WebSphere Portal V4.1
AIX 5L Installation

Install and administer WebSphere Portal in an AIX environment

Understand options and implications of Setup Manager

AIX considerations for WebSphere Portal

Rufus Credle
Denise Hendriks
Sunil Hiranniah
Gord Niguma
Dwight Norwood
Roshan Rao
Bernhard Stimpfle

ibm.com/redbooks
Note: Before using this information and the product it supports, read the information in “Notices” on page v.
Contents

Notices ................................................................................................................................. v
Trademarks .......................................................................................................................... vi

Preface .................................................................................................................................. vii
The team that wrote this Redpaper ..................................................................................... vii
Become a published author ................................................................................................. ix
Comments welcome ........................................................................................................... ix

Chapter 1. Overview ........................................................................................................... 1
1.1 Introduction ..................................................................................................................... 1
1.2 WebSphere Portal components ...................................................................................... 3
  1.2.1 WebSphere Portal Enable ....................................................................................... 3
  1.2.2 WebSphere Portal Extend ....................................................................................... 4
  1.2.3 WebSphere Portal Experience ................................................................................ 5
1.3 WebSphere Portal infrastructure ................................................................................... 6
  1.3.1 WebSphere Portal runtime process flow ................................................................. 6

Chapter 2. Considerations for WebSphere Portal in AIX environment ............................. 9
2.1 Server setup .................................................................................................................... 9
2.2 Remote display .............................................................................................................. 10
2.3 Setup of AIX prerequisites ........................................................................................... 11
  2.3.1 Installation of non-default packages ....................................................................... 11
  2.3.2 Resizing the file systems ........................................................................................ 13
  2.3.3 Announcing a CD-ROM drive to the operating system ......................................... 14
  2.3.4 Upgrading to latest maintenance level .................................................................... 15
  2.3.5 Network setup ........................................................................................................ 15
2.4 Installation planning worksheet ..................................................................................... 15
2.5 Consideration for LDAP ............................................................................................... 19
  2.5.1 Creation of a Lightweight Directory Interchange Format (LDIF) file ..................... 19
  2.5.2 Determine a reasonable LDAP structure for WebSphere Portal .......................... 20

Chapter 3. WebSphere Portal installation using WebSphere Portal Setup Manager ........ 23
3.1 WebSphere Portal Setup Manager ................................................................................ 23
  3.1.1 Information collection for WebSphere Portal installation ....................................... 23
  3.1.2 IBM HTTP Server configuration ........................................................................... 27
  3.1.3 IBM SecureWay Directory Server configuration .................................................... 28
  3.1.4 WebSphere Application Server configuration ........................................................ 30
  3.1.5 Personalization Server configuration ..................................................................... 33
  3.1.6 WebSphere Portal configuration ............................................................................ 33
  3.1.7 Last configuration steps ........................................................................................ 42
3.2 WebSphere Portal installation process ......................................................................... 43

Chapter 4. Post-installation instructions .......................................................................... 51
4.1 DB2 Universal Database ............................................................................................... 51
  4.1.1 Updating WebSphere Portal database configuration ............................................. 51
  4.1.2 Removing unnecessary databases ......................................................................... 53
  4.1.3 Starting and stopping DB2 Universal Database .................................................... 54
4.2 WebSphere Application Server ...................................................................................... 54
  4.2.1 Updating sas.client.props ...................................................................................... 54
4.2.2 Starting and stopping applications from the command line......................... 55
4.3 SecureWay Directory .................................................................................. 56
  4.3.1 Apply SecureWay 3.2.2 eFix 2 ................................................................. 56
  4.3.2 Stopping and starting SecureWay Directory ........................................... 56
4.4 Changing passwords .................................................................................... 56
  4.4.1 Change password for wpsadmin .............................................................. 57
  4.4.2 Change password for wpsbind ............................................................... 57
  4.4.3 Change password for DB2 user wasuser ............................................... 60
  4.4.4 Change password for LDAP Admin user cn=ldapadmin ....................... 65
  4.4.5 Change password for the users ldapdb2, ldap .................................. 67
  4.4.6 Change password for the users db2as, db2fenc1, db2inst1 .................... 67
  4.4.7 Change password for the user httpd .................................................... 67
  4.4.8 Change LTPA password of WebSphere Application Server Security ........ 68

Related publications .......................................................................................... 69
IBM Redbooks .................................................................................................. 69
Referenced Web sites ......................................................................................... 69
How to get IBM Redbooks ................................................................................ 70
IBM Redbooks collections .................................................................................. 70
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.

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 the 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.

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

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

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

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

AIX®, AIX 5L™, Database 2™, DB2®, DB2 Universal Database™, Hummingbird®, IBM®, IBM eServer™, Perform™, pSeries™, Redbooks® (logo), RS/6000®, Secureway®, SP®, Tivoli®, VisualAge®, WebSphere®, xSeries™

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

Lotus®, Lotus Notes®, Notes®, Sametime®, Domino™, iNotes™, Lotus Discovery Server™, Lotus Sametime™, QuickPlace™

The following terms are trademarks of other companies:

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

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

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

C-bus is a trademark of Corollary, Inc. in the United States, other countries, or both.

UNIX is a registered trademark of The Open Group in the United States and other countries.

SET, SET Secure Electronic Transaction, and the SET Logo are trademarks owned by SET Secure Electronic Transaction LLC.

Other company, product, and service names may be trademarks or service marks of others.
This IBM Redpaper will help you plan, install and administer the *IBM WebSphere Portal Version 4.1.2 Enable offering* product in an IBM AIX 5L environment, so that existing enterprise applications can be accessed from portlets using the IBM WebSphere Portal product.

This Redpaper provides easy, step-by-step examples allowing you to rapidly deploy IBM WebSphere Portal Version 4.1.2 on AIX 5L — therefore, providing you with a solid foundation to begin importing and using existing portlets to access your enterprise applications. You will find the recommended process of using Setup Manager to install WebSphere Portal 4.1.2. In addition, you will find an in-depth description of the available options during the Setup Manager process.

A basic knowledge is assumed for AIX, LDAP Directory Services, WebSphere Portal, Java technologies such as servlets, as well as HTML and XML markup languages, and the terminology used in Web publishing.

---

**The team that wrote this Redpaper**

This Redpaper was produced by a team of specialists from around the world working at the International Technical Support Organization, Raleigh Center.
Rufus Credle is a Senior I/T Specialist and certified Professional Server Specialist at the International Technical Support Organization, Raleigh Center. He conducts residencies and develops redbooks about network operating systems, ERP solutions, voice technology, high availability and clustering solutions, Web application servers, pervasive computing, and IBM and OEM e-business applications, all running on IBM @server xSeries Servers. Rufus has held various positions during his IBM career, which have included assignments in administration and asset management, systems engineering, sales and marketing, and IT services. He holds a bachelor’s degree in Business Management from Saint Augustine’s College. Rufus has been employed at IBM for 22 years.

Denise Hendriks is a Managing Director and WebSphere Architect with Perficient, Inc. Denise has two bachelor’s degrees, one in Physics and one in Computer Science, followed by a master’s degree in Electrical and Computer Engineering. She joined IBM and spent ten years as a Lead Developer for VisualAge and WebSphere in various capacities. She has recently joined Perficient, Inc., where she makes extensive use of her skills as a Consultant in WebSphere and J2EE technologies.

Sunil Hiranniah is a Software Engineer and works for IBM Developer Relations Technical Support Center in Dallas, Texas. He has over five years of experience in the Software industry working for various commercial projects. He has ample experience with WebSphere Portal Server, WebSphere Application Server, J2EE, and databases. He has written and published extensively on the WebSphere family of products.

Gord Niguma is an IT Specialist for the Vancouver Innovation Centre in IBM Canada. He has six years of experience in the Web development field, working for customers such as Air Canada and the NHL Players Association. He holds a bachelor’s degree in Computer Science from Dalhousie University and a master’s degree in Computer Science from Simon Fraser University. His areas of expertise include portals and Web content management.

