system ebXML protocol method, set to 1.0 for outbound documents. WebLogic Integration – Business Connect sets this value for inbound documents. |

**Figure 13-2 JMS Integration Window Documents Tab**



# Field Descriptions for JMS Integration Documents Tab

The following describes the fields on the JMS Integration window Documents tab.

The fields are described once for inbound and outbound documents.

The Inbound Documents area is for configuring WebLogic Integration – Business Connect to place documents that have been received from partners and unpackaged on a back-end JMS queue.

The Outbound Documents area is for configuring WebLogic Integration – Business Connect to poll a back-end JMS queue for documents that are to be retrieved, packaged and sent to partners.

Except for the user name and password, you can obtain the information needed to complete the tab from the JMS or JNDI provider's documentation. The information will vary depending on the provider. If you have questions, contact your JMS or JNDI provider.

*JNDI*

Complete the following fields for the Java naming and directory interface (JNDI).

*URL*

Type the network URL that will be used to obtain access to the JNDI service provider for your JMS service. Example: `smqp://localhost:4001/timeout=10000`

*Factory*

Type the name for the JNDI service provider class. Example: `com.swiftmq.jndi.InitialContextFactoryImpl`

*User name*

Type a user name for the JNDI provider. This value could be blank and is typically provided for in the JNDI URL. However, this will depend on the JNDI provider and how it is configured.

*Password*

Type a password for the JNDI provider. This value could be blank and is typically provided for in the JNDI URL. However, this will depend on the JNDI provider and how it is configured.

*Confirm password*

Type the password again.

*JMS*

Complete the following fields for the Java messaging service (JMS).

*Queue connection factory*

Type the connection factory as defined within the JMS provider. This value can be either in the form *`factoryname@routername`* or the JNDI public symbol for the QueueConnectionFactory. Examples: `plainsocket@router1` or `QueueConnectionFactory22`. This would be dependent on your JMS provider and how it is configured.

*Queue*

Type the name of the queue in the form *`queuename@routername`*. Example: `XMLQueue@router1`

*User name*

Type a user name for the JMS provider. This can be the same as your JNDI user name. However, this will depend on how your JMS provider and how it is configured.

*Password*

Type a password for the JMS provider. This can be the same as your JNDI password. However, this will depend on how your JMS provider and how it is configured.

*Confirm password*

Type the password again.

# JMS Integration for Events

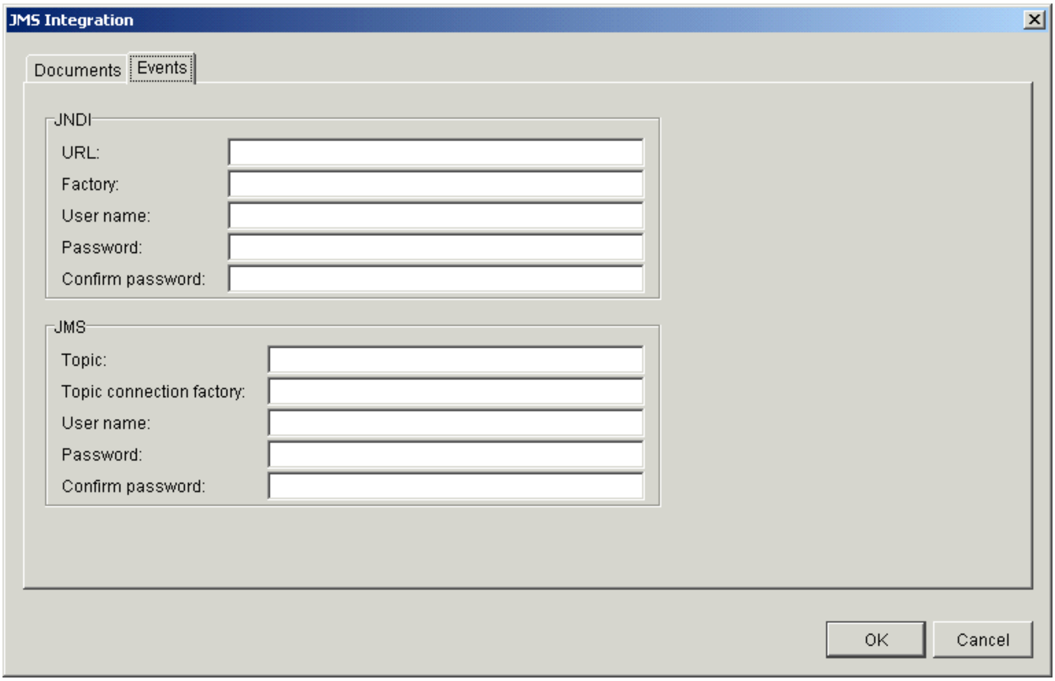
Use the JMS Integration window Events tab to configure the Server application to publish all events to your system's JMS server and locate the information by calling the JNDI provider in your JMS enterprise messaging system. This features enables persistent event logging to the JMS server.

To use this tab your organization must have JMS experience and a working JMS messaging system.

In addition to completing this tab, you must add the names of the JAR or class files or both in the `server.ini` or `server.bat` file in Windows or your environment file in UNIX so the Server application can locate the JMS and JNDI provider. The `server.ini` and `server.bat` files are located in the installation directory `bin` subdirectory. In some cases, you need to add the name of only one JAR file (for example, `swiftmq.jar`), but you might have to include a series of jars or paths.

To display the JMS Integration window Events tab, select Tools →API→JMS and click the Events tab.

**Figure 13-3 JMS Integration Window Events Tab**



# Field Descriptions

The following describes the fields on the JMS Integration window Events tab.

*JNDI*

Complete the following fields for the Java naming and directory interface (JNDI).

*URL*

Type the network URL that will be used to obtain access to the JNDI service provider for your JMS service. Example: `smqp://localhost:4001/timeout=10000`

*Factory*

Type the name for the JNDI service provider class. Example: `com.swiftmq.jndi.InitialContextFactoryImpl`

*User name*

Type a user name that will be used to access the JNDI provider. This value could be blank and is typically provided for in the JNDI URL. However, this will depend on the JNDI provider and how it is configured.

*Password*

Type a password for the JNDI user name. This value could be blank and is typically provided for in the JNDI URL. However, this will depend on the JNDI provider and how it is configured.

*Confirm password*

Type the password again.

*JMS*

Complete the following fields for the Java messaging service (JMS).

*Topic*

Type the name of the topic. Example: `eventTopic`

*Topic connection factory*

Type the connection factory as defined within the JMS provider. This value can be either in the form *`factory_name@router_name`* or the JNDI public symbol for the TopicConnectionFactory. Examples: `plainsocket@router1` or `TopicConnectionFactory22`. This will depend on your JMS provider and how it is configured.

*User name*

Type a user name on the router that has access to the specified topic. This can be the same as the JNDI user name. However, this will depend on your JMS provider and how it is configured.

*Password*

Type the password for the JMS user name.

*Confirm password*

Type the password again.

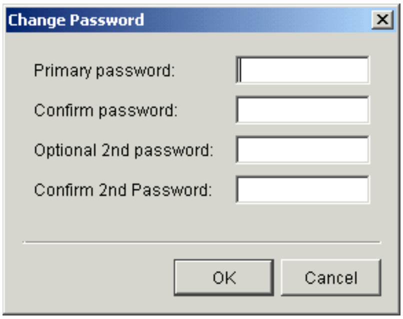
# Change Password Window

Use the Change Password window to set or change an optional primary password for the default Administrator user to open the Administrator and Tracker applications. You also can set or change an optional secondary password to require two passwords to open Administrator and Tracker.

By default there is no password for Administrator and Tracker.

Select Tools→Change Administrator Password in Administrator to open the Change Password window.

**Figure 13-4 Change Password Window**



## Field Descriptions

The following describes the fields on the Change Password window.

*Primary password*

Type the new or changed user password to be used at the login dialog box. The password length is from 1 to 50 characters and can be any combination of numbers and letters. This password is case-sensitive. Setting a password is optional.

Type the password carefully because the characters you type are masked.

WebLogic Integration – Business Connect does not provide a way for you to recover a forgotten password.

*Confirm password*

Type the same password you typed in the primary password field.

*Optional 2nd password*

Type the new or changed optional second user password to be used at the login dialog box. The password length is from 1 to 50 characters and can be any combination of numbers and letters. This password is case-sensitive.

If you require a second password, WebLogic Integration – Business Connect at login prompts the user to enter the second password after the first password is entered.

*Confirm 2nd password*

Type the same password you typed in the Optional 2nd password field.

# Configure Archive Schedule Window

Use the Configure Archive Schedule window to set a schedule for moving Tracker runtime database records to a historical repository called the archive database. You also can archive the actual documents you have sent or received from partners by choosing the backup and archive options on the Company Profile window Preferences tab. See “Company Profile Preferences Tab” on page 9-22.

Select Tools→Configure Schedule→Archive Schedule in Administrator to open the Configure Archive Schedule window.

The following topics are provided:

- Archiving Overview
- Steps for Changing Archive Schedule

# Archiving Overview

By default the archive schedule is set at 12 a.m. Saturday, which means Tracker runtime database records will be moved to the archive database every Saturday at midnight. At the same time, the documents WebLogic Integration – Business Connect has processed are moved from the application's backup directory to the archive directory, if you have elected document archiving.

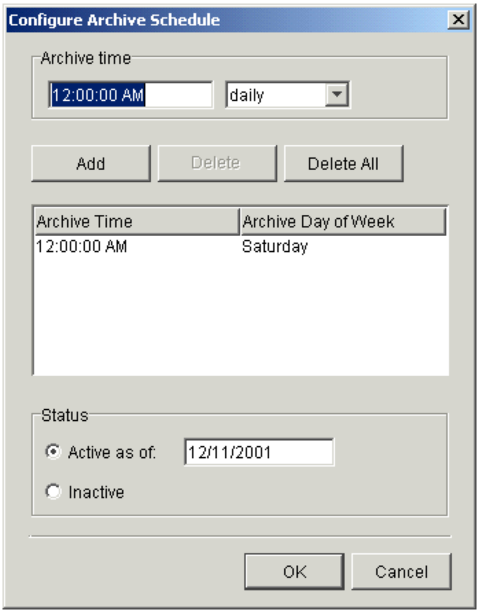
The Server application must be running for Tracker archiving to occur. If the Server is not running at the scheduled archiving time, archiving will not occur and the runtime and archive databases will not change. If the Server is re-started after the scheduled archiving time, archiving will not take place retroactively. Rather, database records will be archived at the next scheduled time, presuming the Server is running.

There are two ways to turn off archiving: Make the archive schedule inactive or delete the archiving times.

WebLogic Integration – Business Connect writes output of Server application activity to a file called `server.log` located in the WebLogic Integration – Business Connect logs directory. When you use the View Server Log utility on Windows, you see the contents of this file as it is being written by WebLogic Integration – Business Connect.

The current output of Server application activity is continuously written to a `server.log` file. When the archive schedule triggers, WebLogic Integration – Business Connect closes the current `server.log` file, renames it using the current date and time, and begins writing output to a new `server.log` file. Closed `server.log` files are named according to the date and time archiving occurred in the following format: `server.log.`*`mm-dd-yyyy-hh-mm`*`-AM` (or `PM`).

**Figure 13-5 Change Archive Schedule Window**



Archive time: 12:00:00 AM, daily

| Archive Time | Archive Day of Week |
|---|---|
| 12:00:00 AM | Saturday |

● Active as of: 12/11/2001

○ Inactive

## Steps for Changing Archive Schedule

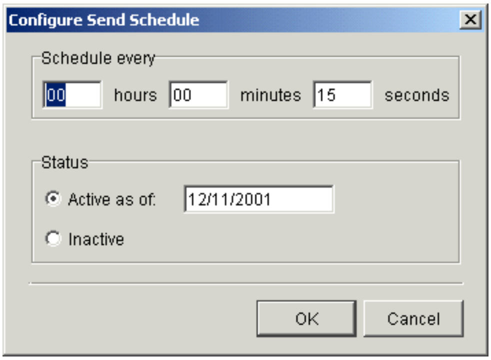
1. Select Tools→Configure Schedule→Archive Schedule in Administrator to open the Configure Archive Schedule window.
2. To change the schedule, change the Archive time values. Type the time you want and select the frequency from the drop-down list. Click Add.
3. To delete part of the schedule, select the times to delete and click Delete. Or, click Delete All to delete the entire schedule. If you delete an entire schedule and do not add one, archiving becomes inactive.
4. To make a schedule inactive without deleting it, click Inactive. You can re-activate the schedule by clicking Active as of. The active as of date is a system-selected date.
5. Click OK to close and save your changes or Cancel to close with saving.

# Configure Send Schedule Window

Use the Configure Send Schedule window to control when WebLogic Integration – Business Connect sends outbound documents to your trading partners. The send schedule does not apply to inbound documents, which are processed as soon as they are received. By default the send schedule is set at 15 seconds. For most users this send interval is adequate.

Select Tools→Configure Schedule→Send Schedule in Administrator to open the Configure Send Schedule window.

**Figure 13-6 Configure Send Schedule Window**



Configure Send Schedule

Schedule every

00 hours 00 minutes 15 seconds

Status

● Active as of: 12/11/2001

○ Inactive

## Field Descriptions

The following describes the fields on the Configure Send Schedule window.

*Schedule every [n] hours [n] minutes [n] seconds*

Set the interval for WebLogic Integration – Business Connect to send documents. Type the interval in hours, minutes and seconds in the corresponding fields. The maximum interval is 99 hours, 59 minutes, and 59 seconds. This field is required.

Allowing a value greater than 24 hours enables you to use intervals that do not match the even-day intervals of the other schedules. For example, you can schedule documents to be sent every 32 hours.

*Status*

Choose one of the following:

Active as of indicates you want WebLogic Integration – Business Connect to use this schedule. WebLogic Integration – Business Connect provides this date, which is the date you make this schedule active. A new schedule is active by default.

Inactive indicates you do not want WebLogic Integration – Business Connect to use this schedule.

# Remove Record Locks Window

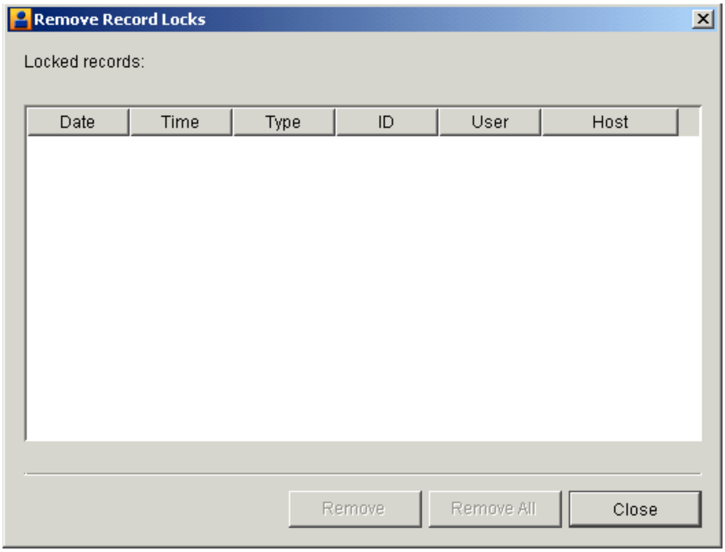
Use the Remove Record Locks window to unlock a record in use by another user. This enables you to make changes to the record even though another user already has accessed it.

When a user opens a record (for example, a company profile), WebLogic Integration – Business Connect locks it to prevent other users from changing it. If another user tries to open the record after the first user has accessed it, WebLogic Integration – Business Connect displays a message that another user has accessed the record and that you can only view but not change it. The remove record locks feature allows you to override this lock on open records.

When the second user, who removed the lock, opens the record, both users can edit it. The first user, who opened the record before the second user unlocked and opened it, does not know that another user has opened the same record. Both users can save changes by clicking OK. If both users change the same field in the record, the change made by the last user to click OK prevails.

Select Tools→Remove Records Lock in Administrator to open the Remove Record Locks window. The window shows information for records in use by other users. If no records are in use, the window is blank. Select the record you want to unlock and click Remove. If you want to unlock all records, click Remove All. Click Close to exit.

**Figure 13-7 Remove Record Locks Window**



## Field Descriptions

The following describes the fields on the Remove Record Locks window.

*Date*

The date the record was locked by another user.

*Time*

The time the record was locked by another user.

*Type*

The type of record.

*ID*

The name of the record.

*User*

The user who is accessing the record.

*Host*

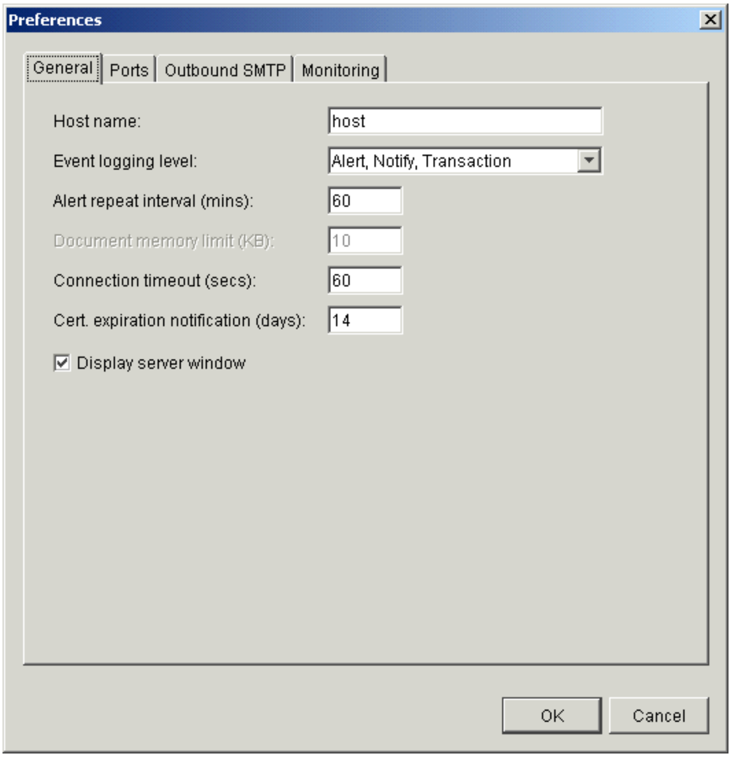
The name of the computer running the Server application.

# Preferences General Tab

Use the Preferences window General tab to set the name of the computer running the Server application, the event logging level, alert message interval, connection time-out interval and certificate expiration notification period.

Select Tools→Preferences in Administrator to open the Preferences window General tab.

**Figure 13-8 Preferences Window General Tab (Windows)**



Host name: host

Event logging level: Alert, Notify, Transaction

Alert repeat interval (mins): 60

Document memory limit (KB): 10

Connection timeout (secs): 60

Cert. expiration notification (days): 14

☑ Display server window

# Field Descriptions

The following describes the fields on the Preferences window General tab.

*Host name*

The fully qualified domain name, registered with the domain name system (DNS), or IP address of the computer where the Server application is running.

*Event logging level*

Select from the drop-down list the message group corresponding to the minimum event levels you want to record in the server log. The following table describes the levels you can set. The number of messages increases the lower you set the level. The lowest level is Alert, Notify, Transaction, Debug.

