IBM WebSphere Business Connection

Administering the System

Version 1.1.0

Note!
Before using this information and the product it supports, be sure to read the general information under "Notices" on page 43.

First Edition (September 2002)

This edition applies to Version 1, Release 1, Modification 0, of *IBM® WebSphere® Business Connection* (5724-D26) and to all subsequent releases and modifications until otherwise indicated in new editions.

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

IBM Canada Ltd. Laboratory
Information Development
8200 Warden Avenue
Markham, Ontario, Canada L6G 1C7

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

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

Contents

Administering the System

This document provides you with step-by-step instructions on performing administrative tasks on your IBM(R) WebSphere(R) Business Connection system. Many of the tasks described in the document, from starting the Business Connection servers through accepting the registration request of a trading partner, are performed through the Business Connection Admin console. Other tasks, such as adding security between Web Service Gateways, are also described.

The Business Connection Admin Console and most of the tasks described in this document apply only to Business Connection and Business Connection Enterprise Editions. The console and the functions described are not available on the Business Connection Express Edition. The last sections of the book—the information on security and on determining the version of your Business Connection edition—apply to all editions.

Administrative tasks that are performed from the Web Services Gateway console, available on all editions of Business Connection, are described in Using the Web Services Gateway.

How this document is organized

This document begins with a description of the Business Connection Admin Console and covers basic operations such as starting and stopping the Business Connection servers. It then shows you how to set up logging and tracing and how to view messages from CrossWorlds and Web Services Gateway.

The next section covers Registration and Provisioning. After you install a Business Connection system and learn about the basic operations, you will want to begin registering with trading partners so that you can exchange information and subscribe to services. If you are a service provider, you'll learn how to create offers and make services available to your partners.

Once you are registered with partners, you can begin using services, such as the Document Exchange service that is a part of Business Connection. Then you'll see how you can view logs for the Document Exchange and Registration and Provisioning services.

Finally, you will be given step-by-step instructions on providing additional security (beyond what was covered in the Installation and Configuration document). You will also see how to determine the version of your product. These sections apply to all editions of WebSphere Business Connection.

Starting the Admin Console

The Business Connection Admin Console looks like this:

Figure: The Welcome screen, with a Business Connection Admin Console banner

Note: As part of the installation of Business Connection, you were instructed to configure an application server in WebSphere Application Server for the System Resources Admin console. If you have not done so, please refer now to Installation and Configuration.

Note that if you have security enabled, you should specify **https** (rather than **http**) in any URL specifications.

To start the application server for the Business Connection Admin Console:

1. If it is not already running, start the WebSphere Application Server.
2. Start the WebSphere Application Server Administrative Console.
3. Right-click on all the application servers and click **Start**.
4. Enter the following URL to bring up the Business Connection Admin Console:
   `http://<fully qualified hostname>/WBC/index.jsp;`
5. If security has been installed on your system, you will be asked to enter a user ID and password. Use the same user ID and password you used when you registered as a company.

Selecting a task from the WebSphere Business Connection Admin Console

To select a task from the console, click one of the entries from the menu bar. The tasks that you can perform are described in the sections that follow:

- "System Control"
- "Log/Trace Setup" on page 3
- "Log Viewer" on page 5
- "Document Exchange" on page 21
- "Registration and Provisioning" on page 9

System Control

From System Control, you can start and stop the CrossWorlds InterChange Server and the Web Services Gateway application server.

Starting the Business Connection servers

To start the servers:

1. From the Business Connection Admin Console, click **System Control**.
2. To start the CrossWorlds InterChange Server, click **Start**.
3. To start the Web Services Gateway application server, click **Refresh Status** to see the current status of the server. Then click **Start**.

   If the status for the Web Services Gateway application server is **Server Unknown**, the application server was not fully stopped. Wait a few minutes and try again.

Stopping the Business Connection servers

To stop the servers:

1. From the Business Connection Admin Console, select **System Control**.
2. To stop the CrossWorlds InterChange Server, click **Stop**.
3. To stop the Web Services Gateway application server, click **Refresh Status** to see the current status of the server. Then click **Stop**.

   If the status for the Web Services Gateway application server is **Server Unknown**, the application server was not fully started. Wait a few minutes and try again.

Log/Trace Setup

The WebServices Gateway and CrossWorlds components provide the ability to log and trace information. You view these logs using the “Log Viewer” on page 5.

The Log/Trace Setup lets you identify *where* you want the logging information stored (if you want it stored somewhere other than the default location).

In addition, Log/Trace Setup lets you specify whether you want tracing enabled and, if so, at which level you want the tracing to occur.

Changing the location of log files

To change the location of the CrossWorlds trace file, Web Services log file, or both:

1. From the Business Connection Admin Console, click **Log/Trace Setup**.
2. To change the name of the CrossWorlds log file, edit the name in the **Logging File Name** field.
3. To change the name of the Web Services Gateway log file, edit the name in the **WorkingDir** field or the **Stdout** field or both.
4. Click **Submit**.

Changing the location of trace files

To change the location of the CrossWorlds trace file, Web Services trace file, or both:

1. From the Business Connection Admin Console, click **Log/Trace Setup**.
2. To change the name of the CrossWorlds trace file, edit the name in the **Tracing File Name** field under CrossWorlds.
3. To change the name of the Web Services Gateway trace file, edit the name in the **Tracing File Name** field under Web Services Gateway. A complete path and file name must be specified.
4. Click **Submit**.

Setting a trace level

Tracing is turned off by default.

To turn on tracing or to change the trace level that is currently set:

1. From the Business Connection Admin Console, select **Log/Trace Setup**.
2. To set tracing or to change the value that is currently shown, click a number in the trace list.
3. Click **Submit**.

Because tracing consumes resources, you will probably want to turn tracing on only when you are trying to discover the cause of a problem. The range of trace levels is 0 through 5 (with 0 being no tracing and 5 being the highest level of tracing).

Log Viewer

The Log Viewer lets you display the logs or trace files for the CrossWorlds InterChange Server and the Web Services Gateway as well as for the Document Exchange and Registration and Provisioning services.

Log File Viewer

From the Log File Viewer, you can view the following:

- CrossWorlds InterChange Server log files
- CrossWorlds InterChange Server trace files
- Web Services Gateway Application Server Stdout log files
- Web Services Gateway Application Server Stderr log files
- Web Services Gateway Application Server trace files

Viewing a log file

To view the messages in a log file:

1. From the Business Connection Admin Console, select **Log Viewer > Log File Viewer**.
2. Click the name of the file you want to view.
3. Click **Open File Viewer**. The log messages are displayed. Notice that the number of messages in the log is shown in the upper right-hand corner.
4. Click **Next** to scroll to the next set of messages. Click **Previous** to scroll to the previous set of messages. Click **First** to return to the first page of messages. Click **Last** to go the last page of messages.

The messages contain information about the time the message was generated, the component that generated the message, the message ID and message type, and the actual message itself.

The messages can be Information messages, providing you with status, or Error messages, which are useful in determining where a problem has occurred.

Viewing a trace file

To view the contents of a trace file:

1. From the Business Connection Admin Console, select **Log Viewer > Log File Viewer**.
2. Click the name of the trace file you want to view.
3. Click **Open File Viewer**. The trace messages are displayed. Notice that the number of messages in the trace file is shown in the upper right-hand corner.
4. Click **Next** to scroll to the next set of messages. Click **Previous** to scroll to the previous set of messages. Click **First**to return to the first page of messages. Click **Last** to go to the last page of messages.

Preparing to use Registration and Provisioning

Before you can begin using the Registration and Provisioning component to register with partners, complete the sections that apply to you.

If you will be using a CrossWorlds TPI Server

If you will be using the TPI server, you must have a company profile in the TPI server. If you have not already created a company profile in the TPI server, perform these steps:

1. Create the directory **<*BCT_HOME*>\partners\<*your company name*>\serv\tpiserver**, if one does not already exist.
2. Create a company profile in CrossWorlds TPI Server. (Refer to the CrossWorlds TPI Server Admin doc).
3. Export the company profile (as a partner profile using XML format) to the <*BCT_HOME*>\partners\<*your company name*>\serv\tpiserver directory.