Dwight Norwood is a Director and Senior Consultant for Courtbridge Consulting Group, an IBM Business Partner located in East Granby, Connecticut. He has 30 years of experience in Information Technology, with 10 years of Lotus Notes and Domino experience. Along with a degree from the University of Notre Dame, he holds a master's degree in Computer Science from Rensselaer Polytechnic Institute and a master's degree in Business Administration from the University of Connecticut. He has written extensively on Notes and Domino development. He has special interests in enterprise knowledge management and publishing, and Web-related security.

Roshan Rao is a Software Developer with three years of experience in design and development of object oriented systems. He has a degree in Commerce from the University of Mumbai and is currently pursuing a master’s degree in Computer Science from Maharishi University of Management. His areas of expertise include Java technologies, messaging, and enterprise application development and integration.

Bernhard Stimpfle is a Solutions Architect for the Pervasive Computing Division in Boeblingen, Germany. He reviews architectures, implements customer-specific product add-ons, and supports major customers on-site in critical situations. He has spent eight years within the IT industry, working for DaimlerChrysler Aerospace and managing his own business. His area of expertise include pervasive computing, UNIX, Java 2 Enterprise Edition (J2EE) programming, and solution architectures. He is a Red Hat Certified Engineer (RHCE) and holds a Diplom-Ingenieur degree in Computer Science from the University of Cooperative Education in Ravensburg, Germany.
Thanks to the following people for their contributions to this project:

Juan R. Rodriguez, Consulting IT Professional  
IBM ITSO Raleigh

Daniel Carrera Martin, IT Specialist  
IBM Spain

Kayoko Suda, IT Specialist, System and Web Solution Center Technical Support  
IBM Japan

David Faller, Portal Development  
IBM Boeblingen

Ernest Davis, PvC Development  
IBM Raleigh

Jacob Vandergoot, WMS Development  
IBM Toronto

Gail Christensen, Cecilia Bardy, Diane O’Shea  
International Technical Support Organization, Raleigh Center

Become a published author

Join us for a two- to six-week residency program! Help write an IBM Redbook dealing with specific products or solutions, while getting hands-on experience with leading-edge technologies. You'll team with IBM technical professionals, Business Partners and/or customers.

Your efforts will help increase product acceptance and customer satisfaction. As a bonus, you'll develop a network of contacts in IBM development labs, and increase your productivity and marketability.

Find out more about the residency program, browse the residency index, and apply online at:  
ibm.com/redbooks/residencies.html

Comments welcome

Your comments are important to us!

We want our papers to be as helpful as possible. Send us your comments about this Redpaper or other Redbooks in one of the following ways:

▶ Use the online Contact us review redbook form found at:  
ibm.com/redbooks

▶ Send your comments in an Internet note to:  
redbook@us.ibm.com

▶ Mail your comments to:  
IBM Corporation, International Technical Support Organization  
Dept. HQ7  Building 662  
P.O. Box 12195  
Research Triangle Park, NC 27709-2195
Overview

IBM WebSphere Portal provides a single point of access to applications, application content, processes, and people in your network. In order to provide this unified access, WebSphere Portal implements rich and valuable functions.

This chapter presents an overview of the IBM WebSphere Portal Enable offering product and briefly introduces the architecture and wide variety of functions of the WebSphere Portal components.

In this chapter, the following topics are described:

- Introduction
- WebSphere Portal offerings and components
- Architecture

1.1 Introduction

IBM WebSphere Portal allows you to establish customized portals for your employees, Business Partners, and customers. As illustrated in Figure 1-1, the framework architecture implemented in this product provides a unified access point to internal and external Web applications as well as portal access to other legacy applications. In this way, users sign on to the portal and receive personalized Web pages.

![Figure 1-1 Horizontal and vertical portals](image)

The personalized single point of access to all necessary resources reduces information overload, accelerates productivity, and increases Web site usage. In addition, portals do much more; for example they provide additional valuable functions such as security, search, collaboration and workflow.
A portal delivers integrated content and applications, plus a unified, collaborative workplace. Indeed, portals are the next-generation desktop, delivering e-business applications over the Internet to all kinds of client devices.

IBM WebSphere Portal Version 4.1 has been designed in response to the following set of fundamental business objectives:

1. A single point of access to all resources associated with the portal domain
2. Personalized interaction with the portal services
3. Federated access to hundreds of data types and repositories, aggregated and categorized
4. Collaboration technologies that bring people together
5. Integration with applications and workflow system

IBM as well as some industry analysts have coalesced around the concept of horizontal and vertical portals. Horizontal portals are the primary infrastructure upon which a portal is built. Vertical portals are built upon the horizontal layer and represent a specific portal instance, usually defined by a major topic or domain.

As illustrated in Figure 1-2 on page 3, the horizontal portal infrastructure consists of several modular subsystems including:

- Presentation layer - A Web user interface plus pervasive device support
- Personalization - The ability to serve dynamic response to the user based on personal profiles
- Collaboration - Tools that allow e-mail, team rooms, shared places, etc. to be exchanged
- Portlets - A framework for easily attaching software modules (portlets) and services
- Applications and workflow - Integration of legacy and new applications
- Search and navigation - Categorizing repositories of content and searching them for relevant information
- Publish and subscribe - The ability to author new content and publish it to subscribers
- Administration and security - Basic Web site services such as page designers, performance monitors, cluster services, and metadata management
- Integration - Metadata sharing, XML, connectors, standards, EAI
WebSphere Portal provides additional services such as single sign-on, security, Web content publishing, search, personalization, collaboration services, enterprise application integration, support for mobile devices, and site analysis.

### 1.2 WebSphere Portal components

IBM WebSphere Portal provides three offerings, each designed to provide the infrastructure you need to build and deploy highly scalable portals. All three offerings share a common framework (the portal server) plus additional products and services. The portal server provides common services such as application connectivity, integration, administration, and presentation that are required across portal environment.

#### 1.2.1 WebSphere Portal Enable

The IBM WebSphere Portal Enable offering lets you quickly build highly scalable portals that simplify and speed your access to personalized information and applications. Portal Enable provides common services including:

- Connectivity and integration to allow access to enterprise data, external unsifted or even your trading partners’ applications.

**Figure 1-2  WebSphere Portal architecture**

**Note:** WebSphere Portal provides an extensible framework for interacting with enterprise applications, content, people, and processes. Self-service features allow end users to personalize and organize their own view of the portal, to manage their own profiles, and to publish and share documents with their colleagues.
Presentation and administration to enable computing desktop customization to match your own work patterns and needs, while providing:

WebSphere Portal
WebSphere Portal provides personalization, user management, security, and other services for constructing the portal site.

WebSphere Personalization
The WebSphere Personalization offering provides personalization technologies for targeting Web content to meet user needs and preferences:

- Rules-based personalization, where the business manager defines a set of business rules that determine which Web content is displayed for a particular user.
- Recommendations, using advanced statistical models and other matching techniques to extract trends from the behavior of Web site visitors. This approach adapts to changing trends in visitor interests without creating new business rules.
- Campaign management, for e-mail and Web-based promotions, such as enrollment offers or product introductions.

Web Content Publisher
This provides a browser-based interface that enables non-technical users to create, contribute and manage content on portals and Web sites in a simple and controlled manner. Features such as template management, workflow management, versioning and access control allow you to publish content quickly and efficiently providing end users access to the most up-to-date information when they need it.

WebSphere Studio Application Developer
These are professional developer tools for creating, testing, debugging, and deploying portlets, servlets, and other assets related to portals and Web applications.

