WebSphere® Business Integrator for Windows NT®

Installation Guide

Version 2.1

GC34-5961-00

WebSphere® Business Integrator for Windows NT®

Installation Guide

Version 2.1

GC34-5961-00

Note

Before using this information and the products it supports, read the information in "Appendix E. Notices" on page 135

First Edition (June 2001)

This edition applies to Version 2.1 of the IBM® WebSphere® Business Integrator (program number 5724-A78) and to all subsequent release and modifications until otherwise indicated in new editions.

Contents

Figures

Preface

This book describes the installation, configuration, and associated procedures required to create an IBM® WebSphere® Business Integrator production or test system. To complete the installation of a development or test system you must also install Business Integrator Solution Studio; see the *WebSphere Studio Business Integrator Extensions Installation Guide*. Before using this book, you must understand the concepts of Business Integrator, as described in the *WebSphere Business Integrator Concepts and Planning* book.

Who this book is for

This book is intended for anyone involved in the installation and configuration of a Business Integrator system.

Before you implement WebSphere Business Integrator

WebSphere Business Integrator uses multiple underlying products and technologies to support the solutions that you create and run. In general, before you implement Business Integrator, you will need to understand the underlying products and technologies that support your solution.

Before you implement Business Integrator, you or other members of your organization will need to be generally skilled in the activities listed below for similar solutions, products and underlying products and technologies. If you and other members of your organization do not possess these skills, you will need to obtain assistance, from qualified services staff, either from IBM or from third parties, to implement Business Integrator. You must be prepared to use the documentation of the underlying products and technologies. (This documentation is provided with Business Integrator or otherwise from IBM.)

When you plan, install, and configure Business Integrator, you will need to understand how to install and configure soem of the underlying products and technologies that you use in your installation. Business Integrator provides the installation of most of the underlying products and technologies into its run time environment. However, you might need to install and configure certain underlying products separately into either the build time or run time environment. You might also need to diagnose and correct installation problems with underlying products and technologies.

Before you design, develop and publish solutions, you will need to be:

- Generally familiar with system integration techniques in a business environment.
- Prepared to use the tools of the underlying products and technologies that your solution requires.
- Familiar with the run time behavior of the underlying products and technologies that your solution requires.
- Familiar with modeling concepts and techniques such as Unified Modeling Language, and related tools, with state machine concepts, and with visual flow composition-modeling concepts and techniques.
- Familiar with Internet and Electronic Data Interchange (EDI) concepts and technologies, if required by your solution.
- Prepared to research the existing applications, systems, and networks that you integrate with Business Integrator.
  - Inside your enterprise, they can be known as legacy systems, back-end systems, enterprise applications, or endpoint applications.
  - Outside your enterprise, they can be known as trading networks, private EDI networks, or similar networks that your solution requires.

Before you deploy, run, manage, diagnose, and tune Business Integrator, you will need to be prepared to use the management, trace, audit, exception handling, diagnostic and related tools of the underlying products and technologies that support your solution. You will need to be prepared to understand the solution itself to the degree needed for these tasks.

How to use this book

The starting point of this book is that you have chosen your topology and know which products will be installed for that topology and the hardware required.

When you have completed your planning, use this book sequentially with each machine in your topology, starting with the base machine.

You are advised to read through this book completely, to gain an understanding of the sequence of the installation and configuration, before starting the installation.

Important notes

You are strongly advised to follow the instructions in this book carefully and in sequence, so that you can successfully install and configure Business Integrator. Some steps might not apply to your topology or to a particular machine in your topology. Use the following flowchart to guide you through the book and always read the ″Use this chapter″ panel at the start of each chapter.

You must also look at the Release Notes provided with Business Integrator for latest information that was not included in this book. You'll find the Release Notes at:

http://www.ibm.com/software/webservers/btobintegrator/support.html

As you do your planning for a Business Integrator system, and as you work through the installation, fill in the spaces provided in the checklists in "Chapter 2. Making notes to help you through this book" on page 5. You'll need this information at various points throughout the installation and configuration. If you provide incorrect passwords, for example, during the installation and configuration, your install might fail and require complete reinstallation.

You are advised to take an image of each machine during the installation at the end of each significant step. The installation process is long and complex. If anything fails during this process, a backup image might save you a significant amount of time.

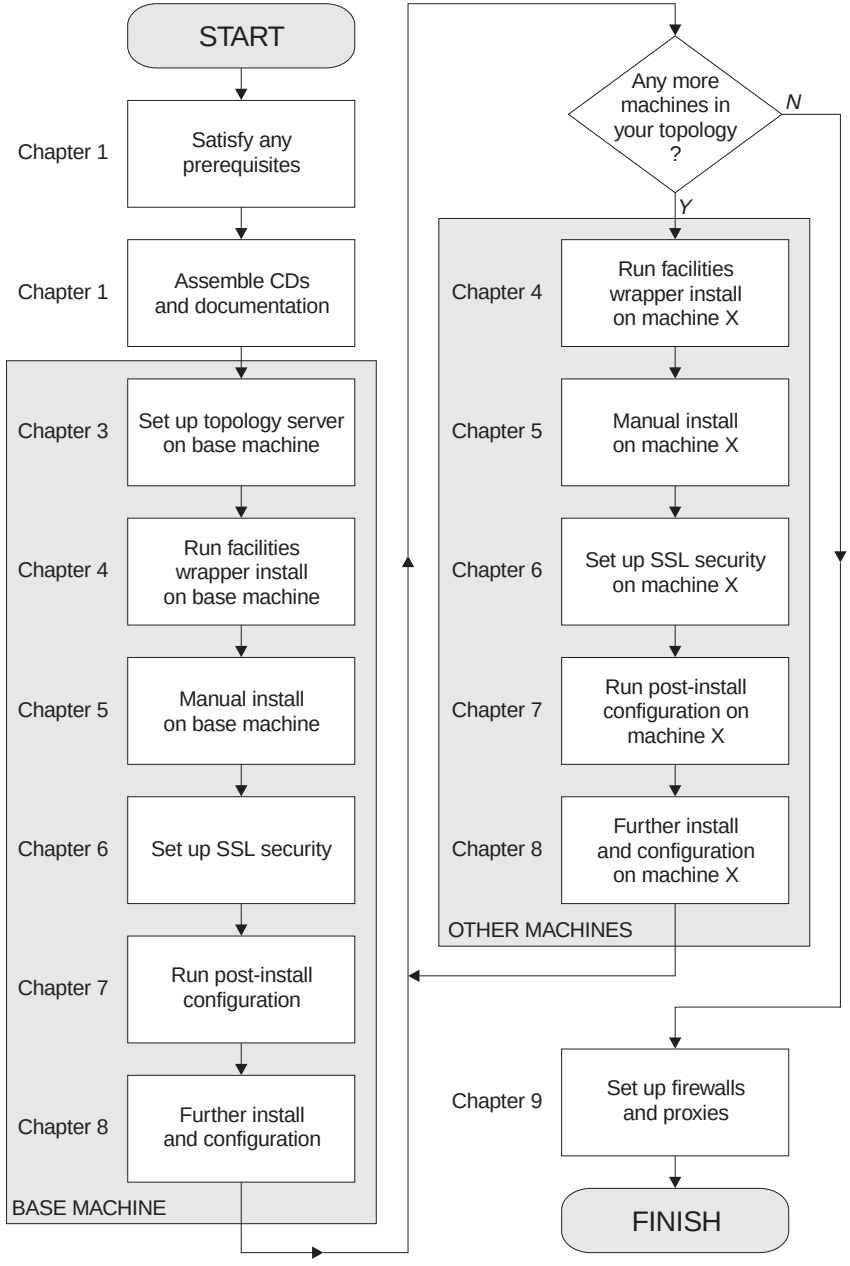


Figure 1. Reading sequence flowchart

During the installation, always use this book first for the installation of all the products. You should not have to use books from another library unless this book points you to one. For example, you should not have to use MQSeries®

Integrator or MQSeries Workflow installation documentation because those products are installed under the Business Integrator wrapper installation.

How to send your comments

IBM welcomes your comments. You can send your comments by any one of the following methods:

1. Electronically to this address:

   `idrcf@hursley.ibm.com`

   Be sure to include your network address if you want a reply.

2. By FAX, to the following numbers:

   `UK: 01962-842327`
   `Other countries: +44-1962-842327`

3. By mail to the following address:

   User Technologies
   Mail Point 095
   IBM United Kingdom Laboratories
   Hursley Park
   Winchester
   Hampshire
   SO21 2JN
   United Kingdom

Terms used in this book

You'll find definitions of many of the terms used in this book in the Glossary in the *WebSphere Business Integrator Concepts and Planning* book. Other terms are explained when they are first used.

Chapter 1. Before starting your installation

Use this chapter
to make sure that you have the right prerequisites to start your installation and the correct set of CDs and documentation. If your prerequisites are incorrect, you are unlikely to install Business Integrator successfully.

This chapter describes what you must check before you begin your installation:

System prerequisites

Make sure you meet these prerequisites before starting your installation.

″Clean″ machines

The machines you use for Business Integrator should be ″clean″. Note that:

- You are recommended to install on machines on which Windows NT has been freshly installed and the partitions cleared so that they do not contain previously installed products unknown to the NT Registry.
- If you try to install Business Integrator on a machine that contains previously installed component products, your install might not complete because of wrong product levels. If the machine does contain products at the wrong level, uninstall them, and ensure that all folders, directories, and files related to these products are completely removed. The *WebSphere Business Integrator Concepts and Planning* book provides a list of products with version and release levels. In particular, you must install WebSphere as part of the wrapper install. If you leave an existing WebSphere on your machine, the wrapper install cannot check that all the required e-fixes have been applied.
- If you try to install on a machine on which Business Integrator has already been installed or partially installed, the resulting configuration might be incorrect if the NT Registry is in an indeterminate state.

Software prerequisites

Before you start the installation, make sure you have satisfied these prerequisites on all the machines in your topology:

- Microsoft® Windows NT® Server, Version 4.0, with Service Pack 6a or higher is required. During installation, you will be told if you do not have the correct service pack and where to find it.
- Internet Explorer Version 5.0 or higher is required. If it is not present, the wrapper installation will fail
- IBM Java™ Runtime Environment Version 1.2.2, Service Release 11, is installed as part of the wrapper installation. If this version of Java is already present on any machine in the topology but it is not the System JVM, uninstall it and allow it to be reinstalled. Unless it is the System JVM, there will be compatibility problems with other Business Integrator components. You must have Service Release 11; you can check the Service Release level by typing `java -version` at the DOS prompt. A response that includes `build cn122-20010308` indicates that Service Release 11 is installed. Any other response means that you should uninstall JRE and take the version from the wrapper installation.
- For use with DB2® Version 7.2 (which equates to Version 7.1.3 with fixpack 3), you are strongly recommended to install MDAC (Microsoft Data Access Components) 2.5. If you do not follow this recommendation, you might encounter unpredictable results. Business Integrator does not check for this prerequisite.

  MDAC 2.5 can be downloaded from:

  `http://www.microsoft.com/data/download_25SP1.htm`

Other prerequisites

You must also meet these prerequisites:

- A TCP/IP network must be installed and configured using a single fixed IP address on each machine. You cannot use Dynamic Host Configuration Protocol (DHCP) because only fixed IP addresses are supported. If you want to use host names, you must ensure that all host names are defined to your name server.
- For your MQSeries configuration, ensure that each machine is enabled as part of a Windows NT domain environment. If you want to use multiple NT domains, ensure that there are appropriate trust relationships between all of the machines in the topology. Without these relationships, MQSeries cannot perform authentication across the cluster. For more information about MQSeries security requirements, see the `MQSeries Planning Guide`, GC33–1349.
- Computer name and host name must match (including upper- and lower-case) on each machine.
- Computer names must follow MQSeries naming conventions.
- All systems must have a temporary directory configured. This can be on any suitable drive, but the corresponding Windows NT environment variables (`TEMP` and `TMP`) must match.

- Machines must use English (United States) regional settings. Do not use any other regional settings on any machine in the topology. You can change regional settings by using the Regional Settings applet from the Windows NT control panel.
- The display screen used to set up the base machine must be run in a minimum of 256 colors and a minimum resolution of 1024x768. If you use fewer colors, the screen will not display properly.
- Display screens used for the wrapper installation must be run at a resolution higher than 640x480 to ensure that MQSeries and related installs do not fail.

Check your installation CDs

Before you start your installation, make sure that the full set of CDs is ready for use and that you have the associated documentation you need. The first table lists the Business Integrator CDs:

CD	Contents
Initial Setup Installer (Topology Server)	Topology Server and HTTP Server installation to set up the base machine. Check the README in the root directory and at: `http://www.ibm.com/software/webservers/btobintegrator/support.html` for the latest information before starting the installation.
Facilities CD 1	Installation of products that make up the facilities.
Facilities CD 2	Installation of products that make up the facilities.
Facilities CD 3	Installation of products that make up the facilities.
Documentation	Business Integrator PDFs; selected documentation (PDFs, or HTML if a product does not supply PDFs, and information centers) for the other products covering both runtime and development. The README in the root directory lists the contents.
Partner Agreement Manager	Used for the manual installation of Partner Agreement Manager. Use the appropriate installation key, which you'll find on the CD label. Note this key because you need it when the CD is in the CD drive.
Partner Agreement Connect	Used for the manual installation of Partner Agreement Connect. Use the appropriate installation key, which you'll find on the CD label.
Partner Agreement View	Used for the manual installation of Partner Agreement View. Partner Agreement Manager is a prerequisite.
DataInterchange	Used for the manual installation of DataInterchange in the Enterprise configuration

WebSphere Studio Business Integrator Extensions	Used for the manual installation of Business Integrator Solution Studio. See the *Solution Studio Installation Guide* for more information.

This table lists the product CDs supplied as part of the Business Integrator media pack:

MQSeries Integrator Version 2.0.1	Used during the wrapper installation, Enterprise configuration only
MQSeries Workflow Version 3.3	Used during the wrapper installation, Enterprise configuration only
WebSphere Personalization	Used for the manual installation of WebSphere Personalization
Tivoli Policy Director (3 CDs)	Used for the manual installation of Tivoli Policy Director

When you manually install Business Integrator components, using the documentation specific to those components to guide you, always read the installation instructions provided in this book first, starting on page 44.

Licence requirements

Make sure that you have the correct number and types of licences to match the topology that you're about to install. The *WebSphere Business Integrator Concepts and Planning* book describes licensing.

Firewalls

If you will be installing firewalls, you need SecureWay® Firewall, version 4.1 or an equivalent firewall product of your choice.

Keeping notes

Important note

As you work through the installation, fill in the spaces provided in the checklists in "Chapter 2. Making notes to help you through this book" on page 5 with passwords, cluster names, and other reference information. You'll need this information at various points throughout the installation and configuration. If you provide incorrect passwords, for example, during the installation and configuration, your install might fail and complete reinstallation be required.

Chapter 2. Making notes to help you through this book

Use this chapter
to help you remember key information. The chapter provides checklists to fill in during the planning phase and during the installation. You'll need this information at various points throughout the installation and configuration. If you provide incorrect passwords, for example, during the installation and configuration, your install might fail and require complete reinstallation.

Take photocopies of these pages if that will help you. Make sure that you take appropriate precautions to keep the information secure.

This information will also be needed when a CSD is applied.

Checklists

Fill in these boxes either in the planning stage or as you work through the installation, as appropriate, so that you have useful reference information:

Endpoints

Machine name:

Publishing name:

Machine name:

Publishing name:

Machine name:

Publishing name:

Machine name:

Publishing name:

Machine name:

Publishing name:

Machine name:

Publishing name:

Topology URL (URL of base machine)

HTTP

user ID:

password:

MQSeries cluster name

JMX RMI port

Password for the database administrative user ID of db2admin

MQSeries Integrator (MQSI)

user ID:

password:

WebSphere Application Server

user ID (not greater than 8 characters):

password:

Solution Manager

user ID:

password:

DCE

user ID:

password:

Policy Director sec_master user ID password

SecureWay Directory Server (LDAP)

cn=root password:

cn=WSBIAdmin,o=ePICUsers, o=epic password:

SSL password

Location of .kdb file for self-signed certificate

Location of .arm file for self-signed certificate

Key label for your self-signed certificate

Partner Agreement Manager installation key (on the CD label)

Partner Agreement Manager partner name

Partner Agreement Manager partner ID

Partner Agreement Manager

user ID:

password:

Partner Agreement View

channel ID:

channel name:

Use the following empty tables to list the products that require manual installation on the machines in your topology, taking the information from the panel that lists the required manual installations (there's an example in Figure 7 on page 23). Use the tables as you work through "Chapter 4. Installing the facilities on the machines in your topology" on page 29 and the following chapters:

Base machine
Machine hostname:
Topology name:
Machine IP address:

Base machine

Machine 1
Machine hostname:
Topology name:
Machine IP address:

Machine 2
Machine hostname:
Topology name:
Machine IP address:

Machine 2

Machine 3
Machine hostname:
Topology name:
Machine IP address:

Machine 4
Machine hostname:
Topology name:
Machine IP address:

Machine 4

Machine 6
Machine hostname:
Topology name:
Machine IP address:

Machine 7
Machine hostname:
Topology name:
Machine IP address:

Machine 7

Machine 8
Machine hostname:
Topology name:
Machine IP address:

Chapter 3. Setting up the topology server on the base machine

Use this chapter

to install the topology server on the base machine. You cannot make progress in the following installation and configuration chapters until you have successfully installed the topology server with its repository. Once you have installed it, you will not have to return to this chapter except for reference.

You must also look at the Release Notes provided with Business Integrator for latest information that was not included in this book. You'll find the Release Notes at:

http://www.ibm.com/software/webservers/btobintegrator/support.html

During the planning phase, you decided on the machine that will be your base machine, and that's where you install the topology server. Business Integrator has only one base machine and only one topology server. When you install facilities on the base machine and the other machines, described in "Chapter 4. Installing the facilities on the machines in your topology" on page 29, the installation process refers to the topology server repository.

The panels shown in this chapter and the following chapters are examples; the content of panels will differ depending on the topology selected.

Before you start

When you install Business Integrator, you must be logged on with a user ID that is a member of the Windows NT Administrators group in the local domain. If you do not have this authority, you will not be able to run the installation program.

When WebSphere Business Integrator accesses DB2 – for example, to create a WebSphere Application Server database or to install PAM – it will use the user ID `db2admin`. If this user ID does not exist, the Business Integrator install will create it. You set the password and use it subsequently.

Ensure that a system environment variable called `TEMP` exists. Select `Start->Settings->Control Panel` and double click on the **System** icon to display the ″System properties″ window. Click on the **Environment** tab, and

look under ″User Variables″ for a TEMP variable. If there isn't one, create one by setting a variable to TEMP. A reasonable setting is `x:\temp` where x is the drive to which the operating system is installed.

You must exit all Windows NT programs before starting the installation procedure. You are guided through the procedure and are prompted for any information required for completion.

Selecting your topology

1. Insert the Initial Setup Installer CD. If the Select Topology panel does not appear automatically, run `bizSelect.cmd` in the root directory on the CD.
2. First, you see the Select Topology Panel with a selectable list of the names of the predefined topologies in a pull-down menu. Selecting the categories in the ″Select Topologies″ pull-down provides short explanations of the different topologies. From the list, select your topology.

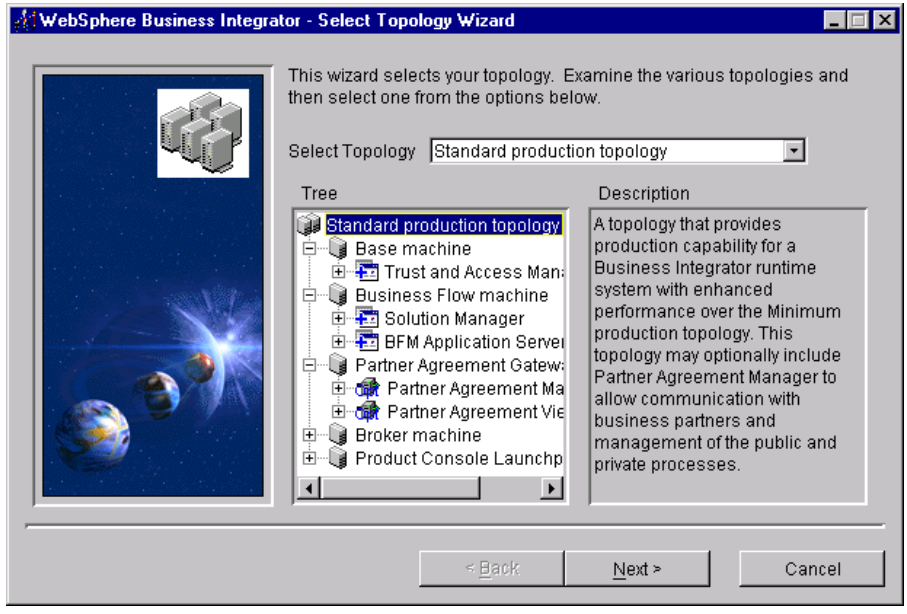


Figure 2. Selecting your topology

3. When you select a topology, a tree view is displayed for that topology. This hierarchical view of the current topology enables you to work downwards:

   ```
   (Topology-->Machine-->Facility-->Software Product)
   ```

   You can examine each topology by navigating the tree view to see which facilities and software products will be installed on each of the machines

for that topology. The icons on the various nodes of the tree view reflect the types of object that they represent. As you highlight various nodes in the tree view, a description of the object represented by that node appears in the Description panel. There are different icons to represent different properties of a given object type; for example, the icon for an optional facility is different from the icon for a required facility.

4. When you have decided on a topology to install, highlight it in the ″Select Topology″ field and click **Next**.

Selecting your options

Any given topology might contain optional facilities that can be installed. If your topology has any optional facilities, they are presented to you and you select which ones to install. There might be cases where there are dependencies between the facilities. For instance, PAV cannot be installed without PAM. So, if you select PAV, PAM is automatically selected.

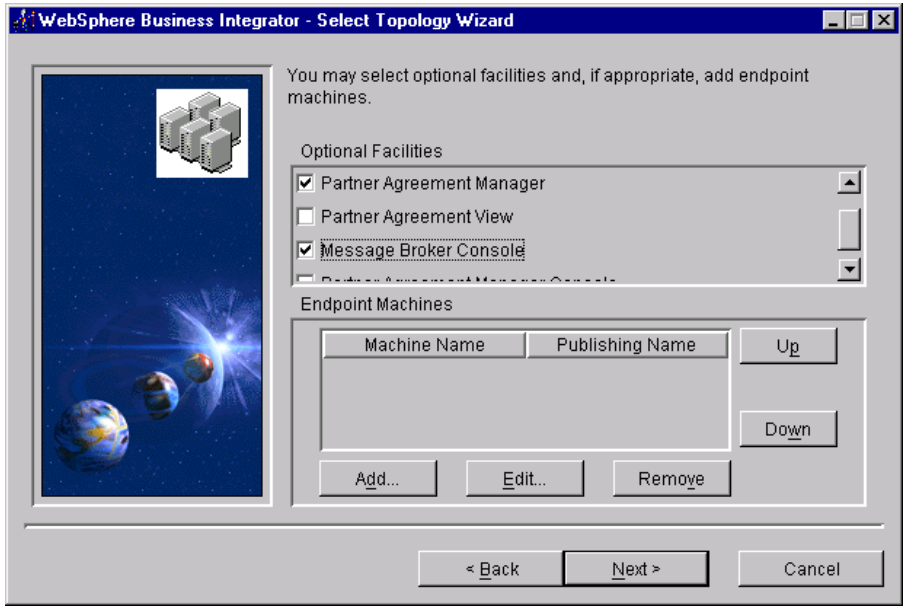


Figure 3. Selecting your options

In addition, you have the option to specify a number of Endpoint machines, as part of the topology, by clicking **Add**. Initially, the list of Endpoint machines is empty. You must include here all the Endpoint machines required in your topology. **You cannot add further Endpoints later.**

This is the pop–up that appears when you click **Add** or **Edit**, enabling you to specify the machine name and publishing name of an Endpoint machine. The

publishing name is the name for the Endpoint when publishing a solution from Solution Studio. The names must match.

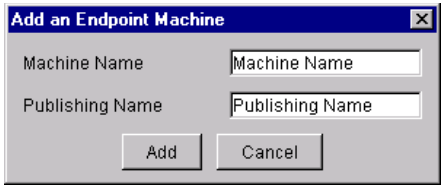


Figure 4. Endpoint machine pop-up

When you are satisfied with your choices, you can move forward to the next panel.

Confirming your selected topology

When you have selected a topology for installation, selected any optional facilities and specified a number of endpoints, you are presented with a final view of the topology, with your choices applied. The view allows you to work with the hierarchical structure of the topology, and to use the **Back** button if you want to review or make changes. When you are satisfied with your choice, write down the names of the machines as known to the topology in the empty tables provided in “Chapter 2. Making notes to help you through this book” on page 5, and click **Next**.