   Note: The name of the file must be: *your company name*.xml. This same name (*your company name*) must be used when using the WebSphere Business Connection to register your company with your partners.

If you will be using Document Exchange

The Registration and Provisioning service, which is described in "Registration and Provisioning" on page 9, includes the exchange of files between trading partners. If you are going to use the Document Exchange service (which is described in "Document Exchange" on page 21), you must complete steps to make a file containing information about your company available to be sent to your partners during the registration process. If you are going to use Document Exchange and you did not already complete this procedure during installation, do the following:

1. From the command window, go to the following directory: <*BCT_HOME*>\wsdl.
2. Open the BCTDE_ServiceDefinition.xml file for edit.
3. In the lft:address location line, replace <*localhost*> with the host name or IP address.
4. Save the changes.
5. Create the directory <*BCT_HOME*>\partners\<*your company name*>\serv\de. Note that <*your company name*> must be the same name you will use to register your company.
6. Copy the BCTDE_ServiceDefinition.xml file and the BCTDE_ServiceInterface.xml file to the directory <*BCT_HOME*>\partners\<*your_company_name*>\serv\de.

During registration, you will deploy files sent to you (by your trading partner). This process is described in "Deploying the Document Exchange service wsdl file from other partners" on page 13.

Important: Please be aware of the following restriction to security if you are using Document Exchange with Large File Transfer and you want to transfer documents

with multiple trading partners. In this case, your company must provide the same user identifier and exchange password to all of its trading partners.

The limitation is because the sending Web Services Gateway can only supply its company identifier and exchange password in a single parameter instead of supplying unique credentials for each registered trading partner.

You have two choices in how you handle the limitation:

- You can run the Document Exchange service with Large File Transfer in an unsecured environment.
- You can run in a secure environment but with the restriction that the user identifier and exchange password exchanged with your partners must always be the same. If your company is performing business with only one partner, the Document Exchange environment will be secured.

If a company has multiple trading partners, it is possible that the company identifier and exchange password could be compromised because the limitation may be known among all trading partners.

Registration and Provisioning

The Registration and Provisioning service provides a variety of functions for users and administrators. For example, the administrator at an organization can register with a trading partner (such as a marketplace or service provider) and request services of that trading partner. The trading partner, in turn, accepts the registration and grants access to services.

A graphical user interface is provided for the administrator registering at the organization. The administrator at the trading partner performs most of the registration tasks (such as accepting a registration) via the Admin Console. All the administrative tasks are described in this section.

If you want to modify the way this service works, refer to the Registration Flow document, which describes the collaboration and associated business objects that are a part of the Registration and Provisioning service.

Overview

The following is an overview of the major steps that occur between the organization and the trading partner when the administrator at the organization initiates a registration request. The actual procedures are listed following the overview, beginning with "Registering as a new participant" on page 11.

This overview assumes that both the organization and the trading partner have a Business Connection edition installed. In addition, before performing any of the steps in this section, you should have completed configuration of the WebSphere Business Connection, including the configuration of optional services, such as the TPI gateway, per the instructions in the Installation and Configuration Guide.

At the organization wanting to register with the trading partner:

1. The administrator at the organization uses an input form to fill out profile information.

   Figure: The registration screen

   - **Company Name** is used as the organization ID and cannot contain any punctuation except for the dash (-), underscore (_), space ( ), and ampersand (&).
   - **Primary Contact** is used as the exchange administrator. The user defined here will have administrative privileges for the exchange.
   - **User ID** is used as the logon ID for the administrator and cannot contain any punctuation except for underscore (_).
   - **Exchange Password** is the password that will be given to other exchanges during registration processes as the password to use when accessing automated services from this exchange, such as the Profile Upload service.
   - **Optional Services** are WebSphere Business Connection-supplied services, which you can enable or disable.

   Note that you will see this screen only once. If you make any mistakes in crucial information (Company Name, for example), you will not be able to

change them later. The only recourse is to drop the WebSphere Member Service database, clear out LDAP, and start over—so be careful with your entries.

The profile information is placed in a repository. The organization repository now has one entry—its own.

2. The administrator then accesses another registration form and indicates the location of the file with the profile information. The profile information is then exported to the exchange partner.

   Figure: The registration screen showing how the file can be imported

   - **Import File Path** is where you select your organization's Profile Export file. This file is located in the <*BCT_HOME*>\partners directory and has the name **<*your organization name*>.zip**.
   - **Organization Owner** is where you specify the password for the organization-owner at the Exchange partner. Note that the user ID and all other user information is the same as the information for your own organization's administrator. You will most likely want to specify a different password here than the password used at your own exchange, because this password will be visible to the administrator at the partner.
   - **Enter Registration Information** is for non-WebSphere Business Connection organizations. You can ignore this field.

At the trading partner:

1. The profile information that was imported is placed in a repository with a pending status.
2. Before the administrator at the trading partner approves the request for registration, the administrator deploys the profile information to the appropriate gateways.
3. The administrator approves the organization's request.
4. The profile information from the exchange partner is sent to your organization via the Profile Upload service.

Alternatively, for non-WebSphere Business Connection partners, the administrator at the requesting organization can fill in the company information in the manual portion of the form.

At the end of the registration process, both the organization requesting registration and the trading partner have profile information about each other in their repositories.

After an organization is registered with its trading partner, it can request services of the trading partner.

The following sections describe the tasks that are done to register a trading partner. Listed first are the activities that the requesting organization would perform (such as registering, changing profile information, and subscribing to an offer). Following that are the activities that the trading partner (marketplace, for example) would perform (such as accepting the registration, managing groups, and creating offers).

Special Note:
As you perform registration tasks, you might see some error messages on your WebSphere Administrative Console similar to the following: `SESN0013E Session Data put value null value entered. The http session put value or HTTP session set attribute method was called from servlet/JSP with a null value. Fix the servlet JSP.` You can ignore these messages and continue with the task.

Registering as a new participant

You begin the registration process by completing a form. The first time the form is called from a browser, the registration program assumes you are setting up your own organization. When you register with the trading partner, this information will also be stored in the trading partner's Federated Partner Profile, just as the information about the trading partner will be stored in the Federated Partner Profile of your system.

Note: If you will be using the Document Exchange service to transfer files to and from a trading partner, see "Preparing to use Registration and Provisioning" on page 7 in the Document Exchange section for information on the steps to follow before you register with a trading partner.

Filling out your organization profile (self-registration)

As the administrator, follow these steps to complete and store the information about your company:

1. Display the Enter Registration Information page. This is the same page that will be accessed later on by other prospective trading partners. On first use, it lets you enter your own profile information.

   To display the registration page, enter:

   `https://<fully qualified hostname>:8080/hostingUI/UIServlet/BCTEnrollmentView`

   where *hostname* is the fully qualified name of your WebSphere Business Connection System (for example, wbc4you.bocaraton.ibm.com).

   Figure: The registration screen for reference as you fill out the form

2. Complete the registration form, filling in all required fields. Fill in your own information as the primary contact.

   Important: If you are using Document Exchange with multiple trading partners, you must use the same exchange password with all partners. Click **Submit**.

   At this point, your own profile is built in your repository and is also exported to the file system in the <*BCT_HOME*>\partners directory with the name <*your organization name*>.zip.

The illustration below shows an example of World-Class Company starting the process of registering with A-1 Marketplace. A-1 Marketplace already has two other companies registered with it.

The registration information has been stored in World-Class Company's own system but has not yet been placed in the repository of A-1 Marketplace.

Figure: The profile is now in the requestor's repository /p>

Sending the profile to the trading partner

The next step is to actually register with the trading partner.

1. Display the Register Using WBC Import File page. (This is the registration page on the WebSphere Business Connection System of your trading partner.) Type:

   `https://<fully qualified hostname>:8080/hostingUI/UIServlet/BCTEnrollmentView`

   where <*hostname*> is the fully qualified name of your trading partner's WebSphere Business Connection system.