1.2.2 WebSphere Portal Extend
The Portal Extend offering includes all products in the Enable offering and adds collaborative components and Web analysis coupled with additional tools to access, organize, and share information. Features include:

- Parallel, distributed, heterogeneous searching capability
- Individual and shared team workspaces with built-in collaborative capabilities
- Collaboration software components
- Web site analyses

Lotus Collaboration Components
Lotus Collaborative Components are building blocks (APIs and JSP tag libraries) for integrating the functionality of Lotus Domino, Lotus Sametime, Lotus QuickPlace, and Lotus Discovery Server into the portal. Developers can leverage the features of Lotus Domino, Lotus QuickPlace, Lotus Sametime, and Lotus Discovery Server, by using these components to add user interface extensions to their portlets and portal pages.

Lotus Collaborative portlets
This provides portal community services and portlets that help teams share portal pages, applications, documents, messaging, and other collaboration tools.
IBM Lotus Extended Search
This offering provides parallel, distributed, heterogeneous searching capabilities. It allows you to search Lotus Notes databases, legacy data stores, Web search sites, Microsoft Index Server, Site Server and Exchange 2000, as well as multiple Lotus Notes domains.

IBM Tivoli Web Site Analyzer
This offering analyzes Web content integrity and site performance, provides usage statistics, and analyzes portal server logs. Reports from Site Analyzer reveal information that can be used to improve the portal for a better user experience.

Lotus Discovery Server Integration
In addition, another concept that is key to WebSphere Portal Extend offering is the Lotus Discovery Server integration. When using Lotus Discovery Server with WebSphere Portal Extend or WebSphere Portal Experience, certain features are automatically enabled inside the portal. Examples of integration include additional menu options that appear when you click on a user name in a portlet, allowing you to perform actions such as searching for all documents by the user selected, or launching a profile of the user that is maintained and stored with the Discovery Server.

1.2.3 WebSphere Portal Experience
The Portal Experience offering includes all products in the Extend offering and adds additional tools and functionality including advanced collaboration, content management and security policy management, creating the most comprehensive portal offering in the market. Features include:
- Advanced collaboration features for e-meetings, application sharing, and whiteboarding (whiteboards are used in teleconferencing applications) enable effective online collaboration as well as the ability to take team rooms offline.
- Data storage for a broad spectrum of digital information including facsimiles, images, PC files, XML, and multimedia.
- Content infrastructure for applications including call center, high-volume claims processing, and accounts payable.
- Folder management and document workflow.
- Sample Java applications as well as advanced application development tools.
- Security policy management tools for e-business and distributed applications.

IBM Content Manager
This offering provides data store capabilities for a broad spectrum of digital business information, for example scanned images, facsimiles, PC files, XML files, and rich multimedia and Web content. Content Manager also provides folder management and document workflow. It provides the content infrastructure for applications from call centers, high-volume claims processing, and accounts payable, to e-commerce catalogues and e-learning.

IBM Tivoli Access Manager
Access Manager provides security policy management tools for e-business and distributed applications. It is a policy-based access control solution for e-business and enterprise applications.
1.3 WebSphere Portal infrastructure

IBM WebSphere Portal provides a framework that breaks the different portal components into portlets to accommodate the aggregation and display of diverse content. Each portlet is responsible for accessing content from its source (for example, a Web site, database, or e-mail server) and transforming the content so that it can be rendered to the client.

From a user's perspective, a portlet is a small window in the portal that provides a specific service or information. From an application development perspective, portlets are pluggable modules that are designed to run inside a portlet container of a portal server.

The portlet container provides a runtime environment in which portlets are installed and used. Portlets rely on the portal infrastructure to access user profile information, participate in window and action events, communicate with other portlets, access remote content, look up credentials, and store persistent data. The Portlet API provides standard interfaces for these functions. The portlet container is not a stand-alone container like the servlet container. Instead, it is implemented as a thin layer on top of the servlet container and reuses the functionality provided by the servlet container.

For more information about Portlet API, refer to the Portlet Development Guide at:

1.3.1 WebSphere Portal runtime process flow

After installation, the portal developer develops and deploys the portal to users. The developer alters the layout and appearance of the default portal page by selecting a theme and skins that WebSphere Portal provides, or by creating a page layout that matches a corporate standard. A portlet programmer writes and registers additional portlets by using the portlet API.

After the portal recognizes user data, a user can log on to the portal. If a user attempts a logon, the incoming request passes through an authentication layer that provides controlled access to the portal. If the logon is authenticated, a single sign-on component stores user information for later use by other programs that require authentication, and user information is placed in a data store, such as an LDAP directory or a relational database. Based on the user information, the portal framework retrieves the portal page layout and customization data from storage. WebSphere Portal processes the layout by generating markup for the portal page and rendering the portlets that are accessible to the user.

Figure 1-3 illustrates the runtime process flow in WebSphere Portal.
Figure 1-3  WebSphere Portal runtime process flow
Considerations for WebSphere Portal in AIX environment

This chapter provides guidelines, recommendations, and tips for installing WebSphere Portal software in an AIX environment.

The intention of this description is to provide as much background of the installation values as possible. Even though you may not find the exact mirror of your setup in one of the scenarios, the description should help to work through common problems.

2.1 Server setup

This section allows you to take into consideration those hardware and software factors that will allow you to setup and configure your WebSphere Portal solution for operation. The following hardware and software items listed here were used to build the WebSphere Portal solution illustrated in this Redpaper.

**Hardware**

The hardware used in these scenarios:

- IBM @server pSeries (RS/6000) 44p Model 170
  - 1x 450 MHz POWER3-II-Processor
  - 2 GB RAM
  - 2x 18 GB hard disk
  - 1x SCSI CD-ROM drive
  - 1x 100 Mbps Ethernet
  - 1x GXT300P Graphics Adapter

Installing WebSphere Portal on a machine that has less than 1 GB RAM is not recommended.

The amount of RAM should be sized dependent on the amount of software packages and the amount of Portlets and Portal add-ons that should go into the system. The same applies for processor speed and hard disk size. Generally more than one hard disk on a SCSI subsystem provides better performance, if they are reasonably configured.
Any network adapter can be used as long as there is a static IP address assigned to it.

It is reasonable to have a graphics adapter installed. If the target machine does not have a graphics adapter, make sure that all graphics-related AIX packages are installed, nevertheless.

**Tip:** To ensure that graphics-related AIX packages are installed compare the installed packages on the target machine with an AIX machine that has a graphics adapter. To compare the packages, issue the command `lslpp -L` and look for package names that start with `X11`.

### Software

The operating system used in these scenarios was AIX 5L Maintenance Level 2.


Also, see 2.3, “Setup of AIX prerequisites” on page 11 to understand how to setup your environment.

The software applications to be installed are:

- DB2 Universal Database V7.2 Enterprise Edition
- WebSphere Application Server 4.02
- WebSphere Portal V4.1
- SecureWay Directory Server V3.2.2
- WebSphere Personalization V4.0

### Additional tools

Additional UNIX tools, such as various GNU tools are helpful during the daily work of a system administrator. Table 2-1 lists a couple of tools that do not get installed by default. They are supported by AIX 4.3.3 and AIX 5L, and they are located on the AIX Toolbox for Linux Applications disk.

**Table 2-1 Short selection of useful UNIX/Linux tools**

<table>
<thead>
<tr>
<th>Software</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>bash</td>
<td>Bourne Again Shell is more user friendly than the Korn Shell and comes with features like command completion.</td>
</tr>
<tr>
<td>ethtool</td>
<td>Graphical sniffer tool that can be very helpful in understanding the network flow.</td>
</tr>
<tr>
<td>gzip</td>
<td>The GNU data compression program (by default installed at AIX 5L).</td>
</tr>
<tr>
<td>unzip</td>
<td>A utility for unpacking zip files.</td>
</tr>
</tbody>
</table>

Note: None of these tools are really required, they are just helpful.