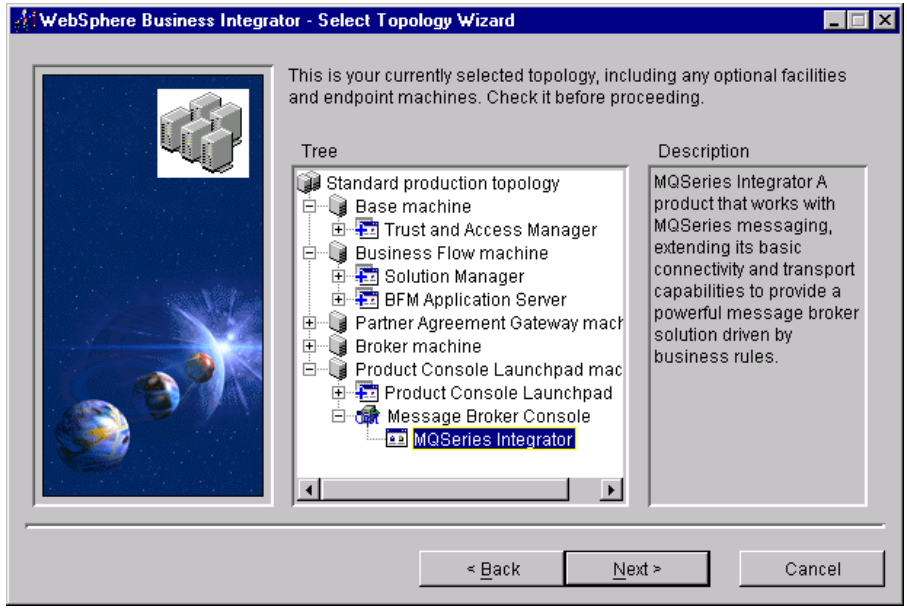


Figure 5. Confirming the topology

On the next panel, enter configuration information. The MQSeries Cluster Name will be used for all MQSeries servers installed as part of the topology. Make sure that you have a unique cluster name and that it is consistent with any existing MQSeries naming standards. The cluster name will be added to the host name to create queue manager names. The JMX RMI port number will be used as the port number for all machines in the topology. So you must use a port number that is free on all machines.

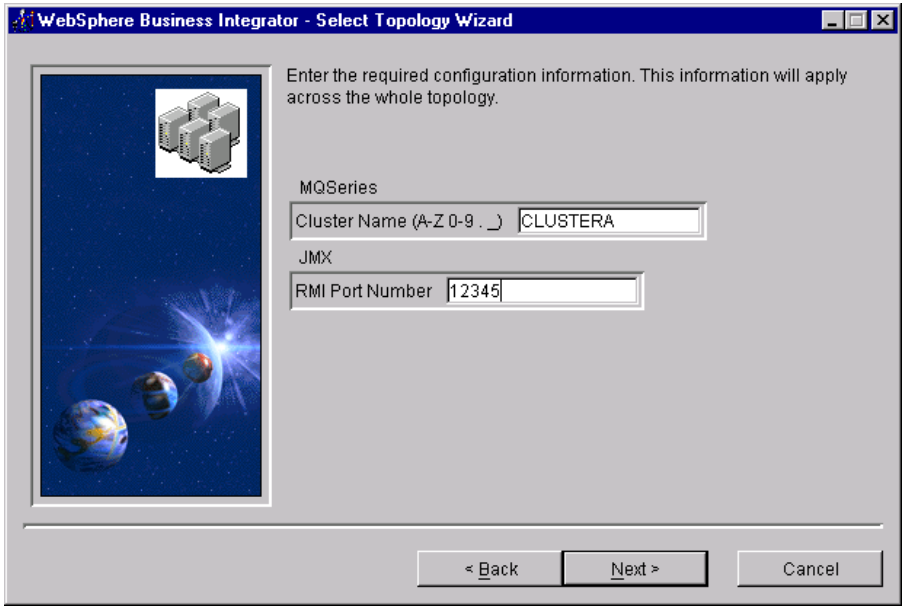


Figure 6. Entering configuration information

Click **Next**.

Listing the chosen products

The final confirmation panel before you install the topology server lists the products to be installed for your topology. It tells you which of those products will be installed automatically and which will be installed manually. Later, there's another panel to remind you of the manual installs.

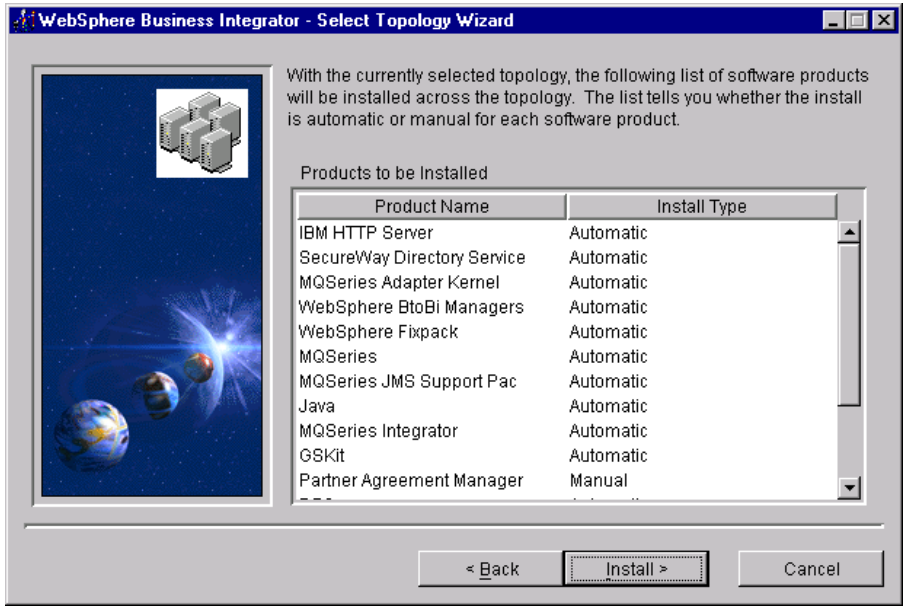


Figure 7. Listing the chosen products

You can sort the two lists by clicking on the header buttons **Product Name** and **Install Type**. Click on **Back** to revisit and, if necessary, change your selections. After you have clicked on **Install**, you cannot return to the ″Select Topology Wizard″ panel.

Installing the HTTP Server and WebDAV

When you click **Install**, the installation procedure for the HTTP Server and WebDAV starts. The installation of the HTTP Server and WebDAV allows Business Integrator to access the topology server repository during the rest of the installation process.

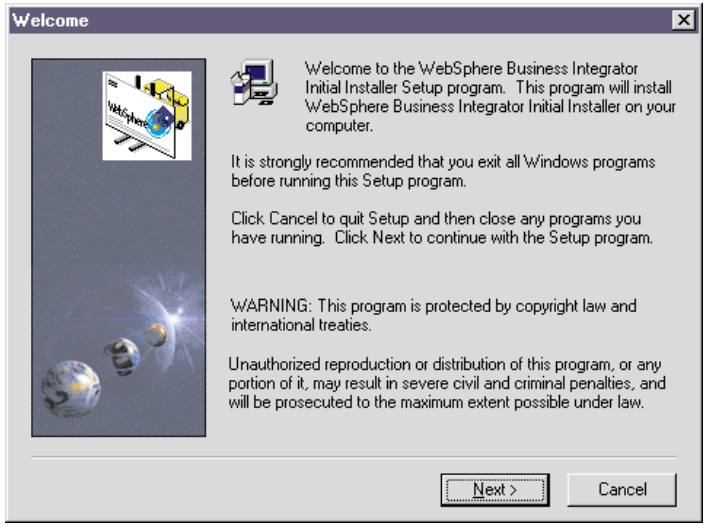


Figure 8. Starting the installation of the HTTP Server and WebDAV

Click **Next** for the licence information panel, which you must read to decide whether or not to accept the conditions set out in the panel. If you choose not to accept the conditions, installation is ended.

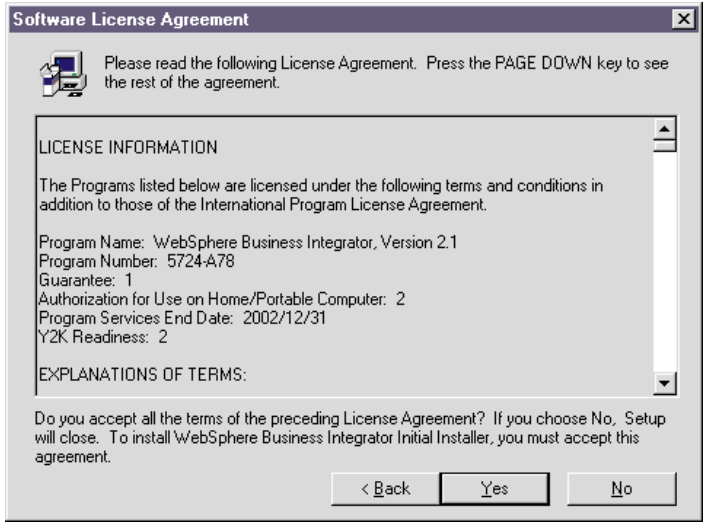


Figure 9. Licence information panel

If you accept the licence conditions, click **Yes** and you are asked for the directory and folder into which to install the HTTP server.

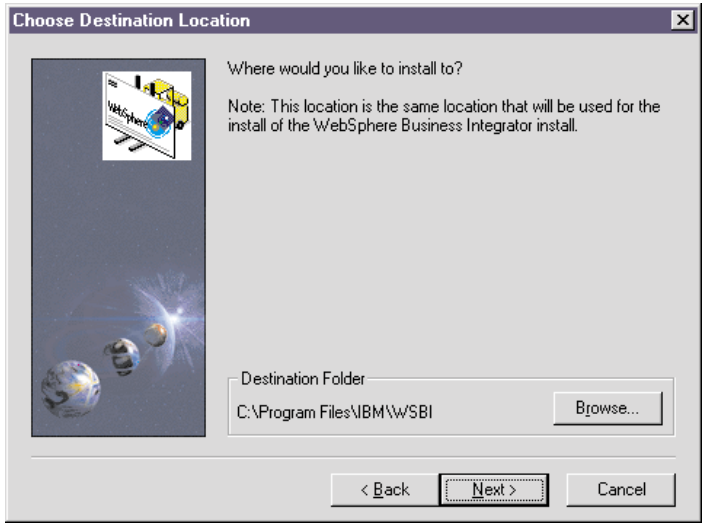


Figure 10. Directory and folder information for the HTTP Server

Use the **Browse** button if you want to change the default drive and folder. Click **Next** and you are asked to select your programs folder. Click **Next** again for a panel that asks if you are satisfied with the settings you have chosen.

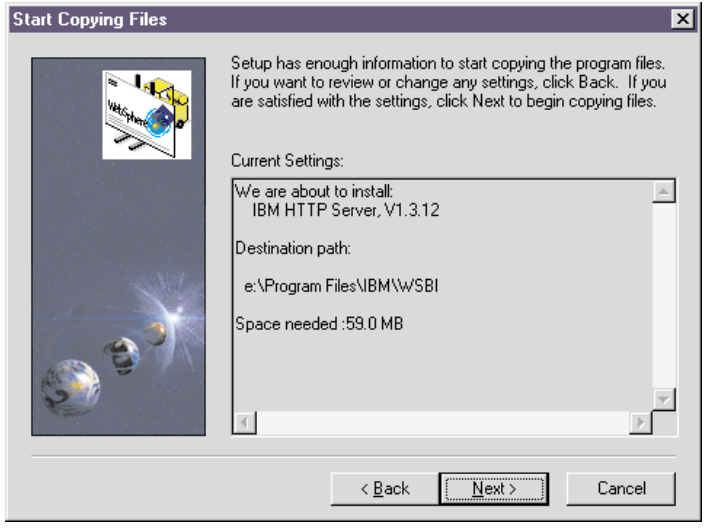


Figure 11. Checking the settings

Use the **Back** button to return to make any changes you require. When you are satisfied, click **Next**.

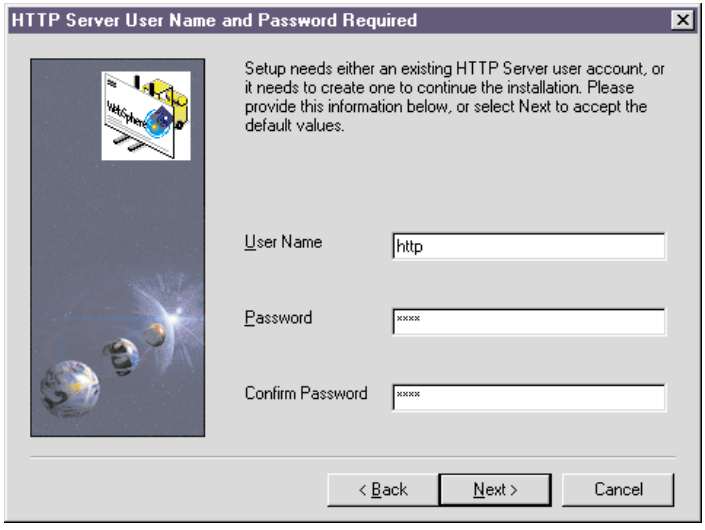


Figure 12. HTTP Server user name and password filled in

Enter the HTTP Server User Name and Password, confirm the Password, and click **Next** to start the installation of the HTTP server and WebDAV. Make a note of these values.

Completing the topology server installation

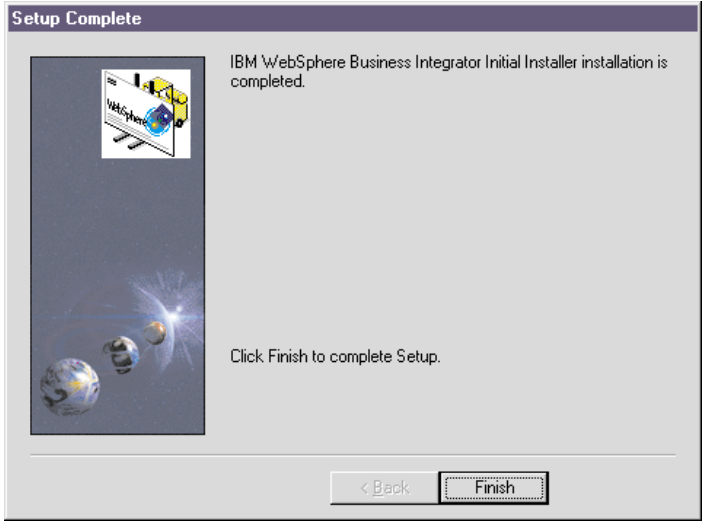


Figure 13. Topology server installation is complete

The final panel tells you that the Initial Installer has installed and configured HTTP for use with the topology repository. Click **Finish** to end.

At this point, make sure that you write down in “Chapter 2. Making notes to help you through this book” on page 5 the topology server URL. The URL is the fully qualified host name of the base machine with `/topology` appended. For example:

```
host.domain.com/topology
```

Do not use the IP address in the URL.

You may now install the relevant facilities on the base machine, starting at “Chapter 4. Installing the facilities on the machines in your topology” on page 29.

Chapter 4. Installing the facilities on the machines in your topology

Use this chapter

to install facilities on the base machine first. When you have completed all the installation and configuration of the base machine using this chapter and the relevant following chapters, return to this chapter to start the installation of the other machines in the topology. You must completely install and configure a machine before starting on another machine. Do not try to run installations on different machines in parallel.

Refer to Figure 1 on page xii in the Preface to understand the installation and configuration sequence and the order in which this and subsequent chapters are used.

This chapter concludes with some pointers to solutions for possible problems, in "What to do if something goes wrong during installation" on page 40

You must also look at the Release Notes provided with Business Integrator for latest information that was not included in this book. You'll find the Release Notes at:

http://www.ibm.com/software/webservers/btobintegrator/support.html

After you've installed the topology server on the base machine, you're ready to install your chosen facilities on the machines in your Business Integrator topology. The wrapper installation will guide you through the use of the Facilities CDs 1, 2, and 3 and the other CDs supplied, as required for each machine in your topology. The Installation Launchpad accesses the topology information stored on the base machine to find out which facilities to install on which machines.

You must install and configure the facilities on the base machine first, using this chapter and the relevant following chapters. Then install and configure facilities on other machines in the topology. **You must complete the installation and configuration of one machine before starting on another.**

When WebSphere Business Integrator accesses DB2 – for example, to create a WebSphere Application Server database or to install PAM – it will use the

user ID db2admin. If this user ID does not exist, the Business Integrator install will create it. You set the password and use it subsequently.

Ensure that a system environment variable called TEMP exists. Select Start->Settings->Control Panel and double click on the **System** icon to display the ″System properties″ window. Look under ″User Variables″ for a TEMP variable. If there isn't one, create one by setting a variable to TEMP. A reasonable setting is x:\temp where x is the drive to which the operating system is installed.

Running the wrapper installation

The installation program takes you through a number of panels as shown in this chapter. Using the panels, you define the machine on which you are installing to be one of the logical machines defined in your topology. You are then guided through the installation of the relevant products on that machine.

1. Insert the Facilities CD 1 into the machine you are about to install. If autorun is enabled, the installation process starts automatically. If it does not, double-click on bizInstall.cmd in the root folder on the CD to start the process. You are presented with the following panel:

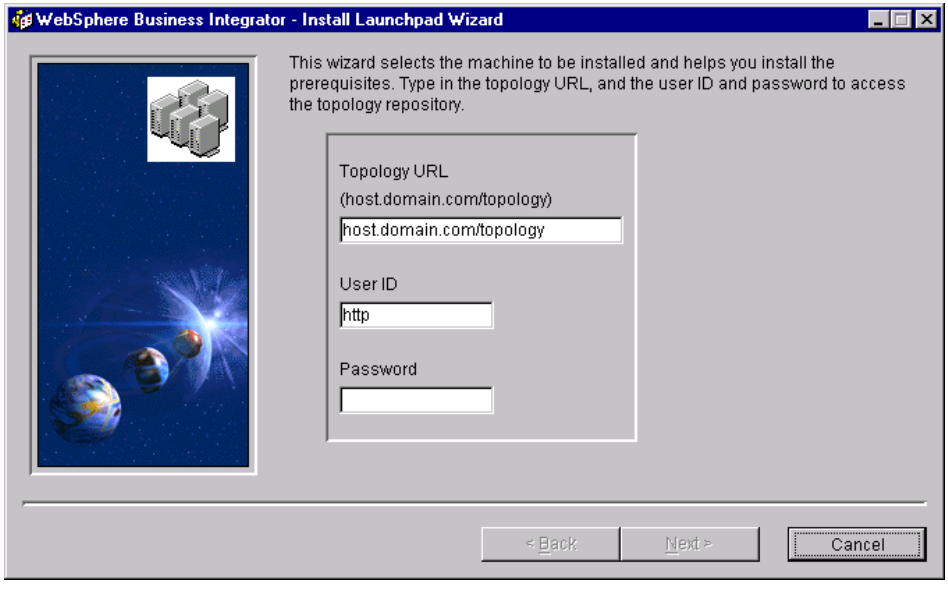


Figure 14. Topology launchpad first panel

2. This panel presents you with some default values. Enter the URL of the topology repository that was installed on the base machine, as described in “Completing the topology server installation” on page 26 and noted in “Chapter 2. Making notes to help you through this book” on page 5.

Check that the user ID is correct and enter the password. The user ID and password required are those of the IBM HTTP server installation on the base machine. The **Next** button is not available until all three fields are filled in.

3. When you click **Next**, you might see a timer icon because the connection is across the network. If the connection fails, you'll receive a message in a dialog box. Possibly:
   - The network is down or not attached.
   - The URL of the topology is incorrect.
   - The user ID or password is incorrect.

   You can't proceed until the connection is successful.
4. The next panel shows you a view of the topology.

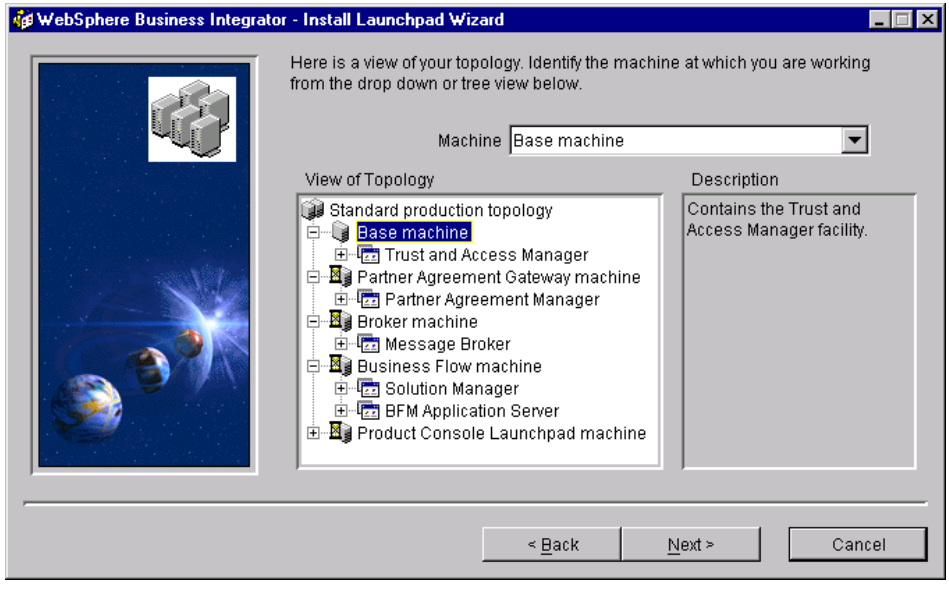


Figure 15. An example view of a topology

Use the drop-down menu or the tree structure to select the logical machine that you want this physical machine (the one you're now working on) to become. The drop-down menu might help you to have an overall view of your topology when there are many machines and facilities.

In the tree view, click on:

- The first item to see a description, in the right-hand pane, of the topology you've selected.

- A machine icon to see a description, in the right-hand pane, of that machine .
- The + sign next to a machine to see the facility or facilities that will be installed on that machine, with a description in the right-hand pane.
- The + sign next to a facility to see the products that make up that facility.

There are four categories of machine, indicated by icons:

a.

A machine that is already installed. If you click on such a machine, the **Next** button is disabled because that machine is already installed.

b.

A machine not currently installed that can now be installed. You may now request installation by clicking on the machine displayed in the tree. The **Next** button will be enabled.

c.

A machine not installed that cannot be installed until other machines have been installed first. You cannot install this machine yet, because other facilities must be installed before you begin on this machine. Such a machine moves into category ″b″ when the other facility or facilities have been installed. For example, the Trust and Access Manager facility must be installed before any other facility.

d.

A machine that is partly installed (perhaps because an installation was not previously completed). You may choose this machine for installation by selecting it and clicking **Next**.

When you've selected a machine, click **Next**.

5. The next panel shows the prerequisites for the facility or facilities on this machine.

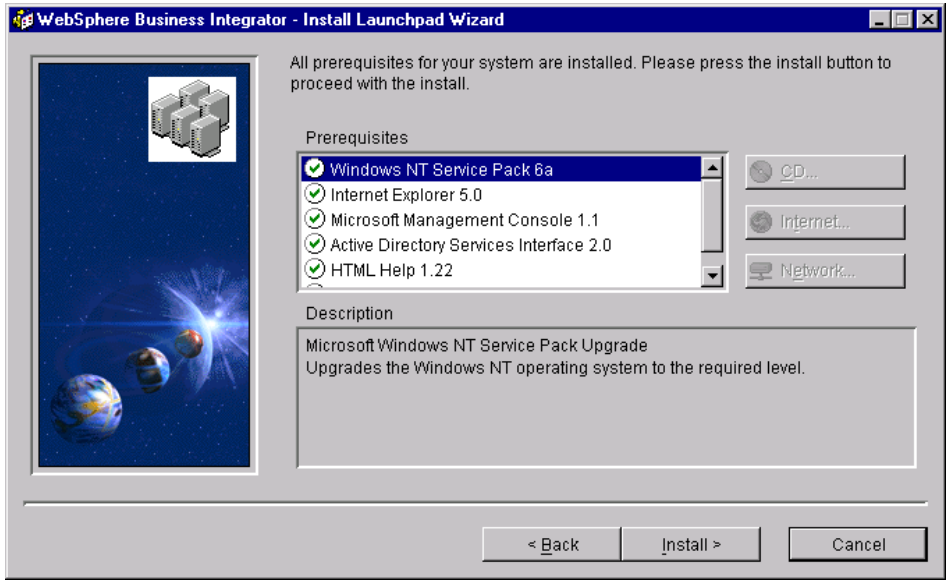


Figure 16. Prerequisites for this facility

You have to install these prerequisites before you can install the facility. A check mark indicates that a prerequisite is installed and a cross indicates that a prerequisite is not installed or is not installed at the required level. Select a prerequisite to see a description of it. The buttons to the right help you with the installation, and become enabled as appropriate:

CD button

If the prerequisite is on Facilities CD 1, the installation will start immediately. If the CD is not in the drive, you are asked to insert it. The prerequisites on CD 1 are:

- Microsoft Management Console
- Active Directory Services Interface
- HTML help
- Microsoft Windows Installer

These prerequisites are not on CD 1:

- Internet Explorer V5 or greater
- Windows NT Service Pack 6a

If any of these prerequisites are required on this machine, a dialog is displayed instructing you to place the correct CD in the drive and use the dialog to run the setup program for the prerequisite software component selected.

After the installation, you might have to reboot your machine, and then you'll return to this panel. If you don't have to reboot, you'll return to this panel.

Internet button
If this button is enabled, click on it to go to the correct site on the internet to install the product in question. Follow the instructions on the Web page to install the prerequisite software component.