**Table 13-2 Event Logging Levels**

| Message level | Description |
|---|---|
| **Alert, Notify, Transaction, Debug** | |
| | Select Alert, Notify, Transaction, Debug to log and display all events that occur in WebLogic Integration – Business Connect, including all normal milestones. As the name implies, this level is intended for providing information useful in performing debugging or troubleshooting. If you select this option, application performance decreases. |
| 0 | Debug event |
| **Alert, Notify, Transaction** | |
| | Select Alert, Notify, Transaction to log and display all events level 1 and greater. Events at this level are normal transactions. This is the default.<br>Examples of events at this level include:<br>■ Receiving a certificate in pending status from an S/MIME client<br>■ Receiving an unmatched MDN<br>■ Placing an inbound document in the Other directory |
| 1 | Normal event |

**Table 13-2 Event Logging Levels (Continued)**

| **Message level** | **Description** |
|---|---|
| **Alert, Notify** | |
| | Select Alert, Notify to list all events levels 2, 3 and greater. Level 2 and 3 events are errors that cause WebLogic Integration – Business Connect to send notifications. |
| 2 | Document rejected<br>Examples of level 2 events include when WebLogic Integration – Business Connect rejects a document because there is no active partner or when the application cannot decrypt a document. |
| 3 | General error<br>Examples of level 3 events include when:<br>■ WebLogic Integration – Business Connect receives an MDN that indicates that a partner could not process a document from you<br>■ You try to start WebLogic Integration – Business Connect when it is already running |
| **Alert** | |
| | Select Alert to list all events levels 4-8. Level 4-8 events are errors that cause WebLogic Integration – Business Connect to send alerts. |
| 4 | Connection exception<br>Level 4 events cause WebLogic Integration – Business Connect to send alerts for expected activity. Contact your network administrator for assistance.<br>An example of an event at this level is when WebLogic Integration – Business Connect cannot connect to the network or to a server. |
| 5 | Transport error<br>Level 5 events are problems with the transport configuration in WebLogic Integration – Business Connect. Contact your WebLogic Integration – Business Connect administrator for assistance.<br>An example of such an event is incorrect settings for a transport, such as an incorrect password or mail server. |

**Table 13-2 Event Logging Levels (Continued)**

| Message level | Description |
|---|---|
| 6 | No transport selected<br>Level 6 events are problems with transport configuration.<br>An example of a such an event is when the partner has not selected a transport method. |
| 7 | Unexpected error<br>Level 7 events are errors not accounted for under other levels.<br>Examples of such events are:<br>■ A document could not be packaged (error building the MIME message).<br>■ Configuration data from the database could not be read. |
| 8 | Duplicate server error<br>A level 8 event is a duplicate server error.<br>An example of such an event is when the server is unable to run because the server already is running. |

*Alert repeat interval (mins)*

The interval in minutes WebLogic Integration – Business Connect waits before it sends you the next alert message about the same alert condition. For example, if WebLogic Integration – Business Connect cannot connect to the mail server, it sends you only one alert e-mail about this failure per interval that you specify. The default interval is 60 minutes.

*Connection timeout (secs)*

This is the time-out value in seconds for any TCP/IP connection.

*Cert. expiration notification (days)*

This is the number of days before an active company certificate expires that the system will issue an alert message warning of the upcoming expiration date. This warning is intended to provide time to replace the certificate before an expired certificate can interrupt trading. The system issues only one alert for a certificate about to expire.

Alerts for certificates about to expire are issued only for active certificates for active company profiles and for active certificates for the WebLogic

Integration – Business Connect API HTTPS server and SOAP-RPC HTTPS server. Alerts are not issued for partner certificates. Alert messages are reported on the Alerts information viewer in Tracker. Alert messages also are sent by e-mail if a notify e-mail address is specified on the Company Profile window Preferences tab.

The Server application must be running for certificate expiration date checking to take place. The Server checks upon start-up and once every 24 hours thereafter.

*Display server window (Windows only)*

Select this check box to display the Server Display window while the Server application is running. This is the default and recommended setting.

If you change the selection, you must restart the Server for the change to take effect.

*Browser path (UNIX only)*

If you previously specified a browser, this field shows the path to your Internet browser. You use a browser to view the online help and to obtain certificates from third-party certificate authorities.

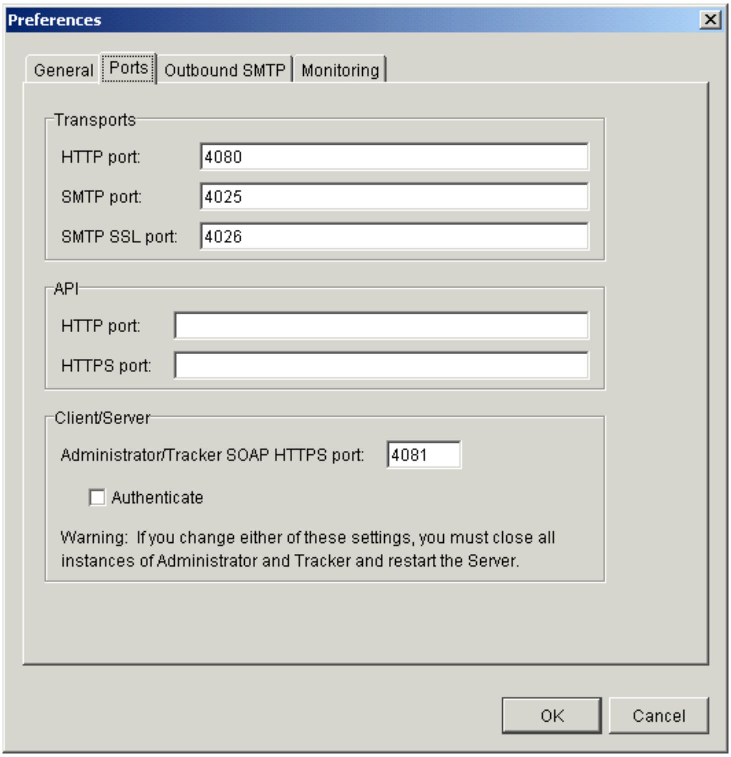
To set or change the browser path, click Browse to open the Browse dialog box. Type the path of the executable file for the browser and click OK to return to the General tab.

# Preferences Ports Tab

Use the Preferences window Ports tab to view or change ports WebLogic Integration – Business Connect uses.

Select Tools→Preferences in Administrator to open the Preferences window General tab. Click Ports to open the Ports tab.

**Figure 13-9 Preferences Window Ports Tab**



Transports

HTTP port: 4080

SMTP port: 4025

SMTP SSL port: 4026

API

HTTP port:

HTTPS port:

Client/Server

Administrator/Tracker SOAP HTTPS port: 4081

☐ Authenticate

Warning: If you change either of these settings, you must close all instances of Administrator and Tracker and restart the Server.

# Field Descriptions

The following describes the fields on the Preferences window Ports tab.

*Transports*

The following port fields are for document transports.

*HTTP port*

The port where the WebLogic Integration – Business Connect HTTP server is listening for inbound documents from the remote trading partner’s HTTP client. The default is 4080.

*SMTP port*

The number of the port that the WebLogic Integration – Business Connect internal SMTP server listens to for inbound documents that are sent via the SMTP transport. The default is 4025.

*SMTP SSL server port*

The number of the port that the WebLogic Integration – Business Connect internal SMTP server listens to for inbound documents that are sent via the SMTP transport with SSL engaged. The default is 4026.

*API*

The following fields are for communications with a remote application program interface (API) client. To communicate with an API client via HTTPS you must also complete a number of other configuration tasks. See "API HTTPS Security" on page 14-8.

*HTTP port*

The port for a remote API client communicating by way of an HTTP server.

*HTTPS port*

The port for a remote API client communicating by way of an HTTPS server.

If you use the API HTTPS port for integration, you must generate or load a certificate for the HTTPS server using the certloader tool. See "Certificate Tool (certloader)" on page 14-14.

*Client/Server*

The following fields are for communication between WebLogic Integration – Business Connect Server and the client applications Administrator and Tracker.

*Administrator/Tracker SOAP HTTPS port*

The number of the port for the SOAP HTTPS server that is built into WebLogic Integration – Business Connect. Administrator and Tracker use this port to securely send updates to the Server application. For details see "SOAP-RPC HTTPS Security" on page 14-2.

If you change this value, you must close Administrator and Tracker and restart the Server application for the change to become effective.

*Authenticate*

Select this check box only if you want the Server application to authenticate a certificate for Administrator and Tracker. For details see "SOAP-RPC HTTPS Security" on page 14-2.

If you change this value, you must close Administrator and Tracker and restart the Server application for the change to become effective.

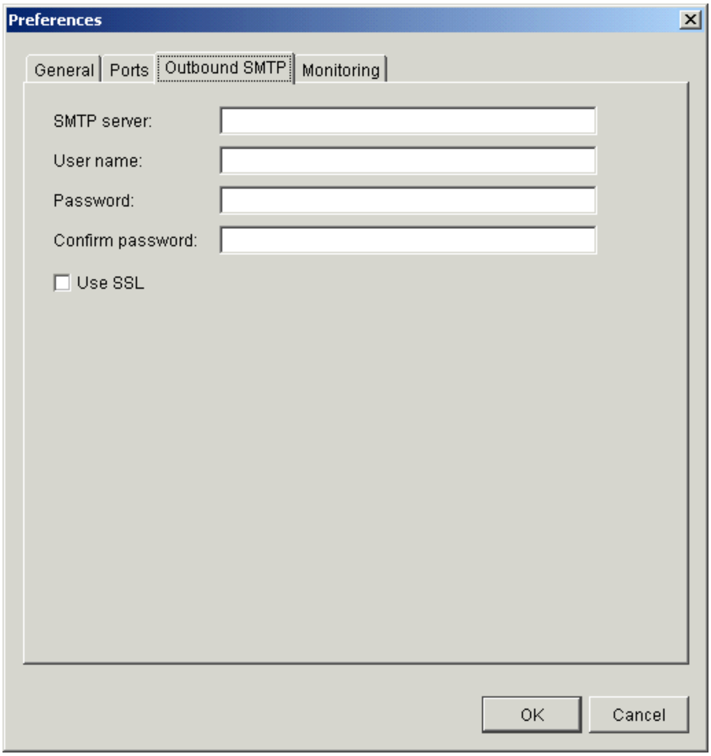
# Preferences Outbound SMTP Tab

Use the Preferences window Outbound SMTP tab to designate one SMTP server for sending documents to all partners via the POP transport (SMTP/POP). The information on this tab is used on the Partner Profile window Outbound Protocols tab for the POP transport for the partner profiles you import or create. You must first complete the Preferences window Outbound SMTP tab before importing or creating partner profiles for the information on this tab to become part of the POP transport configuration.

If you want to use different SMTP servers for sending documents to different partners, you have two options. You can complete the Outbound SMTP tab, create or import the partner profile, and then type new values in the SMTP server field on the POP Transport Options window, which is accessed from the Partner Profile window Outbound Protocol tab. Or, you can leave the Outbound SMTP tab blank and add the SMTP server information in the POP configuration for the partner profile.

Select Tools→Preferences in Administrator to open the Preferences window General tab. Click Outbound SMTP to open the Outbound SMTP tab.

**Figure 13-10 Preferences Window Outbound SMTP Tab**



## Field Descriptions

The following describes the fields on the Preferences window Outbound SMTP tab.

*SMTP server*

Type the fully qualified domain name or IP address of the server used for sending documents to partners by POP (SMTP/POP).

*User name*

Type the user name for the server.

*Password*

Type the password for the user.

*Confirm password*

Type the password again.

*Use SSL*

Select this check box to use Secure Sockets Layer protocol.

# Preferences Monitoring Tab

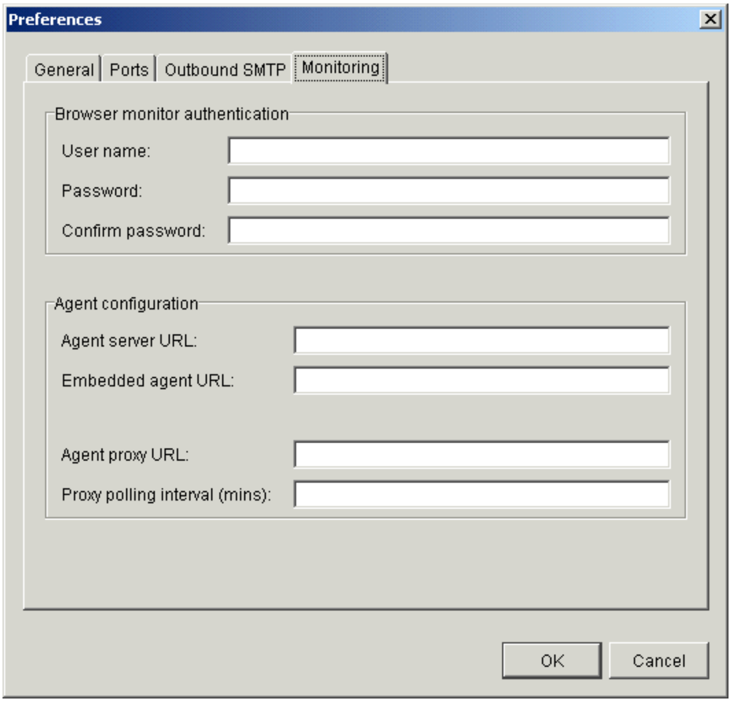
Use the Preferences window Monitoring tab to set a user name and password that authorizes a user to open the WebLogic Integration – Business Connect server monitor page.

Select Tools→Preferences in Administrator to open the Preferences window General tab. Click Monitoring to open the Monitoring tab.

The server monitor page is opened in an Internet browser by selecting Tools→Launch Server Monitor in Administrator or Tracker. The page displays information about Server activities, including document trading data and events. For more information about the page see “Monitoring the Server with a Browser” on page 6-7.

You can set a user name and password that can be used by a single user or that can be shared by two or more users, depending on your organization’s security practices. If you do not set a user name and password, any user can access the server monitor page.

**Figure 13-11 Preferences Window Monitoring Tab**



Preferences

General | Ports | Outbound SMTP | Monitoring

Browser monitor authentication

User name:

Password:

Confirm password:

Agent configuration

Agent server URL:

Embedded agent URL:

Agent proxy URL:

Proxy polling interval (mins):

OK | Cancel

# Field Descriptions

**Note:** The Agent Configuration fields are associated with an unsupported feature. Ignore these fields.

The following describes the fields on the Preferences window Monitoring tab.

*Browser monitor authentication*

The following fields are for setting an optional user name and password for using the Launch Server Monitor option on the Tools menu for monitoring Server application activity on a browser.

*User name*

Type the name of the user who is authorized to access the server monitor page.

*Password*

Type a password for the user.

*Confirm password*

Type the password again.

CHAPTER

# 14 Application Security

The following topics describe available security features for communications between the WebLogic Integration – Business Connect Server application and client applications.

**Concepts**

- "SOAP-RPC HTTPS Security" on page 14-2
- "API HTTPS Security" on page 14-8

**Procedures**

- "Configuring Administrator and Tracker to Authenticate the SOAP-RPC Server" on page 14-5
- "Configuring the SOAP-RPC Server to Authenticate Administrator or Tracker" on page 14-6
- "Configuring an API Client to Use HTTPS" on page 14-11
- "Configuring an API Client to Authenticate the API Server" on page 14-12
- "Configuring the API Server to Authenticate an API Client" on page 14-13

**Tools**

- "Certificate Tool (certloader)" on page 14-14
- "SOAP Configuration Tool (soapconfig)" on page 14-19

# SOAP-RPC HTTPS Security

WebLogic Integration – Business Connect uses Simple Object Access Protocol (SOAP) to enable the the Administrator and Tracker applications to securely send updates to the Server application. WebLogic Integration – Business Connect uses a built-in server for this purpose called the SOAP-RPC HTTPS server.

SOAP is a message-based protocol for accessing services on the Internet. SOAP uses XML syntax to send text commands across the Internet using HTTP. For more information about SOAP, see http://www.w3.org/TR/SOAP/. RPC stands for remote procedure call, which is a common protocol for the client-server model of distributed systems.

The SOAP-RPC HTTPS server has a certificate with a pubic-private key pair. For brevity, this is referred to as the RPC certificate. By default, this is a self-signed certificate with a life of five years that is generated upon installing WebLogic Integration – Business Connect. You can replace the certificate either with another self-signed certificate or with a certificate obtained from a third-party certificate authority. For details see “Certificate Tool (certloader)” on page 14-14.

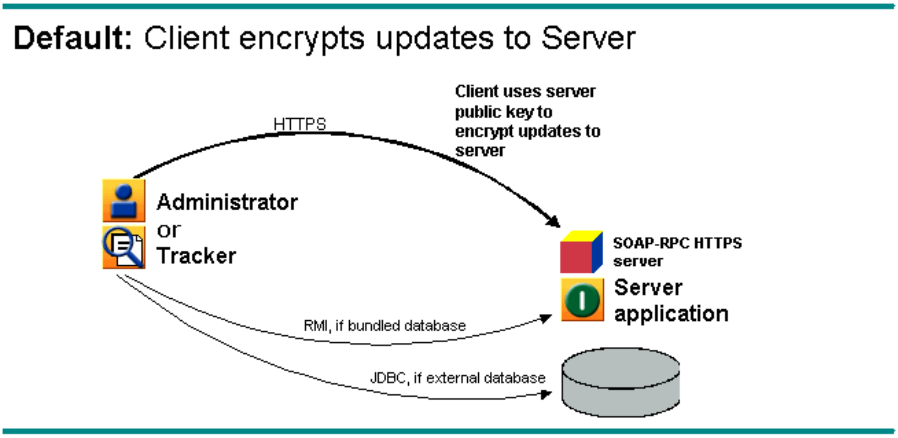
## Default SOAP-RPC HTTPS Security

Administrator and Tracker use the public key in the RPC certificate to encrypt updates to the WebLogic Integration – Business Connect Server application by way of the SOAP-RPC HTTPS server. This security occurs by default; you do not have to do anything to enable it.

Triple DES is the default encryption strength for the SOAP-RPC HTTPS server. Triple DES has a key length of 168 bits.

Figure 14-1 illustrates the default security for the SOAP-RPC HTTPS server.

**Figure 14-1 Default SOAP-RPC HTTPS Server Security**


**Default:** Client encrypts updates to Server
HTTPS
Client uses server public key to encrypt updates to server
Administrator or Tracker
SOAP-RPC HTTPS server
Server application
RMI, if bundled database
JDBC, if external database

## Optional SOAP-RPC HTTPS Security

Two additional, optional layers of security for authenticating certificates are available:

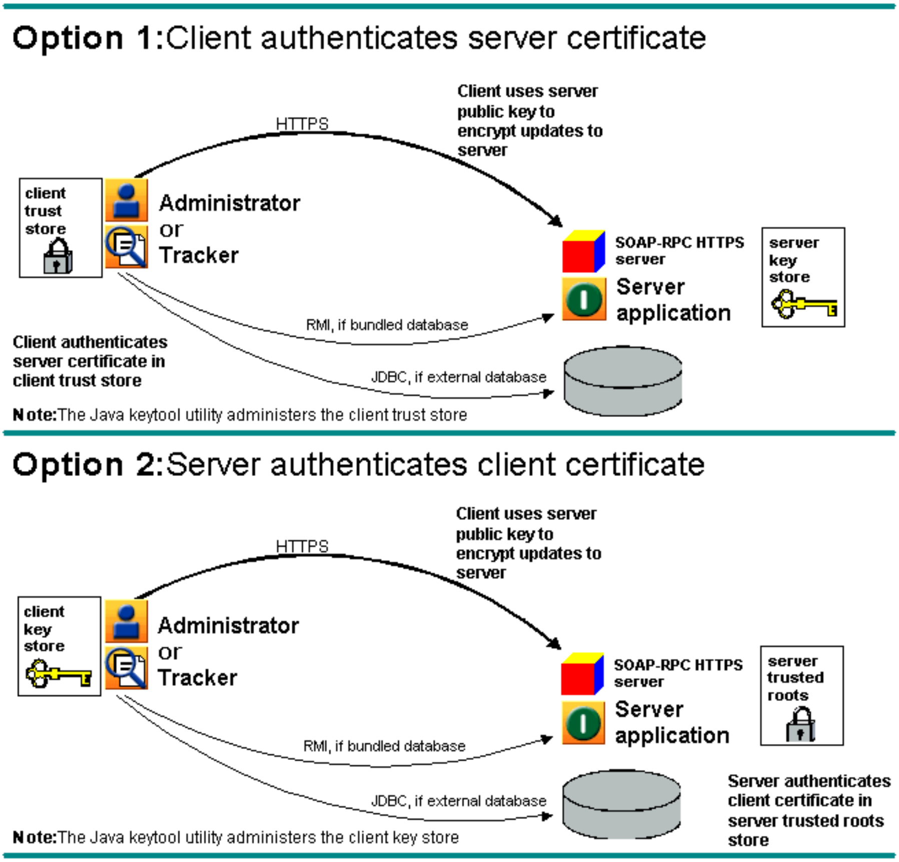
- Configure Administrator and Tracker to authenticate the RPC certificate. This validates that Administrator and Tracker are communicating with the authorized Server application. This authentication requires that you obtain a CA certificate for the Server application.