### 2.2 Remote display

As AIX Server machines tend to be located in server rooms, it is very common when you don’t sit in front of the physical machine, but work remotely from a PC.
The following points should be considered:

- As the X Client - Server connection creates quite an amount of network traffic, a fast and stable network connection is required.
- Windows clients require an additional X Server Software installed, such as Hummingbird Exceed. These X Servers usually require a valid license that can be requested from the appropriate vendor.
- UNIX clients such as Linux based PCs do not require additional software. Furthermore, the connection seems to be faster and more stable than using X Servers on Windows clients.
- Be aware that a sudden network interrupt can corrupt your installation. Please note that some X Servers (including the built-in version of Linux) are able to refresh as soon as the network is up again. It is therefore worthwhile to check in advance with your X Server vendor. If you lose your Display in the middle of the installation process, we highly recommend that you start again from scratch.

Due to a number of problems that can occur using a Remote Display, it may not be reasonable to go with this approach, which would then require an installation in front of the target machine or a non-graphical installation.

The following example shows how to export the Display from the target AIX machine (IP address 9.24.105.133) to another machine, such as a Linux system (IP address 9.24.104.152).

Example 2-1 Export Display to a PC with Linux OS

bernie@stimpfle:~> xhost +9.24.105.133
9.24.105.133 added to access control list
bernie@stimpfle:~> telnet 9.24.105.133
login: root
root's Password:
# DISPLAY=9.24.104.152:0.0
# export DISPLAY
#

You can verify the setup by issuing the command `xclock`. An analog clock should then appear at your screen.

2.3 Setup of AIX prerequisites

This section is intended to show how an AIX 5.1 machine (default installation) was prepared for WebSphere Portal installation.

This procedure may differ depending on the hardware you use. Consult your AIX Administrator if you feel unqualified to prepare the operating system for installation.

Note: All procedures in this chapter must be done as root user.

2.3.1 Installation of non-default packages

WebSphere Portal requires AIX packages that do not get installed automatically on most hardware. We recommend adding three packages:

- X11.adt
To install these packages, open the AIX System Management Interface Tool (SMIT) and select them for installation.

1. Insert AIX 5.1 Disk #1 into your CD-ROM drive and make sure the disk is not mounted.
2. Open SMIT with a fastpath: `smit install_software`.
3. Choose your CD-ROM drive from the list (usually `/dev/cd0`).
4. Click List in the row of SOFTWARE to install.
5. Select all of the upper three packages as done with the `X11.adt` package in Figure 2-1.

![Figure 2-1  Selecting additional AIX packages](image)

6. Click OK to leave the package selection window and click OK again to start installing the selected software packages.

7. SMIT will ask you to insert another disk (see Figure 2-2). Make sure you click in the Output window to be sure it has the focus and then press Enter.
8. After successful installation, leave the tool by clicking **Done** and then **Cancel**.

### 2.3.2 Resizing the file systems

The default file system sizes are too small to install WebSphere Portal. It is required to add more space to the file systems.

Table 2-2 contains the file system sizes we recommend.

**Table 2-2  Recommended values for the sample WebSphere Portal installation**

<table>
<thead>
<tr>
<th>File system</th>
<th>Original size</th>
<th>New size</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>/</td>
<td>32 MByte</td>
<td>320 MByte</td>
<td>Have at least 100 MByte free</td>
</tr>
<tr>
<td>/usr</td>
<td>600 MByte</td>
<td>5.5 GByte</td>
<td>Installation will use 2.5 GByte</td>
</tr>
<tr>
<td>/var</td>
<td>32 MByte</td>
<td>320 MByte</td>
<td>Almost no space is required during installation process</td>
</tr>
</tbody>
</table>
Use SMIT to change a file system size. Issuing the command `smit chfs` leads to a window similar to Figure 2-3.

**Figure 2-3 Changing the file system size using SMIT**

1. Click **Change Characteristics of a Journaled File System**
2. Select the mount point you intend to change.
3. Enter a new value in the field, **SIZE of file system (in 512-byte blocks)**
4. Click **OK**.
5. Close SMIT.

Do this for every mount point that requires a file system size change. You can check the file system sizes using the command: `df -k`.

### 2.3.3 Announcing a CD-ROM drive to the operating system

To be able to install WebSphere Portal from a CD-ROM drive, you must define a mount point inside AIX for it.

1. Open SMIT with the command `smit`.
2. Click **System Storage Management (Physical & Logical Storage)**.
3. Click **File Systems**.
4. Click **Add / Change / Show / Delete File Systems**.

<table>
<thead>
<tr>
<th>File system</th>
<th>Original size</th>
<th>New size</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>/tmp</td>
<td>32 MByte</td>
<td>1.3 GByte</td>
<td>Make sure you have plenty of space free (&gt; 600 MByte)</td>
</tr>
<tr>
<td>/home</td>
<td>32 MByte</td>
<td>1.3 GByte</td>
<td>Database will be created at this mount point</td>
</tr>
<tr>
<td>/opt</td>
<td>32 MByte</td>
<td>800 MByte</td>
<td>About 100 MByte are required during installation</td>
</tr>
</tbody>
</table>
5. Click **CDROM File Systems**.
6. Click **Add a CDROM File System**.
7. Click **List** in the DEVICE name row to select your CD-ROM drive (for example cd0).
8. Choose a mount point by adding a value in the field **MOUNT POINT** (for example /cdrom).
9. Click **OK**.
10. Close SMIT.

### 2.3.4 Upgrading to latest maintenance level

To upgrade your operating system to the latest maintenance level consult the documentation that should be part of the maintenance level package. If you did download the maintenance level from the Internet make sure you follow the instructions that are provided on the Download page.

For this sample installation, the following procedure was used to install maintenance level 2 for AIX 5.1:

```bash
cd /usr/sys/inst.images
gzip -d -c /tmp/510002.tar.gz | tar -xvf -
inutoc /usr/sys/inst.images
installp -acgXd /usr/sys/inst.images bos.rte.install
smit update_all
```

As INPUT device/directory for software choose /usr/sys/inst.images.

Click **OK** to update all software packages.

### 2.3.5 Network setup

There are only two major requirements for network setup for a WebSphere Portal installation:

- **Fixed IP address**
  
  It is not supported to have the server get an IP address from a DHCP server.

- **Configured fully-qualified host name**

  It is required that the server knows itself by the fully qualified host name, also sometimes called fully qualified domain name (FQDN). To be sure that this is configured correctly, you can check with a simple ping before you start installation. For our sample environment the correct command would be:

  ```bash
  ping m10df55f.itso.ral.ibm.com
  ```

### 2.4 Installation planning worksheet

We highly recommend that you develop a planning worksheet before installation. An empty form is provided by the InfoCenter of WebSphere Portal at:


This will also give you an overview of the values that get created on your system and is therefore of great value to AIX System administrators.

For our sample installation, we use the following values in Table 2-3.
Note: The values that do not apply for our installation have been left out. Unfortunately, the sheet in the InfoCenter appears misleading, so we marked the important values for you.