   Figure: The upload screen for reference as you fill out the form
2. Type the name of the file containing your organization profile (**<*BCT_HOME*>\partners\<*your organization name*>**, or use the **Browse** button to locate the file. After you enter the name, enter the Organization Owner's password.

   Note: If you are using Document Exchange with multiple partners, the password must be identical to the exchange password that was selected during self-registration.

   Once this password is set, it cannot be changed because it is used by the partners to authorize access to their Document Exchange service. This password is also the logon password when you log on to your Organization Workspace on your partner exchange.
3. Click **Upload**.

The administrator at the trading partner is notified of the registration request. The administrator then accepts or rejects the request. (The instructions that the administrator follows to accept the request are described in the section "Accepting the registration of the requester" on page 17.)

If the administrator at the trading partner accepts the registration, the organization profile of your company is stored at the trading partner.

For example, using the companies shown in the previous illustration, the organization profile of World-Class Company would now be in the repository of A-1 Marketplace.

Figure: The profile has now been put in partner's repository

The approval of the registration starts a series of processes that culminate in the profile of the trading partner being exported to the requesting organization. Now both partners have information about each other, as shown in the example:

Figure: The partner's profile has now been put in requestor's repository

Confirming the registration

You will receive notification from the trading partner when your registration is approved.

Also, to confirm that the registration process completed correctly, check the database to make sure your partner's profile is now in the database. Do the following:

1. From the Administration Workplace page, click **Customer Service > Customers**.
2. Check to see that your trading partner is listed.

   - If the trading partner is not listed, contact the administrator at the trading partner and ask the administrator to check the *<BCT_HOME>*/logs/wbcuiout.txt log to see which error occurred. After the administrator fixes the problem listed there, the administrator must manually enroll his or her organization at the requesting organization. The requesting administrator must then approve it.
   - If the trading partner is listed but the status is not **Active**, check the logs on your system to see if there is an error and do the appropriate recovery based on the error found. If the error was that the provisioning message was not queued, find the provisioning message in the file ProvisionExport-*<OrgName>*.xml in the TEMP directory and, after fixing the problem with the queues, place the contents of that file on the BCT.RPH_Q queue to reinvoke the provisioning.
   - If the trading partner is listed and the status is **Active**, the registration process completed successfully.

Deploying the Document Exchange service wsdl file from other partners

If you are going to use the Document Exchange service, you must deploys the Document-Exchange-related files sent to you by trading partners during the registration process.

1. From a command window, go to the following directory:
   <BCT_HOME>\partners*<partner company name>*\serv\de
2. Open the BCTDE_ServiceDefinition.xml file for edit.
3. Replace the line

   ```
   location=file:///BCTDE_ServiceInterface.xml
   ```

   with:

   ```
   location=file:///<BCT_HOME>/partners/<partner company name>
      /serv/de/BCTDE_ServiceInterface.xml
   ```
4. Bring up the Web Services Gateway Admin console.
5. Select **List** under **Services**.
6. Click **BCT_DocumentTransfer_Create**
7. In the Add new target section, specify the following:
   a. In the **WSDL Location** field, enter:

      ```
      file:/<BCT_HOME>\partners\<partner company name>
         \serv\de\BCTDE_ServiceDefinition.xml
      ```
   b. For **Location type**, select **URL**.
   c. In the **Target Service Identity Information**, enter:

      ```
      <partner company name>
      ```
   d. Click **Add**.

Performing organization tasks

After your organization has registered with the trading partner, you can subscribe to services that reside on the trading partner. You can also manage your departments and users and update your Personal Profile. You perform these tasks using the Organization Workspace interface.

To gain access to this page, do the following:

1. Type: **https://<*fully qualified hostname*>:8080/hostingUI/UIServlet/BCTSecureLogonView**
2. Enter the user ID and password you used when you registered.

Figure: The screen used to manage company information

Updating your personal profile

To update your organization's information:

1. From the Organization Workspace page, click **Personal Profile > Personal Profile**.
2. When the Detail Information page is displayed, make the necessary changes.
3. If you need to change the contact information, click **Contact** and change the information on that page.
4. Click **OK**.

Subscribing to offers

To subscribe to an offer:

1. Click **Workspace Management > Department Management**.
2. Select your department and click **Subscribed Offerings**.
3. Click **Subscribe New Offer**.
4. Select an offer from the list and click **Next**.
5. Fill in any extended attribute information required. Note that some offers might not have this step, or this step might repeat for each service within an offer. Click **Next**.
6. On the summary screen, review your selections and click **Finish**.

Loading user data from a file

To load user data from a file:

1. Click **Workspace Management > Load User Data**.

   A log of imported user files is displayed.
2. Click **Browse** and then select an XML file containing exported users.
3. Click **Upload this file** to import the users into your organization.

Performing administrative tasks

The previous section described the tasks you perform to update profiles, subscribe to offers, and upload files. These are tasks associated with the administrator who has recently registered with a trading partner.

This section describes the tasks the administrator at the trading partner would perform, such as accepting registration requests and creating offers. The administrator uses this page to perform the tasks:

Figure: The exchange administrator console /p>

This interface is similar to the one for the Organization Workspace.

Accepting the registration of the requester

You use the Customer Service selection of the Administration Workspace to accept the registration request. After you accept the registration request, an e-mail is sent to the requestor. Therefore, you need to make sure that the EMail connector is running. To start the EMail connector from Windows, click **Start > Programs > CrossWorlds > Connectors > EMail Connector**.

As the administrator at the trading partner, you do the following to accept a registration request:

1. From the Administration Workplace page, click **Customer Service > Customer Accounts**.
2. Select an organization that has Status set to **Guest**.
3. Click **Activate** to approve the registration request.

From this screen, you can also click:

- **Members** to view the users for the selected organization
- **Subscribed Offerings** to view the offers to which the organization has subscribed

Managing Groups

When you select **Site Management > Group Management,** you see a list and description of the current groups as well as buttons you can use to add a group, delete a group, and manage members of the group.

Adding new groups

To add groups:

1. From the Groups page, click **New**.
2. When the New Group screen is displayed, type a name for the group.
3. Type a description for the group. The description will be displayed in the Groups window.
4. Click **OK**.

Managing group members

To add or delete members to or from a group:

1. From the Groups page, click **Change**. The members of the group are displayed.
2. Click **Site Management > Group Management**. A list of group attributes is displayed.
3. Click **Members**.
4. If you want to add organizations to the group, click **Add**.

   If you want to delete organizations from the group:

   a. Select the group or groups you want to delete.
   b. Click **Delete**.

Creating an offer

An offer is made up of one or more services. To create an offer, you provide the name of the offer and select the services that will be part of the offer, as follows:

1. Click **Offer > Create Offer**.
2. Type the name of the offer.
3. Type the description of the offer.
4. Select the services that will be packaged into the offer:
   a. Highlight an offer from the Available Services list.
   b. Click **Add** to include it in the offer.
      When you click **Add**, the service is moved to the Selected Services list.
      If you want to remove an offer, highlight the offer in the Selected Services list and click **Remove**.
5. Click **Next**.
6. For each service in an offer, fill in the service-specific data and click **Next**.
7. View and confirm the offer parameters, and then click **Finish**.

Clearing the initial registration

If you encounter any problems with the initial registration of your own organization information on your own exchange, you can perform the following procedure to clear that information and return the system to its initial state.

1. From WebSphere Application Server:
   a. Stop the Default Server Application Server in WebSphere Application Server.
   b. Stop the WebSphere Member Services Application Server
2. Clear the WebSphere Member Services database:
   a. Open the IBM DB2 Control Center and list its databases.
   b. Select and drop the WMS database.
   c. Open a DB2 command window.
   d. Change the directory to **<*drive*>:\wbc\wms\bin**
   e. Run the command: **wms_createdb.db2.bat WMS db2admin <*DB2_password*>**
   f. Enter the command: **wms_populatedb.db2.bat WMS db2admin <*DB2_password*> DB2ADMIN**
3. Clear the LDAP user information:

a. Open the IBM SecureWay Directory Directory Management Tool and rebind as **cn=root**
b. Open **dc=allegro dc=Users** and delete all user records ***except*** uid=spadmin and uid=csr
c. Open **o=root organization** and delete all org records ***except*** o=wbc.