- Configure the Server application to authenticate a certificate owned by Administrator and Tracker. This validates that the Server application is communicating with the authorized Administrator and Tracker. This authentication requires that you obtain a CA certificate for each client computer running Administrator and Tracker.

Configuration for authenticating certificates requires knowledge of Java tools, particularly keytool, which is a key and certificate management utility. It also requires using the WebLogic Integration – Business Connect certloader and soapconfig tools. For details see "Certificate Tool (certloader)" on page 14-14 and "SOAP Configuration Tool (soapconfig)" on page 14-19.

Figure 14-2 illustrates the optional security for the SOAP-RPC HTTPS server.

**Figure 14-2 Optional SOAP-RPC HTTPS Server Security**


Option 1:Client authenticates server certificate
HTTPS
Client uses server public key to encrypt updates to server
client trust store
Administrator or Tracker
SOAP-RPC HTTPS server
Server application
server key store
RMI, if bundled database
JDBC, if external database
Client authenticates server certificate in client trust store
Note:The Java keytool utility administers the client trust store
Option 2:Server authenticates client certificate
HTTPS
Client uses server public key to encrypt updates to server
client key store
Administrator or Tracker
SOAP-RPC HTTPS server
Server application
server trusted roots
RMI, if bundled database
JDBC, if external database
Server authenticates client certificate in server trusted roots store
Note:The Java keytool utility administers the client key store

# Configuring Administrator and Tracker to Authenticate the SOAP-RPC Server

Use this procedure to configure Administrator and Tracker to authenticate a CA certificate for the SOAP-RPC HTTPS server. This authentication validates that the remote Administrator and Tracker applications are communicating with the authorized WebLogic Integration – Business Connect Server application. For details about such authentication, see "Optional SOAP-RPC HTTPS Security" on page 14-3.

## Steps

1. Obtain a digital certificate with a public-private key pair from a certificate authority. Export the certificate from your browser or mail client to a file with an extension of `p12`. The private key must be exported with the file. Export the certificate to include the entire certificate chain.

2. Use the certloader tool to import the CA certificate to the WebLogic Integration – Business Connect keystore. The certificate you import will replace the current RPC certificate. Use the following format:

   ```
   certloader -rpc -l filename password
   ```

   You will use the password again in step 7.

   For details about the tool, see "Certificate Tool (certloader)" on page 14-14.

3. Use the Java keytool to create a truststore on the client computer that runs Administrator and Tracker. This truststore cannot be the `keys.db` file found in the WebLogic Integration – Business Connect keys directory; it must be another file. If you use Administrator and Tracker on more than one client, you must create a truststore for each computer.

   See Sun Microsystems Java documentation for information about using keytool.

4. Use the Java keytool `-import` option to import the certificate and public key to the client truststore. If you use more than one client, you must import the certificate and public key to the truststore of each computer.

5. Use a text editor such as Notepad to open the `DB.properties` file in the WebLogic Integration – Business Connect installation directory. Scroll to Section 3: Miscellaneous Settings. Type `true` after the `SOAP.Admin.CheckTrust= property`.

6. Save and close the `DB.properties` file.

7. Use the SOAP configuration tool to set the client truststore path and truststore password in the `DB.properties` file.

   If you are using the tool from a command line, use the following format:

   ```
   soapconfig -ts truststore -tp truststorepassword
   ```

   If are using the tool's graphical user interface, complete the following fields: Trust store, Trust store password and Confirm trust store password.

   Use the same password as the one used to import the certificate to the WebLogic Integration – Business Connect keystore in step 2.

   For details about the tool, see "SOAP Configuration Tool (soapconfig)" on page 14-19.

8. Restart the WebLogic Integration – Business Connect Server application.

# Configuring the SOAP-RPC Server to Authenticate Administrator or Tracker

Use this procedure to configure the WebLogic Integration – Business Connect Server application to authenticate a CA certificate for Administrator and Tracker. This authentication validates that the Server application is communicating with the authorized remote Administrator and Tracker applications via the SOAP-RPC HTTPS server. For details about such authentication, see "Optional SOAP-RPC HTTPS Security" on page 14-3.

## Steps

1. Request a CA certificate by using the Java keytool to generate a certificate signing request (CSR) with the `-certreq` command and sending the CSR to the CA.

   See Sun Microsystems Java documentation for information about using keytool.

2. Use the Java keytool to create a keystore on the client computer that runs Administrator and Tracker. This keystore cannot be the `keys.db` file found in the WebLogic Integration – Business Connect keys directory; it must be another file. If you use Administrator and Tracker on more than one client, you must create a keystore for each computer.

3. Once the CA has issued the certificate, use the keytool -import command to import the certificate to the client keystore.

4. Use Administrator to make sure the root of the CA certificate is trusted. Select Tools→Certificates→Trusted Roots to open the Trusted Roots window. Scroll through the list of trusted roots. It is possible that the root of the CA certificate already is trusted. If not, import the root underlying the certificate and trust it. See "Trusted Roots" on page 11-51.

5. Use the SOAP configuration tool to set the client keystore path and keystore password in the `DB.properties` file.

   If you are using the tool from a command line, use the following format:

   ```
   soapconfig -ks keystore -kp keystorepassword
   ```

   If are using the tool's graphical user interface, complete the following fields: Key store, Key store password and Confirm key store password. The password is the one you used to export the certificate to a `p12` file from a browser or mail client.

   For details about the tool, see "SOAP Configuration Tool (soapconfig)" on page 14-19.

6. In Administrator, select Tools→Preferences and click the Ports tab. Below the SOAP HTTPS server port field, select the Authenticate check box. Click OK to save the change and close the window.

7. Restart the WebLogic Integration – Business Connect Server application.

# API HTTPS Security

WebLogic Integration – Business Connect supports communicating with an application program interface (API) client by way of HTTP and HTTPS servers that are built into the application.

Communicating by way of the HTTP server with an API client does not require special configuration, beyond specifying the API HTTP port on the Ports tab, which is accessed by selecting Tools→Preferences in Administrator.

Using the HTTPS server, however, requires additional configuration and is explained in the following topics:

- "API Security Summary"
- "Optional API Security"

## API Security Summary

WebLogic Integration – Business Connect supports an API client communicating with the Server application. WebLogic Integration – Business Connect has two built-in servers for this purpose. One is an HTTP server. The other is an HTTPS server. The API HTTPS server enables an API client to use a public key to securely encrypt messages to the Server application.

The API HTTPS server must be used with a certificate and a pubic-private key pair. For brevity, this is referred to as the API certificate. This can be a self-signed certificate or a certificate obtained from a third-party certificate authority. For details see "Certificate Tool (certloader)" on page 14-14.

# Optional API Security

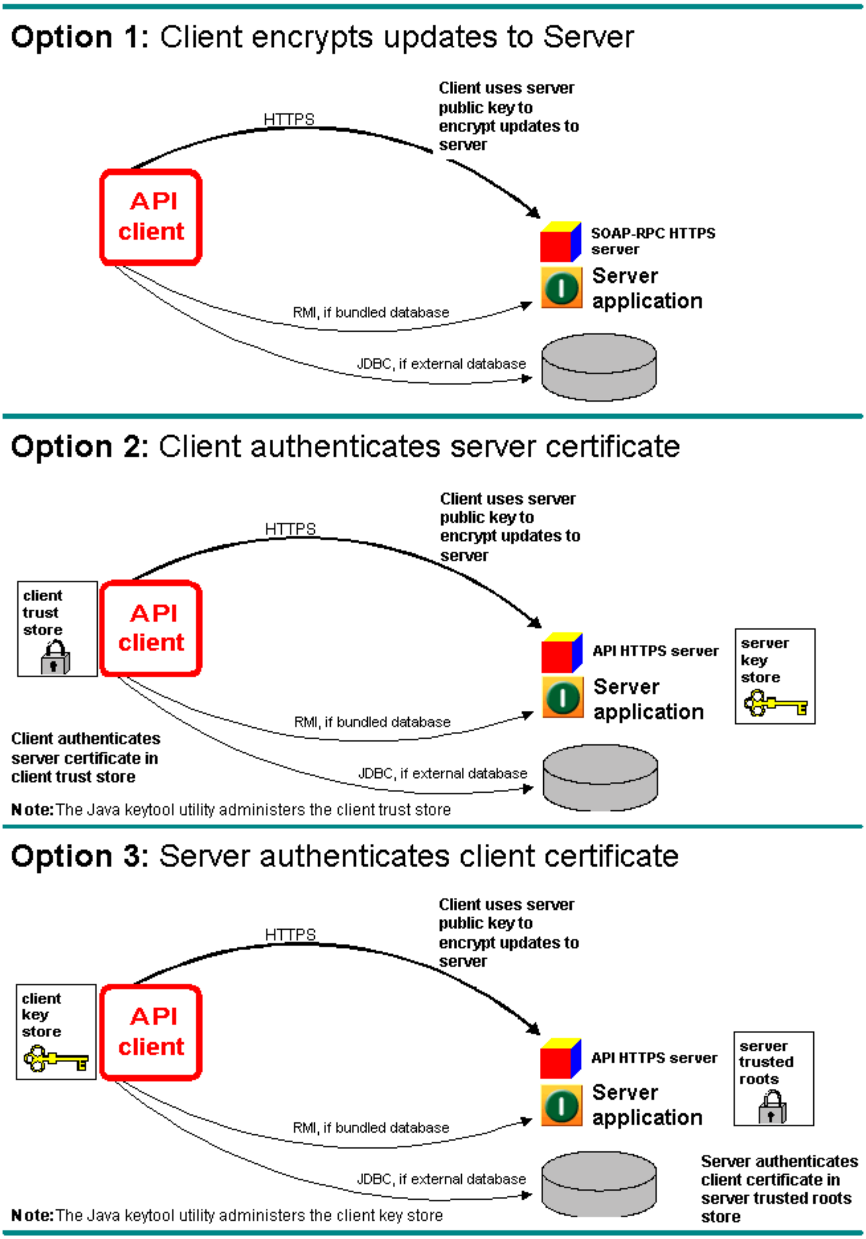
WebLogic Integration – Business Connect supports three security options for communicating with an API client by way of HTTPS, which is HTTP over Secure Sockets Layer protocol. They are:

- Enable the API client to communicate securely with the WebLogic Integration – Business Connect Server application. The API client uses the public key in the API certificate to encrypt messages to the Server application.
- Configure the API client to authenticate the API certificate. This validates that the API client is communicating with the authorized Server application. This authentication requires that you obtain a CA certificate for the Server application.
- Configure the Server application to authenticate a certificate owed by the API client. This validates that the Server application is communicating with the authorized API client. This authentication requires that you obtain a CA certificate for the API client.

Implementing these security options requires knowledge of Java tools, particularly keytool, which is a key and certificate management utility. It also requires using the WebLogic Integration – Business Connect certloader tool. For details see “Certificate Tool (certloader)” on page 14-14.

Figure 14-3 illustrates the optional security for the API HTTPS server.

**Figure 14-3 Optional API HTTPS Server Security**


Option 1: Client encrypts updates to Server
HTTPS
Client uses server public key to encrypt updates to server
API client
SOAP-RPC HTTPS server
Server application
RMI, if bundled database
JDBC, if external database
Option 2: Client authenticates server certificate
HTTPS
Client uses server public key to encrypt updates to server
client trust store
API client
API HTTPS server
Server application
server key store
RMI, if bundled database
JDBC, if external database
Client authenticates server certificate in client trust store
Note: The Java keytool utility administers the client trust store
Option 3: Server authenticates client certificate
HTTPS
Client uses server public key to encrypt updates to server
client key store
API client
API HTTPS server
Server application
server trusted roots
RMI, if bundled database
JDBC, if external database
Server authenticates client certificate in server trusted roots store
Note: The Java keytool utility administers the client key store

# Configuring an API Client to Use HTTPS

Use this procedure to configure the API client to use the public key in the API certificate to encrypt messages to the WebLogic Integration – Business Connect Server application. For details about this security, see "API HTTPS Security" on page 14-8.

## Steps

1. Generate or obtain an API certificate for the API HTTPS server. See "Certificate Tool (certloader)" on page 14-14.

2. In Administrator set the HTTPS port that the API client and the Server application will use. The port is set on the Ports tab, which is accessed by selecting Tools→Preferences. See "Preferences Ports Tab" on page 13-23.

3. Point the API client at the correct port and host running the WebLogic Integration – Business Connect Server application. Include the `jsse.jar` file in the API client's class path. The file is in the WebLogic Integration – Business Connect lib directory.

4. In configuring the API client, see the sample code for the Java classes AlwaysTrustManager and AlwaysTrueVerifier. The sample code is in the WebLogic Integration – Business Connect API directory.

   The API client should use AlwaysTrustManager as the trust manager and AlwaysTrueVerifier as the host name verifier. AlwaysTrustManager will trust all certificates returned from the server. AlwaysTrustManager is required because the server's certificate is not included in the client's keystore. AlwaysTrueVerifier will allow mismatch of the host name of the request and the common name in the certificate. AlwaysTrueVerifier might be required because of the nature of the self-signed certificate being used. The self-signed certificate is generated upon installation using the host name of the server. A server can have multiple host names. So the host name the API client is connecting with might not be the host name in the generated certificate.

5. Restart the WebLogic Integration – Business Connect Server application.

# Configuring an API Client to Authenticate the API Server

Use this procedure to configure an API client to authenticate a CA certificate for the API HTTPS server. This authentication validates that the remote API client is communicating with the authorized WebLogic Integration – Business Connect Server application. For details about such authentication, see "Optional API Security" on page 14-9.

You must first configure the API client to use the API HTTPS server before you can do this procedure. See "Configuring an API Client to Use HTTPS" on page 14-11.

## Steps

1. Do this step if the API certificate is a self-signed certificate. Obtain a digital certificate with a public-private key pair from a certificate authority. Export the certificate from your browser or mail client to a file with an extension of `p12`. The private key must be exported with the file. Export the certificate to include the entire certificate chain.

   Use the certloader tool to import the CA certificate to the WebLogic Integration – Business Connect keystore. The certificate you import will replace the current API certificate. Use the following format:

   ```
   certloader -api -l filename password
   ```

   For details about the tool, see "Certificate Tool (certloader)" on page 14-14.

2. Use the Java keytool to create a truststore on the computer that runs the API client. This truststore cannot be the `keys.db` file found in the WebLogic Integration – Business Connect keys directory; it must be another file.

   See Sun Microsystems Java documentation for information about using keytool.

3. Use the Java keytool `-import` option to import the certificate and public key to the client truststore.

   The API client should not use the Java classes AlwaysTrustManager and AlwaysTrueVerifier.

4. Restart the WebLogic Integration – Business Connect Server application.

# Configuring the API Server to Authenticate an API Client

Use this procedure to configure the WebLogic Integration – Business Connect Server application to authenticate a CA certificate for the API client. This authentication validates that the Server application is communicating with the authorized remote API client. For details about such authentication, see “Optional API Security” on page 14-9.

You must first configure the API client to use the API HTTPS server before you can do this procedure. See “Configuring an API Client to Use HTTPS” on page 14-11.

## Steps

1. Request a CA certificate by using the Java keytool to generate a certificate signing request (CSR) with the `-certreq` command and sending the CSR to the CA.

   See Sun Microsystems Java documentation for information about using keytool.

2. Use the Java keytool to create a keystore on the computer that runs the API client. This keystore cannot be the `keys.db` file found in the WebLogic Integration – Business Connect keys directory; it must be another file.

3. Once the CA has issued the certificate, use the keytool -import command to import the certificate to the client keystore.

4. Use Administrator to make sure the root of the CA certificate is trusted. Select Tools→Certificates→Trusted Roots to open the Trusted Roots window. Scroll through the list of trusted roots. It is possible that the root of the CA certificate already is trusted. If not, import the root underlying the certificate and trust it. See “Trusted Roots” on page 11-51.

5. Restart the WebLogic Integration – Business Connect Server application.

# Certificate Tool (certloader)

Certloader is a command line utility that can perform tasks for enhancing application security. It can generate self-signed certificates containing public-private encryption key pairs. It also can load a certificate containing a public-private key pair that was generated by a third-party certificate authority.

Certloader is used for managing certificates used by two HTTPS servers that are built into WebLogic Integration – Business Connect:

- The SOAP-RPC HTTPS server owns the RPC certificate. This bundled server enables Administrator and Tracker to communicate securely with the WebLogic Integration – Business Connect Server application. Administrator and Tracker use the certificate's public key to encrypt updates to the Server application. A self-signed RPC certificate is generated upon installing WebLogic Integration – Business Connect and stored in the application's keystore.
- The API HTTPS server owns the API certificate. This bundled server enables API clients to communicate securely with the WebLogic Integration – Business Connect Server application. An API client uses the certificate's public key to encrypt messages to the Server application. WebLogic Integration – Business Connect support of API clients is an optional feature. If you want to use the API HTTPS server, you must use certloader to either generate a self-signed certificate or load a certificate obtained from a certificate authority.

In addition to generating self-signed certificates, certloader can import P12 certificate files containing public-private key pairs that have been obtained from a certificate authority. CA certificates are recommended as the API and RPC certificates when you want the client to authenticate the server certificate or the server to authenticate the client certificate or both. For details see "SOAP-RPC HTTPS Security" on page 14-2 and "API HTTPS Security" on page 14-8.

You cannot use certloader to delete a certificate used by the API HTTPS server or SOAP-RPC HTTPS server.

The following topics are provided about certloader:

- "The Default RPC Certificate" on page 14-15
- "Using certloader" on page 14-16
- "Description of certloader Parameters" on page 14-17

# The Default RPC Certificate

During installation, WebLogic Integration – Business Connect uses the name of the host computer for the Server application and the company name you enter to generate the initial RPC certificate. This is a self-signed certificate. Default values are used for the length of the public-private key and the certificate expiration date. Other values are blank by default.

Listing 14-1 shows the information for a default RPC certificate. "Using certloader" on page 14-16 explains how to display the certificate information using the `certloader` command. The certificate also is in the WebLogic Integration – Business Connect trusted roots store. You can view the certificate's information by selecting Tools→Certificates→Trusted Roots in Administrator.

**Listing 14-1 Default RPC Certificate**

```
Name: WORLDWIDE
E-mail address:
Commany: Worldwide Trading
Department:
City:
ISO country code:
Serial number: 5294f5ece4299c75710582f441b6f63a
Algorithm: sha1WithRSAEncryption
Key length: 512
Valid from: Tue Aug 21 10:13:53 MST 2001
Valid to: Mon Aug 21 10:13:53 MST 2006
MD5 Fingerprint: CA:A2:34:28:CB:0D:CD:64:4E:CE:FD:4F:5B:B9:D4:57

Issuer: O=Worldwide Trading, CN=WORLDWIDE
```

Administrator and Tracker use the public key in the RPC certificate to communicate with the Server application; you do not have to configure this.

# Using certloader

The following shows the usage of certloader and its parameters. The words following parameters are the names of variables that are used with the associated parameter. This command is executed in a console or command window.

- Display help about parameters:

  ```
  certloader -?|-help
  ```

- Generate a self-signed certificate for the API HTTPS server or SOAP-RPC HTTPS server:

  ```
  certloader -api|-rpc -g [-c common name] [-o organization
  name] [-u organization unit name] [-loc locality name]
  [-cty country code] [-e e-mail address] [-len 512|1024|2048]
  [-v number[d|m|y]]
  ```

- Load a CA certificate in the WebLogic Integration – Business Connect keystore for the API HTTPS server or SOAP-RPC HTTPS server:

  ```
  certloader -api|-rpc -l filename password
  ```

- Display information about the certificate for the API HTTPS server or SOAP-RPC HTTPS server:

  ```
  certloader -api|-rpc -dump
  ```

Typing `certloader` without a parameter generates an error message. The command must be used with parameters to function.

# Description of certloader Parameters

The certloader parameters are described in the following table.