<table>
<thead>
<tr>
<th>Target data</th>
<th>Our value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>IBM HTTP Server installation directory</td>
<td>/usr/HTTPServer</td>
<td>You will not be asked for this value and you cannot change it.</td>
</tr>
<tr>
<td>IBM HTTP Server user name</td>
<td>httpd</td>
<td>User that gets created and will own the httpd process (see “IBM HTTP Server configuration” on page 27).</td>
</tr>
<tr>
<td>Group of IBM HTTP Server user</td>
<td>httpd</td>
<td>Group that gets created (see “IBM HTTP Server configuration” on page 27).</td>
</tr>
<tr>
<td>Password of IBM HTTP Server user</td>
<td>httpd</td>
<td>See “Change password for the user httpd” on page 67 on how to change this password.</td>
</tr>
<tr>
<td>IBM SecureWay Installation directory</td>
<td>/usr/ldap</td>
<td>It is not possible to change this value during installation.</td>
</tr>
<tr>
<td>SecureWay Suffix</td>
<td>ou=itso,o=ibm,c=us</td>
<td>See 2.5, “Consideration for LDAP” on page 19 to get more background information about the Suffix.</td>
</tr>
<tr>
<td>SecureWay Administrative User</td>
<td>cn=ldapadmin</td>
<td>The root user inside SecureWay. It is possible and save to change this value (see Figure 3-5 on page 29), but value must always start with cn=</td>
</tr>
<tr>
<td>SecureWay Password for Administrative User</td>
<td>ldapadmin</td>
<td>See “Change password for LDAP Admin user cn=ldapadmin” on page 65 on how to change this password.</td>
</tr>
<tr>
<td>WebSphere Application Server Installation directory</td>
<td>/usr/WebSphere/AppServer</td>
<td>It is possible and safe to change this location during setup.</td>
</tr>
<tr>
<td>WebSphere Application Server node name</td>
<td>m10df55f</td>
<td>You will not be asked to change this value. By default the value is equal to your hostname.</td>
</tr>
<tr>
<td>LTPA password</td>
<td>ltpa</td>
<td>See “Change LTPA password of WebSphere Application Server Security” on page 68 on how to change this password.</td>
</tr>
<tr>
<td>WebSphere Application Server: Local Database user ID</td>
<td>wasuser</td>
<td>This value applies to both the UNIX user and the DB2 instance name.</td>
</tr>
<tr>
<td>WebSphere Application Server: Local Database password</td>
<td>wasuser</td>
<td>This value applies to both the UNIX user and the DB2 instance name. See 4.4.3, “Change password for DB2 user wasuser” on page 60 on how to change these passwords.</td>
</tr>
<tr>
<td>WebSphere Application Server: Local Database name</td>
<td>wasdbi</td>
<td>Name of the DB2 database that gets created. It is possible and safe to change this value (see Figure 3-7 on page 32).</td>
</tr>
<tr>
<td>Target data</td>
<td>Our value</td>
<td>Description</td>
</tr>
<tr>
<td>------------------------------------------------</td>
<td>-----------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>WebSphere Application Server:</td>
<td>wasdb</td>
<td>Name of the alias that WebSphere Application Server uses to access its database. It is possible and safe to change this value (see Figure 3-7 on page 32).</td>
</tr>
<tr>
<td>Local Database Alias name</td>
<td></td>
<td></td>
</tr>
<tr>
<td>WebSphere Application Server:</td>
<td>LOOPBACK</td>
<td>DB2 node name used to connect from the database alias to the physical database. It is possible and safe to change this value. Valid entries include IP addresses, hostnames and fully qualified hostnames. LOOPBACK is an internal alias for the value 127.0.0.1.</td>
</tr>
<tr>
<td>Database Node Name</td>
<td>55555</td>
<td>The port DB2 uses to connect from the DB2 client to the DB2 Server. It is possible and safe to change this value (see Figure 3-7 on page 32).</td>
</tr>
<tr>
<td>WebSphere Application Server:</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Database Server Port</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Personalization:</td>
<td>WebSphere Portal</td>
<td>The Application, Personalization Server gets installed to. Do not change this value (see Figure 3-8 on page 33).</td>
</tr>
<tr>
<td>Application Server Name</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Portal: Install Directory</td>
<td>/usr/WebSphere/Portal Server</td>
<td>It is possible and safe to change this location during setup.</td>
</tr>
<tr>
<td>Portal: Hostname</td>
<td>m10df55f.itso.ral.ibm.com</td>
<td>This value requires the fully qualified hostname of your server (see 2.3.5, “Network setup” on page 15).</td>
</tr>
<tr>
<td>Portal: Base URI</td>
<td>/wps</td>
<td>The prefix value of the Portal Application that will appear in the URL right after the hostname. It is possible and safe to change this value (see Figure 3-11 on page 36).</td>
</tr>
<tr>
<td>Portal: Home page</td>
<td>/portal</td>
<td>This is the shortcut to the Portal’s first page which would then be in our example, hostname/wps/portal. It is possible and safe to change this value (see Figure 3-11 on page 36).</td>
</tr>
<tr>
<td>Portal: Customized page</td>
<td>/myportal</td>
<td>This is the shortcut to the Portal’s secured pages which would then be in our example, hostname/wps/myportal. If you are not already authorized, you would be redirected to the login page. It is possible and safe to change this value (see Figure 3-11 on page 36).</td>
</tr>
<tr>
<td>Portal: Proxy host</td>
<td></td>
<td>A proxy host that allows connections to another network. It is possible to change that value at any time.</td>
</tr>
<tr>
<td>Portal: Proxy port</td>
<td></td>
<td>The appropriate port for the above declared proxy host. It is possible to change that value at any time.</td>
</tr>
<tr>
<td>Portal: LDAP server</td>
<td>m10df55f.itso.ral.ibm.com</td>
<td>This value requires the fully qualified hostname of your server (see “Network setup” on page 15).</td>
</tr>
<tr>
<td>Portal: User DN</td>
<td>cn=ldapadmin</td>
<td>Must equal the value as defined above in “SecureWay Administrative User”.</td>
</tr>
<tr>
<td>Portal: User password</td>
<td>ldapadmin</td>
<td>Must equal the value as defined in this table at “SecureWay Password for Administrative User”.</td>
</tr>
</tbody>
</table>
Make sure you check 2.5, “Consideration for LDAP” on page 19 to gather information regarding the setup of your LDAP structure.

The following list gives a summary of items that get created by the Setup Manager:

- **UNIX users that get created:**
  - httpd
  - wasuser
  - ldap
  - ldapdb2
  - db2fenc1
  - db2inst1
  - db2as

- **UNIX groups that get created:**
  - httpd
  - wasgrp
  - ldap
  - db2fadm1
  - db2iadm1
  - db2asgrp
  - dbsysadm

- **DB2 databases that get created:**
  - LDAPDB2: used to store LDAP directory
  - WASDBL: used by WebSphere Application Server
  - XWPSDB: used by WebSphere Portal and WebSphere Member Service
  - DWCNTRL: not used

- **TCP/IP ports in use:**
  - 80 (IBM HTTP Server)
  - 389 (SecureWay Directory Server)
– 900 (WebSphere Application Server Administrative Server)
– 8008 (IBM HTTP Administration Server)
– 90xx (WebSphere Application Server)
– 55555 (DB2 Universal Database Server)

2.5 Consideration for LDAP

This section will definitely not provide enough about the IBM SecureWay Directory and LDAP directories in general. For further documentation describing LDAP see:

▶ *Using LDAP for Directory Integration*, SG24-6163
▶ *Understanding LDAP*, SG24-4986

Depending on the type of installation, WebSphere Portal core component requires a ready-to-use Lightweight Directory Access Protocol (LDAP) structure with at least two users inserted. We will describe how to insert these users and then discuss in an additional section the structure that WebSphere Portal assumes, if you go with the default values.

2.5.1 Creation of a Lightweight Directory Interchange Format (LDIF) file

All major LDAP Server products support the ability to dump the structure content to a plain text file, supporting the LDIF file format. Such an LDIF file can then be used to fill an LDAP Server with a proper structure.

WebSphere Portal comes with two example LDIF files, one ready to fill into a SecureWay Directory Server, another targeting iPlanet Directory.

To use it for your purposes, you have to edit it manually. Compare the one that comes on the CD (for example, CD # 13, /wps2/WPSconfig.ldif) with the one that is printed below that we use for the installation.