4. Clear the user credentials
   a. Open an IBM DB2 command window
   b. Change to the <*BCT_HOME*>\bin directory
   c. Enter ClearSecAuth
5. From the <*BCT_HOME*>\partners directory, delete the company partner folders.
6. If you are using TPI and have deleted the company folder, export the TPI company info again.
7. If you use Document Exchange, resave the serviceDefinition and serviceInterface XML files in the <*BCT_HOME*>\partners\<*your company name*>\serv\de directory.
8. If you are using TPI:
   a. Delete the appropriate entries in <*BCT_HOME*>\bin\tpicfg.in
   b. Delete the appropriate partner profiles in the CrossWorlds TPI Server.
9. From WebSphere Application Server:
   a. Start the WebSphere Member Services Application Server.
   b. Start the Default Server Application Server.

Changing your LDAP administrative password

If you need to change your LDAP administrative password (cn=root) using the SecureWay Directory Configuration program, you also need to make a change to a property file, as follows:

1. Open the following file for edit:
   <*WBCUI_HOME*>\config\LDAPConfig.properties
2. Locate the line **LDAPRootpassword = <*admin password*>**
3. Change the value to your new LDAP administrative password.

Document Exchange

The Document Exchange service enables you to exchange files—even very large files—with your trading partners.

When you select **Document Exchange** from the Admin Console, you can perform administrative tasks, such as forwarding documents, sorting the list of documents you've received, and deleting documents. The administrative tasks are described in this section.

If you want to modify the way this service works, refer to the Document Transfer document, which describes the collaborations and associated business objects that are a part of the Document Exchange service. The collaboration properties you can change are also described in this document in the section "Changing Document Exchange properties" on page 25.

Starting Document Exchange

Before you use the Admin Console to access Document Exchange, you must do the following to start the Document Exchange artifacts:

1. Make sure that the CrossWorlds InterChange Server prerequisites (DB2, MQSeries, and CrossWorlds VisiBroker) are running and that the MQSeries Listener is started.
2. From the CrossWorlds System Manager, start the following collaboration objects by right-clicking them and then clicking **Start**:
   - **SAI_to_BCTDEReceiveConnector_BCT_DocumentTransferInbound**
   - **BCTDESendConnector_to_BCTDESOAPConnector_BCT _DocumentTransferOutbound**
3. From the CrossWorlds System Manager, start the following connectors by right-clicking them and clicking **Start**:
   - **BCTDocTransferSendConnector**
   - **BCTDocTransferReceiveConnector**
   - **BCTDocTransferSOAPConnector**
4. Start the connector agents by following these steps:
   a. Open a command window and change to the following directory: <*CROSSWORLDS*>\Connectors\BCTDocTransferSOAP
   b. Enter the following:
      ```
      bctde_conn_run_soap.bat
      ```
   c. Open a command window and change to the following directory: <*CROSSWORLDS*>\Connectors\BCTDocTransferReceive
   d. Enter the following:
      ```
      bctde_conn_run_receive.bat
      ```
   e. Open a command window and change to the following directory: <*CROSSWORLDS*>\Connectors\BCTDocTransferSend
   f. Enter the following:
      ```
      bctde_conn_run_send.bat
      ```

5. From the WebSphere Application Server, start the Document Exchange application server by right-clicking **BCT_DE** and clicking **Start**.

The inbox

When you receive documents, they are listed in an inbox. When you send documents, they are listed in an outbox. The following is an example of an inbox:

Figure: Picture of inbox with sample documents listed

The inbox shows where in your local file system the document is actually stored, the name of the trading partner who sent the document, the date it was sent, and the subject matter. It also shows the Message Delivery Notification (MDN) ID.

When you send a document (as described in the following section), your trading partner's system responds with an MDN, which is an indication of whether the document was received. Similarly, when a trading partner sends you a document, your system responds to the trading partner with an MDN.

Viewing the inbox

To view the inbox:

1. From the Business Connection Admin Console, click **Document Exchange**.
2. If the outbox is displayed, in the View list, click **Inbox**.

Viewing the outbox

When you send or forward documents to your trading partners, the documents are listed in your outbox.

To view the outbox:

1. From the Business Connection Admin Console, click **Document Exchange**.
2. If the inbox is displayed, in the View list, click **Outbox**.

For the remainder of the tasks in this section, it will be assumed that you are already viewing the Document Exchange screen.

Note that you should use the Document Exchange screens on your *local* computer (where Document Exchange is deployed) to perform the tasks that are described in the following sections. In other words, you can sort documents, delete a document, save documents under a different name, and send documents only from your local computer.

Sorting the inbox

To sort the documents in the inbox:

1. Display the inbox.
2. Click one of the following:

- **From Partner**, to sort the documents according to the partners who sent them
- **File ID**, to sort the documents based on their file names (without the fully qualified path)
- **Received Date**, to sort the documents by the dates on which they arrived
- **Subject**, to sort the documents based on subject

- **File URL**, to sort the documents by their location in the file system (the file name with its fully qualified path)
- **MDN ID**, to sort the documents based on their MDN ID

Sorting the outbox

To sort a document in the outbox:

1. Display the outbox.
2. Click one of the following:

- **To Partner**, to sort the documents according to the partners to whom they were sent
- **File ID,** to sort the documents by their file names (without the fully qualified path)
- **Sent Date**, to sort the documents by the dates on which they were sent
- **Subject,** to sort the documents by subject
- **File URL**, to sort the documents by their location in the file system (the file name with its fully qualified path)
- **Status,** to sort the documents based on their status
- **MDN ID,** to sort the documents based on their MDN ID

Deleting a document from the inbox

To delete a document from the inbox:

1. Display the inbox.
2. Click the radio button next to the document you want to delete.
3. Click **Delete**.
4. When prompted to confirm that you want to delete the document, click **OK**.
5. When you are prompted about whether to delete the document from the file system (in addition to deleting it from the inbox), do one of the following:
   - Click **OK** if you want to delete the file from both the inbox and the file system. If you delete the document from the file system, it is permanently removed.
   - Click **Cancel** if you want to keep the file in your file system but remove the reference from the inbox.

   If you choose to delete the file from the file system, and if there are any references to it in the outbox, an error message is displayed. You are advised to delete the references to the file from the outbox without deleting the file from the file system, and then try this procedure again.

Deleting a document from the outbox

To delete a document from the outbox:

1. Display the outbox.
2. Click the radio button next to the document you want to delete.
3. Click **Delete**.
4. When prompted to confirm that you want to delete the document, click **OK**.
5. When prompted about whether to delete the document from the file system (in addition to deleting it from the outbox), do one of the following:

- Click **OK** if you want to delete the file from both the outbox and the file system. If you delete the document from the file system, it is permanently removed.
- Click **Cancel** if you want to keep the file in your file system but remove the reference from the outbox.

If you choose to delete the file from the file system, and if there are any references to it in the inbox, an error message is displayed. You are advised to delete the references to the file from the inbox without deleting the file from the file system, and then try this procedure again.

Saving a document with a different name

You can save a document under a different name. This is similar to a "Save as" operation. When you save the document under a different name, a copy of the file is created with the new name.

To save a document with a different name:

1. Display the inbox or outbox.
2. Click the document whose file name you want to change.
3. Click **Save As**.
4. Type the new name for the file in the field.
5. After you have typed or selected the new name, click **OK**.

Forwarding a document to a trading partner

To forward a document from either the inbox or the outbox:

1. Display the inbox or outbox.
2. Click the document you want to forward.
3. Click the **Forward** button.
4. In the Partner ID list, click the name of the trading partner to whom you are forwarding the document.
5. Type a subject if you want to include one. The subject will appear in your outbox and in your trading partner's inbox.
6. The file that you selected from the inbox or outbox is listed in the **File Reference** field. If you want to change the file you selected, click **Browse** and select another file.
7. Type a shortened form of the file name in the **File ID** field. The File Reference itself is usually very long, so the shortened form of the file name helps you and your trading partner easily identify the document.
8. Click **Send**.