**Table 14-1 certloader Parameters**

| Parameter | Description |
|---|---|
| `-?, -help` | Displays information about the `certloader` command and its parameters. |
| `-api` | Generates a self-signed certificate, loads a CA certificate or displays information about a certificate. The certificate is used by the API HTTPS server that is within the application.<br>This parameter must be used with other parameters. It cannot be used alone with the `certloader` command. |
| `-rpc` | Generates a self-signed certificate, loads a CA certificate or displays information about a certificate. The certificate is used by the SOAP-RPC HTTPS server that is within the application.<br>This parameter must be used with other parameters. It cannot be used alone with the `certloader` command. |
| `-g` | Generates a self-signed certificate for the API HTTPS server or the SOAP-RPC HTTPS server. This parameter must be preceded by -api or -rpc.<br>You must restart the Server application for the new certificate to become active. The newly active certificate replaces the previous certificate. |
| `-c common name` | This optional parameter is used after -g to create a common name for a self-signed certificate. Common name is a certificate term for the name of a person. This can be the name of the person who generates or owns the certificate. If you do not use this parameter, the name of the host running the Server application is used. |

**Table 14-1 certloader Parameters (Continued)**

| Parameter | Description |
|---|---|
| `-o organization name` | This optional parameter is used after -g to create an organization name for a self-signed certificate. This usually is your company name. If you do not use this parameter, the name of the application's registered user is used. |
| `-u organization unit name` | This optional parameter is used after -g to create an organization unit name for a self-signed certificate. This usually is the name of a department or division within the company. If you do not use this parameter, the value is blank. |
| `-loc locality name` | This optional parameter is used after -g to create a locality name for a self-signed certificate. This usually is a city name. If you do not use this parameter, the value is blank. |
| `-cty country code` | This optional parameter is used after -g to create a two-letter ISO country code for a self-signed certificate. For example, us is United States. If you do not use this parameter, the value is blank. |
| `-e e-mail address` | This optional parameter is used after -g, to create an e-mail address for a self-signed certificate. If you do not use this parameter, the value is blank. |
| `-len 512\|1024\|2048` | This optional parameter is used after -g to create a key pair of a specified length for a self-signed certificate. You can specify 512, 1024 or 2048. If you do not use this parameter, a key length of 512 is generated. |
| `-v number[d\|m\|y]` | This optional parameter is used after `-g` to create an expiration date for a self-signed certificate.<br>Certloader calculates the expiration date based on the number of days, months or years from today's date that you want the certificate to expire. For example, `-v10d` specifies that the expiration date is 10 days from today's date.<br>If you do not use this parameter, the expiration date is five years from today's date. |

**Table 14-1 certloader Parameters (Continued)**

| Parameter | Description |
|---|---|
| `-l filename password` | Loads a P12 formatted CA certificate file containing a public-private key pair. You must specify the name of the file and the password protecting the keys.<br>You must restart the Server application for the new certificate to become active. The newly active certificate replaces the previous certificate. |
| `-dump` | Displays information about the API HTTPS server certificate or the SOAP-RPC HTTPS server certificate. This parameter must be preceded by -api or -rpc. |

# SOAP Configuration Tool (soapconfig)

The soapconfig tool, which is in the application's bin directory, configures the SOAP truststore and keystore settings for communications between Administrator and Tracker and the Server application. You use the soapconfig tool when setting up the certificate authentication security options described in "Optional SOAP-RPC HTTPS Security" on page 14-3 or "Optional API Security" on page 14-9.

Using the soapconfig tool is a step in setting up a truststore or keystore or both for each client computer running Administrator and Tracker. The truststore and keystore actually are set up using the Java keytool. The soapconfig tool is used to point Administrator and Tracker to the truststore or keystore that keytool was used to create. The properties soapconfig manages are in the `DB.properties` file in the WebLogic Integration – Business Connect installation directory.

Keytool manages a keystore of private keys and their associated X.509 certificate chains authenticating the corresponding public keys. It also manages certificates from trusted entities. For information about keytool see http://java.sun.com/.

You can use the soapconfig tool with a graphical user interface or from a command line. The following topics explain how to use it both ways:

- "Using soapconfig as a Command Line Tool" on page 14-21
- "Using soapconfig with the User Interface" on page 14-22

After using soapconfig, you must restart the Server application for the changes to become effective.

Listing 14-2 shows the section of the `DB.properties` file that the soapconfig tool manipulates. Specifically, the tool affects some of the properties that begin with the words `SOAP.Admin`. We recommend that you use the soapconfig tool to change these settings and do not directly edit the `DB.properties` file, unless advised to do so. The soapconfig tool encrypts the password settings and direct editing does not.

**Listing 14-2 DB.properties File**

```
// SECTION 3: MISCELLANEOUS SETTINGS

Cyclone.client.browser=unknown
RMI.Port=
RMIServer=
Debug=0
// SOAP.* settings  used by Administrator and Tracker when
communicating with
// the controller. These values are not used by the Controller when
// initializing the SOAP Server. The Controller values are set
inside the
// Administrator under Tools-Preferences.
SOAP.Admin.Host=
SOAP.Admin.Port=
SOAP.Admin.CheckTrust=
SOAP.Admin.TrustStore=
SOAP.Admin.TrustStorePassword=
SOAP.Admin.KeyStore=
SOAP.Admin.KeyStorePassword=
```

# Using soapconfig as a Command Line Tool

The following shows the usage of soapconfig and its parameters as a command line tool. The words following parameters are the names of variables that are used with the associated parameter.

- Display help about parameters:

  ```
  soapconfig -?|-h|-help
  ```

- Change truststore settings in the `DB.properties` file that are used by Administrator and Tracker:

  ```
  soapconfig [-ts truststore] [-tp truststorepassword] [-ks
  keystore] [-kp keystorepassword]
  ```

Typing `soapconfig` without a parameter opens the Soap Configuration window. This user interface is an alternative to using soapconfig as command line utility. See "Using soapconfig with the User Interface" on page 14-22.

**Note:** Before you use the soapconfig tool, use the Java keytool to create the truststore or keystore or both for Administrator and Tracker.

## Description of Command Line Parameters

The soapconfig parameters are described in the following table.

**Table 14-2 soapconfig Parameters**

| Parameter | Description |
|---|---|
| `-?, -h, -help` | Displays information about the `soapconfig` command and its parameters. |
| `-ts truststore` | The name of the Administrator and Tracker truststore that was created with keytool. A truststore is a keystore that is used to make decisions about trusting entities. A truststore contains trusted certificates information, but not private information. |
| `-tp truststorepassword` | The truststore password. |

**Table 14-2 soapconfig Parameters (Continued)**

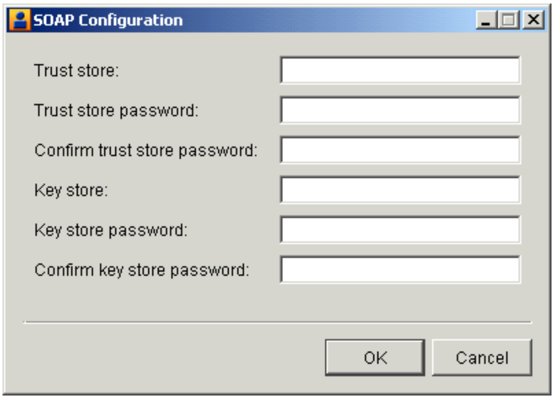
| Parameter | Description |
|---|---|
| `-ks keystore` | The name of the Administrator and Tracker keystore that was created with keytool. A keystore is a database of key information that is used for authentication and data integrity. A keystore contains private information, including private keys. |
| `-kp keystorepassword` | The keystore password. |

# Using soapconfig with the User Interface

To use the soapconfig tool with a graphical user interface, type `soapconfig` on a command line with no parameters and press Enter. In Windows, you also can double-click the `SOAPConfig.bat` file in the WebLogic Integration – Business Connect bin directory to open the window. When you complete the fields and click OK, the window closes and the changes appear in the `DB.properties` file.

**Note:** Before you use the soapconfig tool, use the Java keytool to create the truststore or keystore or both for Administrator and Tracker.

**Figure 14-4 SOAP Configuration Window**



## Description of Soap Configuration Window

The following describes the fields on the Soap Configuration window.

If you are running the tool for the first time, the fields are blank. If you have used the tool before, the default values are the same as the values you entered when you previously used the tool.

*Trust store*

The name of the Administrator and Tracker truststore that was created with keytool. A truststore is a keystore that is used to make decisions about trusting entities. A truststore contains trusted certificates information, but not private information.

*Trust store password*

The truststore password. For security the password appears as asterisks. In `DB.properties` the password is encrypted.

*Confirm trust store password*

The truststore password repeated.

*Key store*

The name of the Administrator and Tracker keystore that was created with keytool. A keystore is a database of key information that is used for authentication and data integrity. A keystore contains private information, including private keys.

*Key store password*

The keystore password. For security the password appears as asterisks. In `DB.properties` the password is encrypted.

*Confirm key store password*

The keystore password repeated.

CHAPTER

# 15 Exporting and Importing Data

The following topics provide information about exporting configuration data in Administrator and log data in Tracker and importing the data to a new installation of WebLogic Integration – Business Connect.

**Procedures**

- "Exporting Data" on page 15-2
- "Importing Data" on page 15-4

This information is about exporting and importing data only within version 2.1 of WebLogic Integration – Business Connect.

You might want to export data and preserve it in the event you want to use WebLogic Integration – Business Connect on a computer other than where you first installed the application.

The utility that enables you to import configuration and log data only allows you to import data into a newly installed instance of WebLogic Integration – Business Connect. The utility does not allow you to import data into an instance of WebLogic Integration – Business Connect that already has data. Moreover, you can only export and import data on the same platform (for example, export from WebLogic Integration – Business Connect on Windows and import to WebLogic Integration – Business Connect on Windows).

# Exporting Data

The following topics are provided for exporting data:

- "Exporting Administrator Data"
- "Exporting Tracker Data" on page 15-3

## Exporting Administrator Data

Use this procedure to export a file containing all data in Administrator about company and partner profiles, schedules, certificates and users. This procedure is only for exporting data from version 2.1 of Administrator.

Only an Administrator user can export Administrator data to a file.

### Steps

1. Select File→Save Administrator Data in Administrator to open the Save Administrator Data dialog box.
2. Type the name of the data file to export and select the export directory. The default file name is `Administrator.dat`.
3. Click Save. The Export Password dialog box opens. Setting a password for the data file you export is an optional step. Setting a password encrypts sensitive data in the file. It also ensures that only a user who knows the password can import the file to Administrator.
4. If you want, type a password in the password field and retype it in the confirm password field. For security, the password appears as asterisks. You can use alphanumeric characters for your password.

   Although not required, a password is recommended. However, there is no way to recover a lost or forgotten password. If you lose or forget your password, you must export the data file again and create another password.

   If you do not want a password for the exported file, leave these fields blank.
5. Click OK to save the data file to the selected directory.

# Exporting Tracker Data

Use this procedure to export a file containing runtime log data in Tracker. Archived data is not exported. This procedure is only for exporting data from version 2.1 of Tracker.

Only an Administrator user can export Tracker data to a file.

## Steps

1. Select File→Save Tracker Runtime Data in Tracker to open the Save Tracker Data dialog box.
2. Type the name of the data file to export and select the export directory. The default file name is `Tracker.dat`.
3. Click Save. The Export Password dialog box opens. Setting a password for the data file you export is an optional step. Setting a password encrypts sensitive data in the file. It also ensures that only a user who knows the password can import the file to Tracker.
4. If you want, type a password in the password field and retype it in the confirm password field. For security, the password appears as asterisks. You can use alphanumeric characters for your password.

   Although not required, a password is recommended. However, there is no way to recover a lost or forgotten password. If you lose or forget your password, you must export the data file again and create another password.

   If you do not want a password for the exported file, leave these fields blank.
5. Click OK to save the data file to the selected directory.

# Importing Data

Use this procedure to import a file containing Administrator data or Tracker data or both. You can import data only into a new instance of WebLogic Integration – Business Connect that does not have any configuration or log data.

This procedure is only about importing to a newly installed instance of WebLogic Integration – Business Connect 2.1 the data exported from a previously installed instance of WebLogic Integration – Business Connect 2.1.

Before performing this procedure you must have exported the data for Administrator or Tracker or both. See "Exporting Data" on page 15-2.

## Steps

1. Install the version 2.1 software.
2. Using the newly installed 2.1 software, start the import database utility in the WebLogic Integration – Business Connect bin directory to open the Import Database window.

   In Windows, in the WebLogic Integration – Business Connect bin directory, double-click `Import.bat`.

   In UNIX, run the following command:

   ```
   installation_directory/bin/import
   ```
3. On the Import Database window, make sure the check boxes for the data files you want to import are selected. The check boxes are Configuration for Administrator data and Logs for Tracker data. Both check boxes are selected by default.
4. Click Browse next to the Configuration File field to open a browse dialog box. Select the `Administrator.dat` file in the directory where you saved the file and click Open. If you created a password for the data file when you exported it, type it in the password field.

5. Click Browse next to the Logs File field to open a browse dialog box. Select the `Tracker.dat` file in the directory where you saved the file and click Open. If you created a password for the data file when you exported it, type it in the password field.
6. Click Import to start the import process. When the process is completed, a message appears confirming the success of the import.
7. Click Close to close the Import Database window.
8. Start the Server application.

CHAPTER

# 16 Document Generator

The Document Generator utility is included with WebLogic Integration – Business Connect. You can use it to create test documents that conform to the structures of X12 EDI or XML formats. To create an end-to-end test, you can generate documents of any size and send them at any interval you choose to another WebLogic Integration – Business Connect server.

The following topics are provided about using Document Generator to create test trading documents.

**Procedures**

- "Creating EDI or XML Test Documents" on page 16-1

**Concepts**

- "Running Document Generator from a Command Line" on page 16-4

## Creating EDI or XML Test Documents

Use this procedure to create EDI or XML test documents in Document Generator and put them in an output directory.

You can run multiple sessions of the Document Generator. Each session can generate different document types, sizes and rates.

# Steps

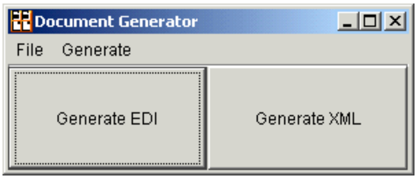
1. On Windows select Programs→WebLogic Integration – Business Connect→Document Generator on the Start menu.

   On UNIX log in to the account you created previously. Ensure that you have X Windows connectivity to the server where you installed the application. Run the following command to open the Document Generator:

   ```
   installation_directory/bin/docgen
   ```

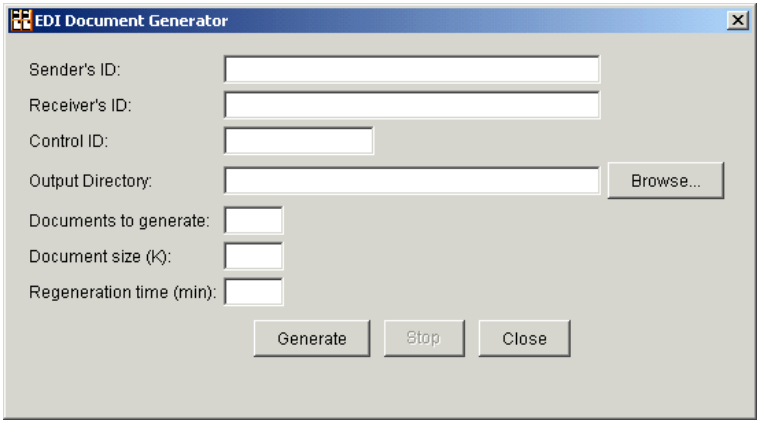
   You also can run the Document Generator from a command line. See “Running Document Generator from a Command Line” on page 16-4.

   **Figure 16-1 Document Generator Window**



2. Click Generate EDI or Generate XML to open the EDI or XML Document Generator window. The two windows are the same, except only the EDI window has a Control ID field.

   **Figure 16-2 EDI Document Generator Window**



3. Complete the fields. See “Field Descriptions” on page 16-3.

4. Click Generate to generate the number and size of documents you specified. The Document Generator continues to generate documents at the interval you specified until you click Stop or close the EDI or XML Document Generator window.

## Field Descriptions

The following describes the fields on the EDI and XML Document Generator windows. For procedure see “Steps” on page 16-2.

*Sender’s ID*

Type the ID of the sender.

*Receiver’s ID*

Type the ID of the receiver.

*Control ID (EDI only)*

Type any numeric control ID. This is the starting number for the document counter.

*Output Directory*

Type the directory where the Document Generator writes the outbound documents. Or, use the Browse button to locate this directory. This is typically the sender’s EDI or XML out directory.

*Documents to generate*

Type any value between `1` and `999999` to indicate the number of documents you want to create per unit of time. The Document Generator creates all of these documents at once.

*Document size (K)*

Type any value between `1` and `999999` to indicate the size of each document you want to create.

*Regeneration time (min)*

Type any value between `1` and `999999` to indicate the time the Document Generator waits to create the next document or set of documents.

# Running Document Generator from a Command Line

You can use Document Generator from a command line without the graphical user interface (GUI). You do this by running a command with parameters for the test documents you want to create. On UNIX, the command is docgen. On Windows in a DOS window the command is "Document Generator" in quotation marks as shown.

You cannot pause the Document Generator from the command line as you can when using the Document Generator GUI. Only one Document Generator at a time can be started from the command line in a single DOS window or terminal window.

**Note:** If you run WebLogic Integration – Business Connect on UNIX and there are spaces in the sender's or receiver's ID, we recommend that you use the Document Generator GUI. See "Creating EDI or XML Test Documents" on page 16-1.

The following topics are provided for running Document Generator from a command line:

- "Command Line Parameters" on page 16-4
- "Command Line Format" on page 16-5

## Command Line Parameters

The following table shows the command line parameters for the Document Generator. They are mapped to the parallel fields on the GUI (see "Creating EDI or XML Test Documents" on page 16-1). The parameters are listed in the order of entry and not the order of the parallel GUI fields.

**Table 16-1 Document Generator Command Line Parameters**

| Command line parameter | GUI field | Description |
|---|---|---|
| sender | Sender’s ID | Type the ID of the sender. |
| recipient | Receiver’s ID | Type the ID of the receiver. |
| size | Document size (K) | Type any value between `1` and `999999` to indicate the size of each document you want to create. |
| numDocsPerInterval | Documents to generate | Type any value between `1` and `999999` to indicate the number of documents you want to create per unit of time. The Document Generator creates all of these documents at once. |
| outFolder | Output Directory | Type the directory where the Document Generator writes the outbound documents. This is typically the sender’s EDI, XML or binary out directory. |
| aDocNum | Control ID | For XML type `1`. For EDI type any numeric control ID. This is the starting number for the document counter. |
| aDocType | not applicable | Type `EDI` or `XML`. |
| interval | Regeneration time (min) | Type any value between `1` and `999999` to indicate the time the Document Generator waits to create the next document or set of documents.<br>This parameter is optional. If not used, the system displays the specified number of documents generated and returns to the command line. |

# Command Line Format

The following are examples for running Document Generator from a command line. Be sure you run the utility from the WebLogic Integration – Business Connect bin directory.

## UNIX

For UNIX, the following example shows the command line format for Company1 to create 7 EDI documents that are 3K in size every 5 minutes and place them in the EDI out directory for sending to Partner1. The control ID is 302.

```
./docgen company1 partner1 3 7 /home/account/ci400/data/company1/ediout 302 edi 5
```

The following example shows the command line format for Company1 to create 5 XML documents that are 24K in size and place them in the XML out directory for sending to Partner1. The control ID is 1. Notice that the last parameter, interval, is omitted, so only a single group of 5 documents will be created.

```
./docgen company1 partner1 24 5 /home/account/ci400/data/company1/xmlout 1 xml
```

If you run the docgen command without any parameters, the GUI opens.

To stop the generator, execute `installation_directory/bin/processes`. From the resulting output, locate the PID associated with docgen, and execute the kill command on the PID.

## Windows

For Windows, the following example shows the proper command line format.

“Document Generator” Company1 Partner1 24 5
C:\installation_directory\data\Company1\xmlout 1 XML

Pressing Ctrl-C (in the DOS window) stops the Document Generator and the system returns to the command prompt.

If there are spaces in the sender’s or receiver’s ID or out directory name, place the IDs or directory name in quotation marks so Windows properly handles the spaces. The following is an example of the format:

"Document Generator" "SenderID" "ReceiverID" Size NumDocsPerInterval
"OutFolder" ControlID DocType [Interval]

CHAPTER

# 17 Tracker

Tracker enables you to monitor your use of WebLogic Integration – Business Connect by providing runtime and archived views of database records of transactions and events. You also can use Tracker to search for and resend documents to your trading partners or resubmit them through the Server application to your translator or business application.