Network button
This button enables you to browse for the product on your machine and across any mapped network drives. You install the product following its own product documentation.

Some prerequisite software – for example, Internet Explorer and Windows NT Service Pack 6a – requires a system reboot after installation. The Install Launchpad warns you if this is the case after you have pressed the CD, Internet, or Network button. If you want to continue the installation, the Install Launchpad closes after the setup program has started or the Internet Browser has been launched.

After the machine has rebooted, the Install Launchpad user interface attempts to launch automatically. If Facilities CD 1 is not in the drive, the Launchpad user interface starts after you have inserted the CD. The Install Launchpad user interface automatically opens at the panel shown in Figure 16 on page 33, displaying the prerequisite software components. You are not prompted to enter the URL, user ID, or password.

6. When the prerequisites are installed, you'll see a column of green check marks to the left of the product names. When all the prerequisites have been installed, the **Install** button is enabled to allow you to start the installation. When you click **Install**, you see a dialog box with **OK** and **Cancel** options:

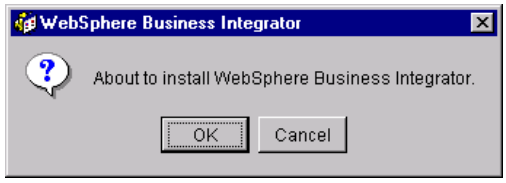


Figure 17. Dialog box to start the installation

When you click **OK**, the wrapper installation begins. If you click **Cancel**, the association between logical and physical machines is removed and the machine is in an uninstalled state. If you have installed a prerequisite and then you click **Cancel**, the installed prerequisite products remain installed.

Clicking **OK** displays a Welcome panel. Click **Next** on the Welcome panel.

7. You now receive an advance notification of products that must be installed manually at the end of the wrapper installation. You may make a note of these products in the empty tables in “Chapter 2. Making notes to help you through this book” on page 5 either now or when the list is displayed later. Also ensure that you have the relevant CDs.

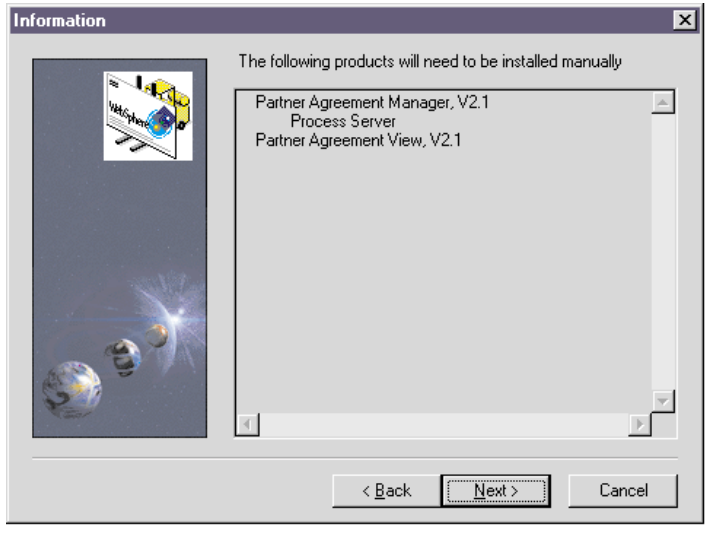


Figure 18. List of products to install manually

8. You are advised that Java Runtime Environment Version 1.2.2 will be installed and will replace any other level of Java present on the system. Accept this level of Java to continue the installation.

Figure 19. Java 1.2.2 installation

9. Select the folder where Business Integrator will be installed. You provide a base location and certain products are installed under this location. Other products, because of their requirements, are installed on the same drive, but in their own folders. For example, MQSeries is installed in directory `Program Files\MQSeries`; DB2 is installed in directory `\sqllib`.

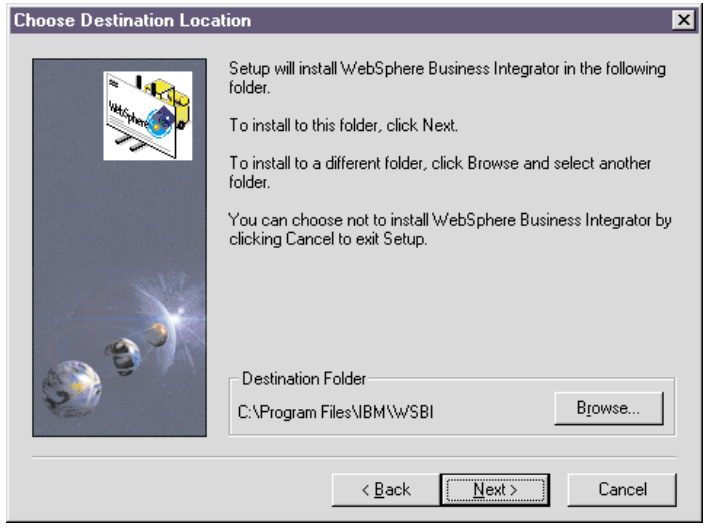


Figure 20. Selecting where to install

10. If the installation program finds Business Integrator facilities already installed, you cannot add any more. Stop the installation and choose a different machine or uninstall the existing facilities on the current machine, as described in “Chapter 11. Uninstalling Business Integrator” on page 107, and start the installation again.

    If you are installing facilities on the base machine, you are recommended to install to the same path as used for the base install; see Figure 10 on page 25.

11. When you have selected the path, click **Next**. The next panel allows you to enter the name you want to use for the product in the ″Program Start″ menu. The default is ″WebSphere Business Integrator″.

12. Click **Next** and you are presented with:
    - A list of facilities
    - A list of products that will be installed
    - A list of products already installed
    - Any products that must be upgraded after the Business Integrator installation has finished
    - Products already present, but the component needed by Business Integrator is not installed
    - The destination path
    - The total disk space needed

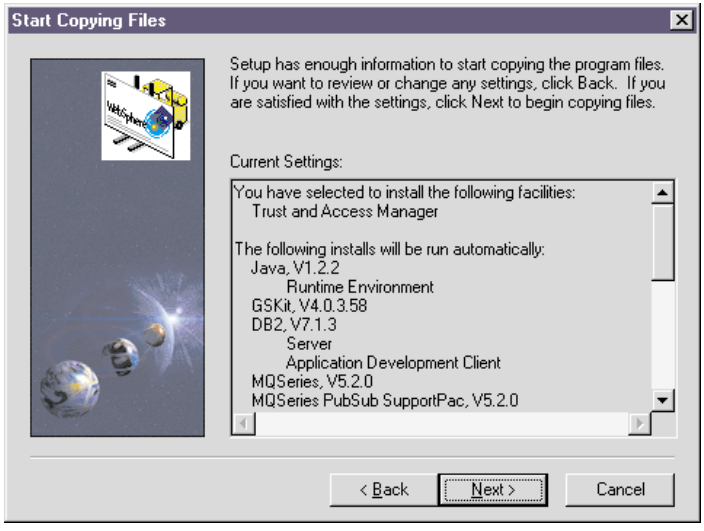


Figure 21. List of products that will be installed

Make a note of the products installed on this machine, using the tables in "Chapter 2. Making notes to help you through this book" on page 5, as a reminder that you must subsequently configure all these products after you have installed everything on this machine.

13. If you are installing DB2, you'll see a Limited License Agreement panel. If you accept the conditions, click **Yes** to continue.
14. If any user ID information is required, it is requested now. For WebSphere Application Server, the user ID must not be greater than 8 characters. When you have entered all the user IDs, the installation starts. You'll be prompted to insert installation CDs.

    When you install the MQSeries WorkFlow CD, it might autorun. If this happens, stop the autostarted install and continue with the wrapper install.

15. When all the installations are complete on this machine, the Business Integrator installation checks the log files and reports on the success or failure of the installations. Products are listed as ″Successful″, ″Failed″, or ″Blocked″. When the install of a product fails, the wrapper installation continues to install the other products. If, however, a product cannot be installed until a failed product has been installed, that product is listed as ″Blocked″. See “What to do if something goes wrong during installation” on page 40 for some guidance about dealing with install failures.

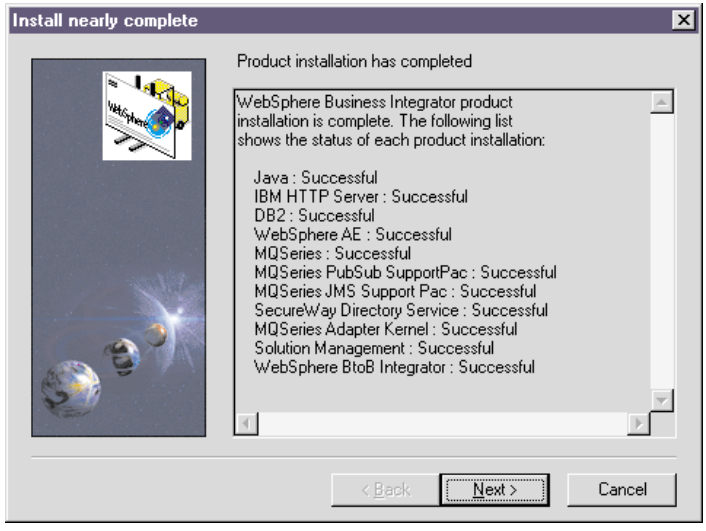


Figure 22. Report on the success or failure of the installations

16. Click **Next** to see a list of products that you manually install. You must install these products before you move on to the configuration steps. Using the information in the panel, fill in one of the tables in “Chapter 2. Making notes to help you through this book” on page 5 and use that information to guide you through the following chapters.

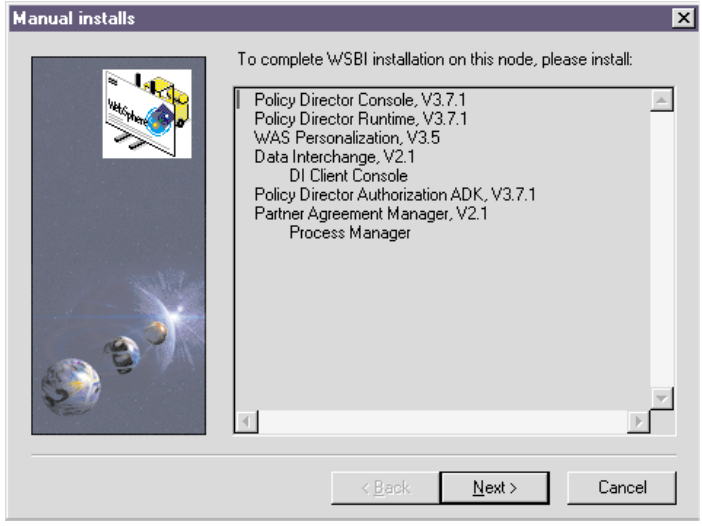


Figure 23. A list of the products to install manually

17. Click **Next** to see the final panel that confirms that the wrapper installation has now completed. Click **Finish** to restart the computer. Do not close the setup window in any other way, because the InstallShield process must be allowed to complete.

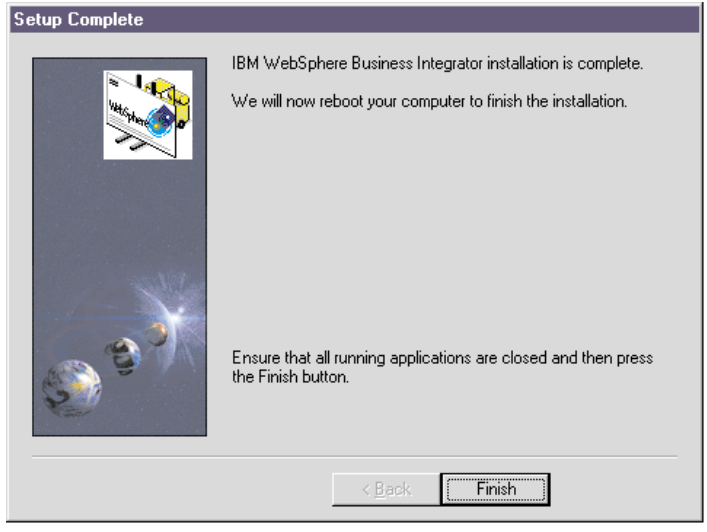


Figure 24. A completed installation

At the end of the installation, a message tells you that the machine will be rebooted after you have clicked **Finish**. If the machine does not reboot, reboot it manually by pressing `Control-Alt-Delete` and selecting **Shutdown**.

18. After rebooting, start the IBM WebSphere Administration Server service from the Services panel.

The next part of the installation

Now go to the next chapter to manually install the products listed in the panel illustrated in Figure 23 on page 39.

What to do if something goes wrong during installation

Here are some actions to consider if the installation goes wrong:

- Make sure you haven't missed anything in the Business Integrator README file and Release Notes. This has the most up-to-date information available for product installation and operation. See:

  `http://www.ibm.com/software/webservers/btobintegrator/support.html`

- If a product installation displays a ″Failed″ status on the Setup complete window, you are advised to review both the Business Integrator installation log and the product's own installation log, at:

  `<system drive>:\winnt\biz_wrapper.log`

  If a second (or subsequent) installation is started, the `biz_wrapper.log` file will be overwritten. You should retain the information contained in this file by making a backup copy before commencing a fresh installation. The information in the file might be of use to service personnel.

- The log names for the products are given in "Log files" on page 112. You can find the files in the directory `X:\winnt` where `X:` is the system drive. These files are intended primarily for use by IBM service personnel, but you might find additional information that helps you to identify the current problem. Check the return codes displayed on the summary panel (these are also written to the Business Integrator log file) against those listed in "Return codes" on page 111.

- When you have identified and corrected the error, you should run that product installation manually, using the appropriate Facilities CD, and, if necessary, relevant product install documentation. You must also run manual installs for any product blocked by the failure of another product. Options for the installs are contained in the `*.ins` files in the `Winnt` directory.

An alternative to running manual installs is to uninstall the machine, as described in “Chapter 11. Uninstalling Business Integrator” on page 107, and restart the wrapper installation. This procedure might be more efficient than running manual installs.

- During installation, you might see a dialog box appear with the message:

  ```
  BIZ1300E Another client machine is currently being installed. Please finish
  the existing installation before initiating any new installation.
  ```

  If this message appears when there is not another machine being installed, the topology repository is still locked following a client failure. To recover from this problem, delete the files `lockdb.dir` and `lockdb.pag` in the IBM HTTP `Server/logs` directory on the base machine.

Chapter 5. Manually installing products

Use this chapter
to manually install products on the base machine first. Once you have completed the installation and configuration of the base machine, use this chapter for the manual installs on the other machines in the topology. You must perform the wrapper install before the manual install. Complete the installation and configuration on each machine in turn. Read the next three paragraphs for more guidance about what you can install now.

This chapter tells you about the manual installation of products after the wrapper installation has completed. You do not have to install all the products listed in the following sections. Your version of the panel shown in Figure 23 on page 39 tells you which products you have to install, and you should have written down the details in "Chapter 2. Making notes to help you through this book" on page 5.

If your version of the panel shown in Figure 23 on page 39 tells you that you should install SecureWay Policy Director for the Trust and Access Manager Plus facility, install it before any other manual installs.

You do not install Partner Agreement Manager and Partner Agreement View, the Policy Director Console (you only prepare for it), or WebSphere Personalization at this point. For those installations, wait until "Chapter 8. Further installation and configuration" on page 63.

Installing SecureWay Policy Director

Installing Policy Director for the Trust and Access Manager Plus facility

1. Install the Policy Director DCE, using `Security_Services\setup.exe` on the Policy Director base CD. Select the ″Standard DCE Install″, not the ″Slim Client Install″, and install the following components:
   a. DCE Runtime Services
   b. DCE Cell Directory Server
   c. DCE Security Server

On the ″Cultural Conventions″ panel, select the check box for **'ENUS1252' = English in US ANSI CP** to ensure that DCE's codepage is the same as LDAP's codepage. If there's a mismatch, the LDAP Web-based Administration service will not work.

2. Do not reboot the system.
3. Install the SecureWay Policy Director Client (NetSEAT) using `Policy_Director\Client\setup.exe` on the Policy Director base CD. Choose:
   - DCE Runtime Only
   - Custom install

   Make sure that **Review/Modify NetSEAT Configuration** and **Enable Integrated Login** are not selected.
4. Do not reboot the system.
5. Install Policy Director Server using `Policy_Director\Server\setup.exe` on the Policy Director base CD. Install all of the following. You can do this by selecting **All**, which invokes the installs in turn.
   a. Policy Director Runtime (PDRTE)
   b. Policy Director Management Server (PDMgr)
   c. Policy Director Authorization Server (PDAcld)
   d. Policy Director Authorization ADK (PDAuthADK)
6. Now reboot the system.

Installing Policy Director for the BFM Application Server Plus facility

1. Install Policy Director Server by installing both:
   a. Policy Director Runtime (PDRTE)
   b. Policy Director Authorization ADK (PDAuthADK)

   using `Policy_Director\Server\setup.exe` on the Policy Director base CD.
2. Now reboot the system.

Installing Policy Director Run Time for the Product Console Launchpad facility

1. Install the Policy Director Runtime (PDRTE) component of Policy Director Server, using `Policy_Director\Server\setup.exe` on the Policy Director base CD.
2. Now reboot the system.

Installing WebSphere DataInterchange

Installing DataInterchange server for the EDI Gateway facility

When you install DataInterchange for the EDI Gateway facility, run `server\setup.exe` and follow the standard installation options on the

DataInterchange CD supplied with Business Integrator. (The creation, population, binding, and granting of the DB2 tables is not required, even though the DataInterchange installation documentation indicates that it is required.)

Installing the DataInterchange client for the EDI Gateway Console facility

When you install the DataInterchange client for the EDI Gateway Console facility, run `client\setup.exe` and select the ″Typical″ install option on the DataInterchange CD supplied with Business Integrator. When asked to reboot the machine after the MDAC install, reboot and then carry on the install after reboot.

Registering DataInterchange databases

After you have installed DataInterchange, you must register its databases as ODBC, as described in the DataInterchange documentation.

Chapter 6. Setting up SSL security

Use this chapter

- To set up SSL (Secure Sockets Layer) for the LDAP (Lightweight Directory Access Protocol) server on your base machine only.
- To set up HTTP SSL on the machine that contains the Interaction Manager facility.
- To set up SSL for the LDAP client on the other machines in the topology.
- To configure HTTP Server for SSL on the PAM facility

This chapter tells you how to set up security under these headings:

You will be asked for security information set up in this chapter when you are running the batch configuration described in "Chapter 7. Configuring the products after installation" on page 57. You cannot proceed to that step unless you have worked through this chapter.

At this point in the installation process, you can:

- Set up your own self-signed certificate now and continue through the rest of the process. Set up a certificate signed by a Trusted Certificate Authority (CA) later.
- Proceed with a certificate signed by a Trusted Certificate Authority, if you have one.

or

- Start the process to obtain a certificate signed by a Trusted Certificate Authority now, because the whole process can take up to two weeks. The *WebSphere Business Integrator Run Time* tells you how to set up a certificate signed by a Trusted Certificate Authority.

This chapter tells you how to create self-signed certificates and how they can be used by clients or servers for validation of SSL. Also included are details on how to configure SSL using certificates with the IBM HTTP Server.

Note: The information in this section has been extracted from the *LDAP Implementation Cookbook*, SG24–5110, to which you should refer if you need additional information.

Creating a self-signed certificate on the base machine

Make sure that you record key information in "Chapter 2. Making notes to help you through this book" on page 5.

For the base machine, follow the instructions below on creating a new key database and generating a self-signed certificate.

Creating a new key database

Use the `gsk4ikm.exe` utility to create a self-signed certificate to enable SSL sessions between clients and servers. `gsk4ikm.exe` is installed as part of the base machine installation, and is in the directory to which you have installed the wrapper install, in subdirectory `Gsk4\ibm\gsk4\bin`. Each client or server using this certificate must have the new root certificate imported, which may impose some administrative burden. Follow these steps, using `gsk4ikm`, to create a server key database (`.kdb file`):

1. Select **New...** from the Key Database File pull-down menu on the top of the main window.
2. On the dialog pop-up, select **CMS key database file** in the Key database type selection list and then type in the name and location of the key database file to be created. This file has an extension of `.kdb`, as, for example, in `ldap_key.kdb`. Then click **OK** to quit the dialog panel.
3. A new dialog pops up that requests your input for a password for the key database file, an optional expiration time, and whether or not the password is to be stashed to a file. Enter a password, an optional expiration time, and make sure that you check the check box next to **Stash the Password to a File?**; otherwise, the applications requiring access to the key database cannot read the file. Click on **OK** to close this dialog. The password is then encrypted and stored in a file with the same name as the key database file but with an extension of `.sth`.
4. Your database file is now created. You can now create a self-signed certificate.

Generating self-signed certificates

1. Create a self-signed certificate:
   a. Select **New Self-Signed Certificate...** from the Create pull-down menu in the main window. In the dialog window, fill in the following information:
      - Key label (a clear, descriptive label for the certificate)
      - Key version (normally X509 V3, unless you have reasons for other versions)

- Key size (512 or 1024, depending on security requirements and country version of `gsk4ikm.exe`)
- Common name
- Organization and other information to identify the owner of the certificate
- Validity period in days

b. Click **OK** to create the certificate. This creates a certificate and adds it to the list of Personal Certificates shown in the main window.

2. From the certificate just created above, you extract the root certificate that is necessary for other communication partners (clients and/or servers) to recognize the newly created certificate. Here are the steps for exporting the root certificate:
   a. Select the new certificate's entry in the Personal Certificate list and click on **Extract Certificate...** on the bottom right in the main window.
   b. Select **Base64-encoded ASCII data** from the Data type list and enter a file name (with a `.arm` extension) and a location (directory) for the new root certificate to be exported to. Then click **OK** to export the root certificate.
   c. You have now created a file that holds your own root certificate. This must be imported to all communication partners (when you have installed them) that will use SSL to connect to this machine.

Each LDAP server should have its own certificate. Sharing certificates across multiple LDAP servers is not recommended. By using different certificates and private keys for each server, your security exposure is minimized if a keyring file for one of the servers is compromised.

Setting up HTTP SSL for the Interaction Manager facility

Make sure that you record key information in "Chapter 2. Making notes to help you through this book" on page 5.

These instructions are for the machine that has the Interaction Manager facility installed. Do not set up HTTP SSL on the Trust and Access Manager Plus, or Web Proxy facility.

Use `gsk4ikm.exe` to create a new self-signed personal certificate, which is required to talk to the browser or Web Proxy:

1. Return the Trust and Access Manager machine, and copy the `.arm` file containing the self-signed certificate into the same location on the Interaction Manager machine. Find the location of the certificate on the TAM machine in the space provided for you to record it in "Chapter 2. Making notes to help you through this book" on page 5.

2. Log off from the current Windows NT session and log back in to the machine as HTTP. This account was set up during installation.

Creating a new key database

Use the gsk4ikm.exe utility to create a self-signed certificate to enable SSL sessions between clients and servers. gsk4ikm.exe is installed as part of the base machine installation, and is in the directory to which you have installed the wrapper install, in subdirectory Gsk4\ibm\gsk4\bin. Each client or server using this certificate must have the new root certificate imported, which may impose some administrative burden. Follow these steps, using gsk4ikm, to create a server key database (.kdb file):

1. Select **New...** from the Key Database File pull-down menu on the top of the main window.
2. On the dialog pop-up, select **CMS key database file** in the Key database type selection list and then type in the name and location of the key database file to be created. This file has an extension of .kdb, as, for example, in ldap_key.kdb. Then click **OK** to quit the dialog panel.
3. A new dialog pops up that requests your input for a password for the key database file, an optional expiration time, and whether or not the password is to be stashed to a file. Enter a password, an optional expiration time, and make sure that you check the check box next to **Stash the Password to a File?**; otherwise, the applications requiring access to the key database cannot read the file. Click on **OK** to close this dialog. The password is then encrypted and stored in a file with the same name as the key database file but with an extension of .sth.
4. Your database file is now created. You can now create a self-signed certificate.

Importing certificates into a key database

The SSL protocol involves the exchange of certificates. Therefore for a client machine to recognize and validate the server, the server's certificate should be imported into a client's key database beforehand during a manual configuration step. Thereafter when initiating an SSL handshake the certificate sent by the server can be validated.

Use these steps to import the new root certificate into other key databases, using gsk4ikm.exe. As discussed, this is required when configuring SSL to validate a certificate sent by a server or client. Follow the steps below to import a certificate:

1. Make sure that the certificate in the format of a .arm file is accessible from this machine – for example, on a diskette.
2. Invoke gsk4ikm.exe on the receiving machine.
3. If you haven't already done so, create a key database file.

4. In the Key Data Contents part of the panel, select **Signer Certificates** and click **Add....**
5. Select **Base64–encoded ASCII data** from the Data Type list and type the certificate file name and location into the appropriate fields. Click **OK** to import the certificate.
6. On the next dialog, supply a label for this certificate and click on OK. (This label is used only to reference certificates, and does not have to match other names or labels.) Go through these steps on each machine that will use this certificate during communication with the machine on which the certificate was created.