*Example 2-2  LDIF file for SecureWay Directory*

```
version: 1

# NOTE: make sure, you use the correct objectclass types!
# for o= use organization
# for ou= use organizationalUnit
# for dc= use domainController
# Do not just copy and paste this! First think about a good structure and
# then change the file that comes with the product.

dn: ou=itso,o=ibm,c=us
objectclass: organizationalUnit
objectclass: top
# Add lines according to this scheme that correspond to your suffix
ou: itso,o=ibm,c=us
ou: itso

dn: cn=users,ou=itso,o=ibm,c=us
objectclass: container
objectclass: top
cn: users

dn: cn=groups,ou=itso,o=ibm,c=us
objectclass: top
objectclass: container
cn: groups
```
2.5.2 Determine a reasonable LDAP structure for WebSphere Portal

WebSphere Portal needs to know about your LDAP structure, as it has to write and read from it, if you tell WebSphere Portal at installation to use a LDAP directory.

The user directory is quite an important item in your business. You should consider before installation about how to build up a reasonable structure. If you feel, that this is unnecessary, skip the chapter and take the default values that WebSphere Portal offers you during installation.

Many companies already use an LDAP directory and may want to put users that get created by WebSphere Portal in a certain branch of their LDAP directory tree.

The following lists a number of important terms that are also used during installation of WebSphere Portal. If you do not understand the description consult the documentation of your LDAP directory implementation and the Redbooks that are mentioned at the beginning of this section.

- **User Object Class**

  All major LDAP directory implementations have pre-setup object class schemas that are common. Such a schema defines what entries a specific leaf in the LDAP branch is able to get. Examples of entries would be surname, telephone, fax or even object class. Some of
the entry fields can be marked that they are required for this schema. So you might need to provide a value for surname but not necessarily for the field of fax.

The User Object Class defines which schema WebSphere Portal should assume for users. The default value is inetOrgPerson. If possible, do not change this value, unless you know what you are doing.

The default value for the Lotus Domino LDAP Directory implementation is dominoPerson.

- **User DN prefix**
  
  Say you create a new user with the user id stimpf86. The user id will be used by your user to log into your Portal.

  At the creation of this user, WebSphere Portal will create a new leaf in the LDAP Directory. The name of the entry will be ‘User DN prefix’='user id','User DN suffix'.

  That means if, if WebSphere Portal in our example setup requests the LDAP to add a user with the userid stimpf86 to the directory, the entry will be:
  
  \( \text{uid=stimpf86, cn=users, ou=itso, o=ibm, c=us} \)  

  (as our User DN prefix is \text{uid=} and our User DN suffix is \text{cn=users, ou=itso, o=ibm, c=us})

  It is pretty common to have as User DN prefix \text{cn} instead of \text{uid}. This might however lead to confusion, as it should be possible to distinguish the common name clearly from the userid attribute. The recommended value is \text{uid}.

- **User DN suffix**
  
  This is the branch in the LDAP Directory, in which WebSphere Portal will look for users and to which it will add users.

  The default value is \text{cn=users, <suffixvalue>}, where suffixvalue is the value that you gave WebSphere Portal during installation. For our concrete example this leads to the value \text{cn=users, ou=itso, o=ibm, c=us} as our suffix is \text{ou=itso, o=ibm, c=us}. That means WebSphere Portal will really create a sub-branch (\text{cn=users}) by default to save your users there. This is a reasonable behavior, if you do not want to have group and user entries in the same place in your LDAP tree.

  If you disagree, you will have to adjust the User DN suffix accordingly.

- **Group Object class**
  
  The Group Object Class defines which schema WebSphere Portal shall assume for groups. The default value is groupOfUniqueNames for Domino it would be dominoGroup. There are not a lot of requirements for this schema. It just needs to be able to hold a list of User Object Class entries.

- **Group Member**
  
  WebSphere Application Server Security will go for members of particular groups with an ID map request, ‘Group Object class’:‘Group Member’ to find a specific user.

  The default value for SecureWay Directory would be uniqueMember, for Domino LDAP it would be member. Do only change the default setting, if you know what you are doing.

- **Group DN prefix**
  
  This is the prefix used in front of groups. The default value is \text{cn}, which should be fine in most cases. So the name of a group would be for example \text{cn=wpsadmins}:

- **Group DN suffix**
  
  This is the branch in the LDAP Directory in which WebSphere Portal will look for groups and to which it will add groups.

  The default value is \text{cn=groups, <suffixvalue>}, where suffixvalue is the value that you gave WebSphere Portal during installation. For our example, this leads to the value
cn=groups,ou=itso,o=ibm,c=us. That means WebSphere Portal will really create a sub-branch (cn=groups) by default to save there your groups. This is a reasonable behavior if you do not want to have group and user entries in the same place in your LDAP tree.

If you disagree, you will have to adjust the Group DN suffix accordingly.
WebSphere Portal installation using WebSphere Portal Setup Manager

This chapter is intended to give a helping hand on how to successfully step through a WebSphere Portal installation. By intention, we used values that seem to be problematic from practical customer experiences, therefore, making your setup easier to accomplish.

We use the Extend Edition of WebSphere Portal, however, installing the Collaboration Features will not be covered in this chapter.

3.1 WebSphere Portal Setup Manager

In this section, we perform the configuration of WebSphere Portal V4.1 using the Setup Manager tool. You will be able to walk through this chapter without having a product installed. At the end of this section you will be asked whether to start the installation or not.

3.1.1 Information collection for WebSphere Portal installation

Before starting WebSphere Portal Setup Manager, make sure you have read Chapter 2, “Considerations for WebSphere Portal in AIX environment” on page 9 and fulfilled all prerequisites.

1. Insert WebSphere Portal Disk 1 as it includes the Setup Manager, open a terminal as root user, and start the Setup Manager with commands as listed below:

   # cd
   # id
   uid=0(root) gid=0(system)
   # mount /cdrom
   # /cdrom/install.sh
If the latest maintenance level is not installed, Setup Manager will now install an update of the JDK.

2. A Welcome window is displayed, as shown in Figure 3-1.

![WebSphere Portal Setup Manager welcome window](image)

This window will inform you about prerequisites for the product. Click **Next** to continue.

3. The next window will show the Program License Agreement. Click **Accept** and then click **Next**.

4. The following window will ask you for your WebSphere Portal Installation Key. Insert the Key and click **Next**. You will see a window similar to Figure 3-2.

![WebSphere Portal Installation Key](image)

**Note:** The Installation Key implies the edition that you have of WebSphere Portal, which is dependent on your Installation Key Setup Manager, will select the correct option for the Edition you purchased.

The Installation Key is included with your set of CD-ROMs. If you cannot find your Installation Key, ask your IBM representative for assistance.

We will use a key that starts the Installation of WebSphere Portal Extend Edition. Other installations will give you more or less options.
5. Figure 3-2 allows you to select the installation options. WebSphere Portal includes three types of installation procedures:

**Quick install**
The Quick installation uses configuration information stored in a response file to automatically install the WebSphere Portal components. The response file, `wporecord.script`, is on CD 1. You should modify the response file and store it on your system before you install WebSphere Portal.

**Standard install**
The Standard installation uses configuration information stored in a response file to automatically install the WebSphere Portal components. The response file is generated during the installation process and provides the required information so you don’t need to enter information during the actual installation.

**Advanced install**
The Advanced installation lets you select the components you want to install. Selected components can be installed on different systems. If you want to add some components after initial install this selection will be chosen.

We use the Standard procedure. Therefore, select **Standard Install** and then click **Next**.

6. You will be asked for the location of the Response File. In our example, we did not create a Response File and left the field blank. Click **Next**.

**Tip:** Setup Manager will create a Response File during this installation procedure and place it in `/usr/IBM/WPO/scripts/wprecord.script`.

This file might be used with the Quick Install option on the same machine or with slight changes on a similar machine.
7. You will see a window similar to Figure 3-3, where you are asked to select the components that should be installed. By selecting components Setup Manager will recognize automatically, which prerequisite packages it will require.