The following topics are provided.

**Concepts**

**Procedures**

**Windows**

# Overview of Tracker

Tracker provides runtime and archived views of records or logs that show your organization’s inbound and outbound document traffic as well as events, including alert messages of high importance. Runtime views display database records before they have been archived. Archive view shows database records that have been archived. You control the frequency of archiving in the Administrator Schedules information viewer.

Tracker has seven information viewers that display database records of inbound, outbound and rejected documents as well as records about alerts, transactions, events and user activities. You can switch between views of the runtime and database records by selecting Runtime or Archive from the Database table drop-down list at the top left. Click Refresh to make sure the latest records are displayed (see “Refreshing the Tracker Display” on page 17-3.)

The following provides an overview of the information viewers in Tracker.

## Alerts

You can view the date, time, partner ID or combined EDI qualifier and ID, contact name, and contact e-mail address for each alert or notification message. You can also view or print the text of the message.

## Traffic

You can view runtime and archive database records for inbound, outbound and rejected documents. There are three Traffic information viewers:

- Inbound Traffic
- Outbound Traffic
- Rejected Traffic

The Inbound Traffic and Outbound Traffic information viewers provide an audit trail for documents you received from or sent to your trading partners. The Rejected Traffic information viewer provides a list of inbound or outbound documents that WebLogic Integration – Business Connect could not process and routed to the rejected directory.

## Transactions

You can view a reverse chronological listing of each milestone event in the processing of in and outbound documents. For each transaction event, you can see the date, time, control ID, ID or combined EDI qualifier and ID, status, and any message associated with it.

# Refreshing the Tracker Display

To view the latest database records, click Refresh or select View→Refresh or press the F5 key. You must refresh the display when you want to view the latest records, especially the latest runtime records.

Tracker database information viewers refresh automatically the first time you display them. Automatic refreshing occurs on the Alerts information viewer when you start Tracker. It also occurs the first time you select another information viewer or change from a runtime to archive display. Apart from the initial display, automatic refreshing does not occur. It is a manual process.

When you click Refresh, the action refreshes records on the currently active information viewer, but not others. For example, say you click Refresh while viewing the Inbound Traffic information viewer. The viewer refreshes the record display. But if you switch to the Outbound Traffic information viewer, you must click Refresh again to also refresh the records displayed in that viewer.

If you want to see continuously updated records of document trading activity, open the server monitor page in a browser by selecting Tools→Launch Server Monitor in Tracker or Administrator.

# Filtering Tracker Records

Tracker has filters that enable you to view many or few runtime or archive database records at a time in information viewers. The filter settings persist from one Tracker session to another until you change them. You set filters by information viewer by database view. For example, the filter settings for the runtime view of the Alerts information viewer apply only to that window.

Slightly different filter windows are provided for runtime and archive database views. The only difference is that the default value for the maximum record display is blank for the runtime filter window and is 100 for the archive filter window.

Click Filter or select View→Filter to access the filter window for an information viewer. Use the optional fields to specify the range of records you want to display and click OK.

# Printing Tracker Records

You can print a list of the records in the currently active information viewer by selecting File→Print or pressing Ctrl-P. Tracker prints to your system's default printer.

The application prints the data as displayed on the current information viewer, so maximizing the window size before you print yields longer horizontal printed records. Although the records print in landscape format, you might have to adjust the column widths in the information viewers to print the columns of data you want. This is necessary to account for differences in fonts and printers.

You can adjust column widths by placing the cursor over the lines between the columns to make a double-arrow appear. Click and hold the left button to adjust the column widths. You also can click and drag columns to change their locations.

# Guidelines for Finding and Reprocessing

You can use Tracker to search for records of documents and, in the case of records of documents in the runtime database, you can submit such documents for reprocessing. Reprocessing involves resending documents to your trading partners or re-submitting documents through WebLogic Integration – Business Connect to your translator or business system. The following guidelines are provided to help you in using the Tracker document find feature. For procedure see “Finding Document Records” on page 17-11.

- “Reprocessing Only the Most Recent Document”
- “Reprocessing Unacknowledged Documents” on page 17-6
- “Reprocessing Rejected Documents” on page 17-6
- “Reprocessing by Control ID” on page 17-7
- “Reprocessing by Partner” on page 17-8

## Reprocessing Only the Most Recent Document

When you reprocess a document, WebLogic Integration – Business Connect creates a new version of it with a new, unique file name. You can reprocess each file name only once. To reprocess a document more than once, you must select only the most recently processed document.

For example, you attempt to send to your partner a document with the control ID 100000000 and a file name of 56in. The document is rejected. You use Tracker to resubmit this document through WebLogic Integration – Business Connect to your translator. WebLogic Integration – Business Connect names the resubmitted document (control ID 100000000) to file name 68in. To resubmit the document (control ID 100000000) a second time, choose file name 68in in the Find window.

**Note:** Tracker cannot reprocess completed documents that have been archived. This includes inbound documents that have been placed in the EDI-in directory and outbound documents for which you have received an MDN.

For procedure see “Finding Document Records” on page 17-11.

# Reprocessing Unacknowledged Documents

When you send a document and you have selected the acknowledge documents option in the partner profile, your trading partner sends you an MDN, which acknowledges the receipt, successful decryption and verification of the document.

If your WebLogic Integration – Business Connect system does not receive an acknowledgment, it attempts to resend the transaction up to the limits in the Partner Profile window Preferences tab. If your system still does not receive an acknowledgment, WebLogic Integration – Business Connect generates and sends you an e-mail alert. You can then locate and resend the unacknowledged document.

From the document status drop-down list on the Find window, select Not Acknowledged to search for unacknowledged documents. When you find the documents you want, you can select them and click Reprocess. WebLogic Integration – Business Connect moves the selected documents to an outbound directory for reprocessing and retransmission to your trading partner.

For procedure see “Finding Document Records” on page 17-11.

# Reprocessing Rejected Documents

You can resend rejected outbound documents to your trading partners and resubmit rejected inbound documents to your WebLogic Integration – Business Connect system for reprocessing.

From the document status drop-down list on the Find window, select Rejected to search for rejected documents. Based on the information about these documents, you should correct whatever condition caused the documents to be rejected before you attempt to reprocess them.

When you find the documents you want, you can select them and click Reprocess. Then the following occurs:

| | |
|---|---|
| For outbound transactions | WebLogic Integration – Business Connect moves the selected documents to an outbound directory for reprocessing and retransmission to your trading partner. During this reprocessing, WebLogic Integration – Business Connect gives the documents new file names. |
| For inbound transactions | The documents are queued for reprocessing by WebLogic Integration – Business Connect and resubmission to your translator. The documents retain the same file names WebLogic Integration – Business Connect gave them when it processed or attempted to process them the first time. |

For procedure see "Finding Document Records" on page 17-11.

# Reprocessing by Control ID

A control ID is the unique identifier assigned to a document by a company's translator application. When you locate a document this way, you can resend it to your trading partners or resubmit it to your WebLogic Integration – Business Connect system for reprocessing.

In the control ID field on the Find window, type the control ID for the document you need to find. The control ID is an alphanumeric ID that has a maximum length of 12 characters. You must include any leading zeros.

When you find the document you want, you can select them and click Reprocess. Then the following occurs:

| | |
|---|---|
| For outbound transactions | WebLogic Integration – Business Connect moves the selected document to an outbound directory for reprocessing and retransmission to your trading partner. During this reprocessing, WebLogic Integration – Business Connect gives the document a new file name. |
| For inbound transactions | The document is queued for reprocessing by WebLogic Integration – Business Connect and resubmission to your translator. The document retains the same file name WebLogic Integration – Business Connect gave it when it processed or attempted to process it the first time. |

For procedure see "Finding Document Records" on page 17-11.

# Reprocessing by Partner

You can search for documents you sent to or received from a certain partner. When you locate the documents, you can resend outbound documents to your trading partners or resubmit inbound documents to your WebLogic Integration – Business Connect system for reprocessing.

From the trading partner drop-down list on the Find window, select the partner associated with the documents you want to find. When you find the documents you want, you can select them and click Reprocess. Then the following occurs:

| | |
|---|---|
| For outbound transactions | WebLogic Integration – Business Connect moves the selected documents to an outbound directory for reprocessing and retransmission to your trading partner. During this reprocessing, WebLogic Integration – Business Connect gives the document a new file name. |
| For inbound transactions | The document is queued for reprocessing by WebLogic Integration – Business Connect and resubmission to your translator. The document retains the same file name WebLogic Integration – Business Connect gave it when it processed or attempted to process it the first time. |

For procedure see “Finding Document Records” on page 17-11.

# Logging on to Tracker

Use this procedure to start Tracker and log on.

## Steps

1. On Windows, select Programs→BEA WebLogic Integration – Business Connect 2.1→Tracker on the Start menu to open the login dialog box.

   On UNIX, ensure you have X Windows connectivity to the server where WebLogic Integration – Business Connect is installed. Log in to the account you created during installation. Run the following command to open the login dialog box:

   ```
   installation_directory/bin/tracker
   ```

2. Type your user ID and password in the appropriate fields. Use the same user ID and password you use to access Administrator.

3. Click OK.

# Manually Archiving Database Records

Use this procedure to force the Server application to archive the runtime database records displayed in Tracker. Activating this feature forces archiving to occur now and overrides the archive schedule, which is accessed from the Schedules information viewer in Administrator. Using this feature also suspends all runtime processing until archiving is completed.

After archiving is completed, you can switch to the archive view in Tracker to review archived database records.

## Steps

1. Select Tools→Run Archiver Now in Tracker. A dialog box displays with a message prompting you to confirm whether you want to archive runtime database records.
2. Click Yes to confirm you want to run the archiving process. A dialog box displays with a message that the archiving process has been scheduled.
3. Click OK to close the dialog box.

# Clearing Tracker Database Records

Use this procedure to clear the Tracker runtime or archive database records.

**Note:** If you clear the runtime database, you will permanently lose all records before they have been archived. Also, if you clear the archive database, you will permanently lose all archived records. Be careful when using these functions.

## Steps

1. Select File→Clear All Archive Logs or File→Clear All Runtime Logs.
2. Click Yes on the confirm delete dialog box to clear all logs.

# Finding Document Records

Use this procedure to find runtime and archive records of documents in Tracker. After you have found the documents you want, you can reprocess runtime documents, but not archived documents. Reprocessing involves resending documents to your trading partners or re-submitting documents through WebLogic Integration – Business Connect to your translator or business system. See "Guidelines for Finding and Reprocessing" on page 17-5.

The document search process enables you to search the Tracker database for one or more documents using a filter and then reprocess them. Searches you can perform include:

- Search for acknowledged and unacknowledged documents and for documents for which no acknowledgments were requested.
- Search for documents that WebLogic Integration – Business Connect rejected because, for example, it could not encrypt or decrypt, sign or verify, or find a valid partner.
- Search for a document based on its control ID or partner ID.

Tracker can find only those documents in the backup or rejected directories. Consequently, your ability to find and resend or resubmit documents depends on how often you elect to run the archive process.

You cannot reprocess a document that WebLogic Integration – Business Connect has successfully received from a partner. If you need to reprocess a document that already has been successfully received and processed, ask your partner to send the document to you again.

If you choose the do not back up option for inbound documents in your company profile preferences, you can use Tracker to access documents only in the rejected directory.

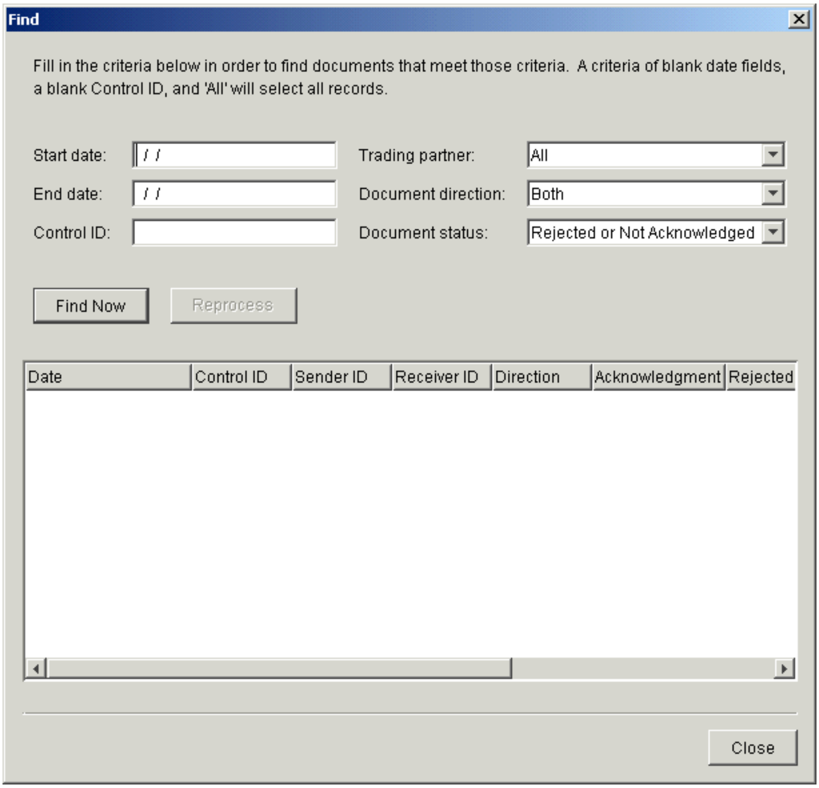
If you choose the back up and archive or the back up and delete option in your company profile preferences, the archive process deletes completed documents or moves them to the archive directory. A completed inbound document is one that has been placed in the inbound document directory. A completed outbound document is one for which you have received an MDN (if you requested one). After these completed documents have been moved or deleted, you can no longer search for them or reprocess them using Tracker.

## Steps

The following are the steps for setting up a filtered search for documents. You do not have to use all the fields on the Find window to perform a search. The fields are available to help you perform a wide or narrow search.

1. Click Find on the Tracker toolbar or select Edit→Find or press Ctrl-F to open the Find window.

**Figure 17-1 Find Window**



Find

Fill in the criteria below in order to find documents that meet those criteria. A criteria of blank date fields, a blank Control ID, and 'All' will select all records.

Start date: / /

End date: / /

Control ID:

Trading partner: All

Document direction: Both

Document status: Rejected or Not Acknowledged

| Date | Control ID | Sender ID | Receiver ID | Direction | Acknowledgment | Rejected |
|---|---|---|---|---|---|---|

2. Choose a date range for your search if you are not searching by a control ID (see the next step). Note the following about the date fields:

   - To search for documents for a single date, type the same date in the start and end date fields.
   - To include documents for all dates in your search, leave the start and end date fields blank.
   - If you type a start date but not an end date, the system lists all documents processed on or after that date.
   - If you type an end date but not a start date, the system lists all documents processed on or before that date.

3. Select a control ID. Because control IDs are unique, you can normally use it as the only search criterion. In other words, when you search for a document by control ID, leave the date fields blank.

   You must type all digits of the control ID, including leading zeros. You cannot use wild cards or Boolean symbols in this field.

4. Select a partner from the trading partner drop-down list to search for documents sent to or received from that partner. Use the default selection All to search for documents for all partners.

5. Select the direction of the traffic you want to display from the document direction drop-down list. The options are:

| | |
|---|---|
| Both | Search for all documents you sent and received. |
| Inbound | Search only for documents you received. |
| Outbound | Search only for documents you sent. |

6. Select a document status from the document status drop-down list. The options are:

| | |
|---|---|
| All | Search for documents in all status categories. |
| Acknowledged | Search for documents for which you received acknowledgments (MDNs). |
| Ack Not Requested | Search for documents for which you did not request acknowledgments (MDNs). |
| Not Acknowledged | Search for documents that timed-out before they could be sent or for which you did not receive acknowledgments (MDNs). |
| Rejected | Search for rejected documents. |
| Rejected or Not Acknowledged | Search for unacknowledged and rejected documents. |

7. Click Search to find documents that meet your search criteria. If documents are found, information about them is displayed (see "Field Descriptions"). If no documents are found, a message to that effect is displayed.
8. When you find the documents you want, you can reprocess one or more documents by selecting them and clicking Reprocess.
9. Click Close to exit the Find window.

## Field Descriptions

The following describes the fields on the Find window for documents that Tracker has found that meet your search criteria. For procedure see "Steps" on page 17-12.

*Date*

The date and time WebLogic Integration – Business Connect processed the document. You can sort records in ascending or descending order by clicking the arrow in this column.

*Control ID*

The document's control ID. For EDI documents, this is the number assigned by the translator.

Documents without control IDs might be binary or XML documents. Or, it is an inbound document that WebLogic Integration – Business Connect could not read and placed in the rejected directory.

*Sender ID*

The ID or combined EDI qualifier and ID of the sender.

*Receiver ID*

The ID or combined EDI qualifier and ID of the recipient.

*Direction*

Indicates whether the document is inbound (you received it) or outbound (you sent it).

*Acknowledgment*

Values that can appear in this field for inbound documents include:

| | |
|---|---|
| Yes | You sent an acknowledgment to the document’s sender. |
| No | You did not send an acknowledgment, or your trading partner did not request that you send one. |
| N/A | Not applicable. |

Values that can appear in this field for outbound documents include:

| | |
|---|---|
| Yes | You received an acknowledgment from the document’s recipient. |
| No | You did not receive an acknowledgment from the document’s recipient, or you did not request that your partner send one. |
| N/A | Not applicable. |
| Unexpected processing error | |

*Rejected*

Values that can appear in this field include:

| | |
|---|---|
| Yes | WebLogic Integration – Business Connect could not process this document and placed it in the rejected directory. |
| N/A | WebLogic Integration – Business Connect successfully processed this document. |

*Transport*

The transport method.

*File*

The file name that your WebLogic Integration – Business Connect assigned to the document, either inbound or outbound.

*Path*

The complete path to the directory where this document is stored. This path is to one of the following directories.

| | |
|---|---|
| Backup directory | WebLogic Integration – Business Connect stores all inbound and outbound documents in this directory. If the document is stored here, it has been processed successfully. The document is stored in this directory until the next time the WebLogic Integration – Business Connect archive process runs. |
| Rejected directory | Documents that WebLogic Integration – Business Connect cannot successfully process are stored in the rejected directory. |

# Alerts Information Viewer

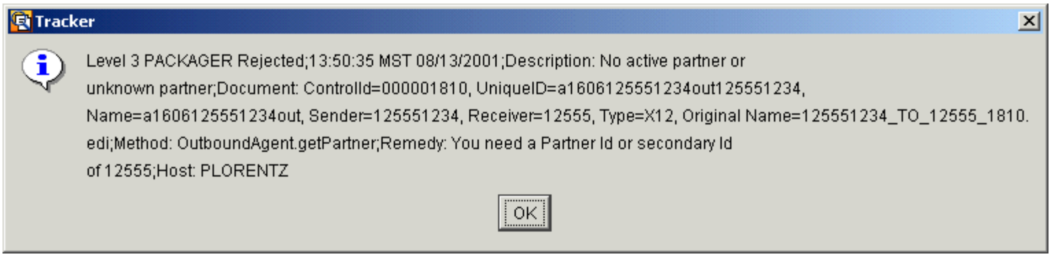
Use the Alerts information viewer to examine records for alerts and notifications.

Access the viewer by selecting **Alerts** on the Tracker bar.

WebLogic Integration – Business Connect continuously performs self-checks to ensure proper operation. When it detects a problem, WebLogic Integration – Business Connect generates an alert or notification that appears in the Alerts information viewer. Simultaneously, WebLogic Integration – Business Connect sends your point of contact an e-mail message that describes the problem in plain text. Such e-mails are sent if a contact person's e-mail address is provided in the alert or notify mail address fields on the Preferences tab of the Company Profile window.

You can view the text of alerts and notifications by placing the cursor over the record line in the Alerts information viewer, right-clicking and selecting **View** on the pop-up menu. This displays a pop-up window with the text of the message. You also can copy a message by right-clicking. You can paste copied messages into a text editor.