Generating self-signed certificates

1. Create a self-signed certificate:
   a. Select **New Self-Signed Certificate...** from the Create pull-down menu in the main window. In the dialog window, fill in the following information:
      - Key label (a clear, descriptive label for the certificate)
      - Key version (normally X509 V3, unless you have reasons for other versions)
      - Key size (512 or 1024, depending on security requirements and country version of `gsk4ikm.exe`)
      - Common name
      - Organization and other information to identify the owner of the certificate
      - Validity period in days

   b. Click **OK** to create the certificate. This creates a certificate and adds it to the list of Personal Certificates shown in the main window.
2. From the certificate just created above, you need to extract the root certificate that is necessary for other communication partners (clients and/or servers) to recognize the newly created certificate. Here are the steps for exporting the root certificate:
   a. Select the new certificate's entry in the Personal Certificate list and click on **Export Key...** on the right in the main window
   b. Select ***.P12** file from the Data type list and enter a file name and a location (directory) for the export key to be stored. Then click **OK** to export key. This key will be used later by the WebProxy machine.
3. Ensure this newly generated self-signed certificate has an asterisk at the start of the line when it has been created, indicating that it is the default certificate.
4. Close `gsk4ikm.exe`.
5. Log off from the current Windows NT session and log back in to the account from which you are going to run the configuration.

Setting up SSL on the other machines

Machines other than the base machine or IM machine where SSL is a requirement should have key databases and certificates imported for validation. Follow the instructions below on creating a new key database and importing certificates into the database.

Creating a new key database

Use the `gsk4ikm.exe` utility to create a self-signed certificate to enable SSL sessions between clients and servers. `gsk4ikm.exe` is installed as part of the base machine installation, and is in the directory to which you have installed the wrapper install, in subdirectory `Gsk4\ibm\gsk4\bin`. Each client or server using this certificate must have the new root certificate imported, which may impose some administrative burden. Follow these steps, using `gsk4ikm`, to create a server key database (`.kdb file`):

1. Select **New...** from the Key Database File pull-down menu on the top of the main window.
2. On the dialog pop-up, select **CMS key database file** in the Key database type selection list and then type in the name and location of the key database file to be created. This file has an extension of `.kdb`, as, for example, in `ldap_key.kdb`. Then click **OK** to quit the dialog panel.
3. A new dialog pops up that requests your input for a password for the key database file, an optional expiration time, and whether or not the password is to be stashed to a file. Enter a password, an optional expiration time, and make sure that you check the check box next to **Stash the Password to a File?**; otherwise, the applications requiring access to the key database cannot read the file. Click on **OK** to close this dialog. The password is then encrypted and stored in a file with the same name as the key database file but with an extension of `.sth`.
4. Your database file is now created. You can now create a self-signed certificate.

Importing certificates into a key database

The SSL protocol involves the exchange of certificates. Therefore for a client machine to recognize and validate the server, the server's certificate should be imported into a client's key database beforehand during a manual configuration step. Thereafter when initiating an SSL handshake the certificate sent by the server can be validated.

Use these steps to import the new root certificate into other key databases, using `gsk4ikm.exe`. As discussed, this is required when configuring SSL to validate a certificate sent by a server or client. Follow the steps below to import a certificate:

1. Make sure that the certificate in the format of a .arm file is accessible from this machine – for example, on a diskette.

2. Invoke `gsk4ikm.exe` on the receiving machine.
3. If you haven't already done so, create a key database file.
4. In the Key Data Contents part of the panel, select **Signer Certificates** and click **Add....**
5. Select **Base64–encoded ASCII data** from the Data Type list and type the certificate file name and location into the appropriate fields. Click **OK** to import the certificate.
6. On the next dialog, supply a label for this certificate and click on OK. (This label is used only to reference certificates, and does not have to match other names or labels.) Go through these steps on each machine that will use this certificate during communication with the machine on which the certificate was created.

Configuring HTTP Server for SSL on the PAM facility

The following instructions are included for setting up SSL manually.

Please note that these instructions do not work for Topology A, on which security options are not installed by default.

1. Follow the instructions described above to set up a new Key Database and generate a self-signed certificate.
2. Start the IBM HTTP Administration Service.
3. From the browser type `http://localhost`. This will bring up the HTTP Server main screen. Click on **Configure server**. Enter the password used when installing WebSphere/HTTP Server (normally the Windows logon ID and password).
4. Set up the security module. Select:
   - **Basic Settings**.
   - **Module Sequence** (Scope: GLOBAL).
   - **Add**.
   - **Select a module to add** and open the drop-down list. Go to the bottom of the list and select **ibm_ssl** from the list. The Module DLL will be placed to the right.
   - **Apply**.
   - **Close**.
   - **Submit**.
5. Set up the secure host IP and additional port for secure server. Select:
   - **Basic Settings**.
   - **Advanced Properties** (Scope: GLOBAL).
   - **Add** button for the ″Specify additional ports and IP addresses″ field - leave the IP address field empty and enter 443 in the port field.

- **Apply**.
- **Close**.
- **Submit**.

6. Set keyfile and SSL timeout values for secure server.
   - Select **Security**.
   - Select **Server Security** (Scope: GLOBAL).
   - Select the radio button **No** for **Enable SSL** to disable SSL for Global scope.
   - Enter the path and keyfile filename. (This is the file created with `ikeyman`.)
   - Enter a Timeout value for SSL Version 2 session IDs. (100 seconds.)
   - Enter a Timeout value for SSL Version 3 session IDs. (1000 seconds.)
   - Select **Submit**.
7. Set up the virtual host structure for secure server.
   - Select **Configuration Structure**.
   - Select **Create Scope** (Scope: GLOBAL).
   - Select **VirtualHost** in the ″Select a valid scope to insert within the scope selected in the right panel″ field.
   - Enter the virtual host IP address or fully qualified domain name.
   - Enter the virtual host port (443).
   - Leave server name blank.
   - Leave alternate name(s) for host blank.
   - Select **Submit**.
8. Set up the virtual host document root for secure server.
   - **Basic Settings**.
   - Select **Core Settings**. (Scope: <virtual host you are working with>).
   - Enter the server name as a fully qualified domain name.
   - Enter the document root directory name.
   - Select **Submit**.
9. Enable SSL and select the mode of Client Authorization. Select:
   - Select **Security**.
   - **Host Authorization**. (Scope: VirtualHost) `<host ip addr:443>`
   - Select radio button **Yes** for **Enable SSL** to enable SSL for Virtual Secure Host.
   - For **Mode of client authorization**, select radio button **None**.
   - Select **Submit**.
10. Repeat steps 7 - 9 and add `localhost:443`.
11. Restart the HTTP Server.

Checking that SSL has been set up correctly

After configuration has been run, using “Chapter 7. Configuring the products after installation” on page 57, start a web browser and point it at `https://<hostname of interaction manager>`. If SSL has been configured correctly, you will be informed that a certificate is required. Click on **View**, and check that the certificate presented is the same as the one you created earlier.

If you have not set up HTTP SSL for the Interaction Manager facility correctly, then, on pointing the browser to http://.., an error page is displayed and the error.log will have the entry:

```
[error] mod_ibm_ssl: SSL Handshake Failed, No certificate.
```

If this is not performed in the HTTP login account, `error.log` will have the entry:

```
[crit] mod_ibm_ssl: GSK could not initialize, Invalid password for keyfile.
```

because of the Windows NT security applied to the `key.kdb` file.

The following will be set up in the `httpd.conf` file by the configuration program to enable SSL:

```
#SSL Support
LoadModule ibm_ssl_module modules/IBMModuleSSL128.dll
Listen 443
<VirtualHost: hostname 443>
ServerName hostname
DocumentRoot <docroot>
SSLEnable
SSLClientAuth none
</VirtualHost>

Keyfile <kdb file>

SSLV2 Timeout 100
SSLV3 Timeout 1000
SSLDisable
```

Chapter 7. Configuring the products after installation

Use this chapter

to help you run the batch configuration file to configure the base machine and subsequently each machine in the topology. Not all the products mentioned in this chapter will necessarily be present on a particular machine.

This chapter also tells you about the e-fixes to be applied before running the batch configuration file.

You must configure the products installed up to this point before moving on to "Chapter 8. Further installation and configuration" on page 63.

This chapter tells you only when you have to intervene in the configuration process and does not describe the configuration process itself. If you want to understand what happens during configuration in more detail, see "Appendix B. Configuration details" on page 117. Most users will not require the level of detail provided in the appendix.

Before you run the batch configuration file

Before you run the batch configuration file, check the following:

1. Before you configure a machine with any of these facilities – BFMWAS Plus, Integrated Console Plus, or WebProxy – you must first import a Policy Director certificate from the machine that has the installed and configured Trust and Access Manager Plus facility. From the `<Policy Director>\ivmgrd\keytabs` folder on the Trust and Access Manager Plus facility, copy file `pdcacert.b64`. Import the file into the `<Policy Director>\keytabs` folder on the facilities mentioned.

   If you reconfigure the TAM machine, for example if you apply the CSD, and you respond ″Y″ to the question ″Do you want to reconfigure LDAP?″ you must copy again

   `<wsbi_install>\Tivoli\Policy Director\ivmgrd\keytabs\pdcacert.b64`

   from the TAM Plus machine to the `<wsbi_install>\Tivoli\Policy Director\keytabs` directory on the appropriate machine. On that machine, unconfigure the Policy Director Run Time Environment and reconfigure it using this file before running the batch configuration file.

2. Use the console icon on the control panel to set the Screen Buffer Size height to ≥4096. This size will enable you to review any errors and check for the success of the configuration.
3. Note that the user name db2admin is used as the administrative user name for all DB2 database accesses – for example, for MQSeries Integrator, LDAP, and WebSphere Application Server. The password, already used during installation, is set to your choice. You must know the current password because you'll be prompted for it during the preparation of PAM and PAV.
4. Review the following sections for any environment variables that must be set so that you're ready when you run the batch configuration file.

Applying e-fixes and CSDs before you run the batch configuration file

You must apply the following fixes before you run the batch configuration file. These e-fixes are on Facilities CD 1 in the efixes directory. When you insert the CD, cancel the autoinstall option so that you can access the directory.

On all machines

On all machines, apply these fixes.

JMS e-fix

Apply the **JMS** e-fix. Copy the \efixes\JMS\mqjms_xafix.jar file into the Program Files\MQSeries\Java\lib directory on all the machines in your topology, and add this JAR file to the system CLASSPATH.

MQAK e-fix

Apply the **MQAK** e-fix. First, change memo.ptf in the \efixes\Mqak directory from read-only by changing the read-only attribute on the file properties panel. Then follow the instructions in the README file included in \efixes\Mqak.

WebSphere e-fix

Check that **WebSphere** has installed properly. On each machine on which the wrapper install has installed WebSphere Application Server, an e-fix to upgrade the WebSphere Java Developer's Kit (JDK) has been included. You must check that this JDK e-fix has been correctly applied.

Using Windows Explorer, locate the JDK directory at

<installation drive>\WebSphere\jdk

and verify that the directory tree contains files.

If the directory is empty, copy the complete tree from the

\WebSphere Fix Pack 3b\jdk

directory on Facilities CD 3 to

`<installation drive>\WebSphere\jdk`

Business Integrator CSDs

Apply the **Business Integrator CSDs**, located at:

`http://www.ibm.com/software/webservers/btobintegrator/`

Trust and Access Manager Plus facility machine

On the machine that contains the Trust and Access Manager Plus facility, apply this e-fix.

MQSeries e-fix

Apply the **MQSeries** e-fix from `\efixes\MQSeries\p57729`.

You have already installed DCE and Policy Director. Now, before configuration, rename the original versions of the four updated programs (found in the MQSeries `bin` directory, (for example, `\Program files\MQSeries\bin`), and replace them with the new versions from the e-fix.

MQSeries will start up when you reboot after all installation and configuration.

Message Broker facility machine

On the machine that contains the Broker facility, apply this CSD.

MQSeries Integrator CSD

On the machine that contains the Broker facility, apply the **MQSeries Integrator** CSD, following the instructions in the README file included in `\efixes\MQSeries Integrator`.

The CSD checks for a level of DB2 that has been superseded by the one installed by Business Integrator. This check might raise a registry error, `BIP8640W`, which you should ignore.

Running the batch configuration file

To start the batch configuration file, go to an NT prompt and change to the `<install directory>\config` directory and enter `Configure` on the command line. The file recognizes the facilities and products that have been installed on the machine, and runs configuration scripts accordingly.

If you stop the configuration and then restart it, you might find that the repository is locked. You'll see a series of these messages, `!! Topology Error – Locked exception from configmain.bat`. To recover from this problem, delete the files `lockdb.dir` and `lockdb.pag` in the IBM HTTP `Server/logs` directory on the base machine and restart the configuration.

MQSeries for Windows NT and MQSeries Publish/Subscribe

The configuration batch file creates an MQSeries log directory. You are prompted for the location of the log directory. The default log directory location is `c:\mqm\log`. Accept this default unless your `c` drive lacks space or you prefer to use a different physical drive for performance reasons.

MQSeries Integrator

You provide the user name and password. Record them in "Chapter 2. Making notes to help you through this book" on page 5.

If you rerun the batch configuration file, you'll probably see System Error 1379 messages. These error message occur because the file is trying to create MQSeries Integrator user IDs that already exist. You can ignore these messages.

MQSeries WorkFlow

A DB2–WorkFlow instance is created for all topologies, even though it is not required by entry-level topologies. Its presence has no effect on the correct working of those topologies.

SecureWay Directory (LDAP)

You will be prompted to set the password for:

- The Administration user ID `cn=root`
- The Business Integrator user `cn=WSBIAdmin,o=ePICUsers,o=epic`

SSL

You will be asked to provide:

- The location of the key database file and the name of the file
- The LDAP user ID and password
- The key database password
- The key label

Policy Director

When the configuration of Trust and Access Manager Plus is started, you will be asked to provide:

- The password of the LDAP server, if the LDAP password has not been defined previously in the LDAP configuration
- A new username and password for DCE
- A new password for `sec_master`

If you rerun the batch configuration file, you might receive a warning message:

```
This web server already supports directory administration.
Are you sure you want to update the current configuration
with new directory administration settings?
Enter 'Y' if to continue configuration , or
Enter 'N' if to exit without any changes.
```

If you choose 'Y', note that you will overwrite any changes you have made to your Policy Director settings since the last batch configuration run. If you choose 'N', the settings will be unchanged and the rest of configuration will continue.

PAM and PAV

The batch file prompts you for the password for the DB2 administrative user ID db2admin. The batch file completes the pre-installation setup of PAM and PAV. Before it completes, the batch file will issue a message to remind you that next you will manually install PAM and, if required, PAV.

If you rerun the batch configuration file, you'll be asked whether you want to create a new database for PAM or to use the existing database. Choose the option to create a new database with a new name. When the configuration has finished, you may safely drop this new database, because it is not required further.

When configuration is complete, you see a large message CONFIG ENDED. If configuration fails, you see a large message CONFIG FAILED. If your configuration run comes to an end without a message, check back for errors.

Chapter 8. Further installation and configuration

Use this chapter

to complete the installation and configuration of some of the machines in your topology after you've run the configuration batch file. If you don't require any of these products on this machine, skip this chapter. None of these products is installed on the base machine.

Make sure you read the ″Notes″ on this page, so that you do things in the right order.

When you have reached the final machine in your topology, include the final step, "Rebooting when all installation and configuration is complete" on page 83

You complete the installation and configuration of some of the machines in your topology as a manual process. This chapter describes the steps in the process in:

Notes:

1. You complete the MQSeries cluster configuration on the TAM/TAMPlus machine at any time after the broker has been configured.

   Open a command window on that machine and change to the `x:\wsbiinstalldirectory\config`, and run `repossetup.bat`.

2. You must install and configure PAM (on the PAM facility) and the PAM Process Manager (on the Product Console Launchpad machine) in a specific sequence, because the manual install of the PAM Process Manager depends on the PAM installation and the PAM configuration depends on the Product Console Launchpad facility:
   a. Install PAM, but do not manually configure it, on the PAM facility machine.
   b. Install and automatically configure the Product Console Launchpad facility, including the manual install of the PAM Process Manager.
   c. Then manually configure PAM using both the PAM facility machine and the Product Console Launchpad machine.

Installing and configuring PAM and PAV for the PAM and PAV facilities

After you have prepared for the installation of PAM and PAV by running the configuration batch file, you can now manually install and configure PAM and PAV. For further information, consult the PAM installation documentation and, in particular, the readme.

Use the PAM and PAV CDs provided with Business Integrator, and take a note of the key, which is on the CD label, before you insert the CD.

Installing PAM

1. On the PAM CD, run `setup.bat`. This setup might take some time.
2. The Installshield Wizard now runs **behind** any active windows.
3. On the ″Welcome″ Panel, click **Next**.
4. Choose the installation type as ″New PAM Installation″. If you want to upgrade your version of PAM, see the PAM installation and configuration documentation.
5. Click **Next**.
6. After InstallShield checks that the prerequisites are present, click **Next**.
7. Choose to install all 3 PAM components.
8. Click **Next**.
9. Enter your license key.
10. Click **Next**.
11. Enter your PAM Partner Name. This is what your partners will refer to you as.
12. Enter your PAM Partner ID. This must be unique amongst your partners. A DUNS number is ideal.
13. Click **Next**.
14. Leave all ports at their default values.
15. Click **Next**.

16. Select **DB2** as the database to be used.
17. Click **Next**.
18. Enter `WSBIPAM` for the Database name, unless you were prompted for another name, which you should enter.
19. Click **Next**.
20. Enter the data modification username `db2admin` for the PAM Process Server database
21. Enter the data modification password for the PAM Process Server database
22. Click **Next**.
23. A schema pop-up box appears. Press **Yes**.
24. Choose and enter a password for the PAM administrator login ID. The login ID is usually ″admin″.
25. Click **Next**.
26. Select **IBM HTTP Server with WebSphere** as the web server that PAM will use.
27. Click **Next**.
28. Leave the HTTP Hostname and port as the default, unless there is a known conflict. If you have a security certificate, and wish to enable SSL, fill in the appropriate details, and make sure that the ″Enable SSL″ box is checked.
29. If you do not have a security certificate, or don’t wish to enable SSL, make sure that the box is unchecked.
30. Click **Next**.
31. Enter the details of your SMTP Server and a username that PAM will use to send notifications.
32. Click **Next**.
33. Select the check box if you wish to enable polling of PAM system resource status, and then enter the polling rate. Otherwise leave the box unchecked.
34. Select the check box if you want to enable the PAM SNMP Agent, and then enter the SNMP Trap receivers. Otherwise leave the box unchecked.
35. Click **Next**.
36. Select the checkbox for **Use LDAP for authorizing users**. Do not select **Use LDAP for storing partner information**.
37. Enter the machine name of the LDAP provider. The TAM or TAM Plus facility is installed on this machine.
38. Enter the LDAP User Distinguished Name and Password. For example: `cn=WSBIAdmin,o=epicusers,o=epic`.
39. Click **Next**.

40. Specify that PAM Process Server and PAM Adapter Server run as services. Enter the password for the user specified in the ″Windows User Name″ field. By default, this is the user you are logged in as.
41. Click **Next**.
42. Select the folder to which you want to install PAM. You must type in the folder name explicitly; if you try to browse and select the folder name, the system might freeze.
43. Click **Next**.
44. Review the information, and then click **Install Now**.
45. When the install has finished, click **Exit**.

Now that you have installed PAM on this machine, go back to “Chapter 4. Installing the facilities on the machines in your topology” on page 29 to install and configure the Product Console facility on its machine. Then you can use the following section,“Installing the PAM Process Manager as part of the Product Console Launchpad facility”, to install the PAM Process Manager on the Product Console facility.

Installing the PAM Process Manager as part of the Product Console Launchpad facility

1. Run the PAM setup program.
2. An InstallShield wizard will appear. Click **Next**.
3. Read the terms of the license. If you accept them, make sure the appropriate checkbox is selected and click **Next**.
4. Choose ″New Partner Agreement Manager Installation″.
5. Click **Next**.
6. The wizard will check for the necessary prerequisites for the installation. After this has completed, click **Next**.
7. Make sure that only the Process Manager is selected for installation.
8. Click **Next**.
9. Enter the PAM Partner Name that you entered for the main PAM install.
10. Enter the PAM Partner ID number that you entered for the main PAM install.
11. Click **Next**.
12. Change the Host Name to reflect the host that the PAM Process Server is installed on.
13. Leave all ports at their default values.
14. Click **Next**.
15. Choose the destination folder for the installation.
16. Click **Next**.

Configuring PAM

To manually configure PAM you use both the PAM machine and the Product Console machine:

1. On the PAM machine, make sure the WebSphere Application Server service, ″IBM WS AdminServer″, is started.
2. On the Product Console machine, bring up the Product Console launchpad, from `Start/Programs/WebSphere Business Integrator/IBM Solution Management/Product Console Launchpad`. Expand the topology tree to locate ″Partner Agreement Manager″. Right click on **WebSphere AE** and click on **WebSphere Admin Console**. Using the WebSphere Administration Console, from `Console/Tasks/Create a Virtual Host` enter the PAM machine hostname and click **Next**. This creates a new virtual host for the PAM machine.

   Add as aliases to this virtual host:

   - The hostname of the PAM machine (note that this is the numeric value)
   - The fully qualified domain name of the PAM machine; for example, `PAM_machine.domain.com`

   If you are not on topology A, remove the aliases and IP address of the PAM machine from the virtual host ″default_host″, by clicking on **default host/advanced** tab.
3. On the PAM machine, run the `pamxml.bat` file, which is in the `config` directory, with these parameters:
   - PARTNER id of your PAM installation
   - Password of the administrative user that will run PAM
4. On the Product Console machine, use the WebSphere Administration console to restart the PamAppServer. To reveal the PamAppServer, you might have to refresh the WebSphere Administration console.
5. On the Product Console machine or on the PAM machine, start the PAM Process Manager. Select the user `pamadmin` from `Administration->Users` and open it. In the `Access` tab, modify the following properties:

   ```
   Business Objects:  Edit
   Processes:         Edit
   Auditor:           Edit
   ```
6. Close the WebSphere Administrative Console on the Product Console machine and then reboot the PAM machine now that the PamAppServer has been started.

Configuring the Gateway Adapter

You need the Gateway Adapter only if PAM is in the topology.

On the product Console machine:

1. Start the WebSphere Administration Console.

2. Ensure that the pamAppServer on the PAM machine is started.

On the PAM machine:

1. Now that PAM has been installed and configured using WebSphere, access the PAM Process Manager using the task bar from Start/Programs/IBM WebSphere Business Integrator/Partner Agreement Manager/Process Manager. This program will attempt a connection to the PAM Process Server started by WebSphere Application Server.
2. Provide your user ID and password to allow you to log on to the Process Manager. When these are successfully verified, you are granted access to the application.
3. Make sure the Adapter service (PAMAS) is running . Now use the import gateway adapter batch file to import the default BPI Adapter definitions into the PAM Adapter server by going into the <wsbi install directory>\config directory under your Business Integrator installation and running impgwadp.bat.
4. Start the Adapter Manager from Start/Programs/IBM WebSphere Business Integrator/Partner Agreement Manager/Adapter Manager from the task bar.
5. The Adapter Manager console will display a list of Adapter Instances. Included in this list will be ″BPI Adapter Type 1 Default Instance″.