You will receive a message that the document is marked for delivery.

Sending a document to a trading partner

To send a document that is not currently listed in your inbox or outbox:

1. From the inbox or outbox screen, click the **Compose Message** button.
2. In the Partner ID list, click the name of the trading partner to whom you are sending the document.

3. Type a subject if you want to include one. The subject will appear in your outbox and in your trading partner's inbox.
4. Type the name of the file (including its path) in the **File Reference** field, or click **Browse** and select a file.

   Note: The file name must not exceed 240 characters.

5. Type a shortened form of the file name in the **File ID** field. The File Reference itself is usually very long, so the shortened form of the file name helps you and your trading partner easily identify the document.
6. Click **Send**.

You will receive a message that the document is marked for delivery.

Stopping Document Exchange

To stop the Document Exchange artifacts:

1. From the CrossWorlds System Manager, stop the collaboration objects by right-clicking them and then clicking **Stop**:
   - **SAI_to_BCTDEReceiveConnector_BCT_DocumentTransferInbound**
   - **BCTDESendConnector_to_BCTDESOAPConnector _BCT_DocumentTransferOutbound**
2. Stop the following connector agents by typing **q** in their respective windows or by pressing Ctrl + C:
   - **bctde_conn_run_soap.bat**
   - **bctde_conn_run_receive.bat**
   - **bctde_conn_run_send.bat**
3. From the CrossWorlds System Manager, stop the connectors by right-clicking them and clicking **Stop**:
   - **BCTDocTransferSendConnector**
   - **BCTDocTransferReceiveConnector**
   - **BCTDocTransferSOAPConnector**
4. From the WebSphere Application Server, stop the Document Exchange application server by right-clicking **BCT_DE** and clicking **Stop**.

Changing Document Exchange properties

The properties for Document Exchange artifacts are located in two places:

- In a property file
- In collaboration objects

This section explains about the attributes and the values that can be specified.

The BCTDE.Properties file

The BCTDE.Properties file has the following attributes:

- **BCT_DSContextFactory** should have the value for the WebSphere Administrative Server initial context factory name, **com.ibm.websphere.naming.WsnInitialContextFactory**.
- **BCT_DataSource** should point to the datasource name, **jdbc/BCTDE**.

- **BCTE_TABLE_DISP_SIZE** is used to control the display of number of rows in the inbox and outbox.

Collaboration Properties

Document Exchange includes two collaborations: BCT_DocumentTransferInbound and BCT_DocumentTransferOutbound. Each of the collaborations has properties associated with it.

BCT_DocumentTransferInbound has two collaboration-specific properties:

- **BCT_LOG** can take a value of **Yes** or **No** for logging in to the Solution Manager.
- **BCT_FILE_DOWNLOAD_DIR** should point to the directory where the Web Services Gateway downloads the file. For reference, check the attribute **lft-directory** on the application server on WebSphere Application Server where the LFT channel is deployed.

BCT_DocumentTransferOutbound has two collaboration-specific properties:

- **BCT_LOG** can take a value of **Yes** or **No** for logging in to the Solution Manager.
- **BCT_SOAP_SERVER_URL** should have the value of the outbound Web Services Gateway SOAP-server URL.

You specify a value for these attributes by modifying their respective collaboration objects. Refer to the Document Transfer document for information about the collaborations objects. Refer to the IBM CrossWorlds documentation for general information about collaborations.

Updating the HTTP Session Timeout

The Document Exchange service is implemented as a synchronous model, so any file transfer initiated by the collaboration waits for the response. If the file size is extremely large (for example, 4 GB), the transfer can take 7 or 8 hours. The HTTP Session Timeout, however, is set to 300 seconds by default. It is therefore recommended that you increase the HTTP Session Timeout if you will be exchanging very large files.

Determining the status of a transferred file

If you send a file but are uncertain of its status, you can use the **status** utility to determine the state of the file transfer. You can also use status to cancel the file transfer.

Status information about large file transfers is written to a status file called statefile, which is located in the working directory of your Web Services Gateway application server. The status utility (status.class) is included in the httpr.jar file and is run from the same directory as statefile.

Note: This utility is provided for use by system administrators only. Do not delete files with names you do not recognize, because the files might be system-generated pieces of a larger file that is in the process of being transferred and that will eventually be reassembled into a single file at the receiving gateway.

To set up the status utility, complete the following steps:

1. Extract **status.class** from *<WSGW_HOME>*/lib/httpr.jar (where *<WSGW_HOME>* is the root directory for your installation of the Web Services Gateway).

2. Copy the file into the working directory of your Web Services Gateway application server.

   Note: By default, this working directory is <*WAS_HOME*>/bin (where <*WAS_HOME*> is the root directory for your installation of IBM WebSphere Application Server). If you are not certain of the working directory, open the WebSphere Administrative Console and look at the **General** tab for the application server on which your Web Services Gateway is running.
3. Open a command prompt and change the directory to the working directory of your Web Services Gateway application server.
4. Enter the following command:

```
java -Djava.protocol.handler.pkgs=com.ibm.axis.transport
   -Dlft-directory=WSGW_root/lft_temp
   -Dlft-piFactory=com.ibm.httpr.file.FileStateManagerFactory
   -classpath WSGW_root/lib/httpr.jar status
   optional_parameter
```

   The command parameters are described in the following table:

Table 1. Status Utility commands

Parameter	Description
-Djava.protocol.handler.pkgs=com.ibm.axis.transport	This parameter describes the transport protocol.
-Dlft-directory=*WSGW_root/lft_temp*	This parameter describes the location where the files being transferred are held in temporary storage. *WSGW_HOME* is the root directory for your installation of the Web Services Gateway, and *lft_temp* is the directory where files being transferred are held temporarily
-Dlft-piFactory=com.ibm.httpr.file.FileStateManagerFactory	This parameter describes the format in which the status information is held (the file format).
-classpath *WSGW_root*/lib/httpr.jar status *optional_parameter*	This parameter puts httpr.jar on the classpath temporarily while the command is executed. The *optional_parameter* is **cancel**.

If you do not type a parameter after **status**, the contents of the state file are displayed in the command window.

If you type status cancel, the contents of the state file are displayed item by item, and you choose whether or not to delete each item. Enter **y** to cancel a transfer or **n** to continue a transfer.

Troubleshooting tip

When you use Compose or Forward to send a file to a trading partner, your outbox is updated as follows:

- **Status** is set to **Attempting Delivery**
- **MDM ID** is set to null

After your trading partner receives the file, the receiving collaboration generates an MDN ID, which is returned to you in the response message. To complete the process, your outbox is updated as follows:

- **Status** is set to **Sent Successfully**
- **MDM ID** is set to the ID returned in the response

If you see a **Send Cancelled** status, the system already cancelled the sending of the document because of some failure. If this happens, check the logs to find the cause of the problem.

If a failure occurs and you receive a fault message or if any other exception occurs, the **Status** field is set to **Send Error**. If, when you check the outbox, you see a **Send Error** status, do the following:

1. Run the status utility (described in "Determining the status of a transferred file" on page 26) to view the status of the file that was sent.
2. If an entry for the file is displayed by the status utility:
   a. Use the status utility to cancel the transfer.
   b. Delete the entry from the outbox.
   c. Compose or forward the message again.
3. If an entry for the file is ***not*** displayed by the status utility, either the transfer was successful but the response was not received from the receiving side or an error occurred before the transfer was initiated. Do the following:
   a. Check to see if any errors occurred before the file was transmitted. For example, check the WebSphere Administrative Console and the ICS logs. If an error did occur before the file transmission:
      1) Delete the entry from the outbox.
      2) Compose or forward the message again.
   b. Confirm with your trading partner that the file was received. Then use the DB2 tools to update the Status and MDN ID for that entry in the outbox.