Therefore it is enough for our sample installation to select only the following two packages:

- Select **WebSphere Portal**
- Select **SecureWay Directory**
As we will not cover the installation of the Collaboration Feature in this chapter we explicitly deselect the following checkbox:

- Deselect **Lotus Collaborative Places and Components**.

**Note:** After clicking one of the checkboxes, the Java GUI will need some time to refresh.


8. Click **Next** to start the prerequisite information collection of the WebSphere Portal Setup Manager.

9. Prerequisite information collection

   In this step of this process, Setup Manager will check for previous installations of WebSphere Portal. You will be informed about dependencies and whether Setup Manager can resolve it without help.

   It will also check for missing prerequisites of the operating system and finally check for problems with the License Use Management.

   If you are missing obvious prerequisites, Setup Manager will tell you about it in the displayed information window and ask you to cancel the installation, solve the problem, and then start the installation again.

   If Setup Manager does not explicitly tell you differently, click **Next** to start the configuration of the individual products inside WebSphere Portal Setup Manager.

### 3.1.2 IBM HTTP Server configuration

In the window shown in Figure 3-4, insert the user information of the user that will own the httpd process. Setup Manager will create the user and group that you specify on the AIX platform for you. In our example, we use `httpd` for both user and group.

We recommend that you change the user's system rights after installation to fit your security guidelines.

The issued username and password combination will also be used for the IBM Administration Server of the IBM HTTP Server that will run by default on port 8008.
3.1.3 IBM SecureWay Directory Server configuration

You will see a window as shown in Figure 3-5 to configure the IBM SecureWay Directory Server. All fields require values, as shown in the following steps.
1. Enter the Suffix for your IBM SecureWay configuration.

   The Suffix you are requested to insert in the first field of Figure 3-5 is a branch that WebSphere Portal will use to add its information.

   Inside that branch WebSphere Portal will by default add two sub-branches. They are:

   - **cn=users**  
     Inside here it will later add the users like leaves.
   - **cn=groups**  
     Inside here it will expect the groups that the users belong.

   You can change this behavior in one of the following configuration windows (see Figure 3-13 on page 38).

   **Note:** If the Suffix you enter does not solely consist of domain controller branches (dc=blabla,dc=bla), Setup Manager will very likely fail to insert the required users into SecureWay Directory. By intention, we use a difficult setup to show how to bypass potential problems.

   For this sample installation we will use as our Suffix, **ou=itso,o=ibm,c=us**. In the Suffix (example: **dc=yourco, dc=com**) field, enter **ou=itso,o=ibm,c=us**.

2. The administrative user is the root user inside SecureWay Directory. This user will not appear in the AIX user environment.

   We use the name **ldapadmin** for the LDAP Administrative user. In the Administrative user field, enter **cn=ldapadmin**.

   **Important:** Do not forget to have **cn=** in front of the username.

   For system administrators: Two AIX users will be created by the SecureWay installation.
ldap
This will be the process owner of the SecureWay Directory Server daemon process (slapd).

ldapdb2
This will also appear as a DB2 instance and will therefore own the appropriate DB2 processes. Its task is to manage the database LDAPDB2 that gets created during SecureWay Directory installation.

These two values are hard-coded and cannot be changed if using WebSphere Portal Setup Manager. Consider installing SecureWay Directory manually if you feel you cannot live with these values.

It is recommended that you change the user's rights after installation to fit to your security guidelines.

3. In the Password for administrative user and Confirm password fields, enter a password for your directory server. You may use any character set, excluding an opening curly bracket { at the beginning and white spaces in general.

4. In the TCP/IP port to use field, leave default value 389.
   Port 389 is the default port to use for LDAP directory servers.

Click **Next** to provide information for the WebSphere Application Server.

### 3.1.4 WebSphere Application Server configuration

To configure WebSphere Application Server with WebSphere Portal Setup Manager you have complete or change the default values of several windows.

1. The first window asks for the WebSphere Application Server home directory. Accept the default value for AIX Systems, /usr/WebSphere/AppServer and click **Next**.

2. In the following window you have to select, whether your DB2 Server installation is on a remote host. Choose **No** to have all components installed on a single machine and click **Next** to continue.

   A description of the choices follows:

   **No**
   This means Setup Manager will create a database itself on the local machine. It will then create a catalog that points to the created database.

   **Yes**
   This means Setup Manager will create only a Catalog that points to a remote DB2 database. It is required that you create this database on the remote DB2 Server installation manually.

3. The next Window requests you to choose the Database Type. Oracle Databases will not be covered in this book. Choose **DB2** and click **Next**.
Figure 3-6 Collecting information about WebSphere Application Server database owner

4. In Figure 3-6, you are asked to insert the DB2 Instance owner to be used for WebSphere Application Server.

   – In the Local Database User ID field, type `wasuser`.
     This user will be created in the AIX environment by the Setup Manager. It will also appear as DB2 instance and will therefore own the appropriate DB2 processes. Its task is to manage the database for WebSphere Application Server and we also use it to manage and own the WebSphere Portal databases, that will be configured on one of the later screens.

   – In the Local Database Group field, type `wasgrp`.
     This AIX environment group will be created by Setup Manager and the above user will be assigned to it. So it is really a UNIX group.

   – In the Local Database Password field, enter a password:
     This password is used for both, the AIX user `wasuser` and the DB2 Instance owner. Therefore, you also need this password to connect to the databases that will be created.

We recommend that you change the user’s permissions after installation to fit to your security guidelines.

Click **Next** to switch to the Collection of the database information window.
5. Complete the following fields as shown in Figure 3-7:

- **Local Database Name**: Type `wasdb1`.
  The name of the database as it will be created by the Setup Manager.

- **Local Database Alias Name**: Type `wasdb`.
  The name of the alias that will be used to access the database. This name must differ from the above value.

- **Node Name**: Leave default value `LOOPBACK`.
  The DB2 name that indicates where to find the physical database. Since the database and the database alias exist on the same machine, LOOPBACK is a good name. It indicates that the database is connected via the loopback device.

- **Database Server Port**: Leave default value `55555`.
  This is the port that the DB2 Server will listen on. It is used for the connection between the database alias and the database itself. Usually, this is configured with a UNIX service name, but we recommend that you add a port number. We recommend that you add this port to your `/etc/services` file after installation. **This port must not be in use by any other application!**

**Important**: The names you specify can only contain 1-8 characters! To avoid potential problems, do not use the special characters such as @, #, and $.

Click **Next** to move to the Personalization Server Setup information.
3.1.5 Personalization Server configuration

Shown in Figure 3-8 is the window for choosing the Application Server Name to which Personalization Server should be installed.

**Important:** Do not change the default value! Leave it as WebSphere Portal.

![Figure 3-8 Configuration of WebSphere Personalization Server](image)

Click **Next** to move to the Portal Server information gathering section.

3.1.6 WebSphere Portal configuration

To configure WebSphere Application Server with WebSphere Portal Setup Manager you have to complete or change the default values of several windows. To do so, complete the following steps:

1. The first window prompts you for the type of installation. Choose **Typical** and click **Next** to proceed.

   The Development Install Type is used by a developer, who wants to set up his PC for Portlet development purposes only. As we rarely find such a situation in an AIX environment, this install type will not be used in our configuration.
2. Figure 3-9 shows the window that prompts you to select the Authentication Mode. For our example, select **Database and LDAP Directory mode**. Click **Next** to continue to the Security configuration.

A description of the choices in this window follows:

- **Database only mode:**
  
  All users will be stored in a proprietary format in one of the internal tables of the WebSphere Portal database. No other applications will be able to access user information without going through WebSphere Portal. For this installation mode, no LDAP Directory is required. Please refer to the product guide to understand the various restrictions that might apply using this installation type.

- **Database and LDAP Directory mode:**
  
  This is the standard mode to use with WebSphere Portal. Basic user information, such as name and password are stored in a LDAP Directory and can accessed by all applications that support the open LDAP protocol and do have permissions to do so.