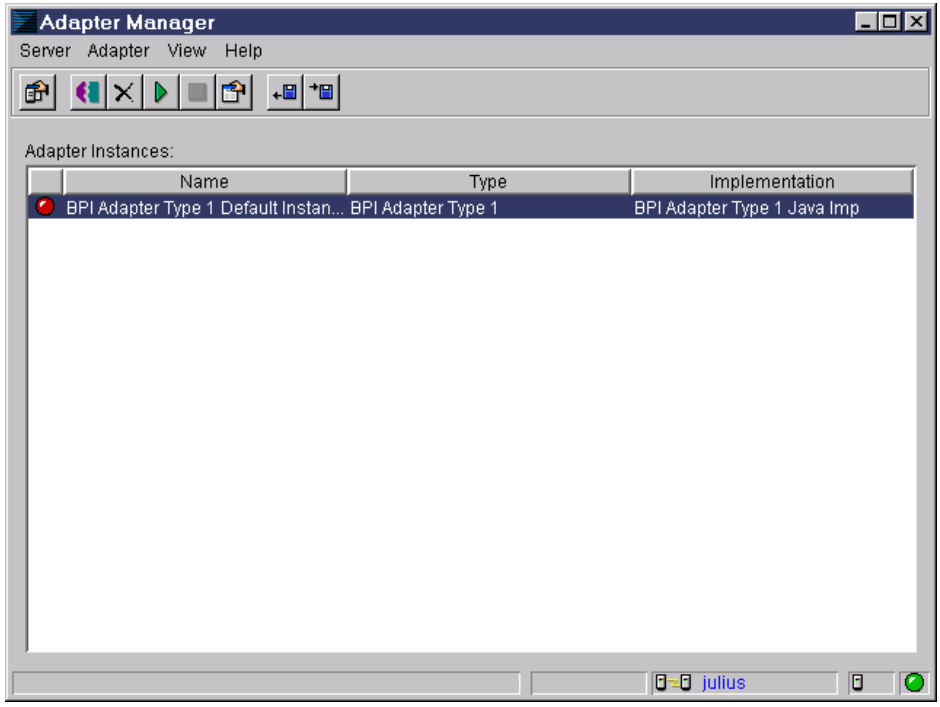


Figure 25. List of adapter instances

6. The `impgwadp.bat` file will create two `ldif` files for configuring MQAK. The two files are for the different receive mechanisms available in MQAK, namely JMS and MQPP. You choose which one to use.
7. Check for the existence of the file

   `<wsbi install directory>\config\BPI_Adapter_Applications_QMUPDATE.ldif`

   (for MQPP) and

   `<wsbi install directory>\config\BPI_Adapter_Applications_JMS_QMUPDATE.ldif`

   (for JMS). These have been created by the `impgwadp.bat` file, and include correct MQSeries Queue Manager names based on your `hostname.clusterName`.
8. To import the files into LDAP, copy the correct `.ldif` file to the TAM machine (where the LDAP server is located), open an NT command window, and enter one of the following commands:
   - For MQPP: `ldif2db -i BPI_Adapter_Applications_QMUPDATE.ldif`
   - For JMS: `ldif2db -i BPI_Adapter_Applications_JMS_QMUPDATE.ldif`

Installing and configuring PAV

You have already installed PAM , as described in the previous section. Now, on the PAM machine:

1. Locate the following file, <PAM Installation>\Alliance\Web\Web-Inf\web.xml and make a copy of it.
2. Open web.xml in a text editor (for example, Notepad) and remove the following section:

```
<!DOCTYPE web-app
    PUBLIC "-//Sun Microsystems, Inc.//DTD Web Application 2.2//EN"
    "http://java.sun.com/j2ee/dtds/web-app_2.2.dtd">;
```

3. Save the altered file as web.xml.
4. From the PAV CD, go to Partner_Agreement_View\PAMSide and run the setup.bat file. This setup might take some time.
5. An InstallShield wizard will then appear, with a welcome screen displayed. Click **Next**.
6. Review the terms of the license. If you accept the terms of the license, make sure that the appropriate radio button is selected.
7. Click**Next**.
8. Enter the Root directory of your PAM installation.
9. Enter the Partner ID of your PAM installation.
10. Click **Next**.
11. After PAV has checked for the necessary prerequisites, click **Next**.
12. Enter the Channel Instance. The default value is recommended.
13. Enter the Channel ID. The default value is recommended.
14. Click **Next**.
15. Choose a destination folder for this part of PAV to be installed in. Accept the default, which is where you have installed PAM.
16. Click **Next**.
17. When prompted whether or not to overwrite existing files, click **Yes to All**.
18. Once the installation is finished, click **Finish**.
19. Reboot the PAV machine and ensure that after it restarts you close and reopen the WebSphere Administrative Console on the Product Console machine and that the pamAppServer has been started.
20. Go to the config directory, <WSBI Installation>\config. Run the pav_channel_command.bat file.
21. From the PAV CD, go to Partner_Agreement_View\WebServerSide and run the setup.bat file.
22. An InstallShield wizard will then appear, with a welcome screen displayed. Click **Next**.

23. Review the terms of the license. If you accept the terms of the license, make sure that the appropriate radio button is selected. Click **Next**.
24. Choose to use ″Other Webserver″, rather than ″Tomcat″.
25. Click **Next**.
26. You will be reminded that you will have to manually configure this installation to integrate with your WebServer. Click **OK**.
27. Choose a destination folder for this part of PAV to be installed in – for example, `<WebSphere Install Directory>\Pav` . You will be required to enter this folder at a later stage.
28. Choose a virtual root for PAV to run under WebSphere.
29. After PAV has checked for the necessary prerequisites, click **Next**.
30. Enter the Channel ID.
31. Enter the Channel Name.
32. Click **Next**.
33. Enter the Partner ID of your PAM installation.
34. Click **Next**.
35. Enter the fully qualified hostname of the PAM machine when prompted for the Webserver hostname.
36. Change the port number, if necessary.
37. Once the installation is finished, click **Finish**.
38. Go to the `config` directory, <WSBI Installation>`\config` . Run the `pav_ws_command.bat` file, with the following parameters:
    - PAV directory, which you entered in step 27.
    - Virtual root, which you entered in step 28, without any leading or trailing slashes.
    - Channel ID.
    - PAV Partner ID. An example value is 777, which is used in the sample processes in step 44. Use this value when going through step 42 to create the channel profiles and the partner.
39. Stop the WebSphere Administrative Console on the Product Console machine and on the PAM machine stop the HTTP and WebSphere services.
40. Find `httpd.conf` in directory <IBM HTTP Server Installation>`\conf`. Make a copy of this file.
41. About 3/4 of the way down the file is a section about aliases. Add in the following line after the alias that is already present:

    ```
    Alias <Virtual Root> "<PAV Install>/webapps/<Virtual Root>
    ```

    If all the defaults at install time were accepted, then the line should be:

    ```
    Alias /WebSphere/PAV/ "C:/WebSphere/PAV/webapps/WebSphere/PAV/"
    ```

42. Follow the instructions in the *Partner Agreement View User's Guide*, available on the documentation CD, on setting channel profiles and adding a Partner Agreement View Partner. In addition to the information in the manual, note that the outbound url of the ″Partner Agreement View 1001″ should be:

    ```
    http://<pam machine name>:80/<Virtual root>/servlet/AppChannelPOBox
    ```

    or, if you are using SSL:

    ```
    https://<pam machine name>:443/<Virtual root>/servlet/AppChannelPOBox
    ```

    The partner that you add should use the PAV Partner ID that you entered as a parameter for the `pav_ws_command.bat` file in step 38.

    To run the sample processes, you must also open the ″Passwords″ folder under the ″Administration″ folder in Partner Agreement Manager, and add the following user name and password:

    Login: AppChannelInboundPartner777
    Password: partner_password

43. Restart the services you stopped in step 39.
44. To test your PAM / PAV installation and configuration, follow the instructions about ″Sample Public Processes″ in the *Partner Agreement View User's Guide*.

Setting up WebSphere Application Server Personalization for the Interaction Manager facility

This section applies to the enterprise edition only.

Installing WebSphere Application Server Personalization for the Interaction Manager facility

You manually install WebSphere Application Server Personalization because it can be installed only after WebSphere Application Server has been installed, configured, and is up and running with the relevant DB2 instance on it.

If you cannot start WebSphere Application Server, modify the communication properties for the DB2 instance on the machine that has the TAM facility:

1. Start the DB2 Control Center on the machine that has the TAM facility.
2. Select the DB2 instance, right click, and select **Setup communications** from the pop-up menu.
3. Disable the NetBIOS, APPC, and IPX/SPX protocols.
4. Reboot the TAM machine.

To install WebSphere Application Server Personalization:

1. Before installing WebSphere Personalization, use the WebSphere Administration console on the Product Console machine to stop the WSBIDeploy application on the Interaction Manager machine. Copy the WSBIDeploy application's command line arguments to a temporary file.
2. Run `setup.exe` from the `nt` folder under WebSphere Personalization on the WebSphere Personalization CD. Pick the option **Use existing application server** when asked whether you want to create a new server on which to install Personalization or to pick an existing one. Once you've made your choice, Personalization install attempts to locate configured servers and display the resulting list. You then pick the server called **WSBIDeploy** from that list, and continue with the install.
3. After installing WebSphere Personalization, install the e-fix from the `Facilities CD1\efixes\WebSphere Personalization\nt` directory. Use the README on this install, and note that you must copy the e-fix directory from the CD to a suitable location, (for example, the `Temp` directory) and edit `EjbRedloy.bat` (using Wordpad or any other editor that can interpret Unix style line-end characters) replacing the parameters as follows:
   - `primaryNodeName = your machine name (without the domain)`
   - `nodeName = your machine name (without the domain)`
   - `server = WSBIDeploy`
   - `root = the install directory of WebSphere`

   Now run `EjbReploy.bat`.
4. Restore the command line arguments to the WSBIDeploy application, making sure to apply the change. Start the WSBIDeploy application.

Configuring WebSphere Application Server Personalization for the Interaction Manager facility

1. Using the WebSphere Application Server Administration Console, browse the WSBIDeploy server configuration and delete the `-classpath` entry in the command line argument string. Apply the change, restart the WSBIDeploy server.
2. At an NT command prompt, change to the `\WebSphere\Personalization\publishToProduction` directory. Run `pznload <hostname> <was_root> -verbose -logfile pznload.out -rulelistfile IMRulesToLoad.txt -reslistfile IMResourcesToLoad.txt`
3. Browse the log file to confirm that the import and configuration ran with no errors. (The log file may be any valid filename that does not conflict with installed product file names.)

See "Configuring WebSphere security for Interaction Manager" on page 76, which addresses both editions of Interaction Manager.

The URL to use for logging onto the Interaction Manager desktop is `https://WebSealhostname`. This will display the custom logon screen described in "Configuring WebSEAL" on page 98.

Setting up MQSeries channel security

The MCA of the `SYSTEM.DEF.SVRCONN` on MQSeries is initially set to "Rogue-User!!". Any channels that are created using the `SYSTEM.DEF.SVRCONN` as their base definition will inherit this value. "Rogue-User!!" is a fictitious user ID that will not work. You must either delete this user ID from the MCA value or change the MCA value to be a valid user that is in the MQM group.

A symptom of the "Rogue-User!!" setting is that the MQSeries Integrator Control Center cannot connect to the configuration manager because the `SYSTEM.BKR.CONFIG` channel has inherited the rogue user ID as its MCA. You must change or remove this value.

For more information about MQSeries security, see the `MQSeries Planning Guide`, GC33–1349.

Configuring Solution Management security

You can enable Solution Management security to prevent unauthorized users from deploying solutions and managing the base products. The procedure below describes how to prevent users who are not members of the Administrators group from running the Platform Console.

1. Start Windows NT Explorer, and navigate to the directory:
   `\wsbiinstalldirectory\lib\java\com\ibm\btobi\topology\explorer`
2. Highlight the file `topexplorer.class` and select the **Properties** option from the "File" menu.
3. When the "Properties" panel appears, click on the **Security** tab.
4. On the "Security" page, click on the **Permissions** button to display the "File Permissions" panel. This panel will indicate that, by default, all users have full control over this file.
5. Highlight the **Everyone** entry, and click on **Remove**.
6. Click on the **Add** button to display the "Add Users and Groups" panel.
7. In the "Names" table, select the **Administrators** entry.
8. Select **Full Control** in the "Type of Access" drop–down list, and click on **Add**.
9. Click on **OK** to close the "Add Users and Groups" panel.
10. You should be returned to the "File Permissions" panel. Click on **OK** to close it.
11. Click on **OK** to close the "Properties" panel.

Configuring the WebSphere Workflow Services (WWFServices) component

Using the WebSphere Administrative Console:

1. Expand **WebSphere Administrative Domain** and expand **Node name Application**
2. Stop the WWFServices Application Server.
3. Expand the branch of ″WWFServices″ tree.
4. Expand the branch of ″WWFContainer″ tree. This will display the enterprisebeans.
5. Select the **WWFQueryHome** enterprisebean.
6. Edit the Deployment descriptor by clicking on the **Edit** button on the right-hand panel.
7. Select the **Environment** tab.
8. Add the following environment properties or modify the values if they already exist:
   - DBPASSWORD Value: specify the DB2 password
   - DBUSER Value: specify the DB2 user
9. Click on **OK** in the ″Deployment Properties″ window.
10. Click on **Apply** in the ″EnterpriseBean:WWFQueryHome″ window.
11. Start the WWFServices Application Server

Configuring WebSphere security

WebSphere security can be enabled to protect its resources: servlets, JSPs, and enterprise beans. The following sections describe the process to configure each of the application servers. Note that some of these steps might take some time to complete.

Global security settings

Security settings are set but not enabled during initial configuration. To make these settings work initially, you must enable security as follows:

1. From the console, go to the `Tasks -> Configure Global Security Settings` panel.
2. Select **Enable security**.
3. Click **Next** and check that the settings apply to your system.

If you disable and then enable security, follow these steps to re-enable security:

1. Select the **Advanced** button under the ″User Registry″ tab, and check that fields contain the following values. If the values are unsuitable, you must enter the correct values. The values should be:

Table 1.

User Filter	(|(&(cn=%v)(objectclass=ePerson))(&(uid=%v)(objectclass=ePerson)))
Group Filter	(&(cn=%v)(objectclass=accessGroup))
User ID Map	*:uid
Group ID Map	*:cn
Group Member ID Map	groupOfNames:member; groupOfUniqueNames:uniqueMember; accessGroup:member

2. Click **OK**. Click **Finish**. Shut down the Administration Console, restart the WebSphere AdminServer Service, and restart the Administration Console.

Configuring WebSphere security for Interaction Manager

Open the WebSphere Administrative Console, which is on the Product Console facility, to point at the Interaction Manager facility. Use ″WSBIAdmin″ as your user ID and use your own password, recorded in “Chapter 2. Making notes to help you through this book” on page 5. WebSphere now establishes your connection.

Configuring WebSphere security for servlets and JSPs on Interaction Manager

The procedures below describe the WebSphere configuration steps for applying security to servlets and JSPs.

1. From the WebSphere Administrative Console go to `Tasks -> Create Enterprise Application`.
2. Enter the Application name as ″IMSecurity″ and click **Next**.
3. Expand **Web Applications**.
4. Select **ePortal** and click **Add**.
5. Select **wsb2bism** and click **Add**.
6. Click **Next** and then click **Finish**.
7. From the Console go to `Tasks -> Configure Application Security`, select **IMSecurity**, and click **Next**. Select **Basic Challenge** as the type of security needed for this application, and then click **Next**. On the next panel, press **Finish**.
8. From the Console go to `Tasks -> Configure Resource Security` and expand **Virtual Hosts**, expand **default_host**, click on a servlet to protect, and click **Next**. When prompted, select to use default method groups. On the next panel, click **Finish**. Repeat the above for each servlet listed below:
   - **Portal**
   - **WorkflowServlet**

- **EventsServlet**
- **MenuActionServlet**
- **AwareletConfigurationServlet**
- **AuditLogCannedSearchServlet**
- **AuditLogServlet**
- **DisplayAuditLogCannedSearchServlet**
- **DisplayAuditLogServlet**
- **DisplayExceptionLogServlet**
- **DisplayLDAPConfigServlet**
- **LDAPConfigServlet**
- **RtServlet**
- **DisplayExceptionLogServlet**
- **TraceDispPickServlet**
- **TraceDispServlet**

9. From the Console go to `Tasks -> Configure Resource Security` and click on **Virtual Hosts**, and click on **default_host**. Select **/ePortal/*.jsp** and click **Next**. When prompted, select to use the default method groups. On the next screen click **Finish**. Repeat for:
   - **/ePortal/*.jsv**
   - **/ePortal/*.jsw**
   - **/wsb2bism/*.jsp**
   - **/wsb2bism/*.jsv**
   - **/wsb2bism/*.jsw**
10. From the Console go to `Tasks -> Configure Security Permissions`. Select the **IMSecurity Application** and click **Next**. Select all the groups and click **Next**.
11. On the ″Grant Permissions″ screen select the user, all the users, or groups of users that can access these servlets.

    The security permissions depend on the level of authorization you want to permit. **Everyone** allows all users to access the protected resources. **All Authenticated Users** allows only authenticated users to access the resources. Permitting individual users and groups restricts the access to these only. You are advised to restrict access to only those users and groups who need to access the resource. Select the selection button and then select **Group** in the pull–down. Place a search filter, for example *****, and then select **Search**. Next select the group to which you want to grant access for these resources.
12. Click **Next** and click **Finish**.

Configuring WebSphere security for enterprise beans on Interaction Manager

1. From the WebSphere Administrative Console, which is on the Integrated Console facility, select the **Edit Enterprise Application** task.
2. Select the **IMSecurity** application.
3. On the ″Application Resources″ panel, expand **Enterprise Beans** and select and add the following beans:
   - **Rhierarchy**
   - **RHMapping**
   - **PersAuthTrans**
   - **AContent**
   - **SessionInfo**
   - **Rule**
   - **RuleUse**
   - **AdminRule**
   - **AdminRuleUse**
   - **CooperativeCache**
   - **MapEJB**
   - **CacheOp**
   - **PersAuthCollec**
   - **PersCollecTrans**
   - **SecEnabler**

   When all the enterprise beans have been added, click **Next** and then **Finish**.
4. From the Console go to `Tasks -> Configure Security Method Groups`. Select **Add a new method group**. Enter **Personalization Group** when prompted for the name of the new method group. Click **Finish**.
5. From the Console, go to `Tasks -> Configure Resource Security`, click on **Enterprise Beans**, and select the enterprise beans that you want to protect (as in step 3). Click **Next**. When prompted to use default method groups, select **No**. Select all the methods and click **Add**. From the ″Method Groups″ list, select **Personalization Group** and click **OK**. Click **Finish**. Follow the above procedure for each listed enterprise bean in step 3
6. From the console go to `Tasks -> Configure Security Permissions`. Select the **IMSecurity** application and click **Next**. Select **IMSecurity-Personalization Group**. On the ″Grant Permissions″ panel, you must select **Everyone**, **Next**, and **Finish**.

Configuring WebSphere Security for TAM and TAM Plus

1. From the WebSphere Administrative Console, which is on the Integrated Console facility, go to `Tasks -> Create Enterprise Application`

2. Enter the application name TAM Security and click **Next**.
3. On the Application Resources screen click on Enterprise Beans. Select the **AMSHome** bean and click **Add**. Then select the **GSOHome** bean and click **Add**. Select **Next**. The two beans should be listed under the EnterpriseBeans folder , as shown below.

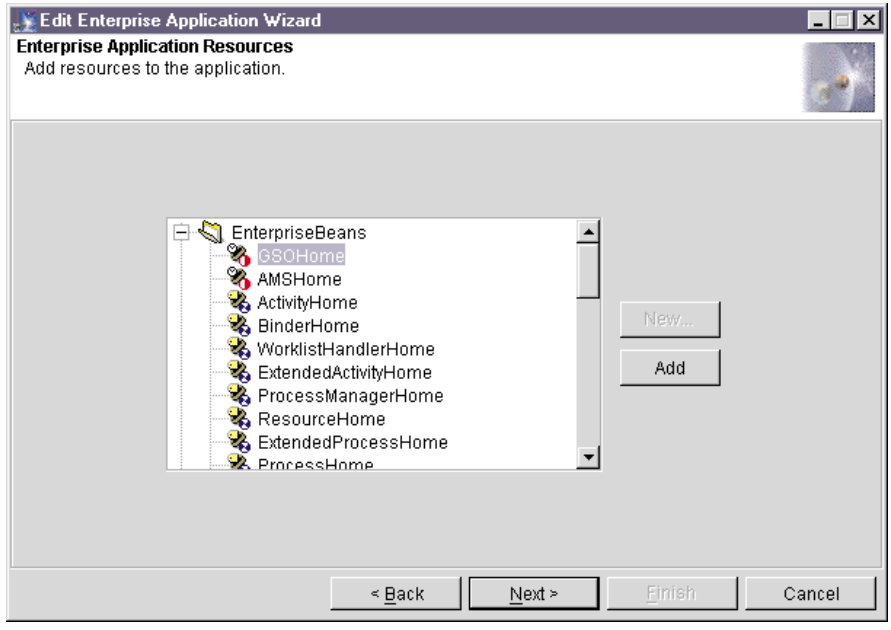


Figure 26. Enterprise Application Resources

Finally, click **Finish**.

4. From the Console go to Tasks -> Configure Application Security. Expand **Enterprise Applications**. Select the **TAM Security** enterprise application and click **Next**. Select **Basic Challenge** as the type of security needed for this application, then click **Next**. On the next screen click **Finish**.
5. From the Console go to Tasks -> Configure Resource Security and click on **Enterprise Beans**. Select the **AMSHome** enterprise beans, and click **Next**. When prompted select to use default method groups. On the next screen, click **Finish**.
6. Repeat step 11 for the GSOHome bean.
7. From the Console, go to Tasks -> Configure Security Permissions. Expand **Enterprise Applications**. Select the **TAM Security** enterprise application, and click **Next**. Select all the method groups to be secured and click **Next**.
8. On the ″Grant Permissions″ panel, choose one of:

- **Everyone**
- **All Authenticated Users**
- Individual groups and users that you want to access these beans

The security permissions depend on the level of authorization you want to permit. **Everyone** allows all users to access the protected resources. **All Authenticated Users** allows only authenticated users to access the resources. Permitting individual users and groups restricts the access to these only. You are advised to restrict access to only those users and groups who need to access the resource. Select the selection button and then select **Group** in the pull–down. Place a search filter, for example *****, and then select **Search**. Next select the group to which you want to grant access for these resources.

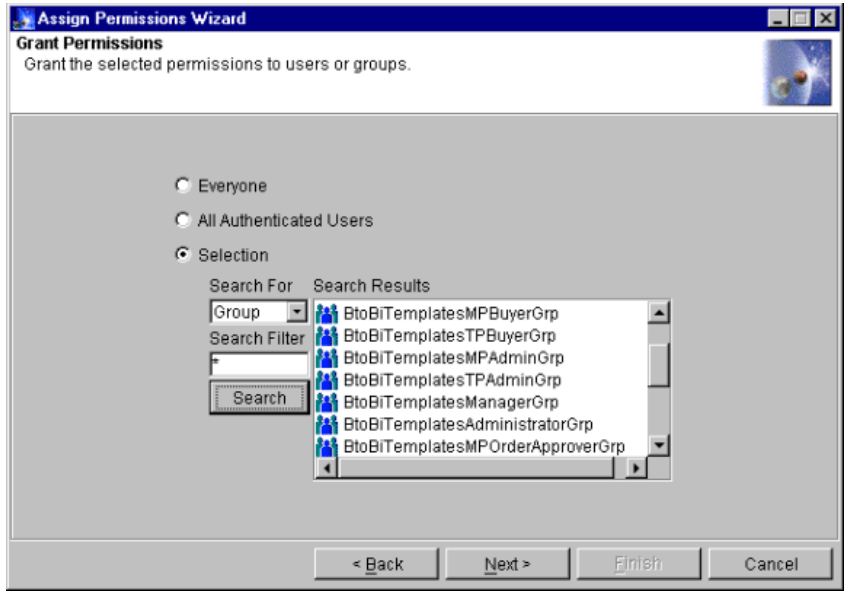


Figure 27. Grant permissions

Click **Next** and click **Finish**.

Configuring WebSphere security for Workflow and Workflow Services

1. From the WebSphere Administrative Console, go to `Tasks -> Create Enterprise Application`.
2. Enter the Application name ″WFSecurity″ and click **Next**.
3. On the ″Enterprise Application Resources″ panel click on **Enterprise Beans**. Select the following beans and click **Add**:
   - **ActivityHome**

- **BinderHome**
- **WorklistHandlerHome**
- **ExtendedActivityHome**
- **ProcessManagerHome**
- **ResourceHome**
- **ExtendedProcessHome**
- **ProcessHome**
- **RequesterHome**
- **AssignmentHome**
- **ExecutionObjectHome**
- **DocumentHome**
- **ContainerCacheHome**
- **WWFServicesHome**
- **WWFQueryHome**

4. Select **Next**. The beans should be listed under the ″EnterpriseBeans″ folder, and ″UR″ should be listed under the Web Applications folder.
5. Select **Finish**.
6. From the Console, go to `Tasks -> Configure Application Security`. Select the **WFSecurity Enterprise Application** and click **Next**. Select **Basic Challenge** as the type of security needed for this application, then click **Next**. On the next panel, click **Finish**.
7. From the Console, go to `Tasks -> Configure Resource Security` and click on **Enterprise Beans**. Select the **ActivityHome** EJB and click **Next**. When prompted to use default method groups, select **Yes**.
8. Repeat the step above for the following beans:
   - **BinderHome**
   - **WorklistHandlerHome**
   - **ExtendedActivityHome**
   - **ProcessManagerHome**
   - **ResourceHome**
   - **ExtendedProcessHome**
   - **ProcessHome**
   - **RequesterHome**
   - **AssignmentHome**
   - **ExecutionObjectHome**
   - **DocumentHome**
   - **ContainerCacheHome**
   - **WWFServicesHome**

- **WWFQueryHome**

9. From the Console, go to `Tasks -> Configure Security Permissions`. Select the **WFSecurity Enterprise Application** and click **Next**. Select all the method groups except for **UserRegistrationMethod** and **Personalization Methods** (if they exist). Click **Next**.
10. On the ″Grant Permissions″ panel, select the **Selection** radio button. Choose **Groups** from the drop–down and put a ***** for the search filter. Click **Search**. Select the **BtoBiTemplatesGrp** group from the list on the right. Click **Next**. Each Method Group should have BtoBiTemplates listed below it.

Installing the Policy Director Console for the Product Console Launchpad facility

Install the Policy Director Console from the Policy Director CD. No configuration is necessary.

To use the console:

1. Select `Start -> Programs -> Policy Directory -> Management Console` to start the console.
2. Enter `sec_master` and its password to access the user registry and object space.

Creating a WebSphere Generic Server for MQSeries Workflow Java Agent

Use the WebSphere Advanced Administrative Console, which is on the Integrated Console facility, to:

1. Select the node for the BFMWAS machine and right click.
2. Highlight **Create**.
3. Select **Generic Server**.
4. Enter the following values:

Server Name	`MQWF Java Agent`
Executable	`%WebSpherePath%\jdk\jre\bin\java.exe`
Command line arguments	`-classpath %WebSpherePath%\lib\ujc.jar; %MQWFPath%\bin\java3300\fmcojagt.jar com.ibm.workflow.agent.Main -yFMC`
Working directory	`%WSBIPath%\logs`
Standard output	`mqwfagentout.txt`
Standard error	`mqwfagenterr.txt`

Note: Replace **%WebSpherePath%**, **%MQWFPath%**, and **%WSBIPath%** with the actual paths of WebSphere, MQSeries Workflow, and WebSphere Business Integrator. The path must include the drive. For example:

Executable: `d:\websphere\jdk\jre\bin\java.exe`

5. Click **OK**.
6. Start the WebSphere Generic Server: **MQWF Java Agent**.

Setting up the Data Access Object utility

Use the Data Access Object documentation, which is in the utilities directory of the Business Integrator Documentation CD, to set up Data Access Object so that you can access your audit logs.