Solution Log Viewer

Logging is built in to the Document Exchange and Registration and Provisioning services. For example, the Document Exchange service logs key events as it moves a document from one trading partner to another. The following illustration shows the type of information that Document Exchange logs:

Table 2. Solution Log Viewer - Document Exchange

Start time	Subsystem	Type	Instance ID	Step Name
2002/04/12 16:25:35.801	Collaboration	Log	JDBC Connector_10 196342881158_1	Collaboration Start
2002/04/12 16:25:36.234	Collaboration	Log	JDBC Connector_10 196342881158_1	Received WSDL

If you want to view the status of a document as it is processed through your gateway into the gateway of a trading partner, you can view the log produced by Document Exchange for that transaction.

Viewing a solution log

To view the log for Document Exchange or Registration and Provisioning:

1. Click **Log Viewer > Solution Log Viewer**.
2. Select the service whose log you want to view from the Select Application list.
3. If you want to see messages from a certain range of dates, type the dates in the From Date or End Date fields.
4. Click **Next** to scroll to the next set of messages. Click **Previous** to scroll to the previous set of messages. Click **First** to return to the first page of messages. Click **Last** to scroll to the last set of messages.

Viewing detailed information

To view detailed information about one of the instances listed in the Solution Log Viewer, click the name of the instance (in the Correlation ID column).

If you choose to view the information for Document Exchange, for example, you see the events that occur as a document is sent from one gateway to another.

Adding logging to your programs

If you are writing services for a Business Connection system, you will want to add logging to your services so that you can view and track your business processes. See Using the Business Connection APIs for information on how to add logging to your service.

Providing security between Business Connection systems

As part of the installation of WebSphere Business Connection, you added security to your system. This section tells you how to add security between two or more Business Connection systems, starting with the procedure to configure HTTPS between two Web Service Gateways.

HTTPS Configuration from Web Services Gateway to Web Services Gateway

HTTPS should be configured from the sending Web Services Gateway to the receiving Web Services Gateway in order to provide data encryption for business exchanges.

To configure HTTPS from the sending Web Services Gateway to the receiving Web Services Gateway:

1. Extract the certificate from the receiving Web Services Gateway machine to a file, as follows:
   a. Click **Start > Programs > IBM HTTP Server > Start Key Management Utility**.
   b. Select **Key Database File > Open**. Select the certificate database that was created during installation (for example, <*BCT_HOME*>\properties\key.kdb). Enter the password for the database when prompted.
   c. Click **Extract Certificate** and save it to **<***BCT_HOME***>\properties\<***Exported_Cert***>.arm**
   d. Close ikeyman.
2. Copy the exported certificate file from the receiving Web Services Gateway to the sending Web Services Gateway and place it in the **<*CROSSWORLDS*>\lib\security**directory.
3. Add the certificate to the trusted certificate database (truststore) on the sending Web Services Gateway computer as follows:
   a. From a command window, change to the following directory: **<*CROSSWORLDS*>\lib\security** directory.
   b. Enter the following command:

      ```
      keytool -import -alias <Receiving_WSGW_Server_HTTP_Server
        _Hostname> -file <Exported Cert>.arm -keystore truststore
      ```

   c. Enter the password that was used to create the truststore during installation.
4. When the **Trust this certificate** prompt appears, type **Yes**.
   From the WebSphere Admin console, select the **WSGW Application Server** and select the **JVM Settings** tab.
5. Add the system properties shown in the table.

   These parameters are used to establish the SSL link between Web Services Gateways. The javax parameters are used to secure the SOAP channels. The httpr parameters are used to secure the LFT channels. The http.auth parameter is used to provide authentication information on the incoming LFT channel.

Field Name	Value
javax.net.ssl.keyStore	<CROSSWORLDS>\lib\security\keystore
javax.net.ssl.keyStorePassword	*<password>*
javax.net.ssl.trustStore	<CROSSWORLDS>\lib\security\truststore
javax.net.ssl.trustStorePassword	*<password>*
httpr.ssl	yes (**Note:** This must be lowercase.)
httpr.passphrase	*<password>*
httpr.keystore	*<CROSSWORLDS>*\lib\security\truststore
http.auth	*<YourCompanyUserId>*: *<YourCompanyExchangePassword>*

6. Restart the WSGW Application Server server.
7. On the sending computer, modify each partner's WSDL' (WSDL prime) file so it establishes an SSL connection to the receiving Web Services Gateway computer For Document Exchange, the WSDL file is located in *<BCT_HOME>*\partners*<company name>*\serv\de\BCTDE_ServiceDefinition.xml.
   a. If the WSDL file contains a SOAP entry, edit the **soap:address location** and modify the URL to use HTTPS instead of http. For example:
      ```
      soap:address location="https://<hostname>
        /wsgwsoap1/soaprpcrouter
      ```
   b. If the WSDL file contains an LFT entry, edit the **lft:address** location and modify the URL to use port 443. For example:
      ```
      lft:address location="httpr://<hostname>:
        443/wsgwlft1/HttprServer#HTTPR.DEMO.REQUEST"
      ```
8. Using the Web Services Gateway admin facility on the sending Web Services Gateway computer, remove the target service and add a new target service, as follows:
   a. Click **Services > List** and click the Web service to be updated (for example, **BCT_DocumentTransfer Create**).
   b. In the WSDL Location field, enter the location and file name of the WSDL. For example, Document Exchange would be specified as:
      ```
      file:/<BCT_HOME>\partners\<partner company name>
         \serv\de\BCTDE_ServiceDefinition.xml
      ```
   c. For **Location Type**, select **URL**.
   d. In the **Target Service Identify Information**, enter:
      ```
      <partner company name>
      ```
   e. Click **Add**.

Securing the SOAP channels

This section describes the process to secure the ***receiving*** SOAP channels so that WebSphere security can protect the resources.

These instructions apply to either the SOAP1 or SOAP2 channel, depending on which channel is specified as an inbound channel. Perform the following steps on the ***receiving*** Web Services Gateway computer to modify the SOAP EAR files.

1. Launch the Application Assembly Tool from the WebSphere Administrative Console **Tools** menu.
2. Cancel the **Welcome to Application Assembly Tool**.

3. Click **File** > **Open** and use the **Browse** button to select the **<*BCT_HOME*>/wsgw/bin/wsgwsoap1.ear** or **<*BCT_HOME*>/wsgw/bin/wsgwsoap2.ear** file.
4. Highlight **Security Roles** and right-click to select **New** to define a security role. Enter **AuthenticatedUsers** for the role name. Click **OK** to save the change.
5. Expand **Web Modules > IBM Web Services Gateway, right-clickSecurity Constraints**, and select **New** to define a new security constraint. Enter a name (for example, <*hostname*>SecurityConstraint), click **Add**, and select the **AuthenticatedUsers** security role created above. Click **OK** to save.
6. After creating the security constraint, you next create a web resource collection. Expand the new security constraint, right-click **Web resource collection**, and select **New.**
7. For Web Resource Name, enter:
   ```
   WSGW SOAP
   ```
8. On the HTTP methods, click **Add** and select **Apply** to add the **GET** method. Then select **POST** from the pulldown and click **OK**.
9. On the URL pattern, click **Add** and then type the following and click **OK**:
   ```
   /soaprpcrouter
   ```
10. Click **OK** to save the Web resource collection.
11. Click **File > Save** to save a modified copy of the wsgwsoap.ear file.
12. Close the Application Assembly Tool.

Perform the following steps on the ***receiving*** Web Services Gateway computer to remove the SOAP Channel:

1. Go to the Web Services Gateway Admin page (**http://<*hostname*>/wsgw/admin**).
2. In the left-hand side, select **Services > List** and select your service that contains the SOAP Channel (for example, BCT_DocumentTransfer_Create)
3. Scroll down to the **Channels** section and click the **Remove** button for the **ApacheSOAPChannel1** (or **ApacheSOAPChannel2**) channel.
4. In the left-hand side, select **Channels > Remove.**
5. Check **ApacheSOAPChannel1** (or **ApacheSOAPChannel2**), and click **OK**.