Figure 17-2 Right-Click a Record and Select View to Display the Message



```
Level 3 PACKAGER Rejected;13:50:35 MST 08/13/2001;Description: No active partner or
unknown partner;Document: ControlId=000001810, UniqueID=a1606125551234out125551234,
Name=a1606125551234out, Sender=125551234, Receiver=12555, Type=X12, Original Name=125551234_TO_12555_1810.
edi;Method: OutboundAgent.getPartner;Remedy: You need a Partner Id or secondary Id
of 12555;Host: PLORENTZ
```

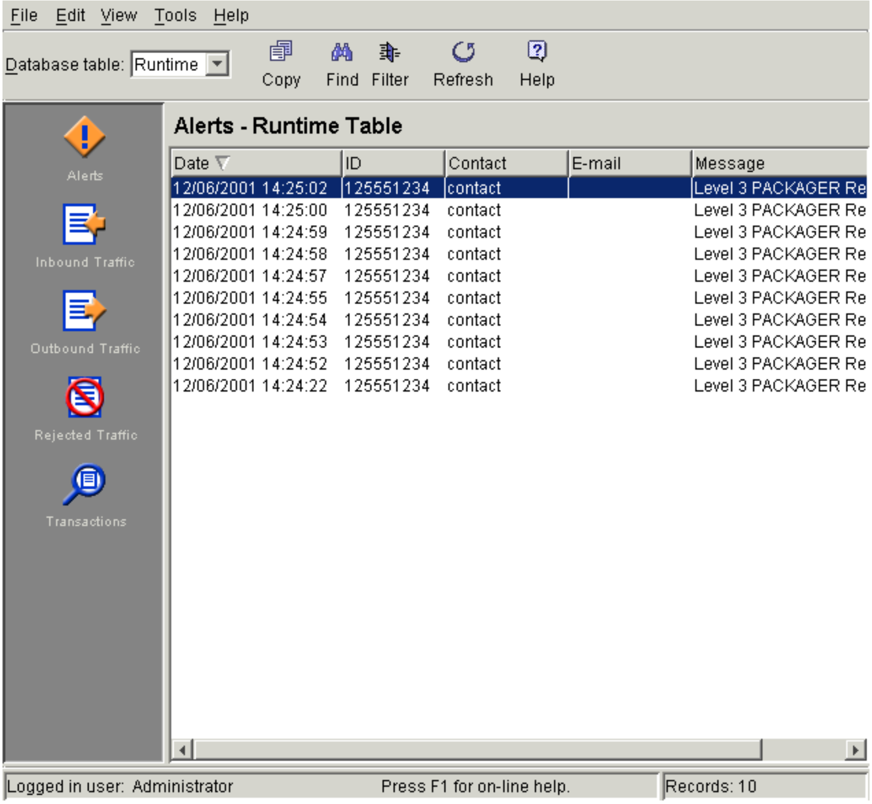
# Description of Alert E-Mail

Identified by the word *alert* in the e-mail subject line, alert messages are sent when WebLogic Integration – Business Connect detects a condition that halts document exchange and requires you to take action. An example is when WebLogic Integration – Business Connect cannot connect to the network or when there is a problem with the WebLogic Integration – Business Connect software.

# Description of Notification E-Mail

Identified by the word *notification* in the e-mail subject line, notification messages are informational and do not require you to take action. Document exchange continues. WebLogic Integration – Business Connect sends a notification, for example, when it rejects a document or when it receives a binary (non-EDI) document from a partner for which it does not have a partner profile.

**Figure 17-3 Alerts information Viewer**



Alerts - Runtime Table

| Date | ID | Contact | E-mail | Message |
|---|---|---|---|---|
| 12/06/2001 14:25:02 | 125551234 | contact | | Level 3 PACKAGER Re |
| 12/06/2001 14:25:00 | 125551234 | contact | | Level 3 PACKAGER Re |
| 12/06/2001 14:24:59 | 125551234 | contact | | Level 3 PACKAGER Re |
| 12/06/2001 14:24:58 | 125551234 | contact | | Level 3 PACKAGER Re |
| 12/06/2001 14:24:57 | 125551234 | contact | | Level 3 PACKAGER Re |
| 12/06/2001 14:24:55 | 125551234 | contact | | Level 3 PACKAGER Re |
| 12/06/2001 14:24:54 | 125551234 | contact | | Level 3 PACKAGER Re |
| 12/06/2001 14:24:53 | 125551234 | contact | | Level 3 PACKAGER Re |
| 12/06/2001 14:24:52 | 125551234 | contact | | Level 3 PACKAGER Re |
| 12/06/2001 14:24:22 | 125551234 | contact | | Level 3 PACKAGER Re |

Logged in user: Administrator    Press F1 for on-line help.    Records: 10

# Field Descriptions

The following describes the fields on the Alerts information viewer.

*Date*

The date and time of the message. You can sort records in ascending or descending order by clicking the arrow in this column.

*ID*

The partner ID or combined EDI qualifier and ID for the document that caused or is related to this message.

*Contact*

The name of the person to whom the message was sent.

*E-mail*

The e-mail address, if any, to which the message was sent. This e-mail address is specified in the Company Profile window Preferences tab.

*Message*

The text of the message.

# Traffic Information Viewers

Use the Traffic information viewers to view runtime and archive database records for inbound, outbound and rejected documents. There are three Traffic information viewers:

- Inbound Traffic
- Outbound Traffic
- Rejected Traffic

Access each viewer by selecting the corresponding icon on the Tracker bar.

The Inbound Traffic and Outbound Traffic information viewers provide an audit trail for documents you received from or sent to your trading partners.

The Rejected Traffic information viewer provides a list of inbound or outbound documents that WebLogic Integration – Business Connect could not process and routed to the rejected directory.

## Reprocessing Documents

You can reprocess documents whose records appear in the runtime database of the Inbound Traffic, Outbound Traffic and Rejected Traffic information viewers. You do this by selecting one or more records, right-clicking, and selecting Reprocess on the pop-up menu. Or, you can select one or more records and select Tools→Reprocess.

Reprocessing does the following:

- For an inbound document, the document is re-submitted to WebLogic Integration – Business Connect for unpackaging. The document is re-submitted in the state WebLogic Integration – Business Connect received it from your partner. For example, if the document was received signed and encrypted, that is how it is re-submitted.
- For an outbound document, the document is re-submitted to WebLogic Integration – Business Connect for packaging and sending to your partner.
- For a rejected document, the inbound or outbound document is re-submitted for inbound or outbound processing.

# Copying, Viewing, or Deleting Records

You can right-click records in the Traffic information viewers to view an inbound or rejected document or to copy or delete a record. The following describes what you can do in each viewer.

In the Inbound Traffic and Rejected Traffic information viewers you can:

- View a document by right-clicking the record and selecting View from the pop-up menu.
- Copy a record by right-clicking it and selecting Copy from the pop-up menu. You can then paste the record contents into a text editor.
- Delete a record by right-clicking it and selecting Delete from the pop-up menu.

In the Outbound Traffic information viewer you can:

- Copy a record by right-clicking it and selecting Copy from the pop-up menu. You can then paste the record contents into a text editor.
- Delete a record by right-clicking it and selecting Delete from the pop-up menu.

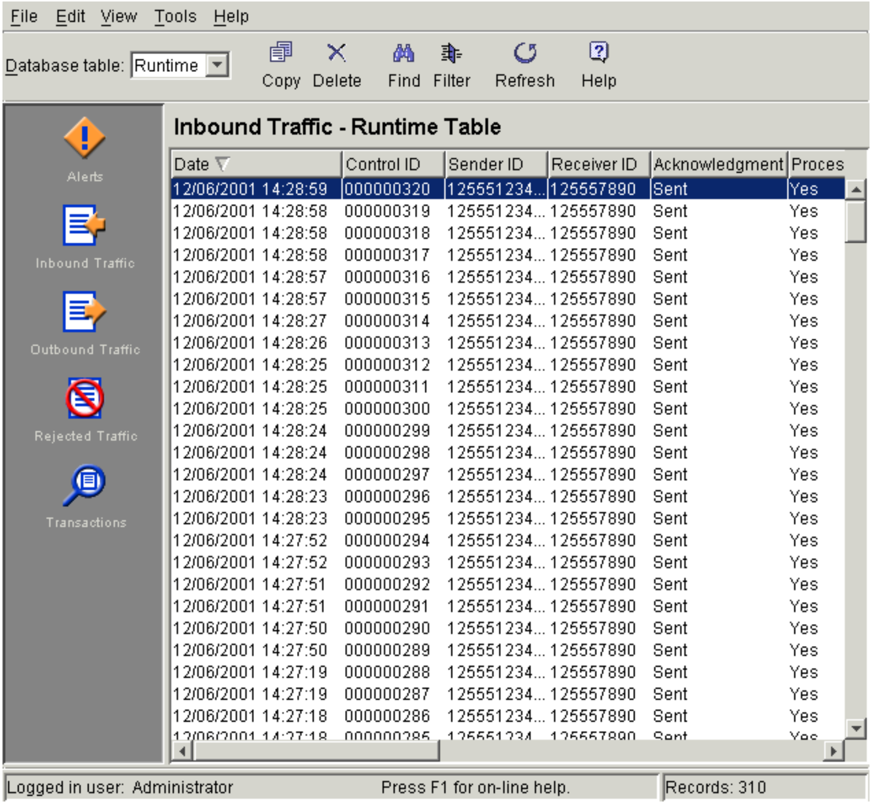
In addition, in the Rejected Traffic information viewer you can double-click a record to view a dialog box with a plain text message about why the document was rejected.

# Viewing Documents

In the Inbound Traffic and Rejected Traffic information viewers, you can display the document by right-clicking it and selecting View from the menu as follows:

- In Windows, to view the document from Tracker you must associate the document type with an application. For example, you can associate documents with the extension `.edi` with a text editor such as Notepad. You can associate `.xml` documents with your Internet browser.
- In UNIX, when you choose View from the menu, the document is displayed in a UNIX viewer, regardless of the type of document. In this viewer, press the plus sign (`+`) key or the Enter key to page down; press the minus sign key (`-`) to page up. Press `q` to close the viewer.

**Figure 17-4 Inbound Traffic information Viewer**



Inbound Traffic - Runtime Table

| Date | Control ID | Sender ID | Receiver ID | Acknowledgment | Proces |
|---|---|---|---|---|---|
| 12/06/2001 14:28:59 | 000000320 | 125551234... | 125557890 | Sent | Yes |
| 12/06/2001 14:28:58 | 000000319 | 125551234... | 125557890 | Sent | Yes |
| 12/06/2001 14:28:58 | 000000318 | 125551234... | 125557890 | Sent | Yes |
| 12/06/2001 14:28:58 | 000000317 | 125551234... | 125557890 | Sent | Yes |
| 12/06/2001 14:28:57 | 000000316 | 125551234... | 125557890 | Sent | Yes |
| 12/06/2001 14:28:57 | 000000315 | 125551234... | 125557890 | Sent | Yes |
| 12/06/2001 14:28:27 | 000000314 | 125551234... | 125557890 | Sent | Yes |
| 12/06/2001 14:28:26 | 000000313 | 125551234... | 125557890 | Sent | Yes |
| 12/06/2001 14:28:25 | 000000312 | 125551234... | 125557890 | Sent | Yes |
| 12/06/2001 14:28:25 | 000000311 | 125551234... | 125557890 | Sent | Yes |
| 12/06/2001 14:28:25 | 000000300 | 125551234... | 125557890 | Sent | Yes |
| 12/06/2001 14:28:24 | 000000299 | 125551234... | 125557890 | Sent | Yes |
| 12/06/2001 14:28:24 | 000000298 | 125551234... | 125557890 | Sent | Yes |
| 12/06/2001 14:28:24 | 000000297 | 125551234... | 125557890 | Sent | Yes |
| 12/06/2001 14:28:23 | 000000296 | 125551234... | 125557890 | Sent | Yes |
| 12/06/2001 14:28:23 | 000000295 | 125551234... | 125557890 | Sent | Yes |
| 12/06/2001 14:27:52 | 000000294 | 125551234... | 125557890 | Sent | Yes |
| 12/06/2001 14:27:52 | 000000293 | 125551234... | 125557890 | Sent | Yes |
| 12/06/2001 14:27:51 | 000000292 | 125551234... | 125557890 | Sent | Yes |
| 12/06/2001 14:27:51 | 000000291 | 125551234... | 125557890 | Sent | Yes |
| 12/06/2001 14:27:50 | 000000290 | 125551234... | 125557890 | Sent | Yes |
| 12/06/2001 14:27:50 | 000000289 | 125551234... | 125557890 | Sent | Yes |
| 12/06/2001 14:27:19 | 000000288 | 125551234... | 125557890 | Sent | Yes |
| 12/06/2001 14:27:19 | 000000287 | 125551234... | 125557890 | Sent | Yes |
| 12/06/2001 14:27:18 | 000000286 | 125551234... | 125557890 | Sent | Yes |
| 12/06/2001 14:27:18 | 000000285 | 125551234... | 125557890 | Sent | Yes |

Logged in user: Administrator    Press F1 for on-line help.    Records: 310

# Inbound and Outbound Traffic Field Descriptions

The following describes the fields on the Inbound Traffic and Outbound Traffic information viewers. The fields are on both viewers, except as noted.

*Date*

The date and time the record was created of the inbound, outbound or rejected document. You can sort records in ascending or descending order by clicking the arrow in this column.

*Control ID*

Possible values include:

* The control ID of an EDI document.

* XML–The document is an XML document without a control ID.

* Binary–The document is a binary document without a control ID.

*Sender ID*

The ID or combined EDI qualifier and ID of the document's sender.

*Receiver ID*

The ID or combined EDI qualifier and ID of the document's recipient.

*Acknowledgment (Inbound Traffic)*

The acknowledgment status of the document. Possible values for inbound documents include:

| | |
|---|---|
| Not Requested | Your partner did not request an acknowledgment. |
| Pending | You received the document, created an MDN, and placed it in the queue to send. |
| Sent | You sent an MDN to your trading partner for this document. |
| Unknown | The acknowledgment status of the document cannot be determined because of an error condition in the database. |

*Acknowledgment (Outbound Traffic)*

The acknowledgment status of the document. Possible values for outbound documents include:

| | |
|---|---|
| Authentication Failed | Your remote trading partner could not verify the document you sent. |
| Decryption Failed | Your remote trading partner could not decrypt the document you sent. |
| Failed | Your remote trading partner could not process the document for unknown reasons. |

| | |
|---|---|
| Not Received | You have not yet received an acknowledgment for a document you sent. |
| Not Requested | You did not request an MDN. |
| Received | You received an acknowledgment for a document you sent. |
| Received, Generic | You received an S/MIME acknowledgment from a mail client. |
| Received, INVALID | You received a non-standard acknowledgment that did not specify a reason the remote trading partner could not process the document you sent. |
| Resend Limit Reached | WebLogic Integration – Business Connect re-sent the document as many times as you specified without receiving a requested acknowledgment. WebLogic Integration – Business Connect sends you an alert and does not attempt to send the document again. |

*Processed (Inbound Traffic)*

Indicates whether WebLogic Integration – Business Connect processed the inbound document. Possible values are:

| | |
|---|---|
| Yes | WebLogic Integration – Business Connect has completed processing the inbound document. |
| No | WebLogic Integration – Business Connect has not completed processing the inbound document. |

*Processed (Outbound Traffic)*

Indicates whether WebLogic Integration – Business Connect processed the outbound document. Possible values are:

| | |
|---|---|
| Yes | WebLogic Integration – Business Connect has completed processing the outbound document. |
| No | WebLogic Integration – Business Connect has not completed processing the outbound document. |

| | |
|---|---|
| Initial Send | WebLogic Integration – Business Connect sent the document and is waiting for an acknowledgment. |
| Retry-*n* | WebLogic Integration – Business Connect has sent the document again because it had not received an acknowledgment. The number of retries this attempt represents is indicated by the number (*n*) following the dash. |
| Retry Limit Exceeded | WebLogic Integration – Business Connect has attempted to re-send the document for the duration specified on the Partner Profile window Preferences tab. |

*Original File*

The file name of the inbound or outbound document. This is the original name of the file as it originated on the sender's system.

*Unique ID*

The identification WebLogic Integration – Business Connect assigns to the document.

*Backup File*

The name of the file as it appears in the backup directory.

*MDN File (Outbound Traffic)*

The name of the MDN file in the backup directory, if you received an MDN from a partner to acknowledge receiving a document from you. This serves to associate the MDN you received with the document you sent.

*Type*

The document type. Possible values include:

| | |
|---|---|
| X12 | X12 EDI document |
| Binary | Binary (non-EDI) document |
| XML | XML document |
| Profile | WebLogic Integration – Business Connect partner profile |
| Certificate | X509 certificate containing the public key |

*Size*

The file size in bytes of the inbound or outbound document.

*Security Level*

The security applied to this document. Possible values include:

| | |
|---|---|
| Clear text | The document is neither encrypted nor signed. |
| Signed | The document is signed. |
| Encrypted | The document is encrypted. |
| Signed, Encrypted | The document is signed and encrypted. |
| Unknown | The security of the document cannot be determined because of an error condition in the database. |

*Transport*

The transport method.

*File (Inbound Traffic)*

The fully qualified path to the document in the EDI-in, XML-in or binary-in directory.

## Rejected Traffic Field Descriptions

The following describes the fields on the Rejected Traffic information viewer.

*Date*

The date and time the document was rejected. You can sort records in ascending or descending order by clicking the arrow in this column.

*Control ID*

Possible values include:

* The control ID of a rejected EDI document.

* NA–The document is an XML or binary document.

*Sender ID*

The ID or combined EDI qualifier and ID of the document's sender.

*Receiver ID*

The ID or combined EDI qualifier and ID of the document's recipient.

*Type*

The document type. The possible values are:

| | |
|---|---|
| X12 | X12 EDI document |
| Binary | Binary (non-EDI) document |
| XML | XML document |
| Profile | WebLogic Integration – Business Connect partner profile |
| Certificate | X509 certificate containing the public key |

*Original File*

The original file name of the rejected document as it was sent by the originator.

*Unique ID*

The identification WebLogic Integration – Business Connect assigns to the document.

*File*

The unique name WebLogic Integration – Business Connect gives to the file. This is the name of the file as it appears in the Rejected directory.

*Transport*

The transport method.

*Reason*

The reason WebLogic Integration – Business Connect rejected the document.

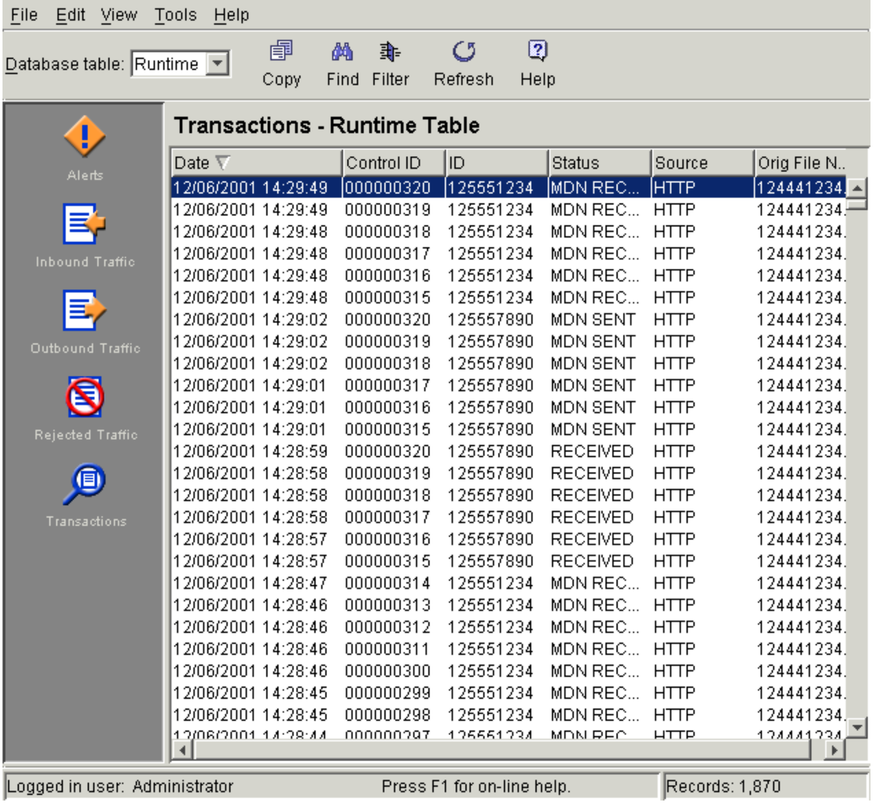
# Transactions Information Viewer

Use the Transactions information viewer to view records about transaction activity. This viewer provides an audit trail for successfully processed and transmitted documents as they move through the system.