Rebooting when all installation and configuration is complete

When you have completed all your installation and configuration, you should reboot all the machines in your topology before attempting any further work on your Business Integrator system. After you have rebooted, allow all startup activity to complete before continuing, to ensure that your machines have started correctly.

Chapter 9. Setting up firewalls and proxies

Use this chapter

to help you install any firewalls and proxies you require. This step is separate from the sequence of installation and configuration described in the preceding chapters.

This chapter is relevant only if you have PAM installed.

If you need firewalls and proxies, you install and configure them manually, as described in:

- "Installing and configuring your firewalls"
- "Installing and configuring the PAM proxy facility" on page 92
- "Installing and configuring the Web proxy facility" on page 96

This chapter describes installation and configuration with and without a digital security certificate. The *WebSphere Business Integrator Concepts and Planning* has already advised you to obtain your certificate in good time to avoid delays during installation.

Installing and configuring your firewalls

The following two sections describe how to install and configure firewalls for an entry-level system and then an enterprise-level system, using SecureWay Firewall, Version 4.1. Other firewall products may be used instead. Your system might already have firewalls installed.

The firewalls provide a layer of security that prevents direct access to the Business Integrator environment. A typical configuration requires two firewalls. This chapter describes the procedures for installing and configuring the firewalls. You are advised to read all of the steps in these sections before starting the installation

Installing firewalls

Refer to the documentation supplied with the software product for installation instructions. For SecureWay Firewall, PDF files of the manuals are on the product CD.

Configuring firewalls in an entry-level system

Use the following procedures to configure both firewalls.

Configuring the outside firewall

The outside firewall lies between the demilitarized zone (DMZ) and the outside world. To configure the outside firewall, use the SecureWay Firewall Configuration tool to:

1. Designate the secure and the non-secure interface.
2. Create a network object named `PAMProxyDMZBox` for the WebProxy machine in the DMZ.
3. Add the following connection:
   - WorldToPAMProxyDMZBox

     Source: World

     Dest.: PAMProxyDMZBox

     Service: Permit All
4. Activate the firewall.

Configuring the inside firewall

The inside firewall lies between the trusted zone and the DMZ. To configure the inside firewall, use the SecureWay Firewall Configuration tool to:

1. Designate the secure and the non-secure interface.
2. Create a network object named `PAMProxyMachine` for the PAMProxy machine in the DMZ.
3. Create a network object `PAMMachine` for the Partner Agreement Manager machine in the trusted zone
4. Create the following rules:
   - IIOP 1/2 (TCP in port >= 900)

     Protocol: tcp

     Source port: Any

     Dest. port: >= 900

     Interface: NonSecure

     Routing: route

     Direction: inbound
   - IIOP 2/2 (TCP in port 900 from secure to inside)

     Protocol: tcp

     Source port: Any

     Dest. port: >= 900

     Interface: Secure

     Routing: route

     Direction: outbound
   - IIOP/ACK 1/2

     Protocol: tcp/ack

Source port: >=900
Dest. port: Any
Interface: Secure
Routing: route
Direction: inbound

- IIOP/ACK 2/2
  Protocol: tcp/ack
  Source port: >= 900
  Dest. port: Any
  Interface: NonSecure
  Routing: route
  Direction: outbound
- IIOPReply 1/2
  Protocol: tcp
  Source port: >= 900
  Dest. port: Any
  Interface: Secure
  Routing: route
  Direction: inbound
- IIOPReply 2/2
  Protocol: tcp
  Source port: >=900
  Dest. port: Any
  Interface: NonSecure
  Routing: route
  Direction: outbound
- IIOPReply/ACK 1/2
  Protocol: tcp/ack
  Source port: Any
  Dest. port: >=900
  Interface: NonSecure
  Routing: route
  Direction: inbound
- IIOPReply/ACK 2/2
  Protocol: tcp/ack
  Source port: Any
  Dest. port: >=900

Interface: Secure

Routing: route

Direction: outbound

5. Add the following services:
   - IIOPOverTCP (IIOP call from the client to Server), with the following rules:

     IIOP 1/2 (green)

     IIOP 2/2 (green)

     IIOP/ACK 1/2 (blue)

     IIOP/ACK 2/2 (blue)
   - IIOPReplyOverTCP, with the following rules:

     IIOPReply 1/2 (green)

     IIOPReply 2/2 (green)

     IIOPReply/ACK 1/2 (blue)

     IIOPReply/ACK 2/2 (blue)
6. Add the following connections:
   - PAMProxyToPAM

     Source: PAMProxyMachine

     Dest.: PAMMachine

     Service: IIOPOverTCP
   - PAMToPAMProxy

     Source: PAMMachine

     Dest.: PAMProxyMachine

     Service: IIOPReplyOverTCP
7. Activate the firewall.

Configuring firewalls in an enterprise-level system

Perform the following procedures to configure both firewalls.

Configuring the outside firewall

The outside firewall lies between the demilitarized zone (DMZ) and the outside world. To configure the outside firewall, perform the following steps from the SecureWay Firewall Configuration tool:

1. Designate the secure and the non-secure interface.
2. Create a network object named `WebProxyDMZBox` for the WebProxy machine in the DMZ.
3. Add the following connection:
   - WorldToWebProxyDMZBox

     Source: World

Dest.: WebProxyDMZBox

Service: Permit All

4. Create a network object named PAMProxyDMZBox for the WebProxy machine in the DMZ
5. Add the following connection:
   - WorldToPAMProxyDMZBox

     Source: World

     Dest.: PAMProxyDMZBox

     Service: Permit All
6. Activate the firewall.

Configuring the inside firewall

The inside firewall lies between the trusted zone and the DMZ. To configure the inside firewall, perform the following steps from the SecureWay Firewall Configuration tool:

1. Designate the secure and the non-secure interface.
2. Create a network object named WebProxyMachine for the WebProxy machine in the DMZ.
3. Create a network object named PAMProxyMachine for the PAMProxy machine in the DMZ.
4. Create a network object InteractionManagerMachine for the Interaction Manager machine in the trusted zone.
5. Create a network object TAMPlusMachine for the Trust and Access Manager machine in the trusted zone.
6. Create a network object PAMMachine for the Partner Agreement Manager machine in the trusted zone
7. Create the following rules:
   - IIOP 1/2 (TCP in port >= 900)

     Protocol: tcp

     Source port: Any

     Dest. port: >= 900

     Interface: NonSecure

     Routing: route

     Direction: inbound
   - IIOP 2/2 (TCP in port 900 from secure to inside)

     Protocol: tcp

     Source port: Any

     Dest. port: >= 900

     Interface: Secure

Routing: route
Direction: outbound

- IIOP/ACK 1/2
  Protocol: tcp/ack
  Source port: >= 900
  Dest. port: Any
  Interface: Secure
  Routing: route
  Direction: inbound
- IIOP/ACK 2/2
  Protocol: tcp/ack
  Source port: >= 900
  Dest. port: Any
  Interface: NonSecure
  Routing: route
  Direction: outbound
- IIOPReply 1/2
  Protocol: tcp
  Source port: >= 900
  Dest. port: Any
  Interface: Secure
  Routing: route
  Direction: inbound
- IIOPReply 2/2
  Protocol: tcp
  Source port: >= 900
  Dest. port: Any
  Interface: NonSecure
  Routing: route
  Direction: outbound
- IIOPReply/ACK 1/2
  Protocol: tcp/ack
  Source port: Any
  Dest. port: >= 900
  Interface: NonSecure
  Routing: route
  Direction: inbound

- IIOPReply / ACK 2 / 2
  - Protocol: tcp / ack
  - Source port: Any
  - Dest. port: >= 900
  - Interface: Secure
  - Routing: route
  - Direction: outbound

8. Add the following services:
   - IIOPOverTCP (IIOP call from the client to Server) with the following rules:
     - IIOP 1 / 2 (green)
     - IIOP 2 / 2 (green)
     - IIOP / ACK 1 / 2 (blue)
     - IIOP / ACK 2 / 2 (blue)
   - IIOPReplyOverTCP with the following rules:
     - IIOPReply 1 / 2 (green)
     - IIOPReply 2 / 2 (green)
     - IIOPReply / ACK 1 / 2 (blue)
     - IIOPReply / ACK 2 / 2 (blue)
9. Add the following connections:
   - WebProxyToInteractionManager
     - Source: WebProxyMachine
     - Dest.: InteractionManagerMachine
     - Service: IIOPOverTCP
   - WebProxyToTAMPlus
     - Source: WebProxyMachine
     - Dest.: TAMPlusMachine
     - Service: IIOPOverTCP
   - PAMProxyToPAM
     - Source: PAMProxyMachine
     - Dest.: PAMMachine
     - Service: IIOPOverTCP
   - InteractionManagerToWebProxy
     - Source: InteractionManagerMachine
     - Dest.: WebProxyMachine
     - Service: IIOPReplyOverTCP
   - TAMPlusToWebProxy

Source: TAMPlusMachine

Dest.: WebProxyMachine

Service: IIOPReplyOverTCP

- PAMToPAMProxy

  Source: PAMMachine

  Dest.: PAMProxyMachine

  Service: IIOPReplyOverTCP

10. Activate the firewall.

Installing and configuring the PAM proxy facility

This section tells you how to install and configure the PAM proxy facility.

Installing the PAM proxy component

To install the PAM Proxy, copy the `PAM Proxy` folder from the PAM CD onto the machine that will be used to host the PAM Proxy. This will become the installation directory for the PAM Proxy.

Configuring the PAM proxy component

1. Make a new copy of `sample.cnf`, which can be found in your PAM proxy directory. Rename the file `PAM_proxy.cnf` and make sure that both it and `PAM_Proxy.exe` are in the permanent working directory.
2. Read the documentation accompanying PAM Proxy to decide whether an 'active' or 'passive' mode is required.

   If you require active mode:

   a. Make sure that all `PASSIVE_PROXY= ...` lines are commented out or deleted.

   b. Change `CACHE_SIZE=...` if required.

   c. Change `IDLE_TIMEOUT=...` if required.

   d. Change `OUTBOUND_LISTENER=pam-proxy.mydomain.com:8471` to reflect the machine on which the PAM Proxy is installed and the port number that will be used to make all outbound connections by the internal PAM machine.

   e. Change `PROXY=proxy_machine.mydomain.com:8481->pam.mydomain.com:10001` to reflect the machine on which the PAM Proxy is installed, the machine on which PAM is installed, and the relevant ports that will be used. The port number associated with the proxy machine is used later when updating the PAM configuration, where it is referred to as the ″Incoming Port″.

   f. Change or add the `EXTERNAL= ...` entries to include all machine/port pairs that are allowed to communicate with the Proxy. Limited wildcarding is permitted. You cannot wildcard the port number or the first field in the IP space.

If you require passive mode:

a. Make sure that all `PROXY= ...` lines are commented out or deleted.

b. Change `CACHE_SIZE=...` if required.

c. Change `IDLE_TIMEOUT=...` if required.

d. Change `OUTBOUND_LISTENER=pam-proxy.mydomain.com:8471` to reflect the machine on which the PAM Proxy is installed and the port number that will be used to make all outbound connections by the internal PAM machine.

e. Read the text and change `PASSIVE_PROXY=proxy_machine.mydomain.com:8481->proxy_machine.mydomain.com:8482->pam2.mydomain.com:1` to reflect the machine on which the PAM Proxy is installed (proxy_machine.mydomain.com), the machine on which PAM is installed, and the relevant ports that will be used. The first port number associated with the proxy machine is used later when updating the PAM configuration, where it will be referred to as the ″Incoming Port″. The second port associated with the proxy machine will be referred to as the ″Pick-Up Port″.

f. Change or add the `EXTERNAL= ...` entries to include all machine / port pairs that are allowed to communicate with the Proxy. Limited wildcarding is permitted. You cannot wildcard the port number or the first field in the IP space.

3. To install PAM Proxy as an NT service, run `PAM_proxy -install` from a command prompt. The PAM_proxy service is installed as PAM Proxy. You can view it from the NT Services control panel. When you install it, the proxy service is set to manual startup. If you want the proxy service to start automatically at system boot, click **Startup**to change the Startup manually from the control panel.

4. Update the PAM configuration to reflect the use of the PAM Proxy:

   a. On the PAM machine, start up PAM Process Manager.

   b. Under your Partner Name, select the ″Administration″ folder.

   c. Select the ″Channels″ folder.

   d. Select any channel that will be using the proxy. Complete this operation for **every** channel individually.

   e. Under the ″Listeners″ tab, select any listener that is using the proxy.

   f. Click **Properties**.

   g. Ensure that **Connect through a proxy server** is checked and complete the following, depending on the values that were entered earlier:

      Incoming Host: ″Numeric IP address of Proxy machine″.

      Incoming Port: as above.

PickUp Port: as above. (For an active proxy install, leave the 'PickUp' port blank.)

h. Under the ″Services″ tab, select any service that is using the proxy.

i. Ensure that **Connect through a proxy server** is checked and complete the following, depending on the values that were entered earlier:

Outgoing Host: ″Numeric IP address of Proxy machine″

Outgoing Port: ″Port number in ″Outbound Listener″ above″

5. Inform all partners of the IP address and incoming port of your proxy server. (They won't need to know about the PAM Server Name and address.)

Installing the Web Proxy component as part of the PAM Proxy facility

The Web Proxy component described in this section is not related to the Web Proxy facility described below.

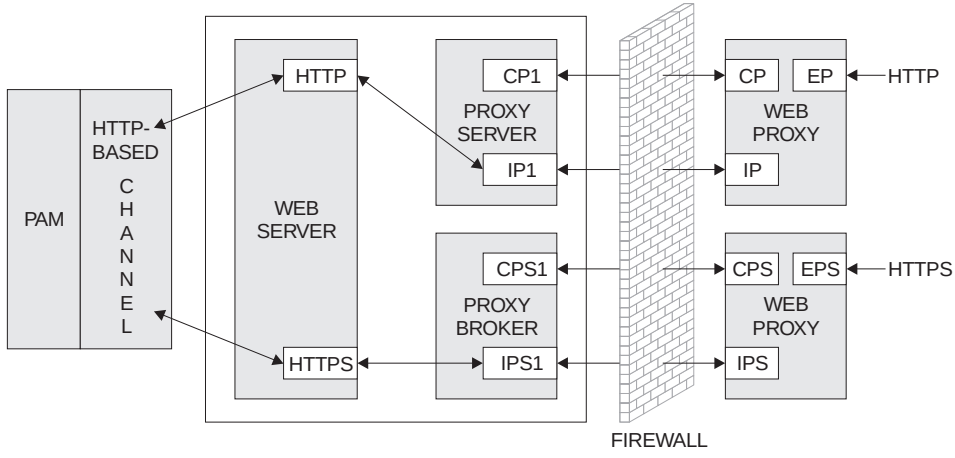


Figure 28. Web Proxy instances

As can be seen from the diagram above, you need two separate instances of the Web Proxy if you are dealing with HTTP and HTTPS connections simultaneously, in the same way that you need two PAV channels. The Proxy broker is an integral part of PAM and will be started automatically, taking its settings from a `.properties` file, which will be detailed later.

When the Web Proxy is used for inbound SSL connections, the server certificate for the Web server, which can be found on the PAM facility, must be created specifying the Web Proxy's IP address, because all inbound connections will be made to the Web Proxy. The certificate itself must be installed on the Web server, and the IP address must be the Web Proxy's IP address.

Install the Web Proxy as follows:

1. Extract the contents of the Webproxy.zip file, found on the Partner Agreement View CD under the ″WebProxy″ folder, into any directory you choose. It is a good idea to create a separate directory for the extracted files.
2. Set your PATH to include the \release subdirectory in the directory where you extracted the Webproxy.zip file. For example, if you extracted the zip file to c:\WebProxy, set your PATH to include c:\WebProxy\release.
3. When you have completed the installation, you can run webproxy.exe, with the necessary parameters, from the command prompt to start the Web Proxy. The parameters are as follows:

   ```
   webproxy  <control port><internal port><external port>
   ```

   For example:

   ```
   webproxy 6000 6001 80 - this instance could be used for HTTP connections
   webproxy 6003 6004 443 - this instance could be used for HTTPS connections
   ```

   If only one parameter is given, the system automatically assigns contiguous internal and external ports, based on the control port number.

Configuring the Web Proxy component

1. In the directory where PAM is installed, find the following file, where XXX is your partner ID:

   ```
   <your PAM installation>\Partners\PartnerXXX\Properties\Partner.properties
   ```

2. Append the following lines, using the port numbers from the HTTP instance above:

   ```
   WebProxy.HTTP.Host=<PAM Proxy's IP address>; mode=server; type=string;
   WebProxy.HTTP.ControlPort=6000; mode=server; type=int;
   ```

   and if you are using SSL, also these lines, using the port numbers from the HTTPS instance above:

   ```
   WebProxy.HTTPS.Host=<PAM Proxy's IP address>; mode=server; type=string;
   WebProxy.HTTPS.ControlPort=6003; mode=server; type=int;
   ```

3. In the directory where PAV is installed, for example c:\WebSphere\PAV, find the following file:

   ```
   <your PAV installation>\conf\AppChannel.properties
   ```

4. For the HTTP PAV channel, edit:

   ```
   pam.host.<HTTP Channel ID>=<PAM Proxy's IP address>
   ```

   and then edit:

   ```
   pam.port.<HTTP Channel ID>=<HTTP Instance External Port>
   ```

5. For the HTTPS PAV channel, edit:

   ```
   pam.host.<HTTPS Channel ID>=<PAM Proxy's IP address>
   ```

and then edit:

```
pam.port.<HTTPS Channel ID>=<HTTPS Instance External Port>
```

Installing and configuring the Web proxy facility

This section tells you how to install and configure the Web proxy facility. There are four products to be installed, all supplied with Business Integrator:

- SecureWay Directory 3.2 client (with the GSK)
- NetSEAT (otherwise known as Policy Director client)
- Run Time Environment
- WebSEAL

Installing the Web proxy facility

1. Install Secureway Directory Client by:
   a. Starting installation from `<Facilities CD3>\SecureWay Directory\setup.exe`
   b. Selecting Custom install
   c. Install the client and GSK
2. Install Policy Director Client (NetSEAT) by:
   a. Starting installation from `<Policy Director Base CD>\Policy_Director\Client\setup.exe`
   b. Installing NetSEAT using DCE Runtime only
   c. Choosing Typical Install
3. Install Policy Director Server by:
   a. Starting installation from `<Policy Director WebSEAL CD>\Windows\Policy_Director\setup.exe`
   b. Installing Policy Director Runtime Environment (PDRTE)
   c. Installing Policy Director WebSeal (PDWeb)

Configuring the Web proxy facility

This configuration is described in two parts. If you already have a digital certificate when you receive Business Integrator, install Business Integrator with SSL at once. Otherwise, install Business Integrator without SSL and add SSL after you have received your certificate.

The *WebSphere Business Integrator Concepts and Planning* explains the need to have purchased a digital certificate, which you obtain from a certification authority

SSL must be set up on this machine, as described in “Setting up SSL on the other machines” on page 52.

Configuration is described one product a time.

Configuring NetSEAT

Run the configuration utility from the Start Menu shortcut, most commonly found at:

`Start -> Programs -> Policy Director -> NetSEAT -> NetSEAT Configuration.`

A window will appear with 2 tabs (**Secure Domains** and **General**).

1. Select **Secure Domains**, if not already displayed.
2. Select **Add** to create a new Secure Domain.
3. In the dialog box that appears, type in the name of the Secure Domain, that was created during the configuration of DCE on the TAM PLUS facility. The secure domain name should be the `hostname_cell`.
4. Click **OK**.
5. Click **Add** and type in the full host name of the Trust and Access Manager Plus facility; for example, `stewart.hursley.ibm.com`.
6. Select the appropriate ″Supported Services″- Security, DSB and CDS
7. Click **OK**.
8. Leave the ″Integrated Login Support″ and ″Advanced Login″ panels as they are.
9. Click **OK**
10. For more information on this feature, please click **Help**.
11. NetSEAT is now configured.

Configuring the Run Time Environment

Before attempting to configure this product, ensure that you have exported Policy Director's Management Server's signed certificate to the machine that is the Web Proxy. Do this by copying `pdcacert.b64` from the Trust and Access Manager Plus machine to the Web Proxy machine

If you already have a security certificate issued by a certificate authority, follow these instructions:

1. Run the configuration utility from the Start Menu shortcut, most commonly found at `Start -> Programs -> Policy Director -> Configuration`.
2. Select ″Policy Director Runtime Environment (PDRTE)″ and click **Configure**.
3. Specify the location of the Policy Director Management Server as being installed on ANOTHER machine. The location will be the Trust and Access Manager Plus facility
4. Enter the host name of the Trust and Access Manager Plus facility that the Policy Director Management Server is on.

5. Leave the listening port as the default 7135.
6. Locate the Policy Director's Management Server's signed certificate on the local machine – `pdcacert.b64`.
7. Click **Next**.
8. Select **LDAP Registry** for the ″User Registry Selection″ and click **Next**.
9. Identify the host name of the computer in which the LDAP server is housed (Trust and Access Manager Plus)
10. Change the port number to 389.
11. Enter the DN for the LDAP database. This will be `o=epic`.
12. Click **Next**.
13. Enable SSL Communication with the LDAP server by clicking on the appropriate radio button.
14. Enter the SSL details that are required:
    - Port number 636
    - The SSL client key database file, which is imported from the Trust and Access Manager Plus facility
    - The password for the client key database file

    Click **Next**. Review the information to make sure that it is accurate.
15. Click **Finish**.

Configuring WebSEAL

1. Run the configuration utility from the Start Menu shortcut, most commonly found at Start -> Programs -> Policy Director -> Configuration.
2. Select ″Policy Director WebSEAL (PDWeb)″ and click **Configure**.
3. Enter the DCE user name and password, which was created during the setup of DCE on the Trust and Access Manager Plus facility.
4. Enter theSecureWay Directory Administrator Name.
5. Enter the SecureWay Directory Administrator Password.
6. Allow TCP HTTP and HTTPS, accepting the default port number.
7. WebSEAL is now configured.

Installing and configuring Trust Association on the Interaction Manager facility

After WebSeal has been installed on the proxy, perform the following steps to set up the Trust Association between WebSeal and WebSphere Application Server.

The Trust Association is a program provided by WebSphere 3.5.3 that intercepts the HTTP request from WebSeal, extracts the user identity, and then creates the WebSphere security context.

1. Copy the trustedservers.properties and webseal36.properties from the [x]:\<wsbi_install>\properties directory to the \properties directory of WebSphere Application Server installation.
2. Edit trustedservers.properties to enable and disable the Trust Association. The defaut is enabled. Edit the first line in the file:

   com.ibm.websphere.security.trustassociation.enabled=true
3. Edit the following line of webseal36.properties to specify the hostname of the WebSeal machine:

   com.ibm.websphere.security.webseal36.hostnames=<webseal_hostname>.<domain_name>,<webseal_hostname>
4. Restart the WebSphere service and there should now be a message that the Trust Association Interceptor was loaded.

Configuring WebSeal junctions

WebSeal is a component of Policy Director that resides in the DMZ. Its purpose is to handle authentication and authorization to Web resources. A junction must be configured to a back-end Web server. In this scenario, this will be IBM HTTP server. The authorization granularity can be for the entire back-end server or for a particular web resource.

An SSL connection must be created between the WebSeal junction and the back-end HTTP Server. The HTTP Server certificate created above must be exported and added to WebSeal certificate key database.

1. From IkeyMan, open the certificate database pdsrv.kdb in the [x]:\<WebSeal_install>\lib\certs directory. The password to open this is pdsrv. Click on the **Export/Import** button. Select the file name and click **OK**. On the Web Proxy machine, using the gsk4ikm.exe utility, open the WebSeal certificate database, which can be found in <Policy Director installation directory>\lib\certs\pdsrv.kdb. The password, when prompted, is pdsrv. Select **Personal Certificates** in the ″Key Database Contents″, press **Export/Import...**. Choose **Import Key** as the action type, **pkcs12 file** as the file type, and provide the name of the file extracted from the Interaction Manager machine.
2. The Trust Association authenticates the WebSeal junction using the logon identity configured when the junction is created. On the Integrated Consoles machine, create a new user within the Policy Director Management Console, typically found at Start -> Programs -> Policy Director -> Management Console. Select the **Account Mgr** tab. When prompted for a user ID and password, use sec_master and the password provided earlier, during configuration. In the tree structure below, right click on **Users** and select **New...**. Input the new user name in the form of WebSeal_<hostname>, where hostname is the host name of the WebSeal machine. In the user dialog, enter:
   - A new unique indentifier, for example WebSeal, for the LDAP cn

- Directory for the LDAP sn
- <LDAP cn>,o=EPICUsers,o=epic for the LDAP dn

Accept the default options and press **OK**.