Perform the following steps on the ***receiving*** Web Services Gateway computer to deploy the modified SOAP EAR files:

1. Stop the **WSGW** application server.
2. Remove the Web Services Gateway Apache SOAP Channel 1 or 2 enterprise application, depending on the channel configured above.
3. Deploy the modified SOAP EAR file by highlighting **Enterprise Applications** on the WebSphere Administrative Console. Right-click and select **Install Enterprise Application**.
4. Select **Browse** and find the wsgwsoap1.ear (or wsgwsoap2.ear) file in the <*WSGW_HOME*>\bin folder. Click **Next** to continue.
5. On the **Mapping Users to Roles** page, highlight **AuthenticatedUsers** and click **Select**.

   Check only the **Select users/groups** and then enter * in the **Search**field and click **Search**. A list of users and groups is displayed.

Select the **cn=OrgOwner,dc=SecurityRole,dc=allegro** group from the **Available Users/Groups**, and click **Add** to add the group. Finally, click **OK**.

6. Click **Next** until you reach the Selecting Application Servers screen. Highlight the modules and then click **Select Server**. Select the **WSGW** application server, and click **OK**.
7. Click **Next**, and then click **Finish**.

   At the completion of the installation wizard, you will be requested to generate application code. Select **No** when this option appears.
8. Start the **WSGW** application server.

Perform the following steps on the **receiving** Web Services Gateway computer to deploy the modified SOAP Channel:

1. Go to the WSGW Admin page (**http://*hostname*/wsgw/admin**).
2. On the left hand side, select **Channels > Deploy**.
3. Fill in the first three fields:

   Channel Name: **ApacheSOAPChannel1**
   Home Location: **ApacheSOAPChannel1Bean**
   End Point Address: **http://<*fully_qualified_wsgw_hostname*>/wsgwsoap1**
4. Click **OK**.
5. On the left-hand side, select **Services > List.**
6. Select the service that should contain the SOAP channel (for example, BCT_DocumentTransfer_Create).
7. Scroll down to the **Channels** section, and select **ApacheSOAPChannel1** (or **ApacheSOAPChannel2**) from the Add Channel pulldown.
8. Click **add**.
9. On the WebSphere Admin Console, restart the Web Services Gateway App Server.
10. Using Microsoft Internet Explorer Version 5.5 or above, enter ***one***of the following URLs to display the Web Services Gateway Admin Console:

    `http://<WSGW_hostname>/wsgwsoap1/soaprpcrouter`

    `http://<WSGW_hostname>/wsgwsoap2/soaprpcrouter`
11. When you are prompted, enter the user ID and password created during self-registration.

The SOAP RPC Router page is displayed.

Securing the LFT channels

This section describes the process to secure the ***receiving*** LFT channels so that WebSphere security can protect these resources.

These instructions apply to either the LFT1 or LFT2 channel, depending on which channel is specified as the inbound channel. Perform the following steps on the ***receiving*** Web Services Gateway computer to modify the LFT EAR files.

1. If it is not already running, launch the Application Assembly Tool from the WebSphere Administrative Console **Tools** menu.
2. Cancel the **Welcome to Application Assembly Tool**.

3. Click **File** > **Open** and use the **Browse** window to select the **<*BCT_HOME*>/wsgw/bin/wsgwlft1.ear** or **<*BCT_HOME*>/wsgw/bin/wsgwlft2.ear**file.
4. Highlight **Security Roles** and right-click to select **New** to define a security role. Enter **AuthenticatedUsers** for the role name. Click **OK** to save the change.
5. Expand **Web Modules > IBM Web Services Gateway LFT Channel, right-click Security Constraints**, and select **New** to define a new security constraint. Enter a name (for example, <*hostname*>SecurityConstraint), click **Add**, and select the **AuthenticatedUsers** security role created above. Click **OK** to save.
6. After creating the security constraint, you next create a Web resource collection. Expand the new security constraint, right-click **Web resource collection**, and select **New.**
7. For Web Resource Name, enter:
   ```
   WSGW LFT
   ```
8. On the HTTP methods, click **Add** and select **Apply** to add the **GET** method. Then select **POST** from the pulldown and click **OK**.
9. On the URL pattern, click **Add** and then type the following:
   ```
   /
   ```
   Click **Apply**. Then type the following and click **OK**:
   ```
   /HttprServer
   ```
10. Click **OK** to save the Web resource collection.
11. Click **File > Save** to save a modified copy of the wsgwlft.ear file.
12. Close the Application Assembly Tool.

Perform the following steps on the ***receiving*** Web Services Gateway computer to remove the LFT Channel:

1. Go to the WSGW Admin page (**http://*hostname*/wsgw/admin**).
2. In the left-hand side, select **Services > List** and select your service that contains the LFT Channel (for example, BCT_DocumentTransfer_Create).
3. Scroll down to the **Channels** section and click the **Remove** button for the **LFTChannel1** (or **LFTChannel2**) channel.
4. In the left-hand side, Select **Channels > Remove.**
5. Check **LFTChannel1** (or **LFTChannel2**) and click **OK**.

Perform the following steps on the ***receiving*** Web Services Gateway computer to deploy the modified LFT EAR files:

1. Stop the **WSGW** application server.
2. Remove the Web Services Gateway LFT Channel 1 or 2 enterprise application, depending on the channel configured above.
3. Deploy the modified LFT EAR file by highlighting **Enterprise Applications** on the WebSphere Administrative Console. Right-click and select **Install Enterprise Application**.
4. Select **Browse** and find the wsgwlft1.ear (or wsgwlft2.ear) file in the <*WSGW_HOME*>\bin folder. Click **Next** to continue.
5. On the **Mapping Users to Roles** page, highlight **AuthenticatedUsers** and click **Select**.

Check only the **Select users/groups** and then enter * in the **Search**field and click **Search**. A list of users and groups is displayed.

Select the **cn=OrgOwner,dc=SecurityRole,dc=allegro** group from the **Available Users/Groups**, and click **Add** to add the group. Finally, click **OK**.

6. Click **Next** until you reach the Selecting Application Servers screen. Highlight ***all*** the modules and then click **Select Server**. Select the **WSGW** application server, and click **OK**.
7. Click **Next**, and then click **Finish**.

   At the completion of the installation wizard, you will be requested to generate application code. Select **No** when this option appears.
8. Start the **WSGW** application server

Perform the following steps on the ***receiving*** Web Services Gateway computer to deploy the modified LFT Channel:

1. Go to the Web Services Gateway Admin page (**http://*hostname*/wsgw/admin**).
2. On the left-hand side, select **Channels > Deploy**.
3. Fill in the first three fields:

   Channel Name: **LFTChannel1**
   Home Location: **LFTChannel1Bean**
   End Point Address**: http://<*fully_qualified_wsgw_hostname*>/wsgwlft1**
4. Click **OK**.
5. On the left-hand side, select **Services > List.**
6. Select the service that should contain the LFT channel (for example, BCT_DocumentTransfer_Create).
7. Scroll down to the **Channels** section, and select **LFTChannel1** from the Add Channel pulldown.
8. Click **add**.
9. On the WebSphere Admin Console, restart the Web Services Gateway App Server.
10. Using Microsoft Internet Explorer Version 5.5 or above, enter ***one***of the following URLs to display the Web Services Gateway Admin Console:

    `http://<WSGW_hostname>/wsgwlft1`

    `http://<WSGW_hostname>/wsgwlft2`
11. When you are prompted, enter the user ID and password created during self-registration.

The Web Services Gateway LFT Channel page is displayed.

Configuring the Web Services Gateway Authentication Filter

The authentication filter is a Web Services Gateway plug-in that parses the SOAP header looking for trading-partner identifiers in the SOAP message. The filter calls WebSphere Member Services to retrieve the HTTP user ID and password associated with the source trading partner. The HTTP header is then updated to contain these fields, which can then be used by WebSphere security to authenticate and authorize trading partners to access Web Services Gateway and Web services resources.

The authentication filter is installed as part of the Web Services Gateway, but it must be associated with a particular service.