Access the viewer by selecting Transactions on the Tracker bar.

In the Transactions information viewer you can copy a record by right-clicking it and selecting Copy from the pop-up menu. You can then paste the record contents into a text editor.

**Figure 17-5 Transactions information Viewer**



Database table: Runtime

Transactions - Runtime Table

| Date | Control ID | ID | Status | Source | Orig File N.. |
|---|---|---|---|---|---|
| 12/06/2001 14:29:49 | 000000320 | 125551234 | MDN REC... | HTTP | 124441234. |
| 12/06/2001 14:29:49 | 000000319 | 125551234 | MDN REC... | HTTP | 124441234. |
| 12/06/2001 14:29:48 | 000000318 | 125551234 | MDN REC... | HTTP | 124441234. |
| 12/06/2001 14:29:48 | 000000317 | 125551234 | MDN REC... | HTTP | 124441234. |
| 12/06/2001 14:29:48 | 000000316 | 125551234 | MDN REC... | HTTP | 124441234. |
| 12/06/2001 14:29:48 | 000000315 | 125551234 | MDN REC... | HTTP | 124441234. |
| 12/06/2001 14:29:02 | 000000320 | 125557890 | MDN SENT | HTTP | 124441234. |
| 12/06/2001 14:29:02 | 000000319 | 125557890 | MDN SENT | HTTP | 124441234. |
| 12/06/2001 14:29:02 | 000000318 | 125557890 | MDN SENT | HTTP | 124441234. |
| 12/06/2001 14:29:01 | 000000317 | 125557890 | MDN SENT | HTTP | 124441234. |
| 12/06/2001 14:29:01 | 000000316 | 125557890 | MDN SENT | HTTP | 124441234. |
| 12/06/2001 14:29:01 | 000000315 | 125557890 | MDN SENT | HTTP | 124441234. |
| 12/06/2001 14:28:59 | 000000320 | 125557890 | RECEIVED | HTTP | 124441234. |
| 12/06/2001 14:28:58 | 000000319 | 125557890 | RECEIVED | HTTP | 124441234. |
| 12/06/2001 14:28:58 | 000000318 | 125557890 | RECEIVED | HTTP | 124441234. |
| 12/06/2001 14:28:58 | 000000317 | 125557890 | RECEIVED | HTTP | 124441234. |
| 12/06/2001 14:28:57 | 000000316 | 125557890 | RECEIVED | HTTP | 124441234. |
| 12/06/2001 14:28:57 | 000000315 | 125557890 | RECEIVED | HTTP | 124441234. |
| 12/06/2001 14:28:47 | 000000314 | 125551234 | MDN REC... | HTTP | 124441234. |
| 12/06/2001 14:28:46 | 000000313 | 125551234 | MDN REC... | HTTP | 124441234. |
| 12/06/2001 14:28:46 | 000000312 | 125551234 | MDN REC... | HTTP | 124441234. |
| 12/06/2001 14:28:46 | 000000311 | 125551234 | MDN REC... | HTTP | 124441234. |
| 12/06/2001 14:28:46 | 000000300 | 125551234 | MDN REC... | HTTP | 124441234. |
| 12/06/2001 14:28:45 | 000000299 | 125551234 | MDN REC... | HTTP | 124441234. |
| 12/06/2001 14:28:45 | 000000298 | 125551234 | MDN REC... | HTTP | 124441234. |
| 12/06/2001 14:28:44 | 000000297 | 125551234 | MDN REC... | HTTP | 124441234 |

Logged in user: Administrator

Press F1 for on-line help.

Records: 1,870

# Field Descriptions

The following describes the fields on the Transactions information viewer.

*Date*

The date and time of the event. You can sort records in ascending or descending order by clicking the arrow in this column.

*Control ID*

The possible values are:

| | |
|---|---|
| Control ID | The control ID of an EDI document. |
| XML | An XML document without a control ID. |
| Binary | A binary document without a control ID. |
| Profile | The document is a profile created with WebLogic Integration – Business Connect. |
| Certificate | The document is an X509 certificate with a public key. |

*ID*

The partner ID or combined EDI qualifier and ID associated with this transaction.

*Status*

The status of the transaction. Possible values include:
For outbound documents:

| | |
|---|---|
| Document Packaged | WebLogic Integration – Business Connect encrypted, signed, and optionally compressed the document. |
| Document Sent | WebLogic Integration – Business Connect sent the document. |
| MDN Received | WebLogic Integration – Business Connect received an acknowledgment from the trading partner indicating the receipt of the document. |

For inbound documents:

| | |
|---|---|
| Document Received | WebLogic Integration – Business Connect received a document from a remote trading partner. |
| Document Transferred | WebLogic Integration – Business Connect decrypted, verified and optionally uncompressed the document and transferred it to the EDI In, XML In, or Binary In directory. |
| MDN Sent | WebLogic Integration – Business Connect sent an acknowledgment to the remote trading partner. |

*Source*

The transport method.

*Original File Name*

The original name of the file. This enables you to distinguish between binary documents because all such documents are listed as binary in the ID field.

*CHAPTER*

# 18 Messages

This section provides lists of system messages that WebLogic Integration – Business Connect generates. These messages are described and, where appropriate, possible remedies for problems are provided.

Although many messages are listed and described, this is not a complete listing. If you encounter a message not described or need help resolving an issue related to operating WebLogic Integration – Business Connect, contact technical support.

The message types are summarized in the following table.

**Table 18-1 Message Types**

| Type | Description |
|---|---|
| Level 0 Messages | Level 0 messages identify normal events in WebLogic Integration – Business Connect. When you set Tracker to display level 0 and above messages, you show most events that occur in WebLogic Integration – Business Connect, including normal milestone events involving the packaging and movement of documents. |
| Level 1 Messages | Level 1 messages identify general notification events requiring no action. When you set Tracker to display level 1 and above messages, WebLogic Integration – Business Connect sends notifications of certain events that are not errors. Level 1 is the default message level in Tracker. |
| Level 2 Messages | Level 2 messages identify documents received from trading partners that WebLogic Integration – Business Connect has rejected. When you set Tracker to display level 2 and above messages, WebLogic Integration – Business Connect logs such errors and sends notifications via e-mail if you provided an e-mail address for notifications on the Company Profile Preferences tab. |

**Table 18-1 Message Types (Continued)**

| Type | Description |
|---|---|
| Level 3 Messages | Level 3 messages identify general errors occurring in WebLogic Integration – Business Connect. When you set Tracker to display level 3 and above messages, WebLogic Integration – Business Connect sends notifications of errors. |
| Level 4 Messages | Level 4 messages identify connection exceptions. When you set Tracker to display level 4 and above messages, WebLogic Integration – Business Connect sends alerts for expected activity. Contact your network administrator for assistance. |
| Level 5 Messages | Level 5 messages identify transport errors. When you set Tracker to display level 5 and above messages, WebLogic Integration – Business Connect sends alerts of problems with the transport configuration. Contact your WebLogic Integration – Business Connect administrator for assistance. |
| Level 6 Messages | Level 6 messages identify that a transport has not been selected for sending documents to a trading partner. When you set Tracker to display level 6 and above messages, WebLogic Integration – Business Connect sends alerts in the event of transport configuration problems. |
| Level 7 Messages | Level 7 messages identify unexpected errors. When you set Tracker to display level 7 and above messages, WebLogic Integration – Business Connect sends alerts of errors not accounted for under other levels. |
| Level 8 Messages | Level 8 messages identify duplicate server errors. When you set Tracker to display level 8 messages only, WebLogic Integration – Business Connect sends alerts. |

# Level 0 Messages

Level 0 messages identify normal events in WebLogic Integration – Business Connect. When you set Tracker to display level 0 and above messages, you show most events that occur in WebLogic Integration – Business Connect, including normal milestone events involving the packaging and movement of documents.

You usually set Tracker to show level 0 messages only as a debugging tool for use in resolving issues external to WebLogic Integration – Business Connect that nonetheless affect the application's performance. Such issues might involve network infrastructure, operating systems, directory or file permissions, or TCP/IP services.

Despite the usefulness of level 0 messages for debugging, the messages themselves denote normal events. On their own, level 0 messages do not require corrective action. It is the sequence or lack of messages in certain contexts that can indicate errors. For this reason, we recommend that beginner users of WebLogic Integration – Business Connect not set Tracker for level 0 messages, except at the direction of customer support. Experienced WebLogic Integration – Business Connect users, however, might find level 0 messages useful in troubleshooting problems.

**Note:** If you turn on level 0 messages, WebLogic Integration – Business Connect processing speed slows considerably.

**Table 18-2 Level 0 Messages**

| Level 0 message | Description |
|---|---|
| Agent started | An agent has started and is running. |
| Alert sent | An alert e-mail message has been created and sent. |
| Archive completed | The archiving process has completed successfully. |
| Backup file has been archived | A confirmation that a file was moved successfully from the backup directory to the archive directory. |
| Backup file has been deleted | A confirmation that a file was deleted successfully from the backup directory during the archiving process. |
| Companies started | Server has completed its startup routine. |
| Companies starting | Server starts all company-based threads (packager, inbound, https servers, and so on). |
| Duplicate MDN received | WebLogic Integration – Business Connect received a message disposition notice (MDN) for an outbound document that already has been acknowledged. This is because the original document was resent automatically, so multiple MDNs were returned. Or, the MDN was not deleted from the transport server after it was processed. |

**Table 18-2 Level 0 Messages (Continued)**

| Level 0 message | Description |
|---|---|
| Duplicate received (automated resend) | WebLogic Integration – Business Connect received more than once a document that a partner resent automatically. WebLogic Integration – Business Connect discards all subsequent documents. |
| File backed up | A file has been copied to the backup directory. |
| MDN received with no matching outbound document | WebLogic Integration – Business Connect received an MDN for which there is no current record of a matching outbound document in the database. This might be because an outbound record was archived. |
| Partner certificate updated | A partner certificate has been changed, and the database has been updated successfully. |
| Partner profile updated | A partner profile has been changed, and the database has been updated successfully. |
| Server configuration completed | Server has successfully configured all agents and threads. |
| Server configuration started | Server starts all agents and threads and also starts building Administrator objects such as companies, partners, certificates and schedules. |
| Server shutdown completed | Server has successfully shut down all agents and threads. |
| Server shutdown started | Server begins the process of cleanly shutting down agents and threads. |
| Software registered | A software registration e-mail message has been created and sent. |

# Level 1 Messages

Level 1 messages identify general notification events requiring no action. When you set Tracker to display level 1 and above messages, WebLogic Integration – Business Connect sends notifications of certain events that are not errors. Level 1 is the default message level in Tracker.

**Table 18-3 Level 1 Messages**

| Level 1 message | Description |
|---|---|
| MDN received | WebLogic Integration – Business Connect has received a message disposition notice (MDN), which confirms that the partner has received the document you sent. |
| MDN sent | WebLogic Integration – Business Connect has sent an MDN to a trading partner to acknowledge receiving a document from that partner. |
| Packaged | WebLogic Integration – Business Connect has successfully packaged a document for delivery. Packaged means the document has been encrypted and MIME wrapped. |
| Received | WebLogic Integration – Business Connect has received a document from a trading partner. |
| Sent | WebLogic Integration – Business Connect has successfully sent a document to a trading partner. |
| Transferred | WebLogic Integration – Business Connect has successfully copied a document received from a trading partner to the inbound and backup directories. |

# Level 2 Messages

Level 2 messages identify documents received from trading partners that WebLogic Integration – Business Connect has rejected. When you set Tracker to display level 2 and above messages, WebLogic Integration – Business Connect logs such errors and sends notifications via e-mail if you provided an e-mail address for notifications on the Company Profile Preferences tab.

Examples of events at this level include when WebLogic Integration – Business Connect rejects a document because there is no active partner or when the application cannot decrypt a document.

**Table 18-4 Level 2 Messages**

| Level 2 message | Description, cause, remedy |
|---|---|
| Received miscellaneous document | WebLogic Integration – Business Connect received a binary or unidentifiable document that could not be associated with a partner. The file was placed in the company's `other` directory.<br>**Cause 1**<br>WebLogic Integration – Business Connect received a binary document for a partner that has not been configured to receive such documents. In other words, there was no matching partner for the inbound document.<br>**Remedy 1**<br>Examine the received file as necessary. Select a company for this partner in the binary company drop-down list in the partner's profile in WebLogic Integration – Business Connect.<br>**Cause 2**<br>A MIME message does not have body parts. WebLogic Integration – Business Connect received an e-mail message without an attachment for this partner.<br>**Remedy 2**<br>Resend or resubmit this document in Tracker. If necessary, examine the document in the other directory to see whether it is the one you need to receive. You then can manually route it to the appropriate application.<br>If you want to receive binary documents from this partner, select a company in the binary company drop-down list in the partner's profile in WebLogic Integration – Business Connect. |

# Level 3 Messages

Level 3 messages identify general errors occurring in WebLogic Integration – Business Connect. When you set Tracker to display level 3 and above messages, WebLogic Integration – Business Connect sends notifications of errors.

An example of an event at this level is when WebLogic Integration – Business Connect receives a message disposition notice (MDN) indicating a partner could not process a document from you. Another example is when you try to start WebLogic Integration – Business Connect when it is already running.

**Table 18-5 Level 3 Messages**

| Level 3 message | Description, cause, remedy |
|---|---|
| Duplicate document | WebLogic Integration – Business Connect received an EDI document with a control ID that was the same as a previously received document's control ID. WebLogic Integration – Business Connect detected this because the check box for preserving inbound binary and XML file names is selected for the partner's profile.<br>**Cause 1**<br>Your partner sent you more than one EDI document with the same control ID.<br>**Remedy 1**<br>If necessary, contact your partner for clarification.<br>**Cause 2**<br>The check box for preserving inbound binary and XML file names is unintentionally selected on the Preferences tab for the partner's profile.<br>**Remedy 2**<br>Turn off the selection for the partner's profile. |

**Table 18-5 Level 3 Messages (Continued)**

| Level 3 message | Description, cause, remedy |
|---|---|
| EDI parsing error | WebLogic Integration – Business Connect attempted to process a malformed X12 or EDIFACT document from your translator and rejected it.<br>**Cause 1**<br>Your translator put a malformed EDI document in the WebLogic Integration – Business Connect EDI outbound directory.<br>**Remedy 1**<br>Have your translator resubmit the document. Or, verify whether the rejected file is an EDI file; if not put the file in the correct outbound directory.<br>**Cause 2**<br>WebLogic Integration – Business Connect received a malformed EDI document from a trading partner. The application determines this by checking the document for certain standard information that EDI documents should have.<br>**Remedy 2**<br>Examine the file and contact the partner to resolve the EDI formatting problem. |

**Table 18-5 Level 3 Messages (Continued)**

| Level 3 message | Description, cause, remedy |
|---|---|
| Insufficient security: not encrypted | WebLogic Integration – Business Connect received an encrypted document from a partner, but was expecting to receive an unencrypted document. Or, WebLogic Integration – Business Connect received an unencrypted document from a partner, but was expecting to receive an encrypted document.<br>WebLogic Integration – Business Connect requires you and your partner to have identical settings for signing documents, encrypting documents, acknowledging documents and signing acknowledgments.<br>**Cause 1**<br>You and your partner do not have synchronized settings for document encryption.<br>**Remedy 1**<br>Make sure you and your partner have the same setting for document encryption on the Partner Profile Security tab for your respective partners. The encrypt documents check box should be either checked or unchecked on both systems. Once the setting is synchronized, have your partner resend the document. |

**Table 18-5 Level 3 Messages (Continued)**

| Level 3 message | Description, cause, remedy |
|---|---|
| Insufficient security: not signed | WebLogic Integration – Business Connect received a signed document or MDN from a partner, but was expecting to receive an unsigned document or MDN. Or, WebLogic Integration – Business Connect received an unsigned document or MDN from a partner, but was expecting to receive a signed document or MDN.<br>WebLogic Integration – Business Connect requires you and your partner to have identical settings for signing documents, encrypting documents, acknowledging documents and signing acknowledgments.<br>**Cause 1**<br>You and your partner do not have synchronized settings for document signing.<br>**Remedy 1**<br>Make sure you and your partner have the same setting for document signing on the Partner Profile Security tab for your respective partners. The sign documents check box should be either checked or unchecked on both systems. Once the setting is synchronized, have your partner resend the document.<br>**Cause 2**<br>WebLogic Integration – Business Connect received an unsigned MDN.<br>**Remedy 2**<br>Make sure you and your partner have the same setting for acknowledgments on the Partner Profile Security tab for your respective partners. The acknowledgment check box should be checked on both systems. |
| Invalid certificate used to verify | The certificate used to sign the document does not match a valid partner certificate.<br>**Cause 1**<br>The certificate the partner is using to sign does not match one of your valid certificates for that partner.<br>**Remedy 1**<br>Verify with the partner that certificates are correct. |

**Table 18-5 Level 3 Messages (Continued)**

| Level 3 message | Description, cause, remedy |
|---|---|
| Invalid MDN received | WebLogic Integration – Business Connect received an MDN that has a disposition of *null* or something other than *processed, displayed* or *dispatched*.<br>**Cause 1**<br>Your partner failed to verify or decrypt a document that you sent.<br>**Remedy 1**<br>Open the MDN with a text editor and determine its disposition. Compare the fingerprints in your and your partner's certificates.<br>**Cause 2**<br>The partner had an unexpected parsing or processing error.<br>**Remedy 2**<br>Examine the disposition of the rejected MDN. Verify with the partner that certificates are correct. |

**Table 18-5 Level 3 Messages (Continued)**

| Level 3 message | Description, cause, remedy |
|---|---|
| Malformed MIME message | WebLogic Integration – Business Connect received a malformed multipurpose Internet mail extensions (MIME) message.<br>**Cause 1**<br>Data were corrupted during transport.<br>**Remedy 1**<br>Examine the rejected file to determine the document type, sender, and so on. Ask the partner to resend the document to you.<br>**Cause 2**<br>The trading partner is using FTP and has unchecked the check boxes for signing, encrypting and acknowledging documents on the Partner Profile Security tab. Because of this, the document was sent in FTP ASCII mode.<br>**Remedy 2**<br>Ask the partner to check the check box for signing or encrypting documents on the Partner Profile Security tab or for compressing documents on the Partner Profile Preferences tab. This ensures documents are sent in FTP binary mode.<br>WebLogic Integration – Business Connect requires you and your partner to have identical settings for signing documents, encrypting documents, acknowledging documents and signing acknowledgments.<br>**Cause 3**<br>WebLogic Integration – Business Connect received via FTP a non-MIME wrapped document either from a partner who has turned off document signing, encrypting, acknowledging and compression in WebLogic Integration – Business Connect or from a partner who uses a trading engine other than WebLogic Integration – Business Connect. WebLogic Integration – Business Connect does not support receiving non-MIME wrapped data.<br>**Remedy 3**<br>If your partner uses WebLogic Integration – Business Connect, ask your partner to turn on document signing, encrypting, acknowledging or compression for sending via FTP. Then ask your partner to resend the document. |

**Table 18-5 Level 3 Messages (Continued)**

| Level 3 message | Description, cause, remedy |
|---|---|
| No active encryption certificate | WebLogic Integration – Business Connect attempted to encrypt a document for a partner for whom you do not have an active certificate.<br>**Cause 1**<br>You have one or more certificates for this partner, but none are active.<br>**Remedy 1**<br>In the Certificates window in WebLogic Integration – Business Connect, select and activate the certificate.<br>**Cause 2**<br>There are no certificates for this partner.<br>**Remedy 2**<br>Ask the partner to send you a certificate.<br>**Cause 3**<br>You do not want to exchange encrypted documents with this partner.<br>**Remedy 3**<br>Clear the encrypt documents check box on the Security tab for this partner profile in WebLogic Integration – Business Connect. |