3. From a command prompt, enter junctioncp -e <webseal_hostname>. Now enter the create command to create the WebSeal junction with the following parameters:

   ```
   create -t ssl -h <hostname> -c -B -U <WebSeal user> -W <password> -j
   /junction name
   ```

   where:

   - <hostname> is the host name of the back-end HTTP server
   - <WebSeal user> is the user created in step 2
   - <password> is the password of the WebSeal user
   - /junction name is the logical name of the junction associated with the back-end server

4. Verify that the junction is running by restarting the WebSeal service and then running the junctioncp command as shown in step 3 above. Next, enter show /junctionname. The server state should be running. If it is not running, check that the back-end HTTP server is running and that the certificate has been properly loaded into the WebSeal certificate database.

Configuring Forms-Based Challenge Page

Use the following instructions to configure WebSeal to use a custom challenge page instead of the browser displaying the login window:

1. Copy the following files to the Web Proxy machine from ...\<wsbi>\Resources\WebSeal directory on the Interaction Manager machine to:
   - [x]:\<WebSeal_Install-path>\www\docs\ContentFrame.html
   - [x]:\<WebSeal_Install-path>\www\docs\MenuFrame.html
   - [x]:\<WebSeal_Install-path>\www\docs\title.html
   - [x]:\<WebSeal_Install-path>\www\docs\index.html
   - [x]:\<WebSeal_Install-path>\www\docs\titleimage.gif
2. Copy the following files to the Web Proxy machine from ...\<wsbi>\Resources\WebSeal directory on the Interaction Manager machine to:
   - [x]:\<WebSeal_Install-path>\www\lib\html\en_US\login.html
   - [x]:\<WebSeal_Install-path>\www\lib\html\en_US\logout.html

   There would be separate directories for each of the different language installations.

3. The index.htmlfile from step 1, and logout.html, from step 2, must be edited to correspond to the WebSeal machine and the correct junction. The URL should be:

   ```
   https://<webseal_host>/<junction name>/ePortal/servlet/
   Portal?Action=Logon&Solution=BtoBiTemplates
   ```

4. The WebSeal configuration file, iv.conf, must be modified so that it uses the custom challenge instead of the basic authentication. The file is located in the [x]:\<Policy Director>\lib directory. The following should be modified:

   - https-forms-auth = yes

5. Restart WebSeal for the changes to iv-conf to take effect. From the Windows Control Panel, select **Services**. Select the service **Policy Director WebSEAL** and press **Stop**. Select the service **Policy Director Auto-Start Service** and press **Start**.
6. To display the custom challenge page correctly, the above files need to be unprotected so that an unauthenticated user is allowed to read the html files. From the Policy Director Management Console, typically found at Start -> Programs -> Policy Director -> Management Console:

   a. Select the **Object Space** tab. You will be prompted to login to the secure domain; the user ID is sec_master with the password provided during configuration.

   b. Expand the ″ACL Policies″ tree

   c. Expand the default_webseal ACL

   d. Select the **Unauthenticated** entry and then right click and select **Properties...**

   e. Select the **Server** tab, and make sure the **Read** box is checked

   f. Select **OK** to set the value

   At this point all resources in the [x]:\ ]:\<WebSeal_Install-path>\www\docs directory and the junctioned servers are unprotected because, by default, the default-WebSeal ACL permissions are inherited down the tree.

7. Start Internet Explorer and enter the following URL:

   ```
   https://webseal_host
   ```

   The custom challenge page is now displayed.

8. To protect resources on the Web Server using Policy Director, you must place the appropriate ACL on a resource. WebSeal provides two levels of authorization, either course-grained or fine-grained. Placing an ACL at the junction level provides course-grained access to the back-end server because all resources will have the same permissions. To provide fine-grained access, you must provide WebSeal with information about the contents of the back-end Web Server.

A CGI program called query_contents provides this information. The query_contents program searches the Web space contents and provides this inventory information to the Management Console on WebSeal. The program comes with the WebSeal installation, but must be manually installed on the back-end Web Server.

The Object Space manager of the Management Console automatically runs query_contents any time the portion of the Protected Object Space representing the junction is expanded in the Object Space management panel. Now that the Console knows about the contents of the third-party application space, you can display this information and apply policy templates to appropriate objects.

To install query_contents, locate the executable program named query_contents.exe and the configuration file named query_contents.cfg in the following directory:

```
[x]:\<WebSeal_Install-path>\www\lib\query_contents
```

a. Ensure the IBM HTTP Server on the junctioned machine is correctly configured.
b. Copy query_contents.exe into the cgi-bin directory of the IBM HTTP Server.
c. Copy query_contents.cfg into the \winnt directory.
d. Edit the query_contents.cfg file to correctly specify the document root directory for the Web server. This is the starting place where the query_contents program will start reading.

   For example, to list the resources for the WebSphere default_host files, specify the following: docroot=C:\WebSphere\hosts\default_host.

9. Verify that query_contents is set up correctly. From an NT prompt on the back-end Web Server, execute the query_contents program from the \IBM HTTP Server\cgi-bin directory as follows: MSDOS> query_contents dirlist=/.

   You should see something similar to the following output:

   ```
   100
   admin//
   default-app//
   ```

   The number 100 is a return status that indicates success. It is most important to see at least the number 100 as the first (and perhaps only) value. If you see an error code instead, then the configuration file is not in the correct place, or does not contain a valid document root entry. Check the configuration of the query_contents.cfg file and make sure that the document root exists.

10. From the Policy Directory Management Console, expand the tree where the WebSeal junction is listed. You should see the directory list expanded under the junction.

At this point, specific ACLs can be applied to resources, thus providing fine-grained authorization.

Chapter 10. Servicing your system

Use this chapter
to help you apply service to your Business Integrator system.

All service for Business Integrator will be provided on the Web site at:
`http://www.ibm.com/software/webservers/btobintegrator/`

Chapter 11. Uninstalling Business Integrator

Use this chapter
to help you uninstall the Business Integrator code and the packages integrated into that code.

You run the uninstall program separately on each machine in the topology. Do not run the uninstall program on the base machine until you have uninstalled Business Integrator on all the other machines in the topology. When you run the uninstall program on the other machines in the topology, the uninstall program informs the topology server that the facility being uninstalled should be marked as uninstalled and therefore may subsequently be reinstalled on another machine.

Uninstalling on the machines in the topology

You must be logged on with a user ID that is a member of the Windows NT Administrators group in the local security domain to complete uninstallation. You can uninstall Business Integrator in either of the following ways:

1. Start Uninstallation from the Business Integrator program folder. Open the program folder created during installation (by default this is IBM WebSphere Business Integrator). Select the Uninstall WebSphere Business Integrator icon to run the uninstall program.
2. Start Uninstallation by selecting ″IBM WebSphere Business Integrator″ from the Add/Remove Programs icon in the Control Panel.

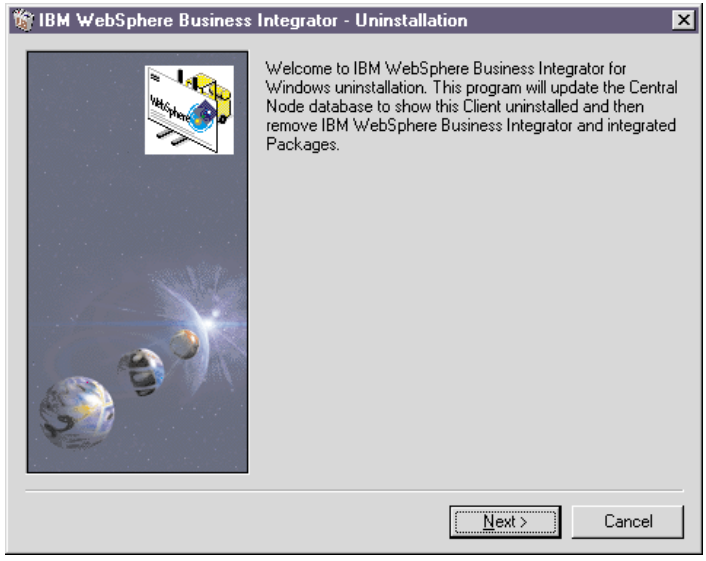


Figure 29. Welcome panel for uninstallation

If one or more CSDs has been installed, this first panel will look slightly different, as shown below.

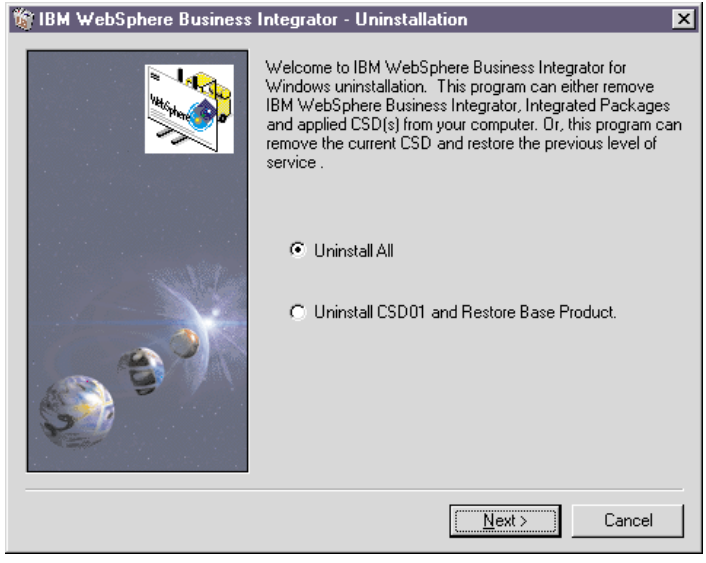


Figure 30. Uninstalling either the Business Integrator code or uninstalling a CDS

However, Business Integrator can still be completely uninstalled from this panel by selecting the ″Uninstall All″ option, and then pressing ″Next″. If you choose to uninstall a CSD, you roll back one CSD at a time by pressing ″Next″.

When you press ″Next″, the uninstall program queries the topology server, which replies with a list of the facilities that must be uninstalled and a list of the integrated packages that will be uninstalled.

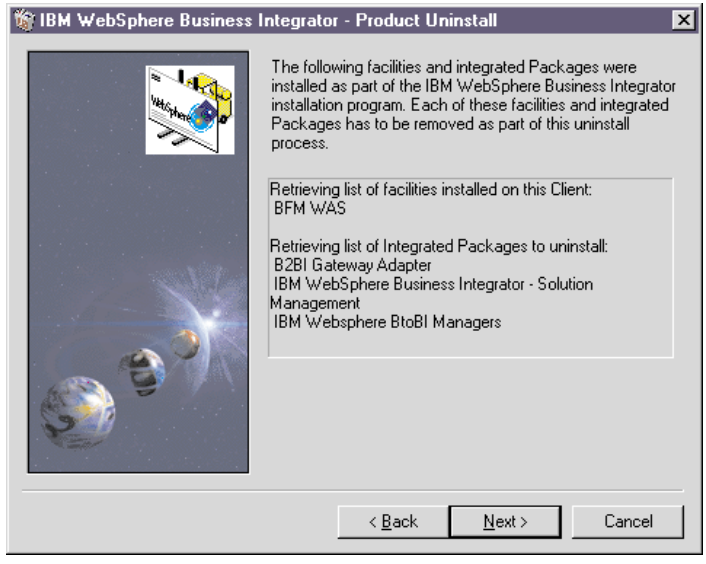


Figure 31. A list of the facilities and integrated packages that will be uninstalled

Press ″Next″ to start the uninstall process for this machine.

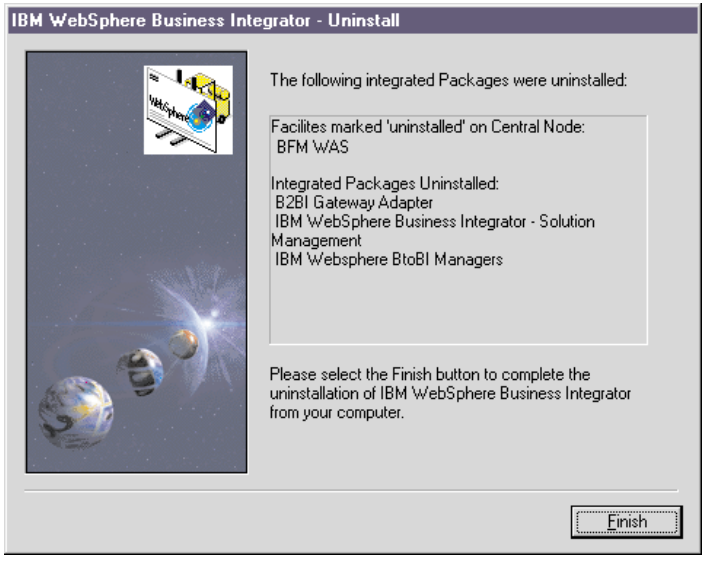


Figure 32. Completing an uninstallation

Press ″Finish″ to start the uninstallation of the indicated items. You'll see the standard uninstall panel during the uninstallation.

Uninstalling on the base machine

After you have uninstalled Business Integrator on the machines in the topology, you can safely run the uninstall program on the base machine.

Finally, check for the presence of the `topology.xmi` file in the `<WebSphere Business Integrator installation directory>\topology\remote` directory. If it is present, delete it.

Appendix A. Error messages and return codes during installation

This appendix lists the return codes that you might see during installation.

“Log files” on page 112 gives a list of the installation log files produced during the Business Integrator wrapper install.

Return codes

Return codes that might be displayed on the installation summary window:

0	Success
1	General error
2	Invalid mode
3	Required data not found in response file
4	Not enough memory available
5	File does not exist
6	Cannot write to the response file
7	Unable to write to log file
8	Invalid path to response file
9	Not a valid list type
10	Data type invalid
11	Unknown error during setup
12	Dialog boxes are out of order
51	Cannot create the specified folder
52	Cannot access the specified file of folder
53	Invalid option selected
61	Check of product registry keys failed OR an error was found in the product install log
63	Product log file not found

Log files

These installation log files are in the Windows `Winnt` directory and are named as follows:

MQSeries for Windows NT	MQSeries.log
MQSeries Integrator	mqsi.log
MQSeries Pub/Sub SupportPac	mqpubsub.log
MQSeries Adapter Kernel	mqak.log
MQSeries Workflow	mqwf.log
Java Messaging Service (MQSeries classes for Java)	JMS.log
WebSphere Application Server Advanced Edition	WAS.log
HTTP Server	http.log
GSKit	gskit.log
WebSphere fixpack	WASFIX3b.log
Java	JDK122.log
Managers	BtoBi.log
Gateway Adapter	GatewayAdapter.LOG
Solution Management	hursm.log
SecureWay Directory Services	ldap.log
Initial Installer	biz_initial.log
Wrapper install	biz_wrapper.log

The DB2 log is in its own `Db2log` directory:

DB2	Db2.log

The log for the batch configuration file is in the Windows `temp` directory:

Batch configuration file log	wsbiconfig.log

The logs for the Select Topology wizard and the Install Launchpad wizard are in the `<wsbi>\logs` directory.

Select Topology wizard	AdminMessages1.log AdminMessages2.log AdminMessages3.log

Install Launchpad wizard	AdminMessages1.log AdminMessages2.log AdminMessages3.log

When AdminMessages1.log is full, its contents are transferred to AdminMessages2.log. Then, before the next transfer, the contents of AdminMessages2.log are moved to AdminMessages3.log. When all three are full, the next transfer deletes the contents of AdminMessages3.log.

Additional information about IC* messages at install

Most of the IC* messages that appear at install time are single-line, self-explanatory messages. However, for some messages there is additional information.

IC0259

Message IC0259 provides a TMAPI.ERROR error code, which indicates that there is a problem accessing the topology server.

If the error that caused one of these messages is transitory, such as a network outage, you can reissue TMAPI commands from the <install_directory>\bin directory using the syntax from the biz_wrapper.log file in the Windows Winnt directory.

0 Command completed OK

Explanation: All OK

System Action: Whatever the command was, it worked.

User Response: None.

1 Computer System not found

Explanation: A command was issued that passed a computer system. The computer system identified by the hostname passed could not be found in the topology.

System Action: The command halted without further progress.

User Response: Depends on how the command was issued. Normally this would be a programming problem where the wrong value was passed. Use bizTmapiUtility -list >topology.list to look at the topology and see if the computer system is present.

2 Facility not found

Explanation: A command was issued that passed a facility. The facility identified by the facility id passed could not be found in the topology (on the computer system that was also passed if appropriate).

System Action: The command halted without further progress.

User Response: Depends on how the command was issued. Normally this would be a programming problem where the wrong value was passed. Use bizTmapiUtility -list >topology.list to look at the topology and see if the computer system is present. This may be an expected return code in some cases.

3 Product not found

Explanation: A command was issued that passed a product id. The product identified by the product id passed could not be found in the

topology (on the computer system that was also passed).

System Action: The command halted without further progress.

User Response: Depends on how the command was issued. Normally this would be a programming problem where the wrong value was passed. Use bizTmapiUtility -list >topology.list to look at the topology and see if the product id is present. This may be an expected return code in some cases.

---

4 Artifact not found

Explanation: A command was issued that passed an artifact id. The product identified by the artifact id passed could not be found in the topology (on the computer system and product that was also passed).

System Action: The command halted without further progress.

User Response: Depends on how the command was issued. Normally this would be a programming problem where the wrong value was passed. Use bizTmapiUtility -list >topology.list to look at the topology and see if the artifact id is present. This may be an expected return code in some cases.

---

5 Property not found

Explanation: A command was issued that passed a property. The property identified by the property id passed could not be found in the topology.

System Action: The command halted without further progress.

User Response: Depends on how the command was issued. Normally this would be a programming problem where the wrong value was passed. Use `bizTmapiUtility -list >topology.list` to look at the topology and see if the property is present on the object being accessed.

---

6 Too many computer systems found

Explanation: A command was issued that passed a computer system. More than one computer system in the topology has the same hostname.

System Action: The command halted without further progress.

User Response: Use `bizTmapiUtility -list >topology.list` to look at the topology and see if the hostname appears more than once. You will need to reinstall your complete topology to remove this problem.

---

7 Bad hostname

Explanation: A command was issued that passed a computer system. The hostname passed could not be resolved by a nameserver.

System Action: The command halted without further progress.

User Response: Define the hostname to the local nameserver.

---

10 General error

Explanation: A general error has occurred in accessing the topology repository.

System Action: The command halted without further progress.

User Response: Look at the `AdminMessages.log` file for more information. Use `bizTmapiUtility -diagnose` to determine the problem. Try rebooting the Base machine and the local machine. If problem persists contact your support representative.

---

11 Wrong number of arguments

Explanation: A command has been passed with the wrong number of arguments.

System Action: The command did not complete.

User Response: Use the correct number of parameters.

12 Incorrect command

Explanation: A put or get command is expected. Neither of these commands was issued.

System Action: The command did not complete.

User Response: Use `bizTmapiGet` or `bizTmapiPut` to call `TmapiCommand`.

13 Command type incorrect

Explanation: The command type (for example, FacilityInstallState, Topology, FacilityHostname) is not recognized.

System Action: The command did not complete.

User Response: Use an expected command type.

14 Authorization failed

Explanation: The username and password are not correct.

System Action: The command halted without further progress.

User Response: Check the username and password in the Tmapi.properties file. These must match the values specified on the HTTP Server on the base machine (see httpd.conf). Use bizTmapiUtility -diagnose to check the problem has been fixed.

15 Topology locked

Explanation: The topology is locked by another user.

System Action: The command halted without further progress.

User Response: Rerun when the topology is not being used. If no other user is using the topology server then use `bizTmapiUtility -unlock` to force the topology file to be unlocked. Or delete the `lockdb.dir` and `lockdb.pag` files in the IBM Http `Server/logs` directory.

16 Not locked by user

Explanation: The topology is about to be updated but it is not locked by this user.

System Action: The command halted without further progress.

User Response: Look at the `AdminMessages.log` file for more information. Use `bizTmapiUtility -diagnose` to determine the problem. Try rebooting the Base machine and the local machine. If problem persists contact your support representative.

17 Not locked

Explanation: The topology is about to be unlocked but it is not locked.

System Action: The command halted without further progress.

User Response: Look at the `AdminMessages.log` file for more information. Use `bizTmapiUtility -diagnose` to determine the problem. Try rebooting the Base machine and the local machine. If problem persists contact your support representative.

18 Connection failed

Explanation: A connection to the topology server failed.

System Action: The command halted without further progress.

User Response: Look at the `AdminMessages.log` file for more information. Use `bizTmapiUtility -diagnose` to determine the problem. Try rebooting the Base machine and the local machine. It may be caused by a network problem. If problem persists contact your support representative.

Appendix B. Configuration details

This chapter provides detailed information of the configuration batch file processing that takes place during post-installation configuration. It adds to the information provided in "Chapter 7. Configuring the products after installation" on page 57, which describes the configuration in terms of your input to the process. The following sections will help you to understand the configuration process, if you need to. Many users will not have to refer to this information.

How the configuration works

Before the sections that describe in some detail what happens during configuration, this section gives you an overview of the way configuration works.

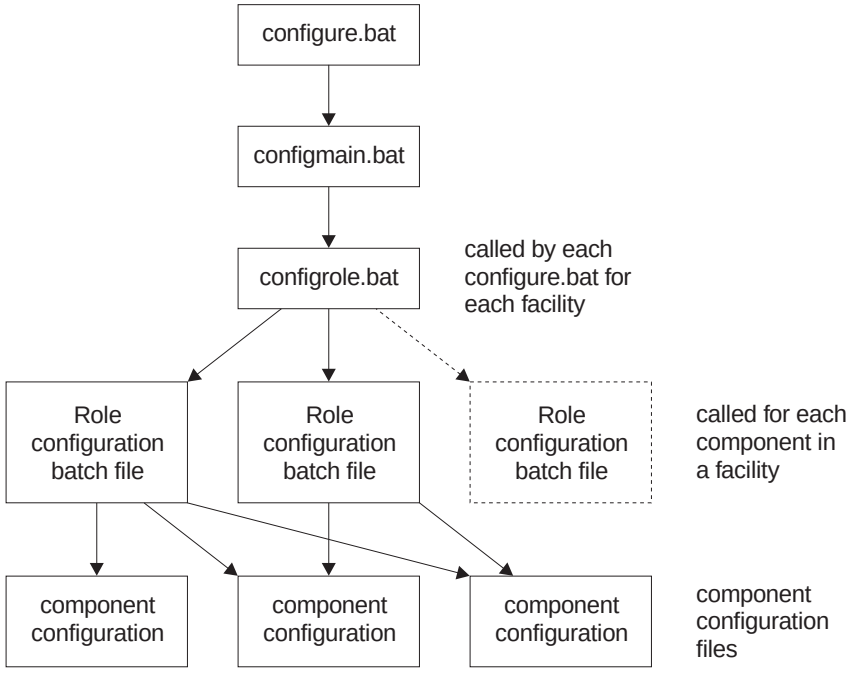


Figure 33. Overview of the configuration batch file

`Configure.bat` is a stub that sets up logging for the configuration process. It calls `configmain.bat`, which sets up directories and various topology entries. It controls the order in which the system is configured by calling `configrole.bat` with the required roles. `configrole.bat` calls the appropriate role configuration batch file, which will call one or several of the component configuration files as required to configure the components as necessary.

The configuration batch file cannot perform all of the necessary processing. It calls a support executable called Appender. “Appendix D. The Appender executable file” on page 129 describes its functions. The workings of Appender might be of interest if you want to follow the workings of the configuration batch files.

Configuration details for MQSeries products

The configuration batch file runs a number of batch files to configure the MQSeries products that are appropriate to this machine. There are up to five MQSeries products to configure.

MQSeries for Windows NT and MQSeries Publish/Subscribe

For MQSeries for Windows NT and MQSeries Publish/Subscribe, there are four configuration files.

ConfMQTAM.bat

This file configures MQSeries on the TAM (Entry) and TAMPlus (Enterprise). It:

1. Sets the hostname (%hostname%) from the computer name (%COMPUTERNAME%).
2. Pulls the cluster name (%cluster%) from the topology repository.
3. Sets the queue manager based upon the hostname and clustername (%hostname%.%cluster%)
4. Finds the port on which the queue manager will be listening (starting from 1414, the default MQSeries listening port). This is written into the topology as %mqport%.
5. Sets the name of the previously configured queue manager (%qmgr0%) to blank (no prior qmgr)
6. Sets the hostname of the machine where qmgr0 is configured (%mqhost0%) to the value of %hostname%. Although the queue manager name is blank, you need this name for configuring channel connections.
7. Configures MQSeries by calling ConfMQ.bat

ConfMQ.bat

This batch file is used to configure all roles, not just the TAM/TAMPlus facilities. It:

1. Creates an MQSeries log directory. The default log directory is `c:\mqm\log`. If you want to modify this, change the entry in the `configure.bat` batch file.
2. Creates the queue manager and checks the return code. If a terminal error occurs, configuration stops.
3. Starts the MQSeries queue manager and services
4. Copies standard MQSeries (for this implementation) configuration commands for the queue manager held in file `ConfMQ.mqs` to (temporary file) `Bizmq1.mqs`.
5. Appends commands to create the cluster sender and/or the receiver channels, based on the facility being configured to `\bizmq1.mqs`.
6. Configures Pub/Sub with a single command to start the broker for the queue manager (%qmgr%).