Perform the following steps on the Client Web Services Gateway:

1. Open a browser and enter
   `http://<Web Service Gateway hostname>/wsgw`
2. Click **Services > List**, and then select the Web Service (for example, **BCT_DocumentTransfer_Create**).
3. In the Request Filters section, add the BCTWSAuthenticationFilter. The position does not matter.
4. List the service to verify that the request filter is now included.

The SOAP message sent from the Web Services Gateway will now contain the basic authentication header in the HTTP(s) message.

Providing security for Web services

This section describes how to apply security to Web services.

Access to a protected Web service is based on role-based authentication using WebSphere security. Specific roles are defined during construction of an Enterprise Application Resource (EAR) file. Individual users or groups are assigned to roles at deployment. The setting of roles and assigning these to methods are performed using the Application Assembly Tool, which is part of WebSphere Application Server.

The installation includes a wsgwauth.ear file. Generating a *<webservice>*.ear file and importing this into wsgwauth.ear file protects a target Web service. This modified wsgwauth.ear file is then installed in WebSphere Application Server, whereupon users are assigned to the previously defined roles. Therefore, authorized access to Web-service methods is based on the role model, and authentication is based on WebSphere Application Server

Creating a <webservice>.ear file

The first step is to generate the facade EJB using the WSGWAuthGen.bat script. The script is located in the [x]:*WSGW_HOME*\scripts\auth folder. The script takes two arguments.

- The URL defining the location of the gateway installation
- The name of the Web service deployed in the gateway

To generate the facade EJB do the following:

1. Go to a command prompt and switch the directory to <WSGW_HOME>\scripts\auth.
2. Enter the WSGWAuthGen command as follows:
   WSGWAuthGen http://<WSGW_Hostname>/wsgw
   BCT_DocumentTransfer_Create

   Note that the URL should include the root context and that the deployed service is case-sensitive.

Upon successful execution of this script, a ***<webservice>*.ear** file is created in the <*WSGW_HOME*>\scripts\auth folder and also a subfolder called <ejb>. This directory is temporary and may be deleted. The EAR file will be used to implement security on the Web Services Gateway for this particular service.

To complete the steps of assigning roles and protecting methods, use the Application Assembly Tool (AAT) that comes with WebSphere. The following instructions are specific to AAT. The process discussed involves making changes to the file wsgwauth.ear, which can be found in the <*WSGW_HOME*>\lib directory. In order to protect the installation copy of this file, make a copy of it.

1. Launch the Application Assembly Tool from the WebSphere task menu.
2. Cancel the **Welcome to Application Assembly Tool**.
3. Select **File** > **Open** and use the **Browse** button to select the <*BCT_HOME*>\wsgw\lib\wsgwauth.ear file.
4. Import the <*webservice*.ear> file into the wsgwauth.ear using the following instructions:
   a. Click on the **EJB Modules** folder in the left-hand pane.
   b. Right-click and select **Import**. Use the file dialog to select the generated ear file <WSGW_HOME>\scripts\auth\<webservice.ear>.
   c. A dialog box is presented offering a choice of **Select Modules to Import**. Select the name of the Web service and click on **OK**.
   d. A **Confirm Values** dialog box is presented. Click **OK**.
5. Expand the EJB Modules folder in the left-hand pane to see the name of the Web service just imported. This will be called <web service>.
6. Now that you have imported the EAR file, you can begin to define roles and assign roles to methods.
   a. Expand the <*Web-service*> EJB module and highlight the **Security Roles** option.
   b. Right-click and select **New** to define a security role. Enter **Authenticated Users** for the role name. Click **OK** to save.
   c. To assign defined roles to Web-service methods, select **Method Permissions** in the left-hand pane under the <web-service> EJB. Right-click and select **New**.
   d. Enter ProtectedMethods as the method permission name.
   e. In the **Methods** pane, click **Add** for methods.
   f. Expand the tree down to the Remote branch and select the method(s) to be protected. For example, for Document Exchange, the method to select is m_BCT_DocumentTransfer()
   g. Click **OK** to save.
   h. In the **Roles** pane, click **Add**.
   i. Select a previously defined role from the list. For example, **Authenticated Users**. Click OK to save.
   j. Click **OK**.
7. The next stage is to ensure the Authorization EJB is able to reference the new EJB just imported. To do this:
   a. Expand the **<EJB Module >_<web service> > Session Beans>. Select the <*Web service*>. Then** select the **Bindings** tab on the right side pane, and copy the JNDI name into the clipboard. You will use this name in step d below.

b. Expand the **WSGW Authorization** EJB module, and then expand **Session Beans** > **Authorization** and click on **EJB References**. Right-click and select **New**.

c. Enter WSGWReference as the name for the reference and use the **Link** pulldown field to select the newly imported **<*Web service*>**. All the other fields in the pane will be populated automatically. Accept all these defaults.

d. Click on the **Bindings** tab and enter the JNDI name that was copied in step a. This should be in the form of **websphere/WSGW/Security/<*WebServiceName*>**. Click **OK** to save.

e. Select **File** > **Save** to save a modified copy of the wsgwauth.ear file.

f. Close the Application Assembly Tool.

8. Deploy the wsgwauth.ear file by highlighting **Enterprise Applications** on the WebSphere Administrative Console. Right-click and select **Install Enterprise Application**.
9. Select **Browse** and find the wsgwauth.ear file in the <*WSGW_HOME*>\bin folder. Click **Next** to continue. Next you will see the following message:

   ```
   The application contains method permissions. Do you wish to deny access to
   unprotected methods?
   ```

   Select **No**.
10. On the **Mapping Users to Roles** page, highlight **AuthenticatedUsers** and click **Select**. Check only the **Select users/groups** and then enter * in the **Search** field and click **Search**. A list of users and groups is displayed. Search the **cn=OrgOwner,dc=SecurityRole,dc=allegro** group from the **Available Users/Groups**, and click **Add** to add the group to the **Select Users/Groups**. Finally, click **OK**.
11. Click **Next** until you reach the Binding Enterprise Beans to JNDI Names screen. Click **Next** and the following message appears:

    Duplicate EJB JNDI Name message will appear.

    Click **No** to proceed.
12. Click **Next** until you reach the Selecting Application Servers screen. Highlight both modules and then click **Select Server**. Select the **WSGW** application server, and click **OK**.
13. Click **Next**, and then click **Finish**. At the completion of the installation wizard, you will be requested to generate application code. Select **Yes** when this option appears, and then click **OK** to deploy the code. Do not change any of the default values.
14. Using the Web Services Gateway Administrative console, select the Web service to protect (for example, BCT_DocumentTransfer_Create). Make sure **Authorization Policy - Control access to this service** is checked.
15. Restart the **WSGW** application server from the WebSphere Administrative Console.

Determining your product version

For Business Connection and Business Connection Enterprise Editions, you use the BCTVPDVersion program to determine the version of your product. Do the following:

1. Open a command window.
2. Enter the following:

   ```
   BCTVPDVersion.bat
   ```

For Business Connection Express Edition, do the following:

1. Open a command window.
2. Go to the following directory:

   ```
   <BCT_HOME>\wsgw
   ```

3. Open the Readme file to view the product information.

Notices

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

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

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

The following paragraph does not apply to the United Kingdom or any other country where such provisions are inconsistent with local law:
INTERNATIONAL BUSINESS MACHINES CORPORATION PROVIDES THIS PUBLICATION "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF NON-INFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. Some states do not allow disclaimer of express or implied warranties in certain transactions, therefore, this statement may not apply to you.

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

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

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

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

WebSphere Business Connection Lab Director
IBM RTP Laboratory
3039 Cornwallis Road
P.O. BOX 12195

Raleigh, NC 27709-2195
U.S.A

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

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

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

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

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

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

COPYRIGHT LICENSE:

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

Programming interface information

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

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

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

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

Trademarks and service marks

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

IBM
alphaWorks
AIX
CrossWorlds
DB2
DB2 OLAP Server
DB2 Universal Database
DeveloperWorks
MQSeries
SecureWay
WebSphere

Lotus is a trademark of International Business Machines Corporation and Lotus Development Corporation in the United States, other countries, or both.

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

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

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

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