**Table 18-5 Level 3 Messages (Continued)**

| Level 3 message | Description, cause, remedy |
|---|---|
| No active partner | WebLogic Integration – Business Connect attempted to process a document for which there is no active partner.<br>**Cause 1**<br>An EDI or XML document was dropped in the corresponding outbound directory. The document's recipient ID does not match any active partner.<br>**Remedy 1**<br>Import and activate the profile of the partner to whom the document addressed. Resend the document in Tracker.<br>If you do not want to send documents to this partner, make sure your EDI translator or XML application does not place documents in the outbound directories for WebLogic Integration – Business Connect.<br>**Cause 2**<br>WebLogic Integration – Business Connect received a document from an inactive or nonexistent partner.<br>**Remedy 2**<br>If you do not have a profile for this partner, ask the partner to send you one that you can import to WebLogic Integration – Business Connect.<br>If you have a profile for this partner but it is inactive, activate it in the Partner window in WebLogic Integration – Business Connect. |

**Table 18-5 Level 3 Messages (Continued)**

| Level 3 message | Description, cause, remedy |
|---|---|
| No active signer certificate | WebLogic Integration – Business Connect attempted to sign a document or an MDN for a company for which there is no active certificate.<br>**Cause 1**<br>A certificate exists for this company profile, but it is not active.<br>**Remedy 1**<br>In the Certificates window in WebLogic Integration – Business Connect, select and activate the certificate.<br>**Cause 2**<br>There is no certificate for this company profile.<br>**Remedy 2**<br>Generate a self-signed certificate from the Certificates window in WebLogic Integration – Business Connect. Or, import a third-party certificate.<br>**Cause 3**<br>You do not want to exchange signed documents with this partner.<br>**Remedy 3**<br>Clear the sign documents check box on the Security tab for this partner profile in WebLogic Integration – Business Connect. |

**Table 18-5 Level 3 Messages (Continued)**

| Level 3 message | Description, cause, remedy |
|---|---|
| Returned message | WebLogic Integration – Business Connect received a message from a partner who has an ID identical to yours.<br>**Cause 1**<br>You are trading documents with yourself (that is, testing with a single company exported or imported as the partner).<br>**Remedy 1**<br>Create another company profile with a different ID. Export and import the second company and have the first company trade with the second company.<br>**Cause 2**<br>The transport server (most likely SMTP-POP) has returned or bounced the message.<br>**Remedy 2**<br>Verify the partner’s e-mail address and the state of the SMTP-POP server and connection.<br>**Cause 3**<br>There are two real-world companies with identical IDs.<br>**Remedy 3**<br>Create another company profile with a unique ID or ask your partner to do so. |
| Security framework failed to verify signature | WebLogic Integration – Business Connect failed to verify the signature of a document. This indicates that the document you received has changed in some way from the original document that your partner sent you.<br>**Cause 1**<br>The document was corrupted in transport.<br>**Remedy 1**<br>Ask your partner to resend the document to you.<br>**Cause 2**<br>An untrusted party attempted to send you a document.<br>**Remedy 2**<br>Ask your partner to verify the document. |

**Table 18-5 Level 3 Messages (Continued)**

| Level 3 message | Description, cause, remedy |
|---|---|
| Security framework unable to verify - certificate expired | The certificate your partner used to sign a document you received has expired.<br>**Cause 1**<br>The certificate has expired.<br>**Remedy 1**<br>Ask your partner to generate or purchase a new certificate.<br>**Cause 2**<br>Your and your partner's system time or time zone settings are not synchronized.<br>**Remedy 2**<br>You and your partner should synchronize your system clocks. WebLogic Integration – Business Connect calculates Greenwich Mean Time (GMT) for document traffic based on the local time zones you select in WebLogic Integration – Business Connect and for your operating system. This serves to synchronize time between you and your trading partners. Make sure you and your partner have selected your local time zones in WebLogic Integration – Business Connect and in your operating systems. |

**Table 18-5 Level 3 Messages (Continued)**

| Level 3 message | Description, cause, remedy |
|---|---|
| Security framework unable to verify - certificate not yet valid | The partner's certificate that is used to verify an inbound document is not valid. This is because the date the certificate was created is later than your system's current date.<br>**Cause 1**<br>The certificate is not valid yet.<br>**Remedy 1**<br>Contact the partner. Wait until the certificate is active or request the partner to generate or purchase a new certificate.<br>**Cause 2**<br>Your and your partner's system time or time zone settings are not synchronized.<br>**Remedy 2**<br>You and your partner should synchronize your system clocks. WebLogic Integration – Business Connect calculates Greenwich Mean Time (GMT) for document traffic based on the local time zones you select in WebLogic Integration – Business Connect and for your operating system. This serves to synchronize time between you and your trading partners. Make sure you and your partner have selected your local time zones in WebLogic Integration – Business Connect and in your operating systems. |
| Security framework unable to verify - invalid signature | The certificate within an S/MIME document you received has changed.<br>**Cause 1**<br>The document was corrupted during transport.<br>**Remedy 1**<br>Contact the partner and request a resend or wait for an automatic resend.<br>**Cause 2**<br>Your trading partner might have changed his or her certificate without updating you.<br>**Remedy 2**<br>Ask your trading partner to send you a new certificate. |

**Table 18-5 Level 3 Messages (Continued)**

| Level 3 message | Description, cause, remedy |
|---|---|
| Security framework unable to verify - root not found | The root certificate of the certificate used to sign a received document does not exist in the root store.<br>**Cause 1**<br>The document was corrupted during transport.<br>**Remedy 1**<br>You can either ask your partner to resend the document to you or you can wait until WebLogic Integration – Business Connect automatically resends the document to you. |
| Security framework unable to verify - unknown root | The certificate your partner used to sign a document has an unknown or untrusted root certificate.<br>**Cause 1**<br>The certificate chain that your partner uses to sign documents does not match one of the valid certificate chains you have for that partner.<br>**Remedy 1**<br>Ask your partner to verify whether the partner's certificate and your certificate are correct.<br>**Cause 2**<br>An untrusted party attempted to send you a document.<br>**Remedy 2**<br>Ask the partner to verify the document that was sent. |
| The returned MDN MIC value was invalid | WebLogic Integration – Business Connect received an MDN with a MIC (message integrity check) that does not match that of the corresponding outbound document.<br>**Cause 1**<br>A non-trusted party has sent the MDN.<br>**Remedy 1**<br>Contact the partner to verify the state of the remote servers and network. |

**Table 18-5 Level 3 Messages (Continued)**

| Level 3 message | Description, cause, remedy |
|---|---|
| Unable to decrypt | The decryption of a public key-encrypted MIME message failed.<br>**Cause 1**<br>The public key the partner is using to encrypt does not match one of your valid private keys.<br>**Remedy 1**<br>Verify with the partner that the certificates are correct.<br>**Cause 2**<br>The data was corrupted during transport.<br>**Remedy 2**<br>Contact the partner and request a resend. |
| XML parsing error | WebLogic Integration – Business Connect attempted to process a malformed XML document and rejected it.<br>**Cause 1**<br>Your XML application put a malformed XML document in the WebLogic Integration – Business Connect XML outbound directory.<br>**Remedy 1**<br>Have your XML application resubmit the document. Or, verify whether the rejected file is an XML file; if not put the file in the correct outbound directory.<br>**Cause 2**<br>WebLogic Integration – Business Connect received and rejected a malformed XML document.<br>**Remedy 2**<br>Examine the file and contact the partner to resolve the formatting problem. |

# Level 4 Messages

Level 4 messages identify connection exceptions. When you set Tracker to display level 4 and above messages, WebLogic Integration – Business Connect sends alerts for expected activity. Contact your network administrator for assistance.

An example of an event at this level is when WebLogic Integration – Business Connect cannot connect to the network or to a server.

**Table 18-6 Level 4 Messages**

| Level 4 message | Description, cause, remedy |
|---|---|
| Resend limit reached | WebLogic Integration – Business Connect has resent the document the configured number of times but has not received an acknowledgement from the trading partner.<br>**Cause 1**<br>If you are sending documents by e-mail, the e-mail address might be incorrect.<br>**Remedy 1**<br>Verify the e-mail address with your trading partner.<br>**Cause 2**<br>The partner's transport server is failing or not in service.<br>**Remedy 2**<br>Contact the partner.<br>**Cause 3**<br>The partner is not online.<br>**Remedy 3**<br>Contact the partner and verify that the partner’s trading engine is online.<br>**Cause 4**<br>If you are sending documents by FTP, the FTP information might be incorrect.<br>**Remedy 4**<br>Verify with your partner the FTP inbox and pickup directories and the FTP server. |

# Level 5 Messages

Level 5 messages identify transport errors. When you set Tracker to display level 5 and above messages, WebLogic Integration – Business Connect sends alerts of problems with the transport configuration. Contact your WebLogic Integration – Business Connect administrator for assistance.

An example of such an event is incorrect settings for a transport, such as an incorrect password or mail server.

**Table 18-7 Level 5 Messages**

| Level 5 message | Description, cause, remedy |
|---|---|
| Network error: inbound<br>or<br>Network error: outbound | WebLogic Integration – Business Connect is unable to send or receive documents due to transport protocol or network problems.<br>**Cause 1**<br>The FTP or POP server is offline.<br>**Remedy 1**<br>Verify the status of the POP server or FTP server or both.<br>**Cause 2**<br>The local network is down.<br>**Remedy 2**<br>Verify the network status.<br>**Cause 3**<br>A firewall might be impeding document transport.<br>**Remedy 3**<br>Verify correct connectivity through the firewall for inbound and outbound documents. |

**Table 18-7 Level 5 Messages (Continued)**

| Level 5 message | Description, cause, remedy |
|---|---|
| Unable to send | WebLogic Integration – Business Connect cannot send documents due to transport protocol or network problems.<br>**Cause 1**<br>The SMTP or FTP server is offline.<br>**Remedy 1**<br>Verify the status of the SMTP or FTP server.<br>**Cause 2**<br>The local network or Internet connection is down.<br>**Remedy 2**<br>Verify the network status.<br>**Cause 3**<br>The partner's HTTPS server is offline.<br>**Remedy 3**<br>Contact the partner and verify the status of the HTTPS server. |

# Level 6 Messages

Level 6 messages identify that a transport has not been selected for sending documents to a trading partner. When you set Tracker to display level 6 and above messages, WebLogic Integration – Business Connect sends alerts in the event of transport configuration problems.

**Table 18-8 Level 6 Messages**

| Level 6 message | Description, cause, remedy |
|---|---|
| Active transport for partner has been disabled | The partner is no longer listening on the active transport.<br>**Cause 1**<br>A partner profile has been electronically updated. In other words, your partner has switched from one transport to another for receiving documents.<br>**Remedy 1**<br>Activate a new transport for the partner. |
| No active transport | WebLogic Integration – Business Connect attempted to send a document or MDN to a partner who does not have an active transport.<br>**Cause 1**<br>You created or imported a partner profile, but did not activate a transport.<br>**Remedy 1**<br>Activate a transport for the partner on the Partner Profile Transports tab. |

# Level 7 Messages

Level 7 messages identify unexpected errors. When you set Tracker to display level 7 and above messages, WebLogic Integration – Business Connect sends alerts of errors not accounted for under other levels.

Examples of such events are:

- A document could not be packaged (error building the MIME message)
- Configuration data from the database could not be read

**Table 18-9 Level 7 Messages**

| Level 7 message | Description, cause, remedy |
|---|---|
| Any level 7 message | All of level 7 (unexpected exception) events indicate application bugs.<br>**Cause 1**<br>Level 7 events indicate application bugs.<br>**Remedy 1**<br>Report the events to technical support. |

# Level 8 Messages

Level 8 messages identify duplicate server errors. When you set Tracker to display level 8 messages only, WebLogic Integration – Business Connect sends alerts.

An example of such an event is when the server is unable to run because the server already is running.

**Table 18-10 Level 8 Messages**

| Level 8 message | Description, cause, remedy |
|---|---|
| Unable to create directory. Shutting down | Server attempted to create the necessary directories and failed.<br>**Cause 1**<br>The directories are not set correctly.<br>**Remedy 1**<br>Verify the directories in the company, partner and tools panels.<br>**Cause 2**<br>The current user does not have write permission.<br>**Remedy 2**<br>Verify the current user has write permission in the application install directory. |

# A ISO Country Codes

The following table provides the International Organization for Standardization (ISO) two-character country codes. You can use one of these codes in the ISO country code field on the Company Profile window Identity tab. See "Company Profile Identity Tab" on page 9-19.

For updates or countries not listed in this table, search the Internet for "ISO country codes."

**Table B-11 ISO Country Codes**

| Code | Country |
|---|---|
| af | Afghanistan |
| al | Albania |
| dz | Algeria |
| as | American Samoa |
| ad | Andorra |
| ao | Angola |
| ai | Anguilla |
| aq | Antarctica |
| ag | Antigua and Barbuda |
| ar | Argentina |
| am | Armenia |
| aw | Aruba |

**Table B-11 ISO Country Codes (Continued)**

| Code | Country |
|---|---|
| au | Australia |
| at | Austria |
| az | Azerbaidjan |
| bs | Bahamas |
| bh | Bahrain |
| bd | Bangladesh |
| bb | Barbados |
| by | Belarus |
| be | Belgium |
| bz | Belize |
| bj | Benin |
| bm | Bermuda |
| bt | Bhutan |
| bo | Bolivia |
| ba | Bosnia-Herzegovina |
| bw | Botswana |
| bv | Bouvet Island |
| br | Brazil |
| io | British Indian Ocean Territory |
| bn | Brunei Darussalam |
| bg | Bulgaria |
| bf | Burkina Faso |
| bi | Burundi |

**Table B-11 ISO Country Codes (Continued)**

| Code | Country |
|---|---|
| kh | Cambodia |
| cm | Cameroon |
| ca | Canada |
| cv | Cape Verde |
| ky | Cayman Islands |
| cf | Central African Republic |
| td | Chad |
| cl | Chile |
| cn | China |
| cx | Christmas Island |
| cc | Cocos (Keeling) Islands |
| co | Colombia |
| km | Comoros |
| cg | Congo |
| ck | Cook Islands |
| cr | Costa Rica |
| hr | Croatia |
| cu | Cuba |
| cy | Cyprus |
| cz | Czech Republic |
| dk | Denmark |
| dj | Djibouti |
| dm | Dominica |

**Table B-11 ISO Country Codes (Continued)**

| Code | Country |
|---|---|
| do | Dominican Republic |
| tp | East Timor |
| ec | Ecuador |
| eg | Egypt |
| sv | El Salvador |
| gq | Equatorial Guinea |
| er | Eritrea |
| ee | Estonia |
| et | Ethiopia |
| fk | Falkland Islands |
| fo | Faroe Islands |
| fj | Fiji |
| fi | Finland |
| cs | Former Czechoslovakia |
| su | Former USSR |
| fr | France |
| fx | France (European Territory) |
| gf | French Guyana |
| tf | French Southern Territories |
| ga | Gabon |
| gm | Gambia |
| ge | Georgia |
| de | Germany |

Table B-11 ISO Country Codes (Continued)

| Code | Country |
|---|---|
| gh | Ghana |
| gi | Gibraltar |
| gb | Great Britain |
| gr | Greece |
| gl | Greenland |
| gd | Grenada |
| gp | Guadeloupe (French) |
| gu | Guam (USA) |
| gt | Guatemala |
| gn | Guinea |
| gw | Guinea Bissau |
| gy | Guyana |
| ht | Haiti |
| hm | Heard and McDonald Islands |
| hn | Honduras |
| hk | Hong Kong |
| hu | Hungary |
| is | Iceland |
| in | India |
| id | Indonesia |
| int | International |
| ir | Iran |
| iq | Iraq |

**Table B-11 ISO Country Codes (Continued)**

| Code | Country |
|---|---|
| ie | Ireland |
| il | Israel |
| it | Italy |
| ci | Ivory Coast (Cote D'Ivoire) |
| jm | Jamaica |
| jp | Japan |
| jo | Jordan |
| kz | Kazakhstan |
| ke | Kenya |
| ki | Kiribati |
| kw | Kuwait |
| kg | Kyrgyzstan |
| la | Laos |
| lv | Latvia |
| lb | Lebanon |
| ls | Lesotho |
| lr | Liberia |
| ly | Libya |
| li | Liechtenstein |
| lt | Lithuania |
| lu | Luxembourg |
| mo | Macau |
| mk | Macedonia |

**Table B-11 ISO Country Codes (Continued)**

| Code | Country |
|---|---|
| mg | Madagascar |
| mw | Malawi |
| my | Malaysia |
| mv | Maldives |
| ml | Mali |
| mt | Malta |
| mh | Marshall Islands |
| mq | Martinique (French) |
| mr | Mauritania |
| mu | Mauritius |
| yt | Mayotte |
| mx | Mexico |
| fm | Micronesia |
| md | Moldavia |
| mc | Monaco |
| mn | Mongolia |
| ms | Montserrat |
| ma | Morocco |
| mz | Mozambique |
| mm | Myanmar |
| na | Namibia |
| nr | Nauru |
| np | Nepal |

**Table B-11 ISO Country Codes (Continued)**

| Code | Country |
|---|---|
| nl | Netherlands |
| an | Netherlands Antilles |
| net | Network |
| nt | Neutral Zone |
| nc | New Caledonia (French) |
| nz | New Zealand |
| ni | Nicaragua |
| ne | Niger |
| ng | Nigeria |
| nu | Niue |
| nf | Norfolk Island |
| kp | North Korea |
| mp | Northern Mariana Islands |
| no | Norway |
| om | Oman |
| pk | Pakistan |
| pw | Palau |
| pa | Panama |
| pg | Papua New Guinea |
| py | Paraguay |
| pe | Peru |
| ph | Philippines |
| pn | Pitcairn Island |

**Table B-11 ISO Country Codes (Continued)**

| Code | Country |
|---|---|
| pl | Poland |
| pf | Polynesia (French) |
| pt | Portugal |
| pr | Puerto Rico |
| qa | Qatar |
| re | Reunion (French) |
| ro | Romania |
| ru | Russian Federation |
| rw | Rwanda |
| gs | S. Georgia & S. Sandwich Isls. |
| sh | Saint Helena |
| kn | Saint Kitts & Nevis Anguilla |
| lc | Saint Lucia |
| pm | Saint Pierre and Miquelon |
| st | Saint Tome (Sao Tome) and Principe |
| vc | Saint Vincent & Grenadines |
| ws | Samoa |
| sm | San Marino |
| sa | Saudi Arabia |
| sn | Senegal |
| sc | Seychelles |
| sl | Sierra Leone |
| sg | Singapore |

**Table B-11 ISO Country Codes (Continued)**

| Code | Country |
|---|---|
| sk | Slovak Republic |
| si | Slovenia |
| sb | Solomon Islands |
| so | Somalia |
| za | South Africa |
| kr | South Korea |
| es | Spain |
| lk | Sri Lanka |
| sd | Sudan |
| sr | Suriname |
| sj | Svalbard and Jan Mayen Islands |
| sz | Swaziland |
| se | Sweden |
| ch | Switzerland |
| sy | Syria |
| tj | Tadjikistan |
| tw | Taiwan |
| tz | Tanzania |
| th | Thailand |
| tg | Togo |
| tk | Tokelau |
| to | Tonga |
| tt | Trinidad and Tobago |

**Table B-11 ISO Country Codes (Continued)**

| Code | Country |
|---|---|
| tn | Tunisia |
| tr | Turkey |
| tm | Turkmenistan |
| tc | Turks and Caicos Islands |
| tv | Tuvalu |
| ug | Uganda |
| ua | Ukraine |
| ae | United Arab Emirates |
| uk | United Kingdom |
| us | United States |
| uy | Uruguay |
| um | USA Minor Outlying Islands |
| uz | Uzbekistan |
| vu | Vanuatu |
| va | Vatican City State |
| ve | Venezuela |
| vn | Vietnam |
| vg | Virgin Islands (British) |
| vi | Virgin Islands (USA) |
| wf | Wallis and Futuna Islands |
| eh | Western Sahara |
| ye | Yemen |
| yu | Yugoslavia |

**Table B-11 ISO Country Codes (Continued)**

| Code | Country |
|---|---|
| zr | Zaire |
| zm | Zambia |
| zw | Zimbabwe |

# Index