ConfMQ.mqs

This file contains the definitions for:

1. Creating default dead letter queue

2. Disabling channel events
3. Changing server connection channel to prevent unwanted client access
4. Defining administration connection

ConfMQother.bat

This file contains commands for configuring facilities other than TAM and TAMPlus. It:

1. Sets the hostname (%hostname%) from the computer name (%COMPUTERNAME%).
2. Pulls the cluster name (%cluster%) from the topology repository.
3. Generates the port that the queue manager will be listening on (starting from defaults of 1414, but we can't be certain this is available). Set mqport to this value, and write it into the topology repository.
4. Sets the queue manager based upon the hostname and clustername (%hostname%.%cluster%)
5. Obtains the port number on which the TAM or TAMPlus queue manager is listening from the topology.

MQSeries Integrator

MQSeries Integrator has a single configuration batch file, BIZ_mqsicfg. It:

1. Prompts for the MQSeries Integrator administration user ID and password.
2. Creates the user ID and adds it to the relevant MQSeries Integrator groups.
3. Obtains the db2admin user ID and password, which are held in %Db2user ID% and %Db2pswd%, because MQSeries Integrator uses DB2.
4. Pulls the hostname of the db2 server from the topology repository (db2 server is on TAM/TAMPlus).
5. Creates the default MQSeries Integrator databases (MQSIBKDB,MQSICMDB,MQSIMRDB)
6. Binds to the databases.
7. Updates the registry with the ODBC entries for the databases
8. Creates configuration manager
9. Creates broker
10. Starts the configuration manager
11. Starts the broker.

MQAK

There is no configuration to be run. The configuration of MQAK is done during the installation of MQAK and the B2BI managers.

MQSeries WorkFlow

During MQSeries WorkFlow configuration, some parameters take 'default' values. You can override these values by setting some environment variables before starting the configuration, either by writing a batch file to set the variables or by setting them through the NT control panel.

For WorkFlow Server:

BIZ_WFCONF=FMC	The name of the configuration ID for WorkFlow *
BIZ_WFPREF=FMC	The Queue Prefix *
BIZ_WFGRP=FMCGRP	The System Group *
BIZ_WFSYS=FMCSYS	The System *
BIZ_WFQMAN=FMCQMSV	The Queue Manager *
BIZ_WFCLUS=FMCGRP	The MQSeries Cluster *
BIZ_WFDB=FMCDB	The database
BIZ_WFPORT=5010	The port used for MQSeries *

The items marked '*' are stored in the topology because they are needed by the Client and the Java Agent. BIZ_WFSERVICE, the name of the NT Service, is also stored in the topology.

For WorkFlow Client:

BIZ_WFCONF=FMC	The name of the configuration ID
BIZ_WFQMAN=FMCQMCL	The Queue Manager
BIZ_WFPORT=5010	The port used for MQSeries

For WorkFlow Java Agent:

BIZ_WFCONF=FMC	The name of the configuration
BIZ_WFQMAN=FMCQMJV	The Queue Manager
BIZ_WFPORT=5010	The port used for MQSeries
BIZ_WFAGENT=MQWFAGENT	The name of the Agent

Configuration details for Policy Director

The configuration batch file configures Policy Director if appropriate to this machine.

Configuring on the TAMPlus facility

When the configuration of TAMPlus is started, Policy Director is configured in the following way. The batch file:

1. Asks you for the username and password of the LDAP server, if the LDAP username and password has not been defined previously in the LDAP configuration.
2. Asks you to generate a new username and password for DCE.
3. Asks you to generate a new Policy Director password.

   When these are collected, the script continues to configure Policy director.
4. The SecureWay Directory (LDAP) service is started.
5. The default Policy Director Schema (secschema) is added to LDAP.
6. The Policy Director suffix (secAuthority=Default) is added using a ldif file.
7. The DCE cell is configured using a cell name of hostname_cell and is set to autostart. It configures the Security Server and Cell Directory Server.
8. NetSEAT is configured using the cell name configured above.
9. The Policy Director Runtime Environment has now been configured with a DN of o=epic.
10. The Policy Director Management Server has now been configured using the SSL listening port of 7135, a SSL certificate lifetime of 365 days, and a connection timeout of 7200 seconds.
11. **After configuration of the TAMPlus facility, right click on the NetSeat icon and select properties. Enable GSS and SSL and press configure, check that the machine name is correct and press OK and then OK again.**

Configuring on the Integrated Console Plus facility

The configuration batch file calls the Policy Director Console script to configure the console.

1. Before the configuration files are run on the ICPlus the `pdacert.b64` file must be copied from the TAMPlus facility, imported onto the ICPlus facility, and saved to the `<PDDir>\ivmgrd\Keytabs` folder
2. The runtime environment is configured using the `pdcacert.b64` file that is created on the TAMPlus facility.

Configuring on the BFM Application Server Plus facility

The configuration batch file calls the Policy Director Runtime script to configure the runtime environment.

1. Before the configuration files are run on the ICPlus, the `pdacert.b64` file must be copied from the TAMPlus facility, imported onto the ICPlus facility, and saved to the `<PDDir>\ivmgrd\Keytabs` folder .
2. The runtime environment is configured using the `pdcacert.b64` file that is created on the TAMPlus facility.

Configuration details for WebSphere products

The configuration batch file runs a number of batch files to configure the WebSphere products appropriate to this machine.

Note that the installation of WebSphere Application Server Personalization is a manual step after the configuration batch file has run.

WebSphere Application Server

A WebSphere Business Integrator deploy default application server is imported to WebSphere by `db2cliws.bat`to configure WebSphere Application Server.

WebSphere DataInterchange Server

The DataInterchange batch file configuration consists of the following:

1. Three databases are created on the TAMPlus Facility. The databases are:

   Ediec31e
   Edict31e
   Config32
2. The first two databases then have they default parameters changed in relation to the log file size and number of primary and secondary logs.
3. The databases are then bound.
4. The tables and views are now set up with the data from the ddl files in the ddl directory.
5. Grant statements are then issued to the first two databases for access from the DI client to the databases.
6. Data is then loaded into the tables set up earlier. The ixf files are used in the data directory.
7. Grant statements are then run so that the DataInterchange Server can access the tables in the database.

The configuration is now complete.

Installation preparation and configuration details for PAM and PAV

`configrole.bat` calls `PrePAMconfig.bat`, if there is a PAM or PAV facility in the topology.

PrePAMconfig.bat

PrePAMconfig.bat calls four other batch files, which each configures a product or group of products:

1. `baseconfig.bat` configures the base products on the PAM facility – for instance, MQSeries or JMS.
2. `Http.bat` configures IBM HTTP Server.

3. db2cliws.bat configures DB2 and WebSphere
4. PAM.bat runs the pre-PAM configuration.

PAM.bat

PAM.bat is mainly used to set up all the parameters needed for the WSBIPAM database creation – for instance, newdb.bat

1. The first parameter it gets, DB2_SERVER_DIR, involves querying the topology repository.
2. The DB_INSTANCE parameter is then set to WSBIPAM.
3. DB_USERNAME is hard coded to db2admin. This must exist and the corresponding password must be entered when prompted for; otherwise, the importation of stored procedures, as part of the DB2 Schema, will not work later on.
4. Three .jar files are moved from the \config directory to the appropriate place under the Java directory. These are required by PAM later on.
5. A new remote DB2 connection is created, which will be used by PAM to access the DB2 server.
6. The database name defaults to WSBIPAM, but, if a database of this name exists, a new name is prompted for.
7. The batch file newdb.bat is called. This file creates the database that PAM requires.

Appendix C. Configuration details for PAM and PAV

This chapter provides detailed information about the batch file processing that takes place during post-installation configuration of PAM and PAV. It adds to the information provided in “Chapter 8. Further installation and configuration” on page 63, which describes the configuration in terms of your input to the process. The following sections will help you to understand the configuration process, if you need to. Many users will not have to refer to this information.

PAMxml.bat

The main purpose of the `PAMxml.bat` file is to configure WebSphere so that it can run PAM as an application within WebSphere. It also does some supplementary actions, including setting the PAM install path in the topology repository and configuring the NT services associated with PAM.

1. The `PAMxml.bat` file takes two parameters - the PAM partner ID and the PAM administration password.
2. The batch file first sets the path to include the `appender.exe`. It locates the main Business Integrator installation, and sets up a log file called PAMXML.log in the main Business Integrator logs directory.
3. The PAM Adapter Server NT service is altered to depend, not on PAM’s NT service, but on WebSphere’s NT service, IBM WebSphere AdminServer. The PAM NT service is disabled, because it is no longer required.
4. The hostname for the machine is captured for later use.
5. The topology repository is updated to include the directory where PAM is installed.
6. The WebSphere installation on the current machine is found and the path is stored as an 8.3 formatted directory name in an NT variable (BIZ_WSDIR).
7. The `.xml` file used in configuring PAM with WebSphere is located and moved to the `BIZ_WSDIR\bin` directory.
8. The WebSphere Administration Node Name and Node Name are initialized to be the hostname of the machine.
9. The ’Alliance’ directory, under the main PAM directory, is located to be used in the forthcoming xmlconfig call.

10. Given the Partner ID, which is passed as a parameter to the file, the location of the PartnerXXXX directory, again under the PAM directory, can be established and used in the xmlconfig file. It is stored in 8.3 format.
11. The administration password of PAM is collected from the command line.
12. The platform is FIXED to enable operation on Windows NT. The servlet engine name, web application name, application server name as all set using FIXED values.
13. DB2 is located on the machine and the install path is stored as a parameter.
14. Java is also located, and the install path stored as a parameter. The `xmlconfig` utility is run from within `BIZ_WSDIR\bin` using as parameters some of the variables set earlier in the batch file.

pav_channel_command.bat

The main purpose of `pav_channel_command.bat` is to configure WebSphere so that it can run the PAV channel as an application within WebSphere. It doesn't take any parameters.

1. The batch file first sets the path to include the `appender.exe`.
2. It locates the main Business Integrator installation, and sets up a log file called `pav_channel_command.log` in the main Business Integrator logs directory.
3. The hostname for the machine is captured for later use.
4. The topology repository is updated to include the directory where PAM is installed.
5. The WebSphere installation on the current machine is found and the path is stored as an 8.3 formatted directory name in an NT variable (BIZ_WSDIR).
6. The .xml file used in configuring PAM with WebSphere is located and moved to the `BIZ_WSDIR\bin` directory.
7. The WebSphere Administration Node Name and Node Name are initialized to be the hostname of the machine.
8. The servlet engine name, web application name, application server name as all set using FIXED values. These values are the same as the one described in `PAMxml.bat`.
9. The `xmlconfig` utility is run from within `BIZ_WSDIR\bin` using as parameters some of the variables set earlier in the batch file.

pav_ws_command.bat

pav_ws_command.bat configures WebSphere so that PAV can operate as a WebSphere application. It has four parameters: the directory where PAV is installed, the virtual root, the PAV channel ID and the Partner ID assigned to the PAV partner.

1. The batch file first sets the path to include the appender.exe.
2. It locates the main Business Integratorinstallation, and sets up a log file called pav_ws_command.log in the main Business Integrator logs directory.
3. The hostname for the machine is captured for later use.
4. The WebSphere installation on the current machine is found and the path is stored as an 8.3 formatted directory name in an NT variable (BIZ_WSDIR).
5. The .xml file used in configuring PAV with WebSphere is located and moved to the BIZ_WSDIR\bin directory.
6. The WebSphere Administration Node Name and Node Name are initialized to be the hostname of the machine.
7. The servlet engine name, web application name, application server name as all set using FIXED values.
8. The PAV installation directory is set using the parameter from the command line.
9. The virtual root is also set using a value passed as a parameter.
10. The virtual root URI and resource location are set using the same parameter.
11. The channel ID and Partner ID are set as variables, ready to be passed to xmlconfig.
12. The xmlconfig utility is run from within BIZ_WSDIR\bin using as parameters some of the variables set earlier in the batch file.

Appendix D. The Appender executable file

The configuration batch files, described in “Chapter 7. Configuring the products after installation” on page 57 and in more detail in “Appendix B. Configuration details” on page 117, use functions from a support executable called Appender. Unless you are particularly interested in the way configuration works, you will not have to study this appendix.

The functions in Appender, the command line to exercise the function, the function description, and examples follow.

Function: a - Append one file to another

Description: Appends the contents of a file to the end of another file. The file that is appended is unchanged.

Usage: appender a <FileToAppend><File to append to>

Example:appender a ″%temp%\ssl.txt″ ″c:\program files\ibm http server\conf\httpd.conf″

Function: b - Get the WSBI roles and save them in a batch file, space delimited

Description: Reads the list of roles from the registry for WSBI and saves them as a space delimited list in a batch file. The batch file can be run to set the BPIPROLES environment variable.

Usage: appender b <registry key><batch file>

Function: c - Comment out a line in a file

Description: Reads an input file and places characters at the beginning of the line specified. Can be used to prefix lines in a file. The original file will be modified.

Usage: appender c <comment characters><Line to comment><file to process>

Example: appender c ″#″ ″my test line″ ″c:\program files\my file.txt″

Function: d - Strip the drive from a fully qualified path

Description: Strips the drive letter from any drive/file path. The resulting environment variable will terminate with a ’:’ Sets the BPIPCONFIG environment variable.

Usage: appender d<path><batch file to create>

Example:

```
appender d "c:\program files\my file.txt" %temp%\~tmp.bat
call %temp%\~tmp.bat
del %temp%\~tmp.bat
```

The environment variable BPIPCONFIG will now be set to c:

Function: e - Echo replacement - Appends a line to a file

Description: Echoes a string to a file. Used to overcome some of the failings in the normal echo command when special characters are used.

Usage: appender e<line to echo><file to append to>

Example:appender e "#SSL Support" %temp%\ssl.txt

Function: f - Replace one string with another

Description: Replaces all occurrences of one string in a file with another. Optionally writes the output to a new file. If a new file is not specified then the original file is overwritten with the changed file.

Usage: appender f<string to find><string to replace><file to process><optional file to write to>

Example:appender f @[BIZ_mqakdir] "c:\program files\mqak" "c:\mydir\bin\bizSetEnv.bat"

All occurrences of '@[BIZ_mqakdir]' will be replaced with 'c:\program files\mqak'

Note: You cannot use %variable% as a replaceable parameter as batch files interpret these as variables.

Function: g - Get a Username and password from the user using an input box

Description: Creates a Windows input box that allows the user to enter a username and password as a hidden string. The title of the box is passed in to the function and is displayed on the title bar of the input box. The user input is saved as BIZ_USER and BIZ_PW..

Usage: appender g<Title of input box><batch file to create>

Example:

```
appender g "Input LDAP Username and Password" %temp%\~tmp.bat
call %temp%\~tmp.bat
del %temp%\~tmp.bat
```

BIZ_USER and BIZ_PW will now be set to the users input.

Function: h - Get the first CD Rom drive letter

Description: Retrieves the FIRST CD Rom drive letter and saves it as variable CDROM. If no CD Rom is found the variable will be blank. The output is the CD rom drive letter ONLY.

Usage: appender h<batch file to create>

Example:

```
appender h %temp%\~tmp.bat
call %temp%\~tmp.bat
del %temp%\~tmp.bat
```

CDROM will now be set to the CD Rom drive letter.

Function: i - Insert a line into an existing file at a defined location

Description: Inserts a string into a file after the search string

Usage: appender i<File to insert into><String to search for><String to insert>

Example: appender i ″c:\myfile\etc\slapd32.conf″ ″ibm-slapdSuffix: cn=localhost″ ″ibm-slapdSuffix: o=ePIC″

Function: k/K Case change a string

Description: k/K Case change a string

Usage: appender k<String to change><String to search for><String to insert>

Example:

```
appender k ″My String″ %temp%\~tmp.bat
call %temp%\~tmp.bat
del %temp%\~tmp.bat
```

BIZ_STR will now contain 'my string'

Function: l - Log string to log file with date/time stamp

Description: Write a string to a file. Prefix it with a date/time.

Usage: appender l<string to log><log file>

Example:

```
appender l ″My Log String″ %temp%\log.txt
Log.txt will contain the string:
[09:12:20 03/08/01] My Log String
```

Function: p - Get a password from the user using an input box

Description: Creates a Windows input box that allows the user to enter a hidden string. The title of the box is passed in to the function and is displayed on the title bar of the input box. The user input is saved as BIZ_PW.

Usage: appender p<Title of input box><batch file to create>

Example:

```
appender p ″Input Password for Username Bloggs″ %temp%\˜tmp.bat
call %TEMP%\˜tmp.bat
del %TEMP%\˜tmp.bat
```

Function: q - command retrieves an entry from the NT registry HKEY_CURRENT_USER

Description: Retrieves a registry entry from the HKEY_CURRENT_USER tree. A batch file is created with the environment variable BPIPCONFIG set.

Usage: appender q<key to search><entry to retrieve><batch file to create>

Example:

```
appender r ″SOFTWARE\IBM\Mysoftware\CurrentVersion″ InstallPath
                    %temp%\˜tmp.bat
call %temp%\˜tmp.bat
del %temp%\˜tmp.bat
```

The value of the InstallPath key will now be available in the BPIPCONFIG environment variable.

Function: r - command retrieves an entry from the NT registry HKEY_LOCAL_MACHINE

Description: Retrieves a registry entry from the HKEY_LOCAL_MACHINE tree. A batch file is created with the environment variable BPIPCONFIG set.

Usage: appender r<key to search><entry to retrieve><batch file to create>

Example:

```
appender r ″SOFTWARE\IBM\Mysoftware\CurrentVersion″ InstallPath
                    %temp%\˜tmp.bat
call %temp%\˜tmp.bat
del %temp%\˜tmp.bat
```

The value of the InstallPath key will now be available in the BPIPCONFIG environment variable.

Function: s - Changes a service startup to Automatic

Description: Changes an NT service startup to Automatic

Usage: appender s<Service name>

Example: appender s ″IBM Secureway Directory V3.2″

Function: t - Get a path using an input box

Description: Creates a Windows input box that allows the user to enter a string. The title of the box is passed in to the function and is displayed on the title bar of the input box. The user input is saved as BIZ_PATH.

Usage: appender t<Title of input box><batch file to create>

Example:

```
appender t ″Input location of Input File″ %temp%\˜tmp.bat
call %temp%\˜tmp.bat
del %temp%\˜tmp.bat
```

Environment variable BIZ_PATH will now be set to the users input.

Function: u - Convert paths from NT to UNIX style

Description: Converts each occurrence of '\' with '/' to create UNIX style paths. The output of the conversion is written to the file specified.

Usage: appender u<input string><file to write to>

Example:

```
appender u ″keyfile c:\program files\key.kdb″ %temp%\ssl.txt
```

File %temp%\ssl.txt will contain the string keyfile c:/program files/key.kdb

Function: v - Show version information

Description: Outputs the version of the Appender program.

Usage: Appender v

Function: x - Convert a decimal to hex

Description: Converts a decimal value to its hex equivalent and stores it in the BIZ_HEX variable.

Usage: Appender x<Value to change><Value to change>

Example:

```
appender x ″1020″ %temp%\˜tmp.bat
call %temp%\˜tmp.bat
del %temp%\˜tmp.bat
```

Environment variable BIZ_HEX will now be set to 3FC.b

Appendix E. Notices

This information was developed for products and services offered in the U.S.A.

IBM may not offer the products, services, or features discussed in this document in other 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.

For license inquiries regarding double-byte (DBCS) information, contact the IBM Intellectual Property Department in your country or send inquiries, in writing, to:

IBM World Trade Asia Corporation Licensing
2-31 Roppongi 3-chome, Minato-ku
Tokyo 106, Japan

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

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

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

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

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

IBM United Kingdom Limited
Intellectual Property Department
Hursley Park
Winchester SO21 2JN
United Kingdom

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 information 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 measures may have been made on development-level systems, and there is no guarantee that these measurements will be the same on generally available system. Furthermore, some measurements may have been estimated through extrapolation. Actual results may vary. Users of this document should verify the application data of 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 claim related to non-IBM products. Questions on 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 include 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.

Trademarks

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

- DB2
- IBM
- MQSeries
- SecureWay
- WebSphere

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

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

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

Bibliography

This bibliography lists the books in the IBM WebSphere Business Integrator and associated libraries.

IBM WebSphere Business Integrator library

The Business Integrator library consists of the following books:

- *WebSphere Business Integrator Concepts and Planning, GC34-5960*

  This book introduces the Business Integrator system, providing a high-level system overview, defining the system capabilities, and describing its value to e-businesses. This book also provides the information that you need to plan the installation of Business Integrator.

- *WebSphere Business Integrator Installation Guide, GC34-5961*

  This book is a guide to installing and configuring Business Integrator, It contains information about:

  – Selecting your required topology
  – Installing and configuring the base products and software components of Business Integrator on each machine in the topology
  – Installing and configuring firewalls and proxies

- *WebSphere Studio Business Integrator Extensions Installation Guide, SC34-5962*

  This book is a guide to installing and configuring Solution Studio, It also contains information about setting up clients and servers, and creating projects.

- *WebSphere Business Integrator Run Time*

  This book is a comprehensive guide to the Business Integrator runtime system, providing the following information:

  – Detailed conceptual information about the runtime components of Business Integrator.
  – Deployment of solutions to the runtime system
  – System administration, such as starting and stopping software components and base products, defining users, and using the Exception Console.
  – General problem determination information, including how to trace and debug, and information on obtaining help from technical support

- *WebSphere Business Integrator Messages*

  This book lists the error messages that are produced by Business Integrator and provides references to the documentation for the messages of base products.
- *WebSphere Studio Business Integrator Extensions Developer's Guide*

  This book describes how to create a Business Integrator solution, beginning with the solution design phase, to the solution implementation phase, and finally the solution deployment phase using a sample business problem. This book also provides procedures for assembling a Business Integrator solution in the run-time environment and a description of how to use the Solution Studio for solution design and implementation.
- *WebSphere Business Integrator DataInterchange for Windows NT User's Guide, SC34-5963*

  This book is a guide to installing and using DataInterchange, in the Business Integrator environment.

You can find the latest versions of the books at the following Web site:

`http://www-4.ibm.com/software/webservers/btobintegrator/`

This site contains links to the Web sites of the underlying products of IBM WebSphere Business Integrator.

Related documentation

The `utilities` subdirectory on the Documentation CD contains documentation about utilities that can prove useful in building and running solutions. This documentation is not available on the IBM WebSphere Business Integrator Web site.

WebSphere Business Integrator also provides a number of external application programming interfaces (API). HTML documentation that is generated using the Javadoc tool is provided for these APIs. For a list of the APIs, refer to the *WebSphere Business Integrator Run Time* book.

WebSphere Partner Agreement Manager library

The Partner Agreement Manager Version 2 Release 1 library consists of:

- *Partner Agreement Manager Installation Guide*, GC34-5964
- *Partner Agreement Manager Administrator's Guide*
- *Partner Agreement Manager User's Guide*
- *Partner Agreement Manager Adapter Developer's Guide*
- *Partner Agreement Manager Script Developer's Guide*
- *Partner Agreement Manager API Guide*
- *Partner Agreement Manager Adapters for MQSeries User's Guide*
- *Partner Agreement View User's Guide*, GC34-5965
- *WebSphere Partner Agreement Manager Business Process Integration Adapter Guide.*

DataInterchange library

The DataInterchange Version 3 Release 1 library consists of:

- *DataInterchange Client User's Guide*, SB34-2010
- *DataInterchange Administrator's Guide*, SB34-2002
- *DataInterchange Installation Guide*, GB09-8070
- *DataInterchange Messages and Codes*, SB34-2000
- *DataInterchange Programmer's Reference*, SB34-2001

Other Libraries

You can find important information in the libraries of the following products:

- DB2® UDB
  - *IBM DB2 Universal Database Quick Beginnings Version 6.1* , S10J-8149
- MQSeries®
  - *MQSeries for Windows NT Quick Beginnings*, GC34-5389
  - *MQSeries System Administration*, SC33-1873
  - *MQSeries Using Java*, SC34-5456
  - *MQSeries MQSC Command Reference*, SC33-1369
  - *MQSeries Queue Manager Clusters*, SC34-5349
  - *MQSeries Integrator Introduction and Planning*, GC24-5599
  - *MQSeries Workflow Getting Started with Buildtime*, SH12-6286
  - *MQSeries Workflow Getting Started with Runtime*, SH12-6287
  - *MQSeries Adapter Kernel for Multiplatforms: Quick Beginnings*, GC34-5855
  - *MQSeries Adapter Kernel for Multiplatforms: Problem Determination Guide*, GC34-5897

  - *MQSeries Adapter Builder for Windows NT: Using the Control Center*, GC34-5882
- SecureWay®
  - *SecureWay Policy Director Up and Running*, SCT6-3KNA
  - *SecureWay Policy Director Base Administration Guide*
  - *SecureWay Firewall User's Guide*, CG31-8658
- VisualAge®
  - *VisualAge Java, Enterprise Edition Getting Started*
  - *VisualAge C++ Professional for Windows NT Getting Started*
- WebSphere™ Application Server
  - *Introduction to WebSphere Application Server*, SC09-4430

Index

R

S

T

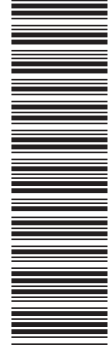
U

W

Part Number: BIZAAB00

Printed in the United States of America
on recycled paper containing 10%
recovered post-consumer fiber.

(1P) P/N: BIZAAB00



GC34-5961-00