  Extended user information and Portal specific data will be held by WebSphere Portal database or WebSphere Member Service database.

  This Installation mode requires an LDAP directory such as the SecureWay Directory Server. If you are unsure use this mode.

- **Custom User Registry mode:**
  
  A custom user registry allows you to use, for example, a legacy system to hold your users. You would need to provide a proper Custom User Registry implementation. Check the WebSphere Application Server documentation to get more information about how to implement a custom user registry or check the WebSphere Application Server InfoCenter at:

  http://www-3.ibm.com/software/webservers/appserv/doc/v40/ae/infocenter/was/0502.html
If you intend to use a custom user registry, do the following:

i. First, install WebSphere Application Server on its own.

ii. Implement the custom user registry code in WebSphere Application Server and make sure your code works without any problems.

iii. After you have a proper setup established, install WebSphere Portal.

Figure 3-10 WebSphere Application Server Security Configuration

3. Figure 3-10 shows the window that lets you choose to enable WebSphere Application Server Security during the installation or not.

Please note that WebSphere Application Server Security has nothing to do with SSL or https. WebSphere Application Server supports securing certain resources, which means that those cannot be accessed without having the right permission. This capability is used by WebSphere Portal to distinguish between public resources and resources (for example Portlets) that can only be accessed by specific users.

If you do not have WebSphere Application Server already installed and have not enabled Security in that installation, then choose Now. Only in case you had WebSphere Application Server already installed and at this installation Security is already enabled, you would choose later.

We did not have any WebSphere product on our system prior to installation, therefore, choose Now and click Next.

4. The next window will ask you for the LTPA password. Type in a proper password and make sure you remember it!

Important: If you use a pre-existing WebSphere Application Server and it had global security configured, you must provide exactly the same LTPA password that you have entered before. This applies also, if security is currently disabled. Otherwise, you will not be able to start WebSphere Application Server and it will cause an install failure.
Click **Next** to move to the Portal Server configuration window.

![Figure 3-11 Portal Server configuration](image)

5. As shown in Figure 3-11, Setup Manager will prompt you for configuration settings related to the Portal application itself.

   - In the **Install Directory** field: Leave default value `/usr/WebSphere/PortalServer`.
     The directory WebSphere Portal will be installed. The default directory on AIX is `/usr/WebSphere/PortalServer` and is a good choice. Changes to the default will not lead to problems.

   - In the **Hostname** field: Type `m10df55f.itso.ral.ibm.com`.
     The fully qualified hostname of the Portal Server machine. If the value that Setup Manager recommends is not correct (for example, it shows only the hostname instead of the fully qualified hostname), you should double check your network environment. Your prerequisites might not be correct.

   - In the **Base URI** field: Leave default value `/wps`.
     The base URI that will appear in all links that point to WebSphere Portal. Inserting a slash (`/`) only or leaving the value empty might lead to problems. Please note that Setup Manager will then need to change the settings of the Default Server in the WebSphere Application Server as it already occupies the resource slash (`/`).

   - In the **Home page** field: Leave default value `/portal`.
     This value defines the last part of the URL that is used to access the public resources of WebSphere Portal. Public resources means resources that do not require authentication. This value must not be empty.

   - In the **Customized page** field: Leave default value `/myportal`.
     This value defines the last part of the URL that is used to access non-public resources that is resources that require authentication. The value must not be empty and must differ from the value above.
In the Proxy host: Leave blank.

If your WebSphere Portal host does not have direct access to a certain network, like the Internet, but resources such as Portlets shall have access to the Internet, you need to provide a Proxy hostname that allows that access. You can easily configure this after installation as well. You cannot provide a SOCKS Server hostname here.

In the Proxy port field: Leave blank.

The appropriate port for the Proxy host as described above.

Click Next to move to the LDAP Server Access configuration.

Figure 3-12  LDAP Server Access information

6. Figure 3-12 shows that Setup Manager allows you choose among various LDAP Directory Server implementations.

As we intend to install SecureWay Directory using the Setup Manager, complete the following fields with appropriate values:

LDAP Server: Type m10df55f.itso.ral.ibm.com

The fully qualified hostname of the LDAP Server. Installation will fail if you only use the short name, such as localhost. So we use m10df55f.itso.ral.ibm.com

– User DN: Type cn=ldapadmin

This is the distinguished name of the LDAP Administrative User. (See the description in 2.5.2, “Determine a reasonable LDAP structure for WebSphere Portal” on page 20 about the LDAP Administrative User; and 3.1.3, “IBM SecureWay Directory Server configuration” on page 28, where we defined this user). The default value is the one used during SecureWay Directory Server configuration, which is in our case cn=ldapadmin. If you need to change this value, remember not to put in just the user name but the distinguished name of the user. Another example would be cn=Manager,dc=ibm,dc=com.
– User password: Enter password.
  The proper password for the LDAP Administrative User.
– Suffix: Type ou=itso,o=ibm,c=us
  The base tree in which WebSphere Portal will add its branches. See 3.1.3, “IBM
  SecureWay Directory Server configuration” on page 28, where we defined this Suffix.
– LDAP port number: Use the default value.
  Leave this value as 389, as it is the default port for LDAP to communicate unencrypted.
Click Next to go to the Portal LDAP configuration.

Figure 3-13 WebSphere Portal related LDAP configuration options

7. Figure 3-13 shows the window for a extended configuration of the LDAP settings to use
with WebSphere Portal.

  Make sure you have read and understood 2.5.2, “Determine a reasonable LDAP structure
for WebSphere Portal” on page 20 before changing any values on this window. If you do
not have a reason to change these values, the defaults will be fine.

Click Next to move to the Portal Server Database Selection.
8. As shown in Figure 3-14 you have to select three options via radio buttons:

- **Database backend section**: Select **DB2 Universal Database Server**.
  We chose the DB2 Universal Database Server because we will use DB2 instead of Oracle for the WebSphere Portal databases.

- **Portal Server database configuration scripts section**: Select **Create and initialize a new database (DB2 Only)**.
  Since this is a fresh install on a clean machine, we chose this option. If we do not have a local DB2 Server installation, it would not create the database. You would then need to do that manually on a remote DB2 Server machine.

- **Do you want to share the database with Member Services?**: Select **Share the database**.
  Consult your DB administrator for the most reasonable setup for your installation.

Setup Manager will only create a single database that is used by WebSphere Portal and WebSphere Member Services.
• Do not share the database
  Setup Manager will create two separate databases. The WebSphere Portal database (xwpsdb) with 63 tables and the WebSphere Member Services database (wms) with 40 tables.

Click **Next** to insert the WebSphere Portal Database Configuration information.

![Figure 3-15 Portal Server database configuration](image)

9. The Additional Database Configuration window shown in Figure 3-15 lets you insert important information for WebSphere Portal to access its database.
   - In the Database name field: Type *wpsdb*.
     
     It is really the database alias name that is requested here. That means the name of the database as WebSphere Portal sees it.
     
     Consult the *DB2 Administration Handbook* if you need more background information on databases and database aliases.

     **Important:** The name can only contain 1-8 characters! To avoid potential problems, do not use special characters such as @, #, and $.

   - In the Database user field: Type *wasuser*.
     
     This user will **not** be created in the AIX environment by the Setup Manager. Therefore the user must be pre-existing or must be created by another subcomponent of the Setup Manager. The user needs to be a valid DB2 instance user, as it will be required to own the appropriate DB2 processes. Its task is to manage the database(s) for WebSphere Portal.
     
     We will use the same value as for the WebSphere Application Server database, *wasuser*.
In the User password field: Enter a password.
Use an appropriate password. If you use the same user as for WebSphere Application Server (see Figure 3-6 on page 31) as we do in this example, make sure you issue also the same password.

In the JDBC database driver field: Use the default.
For DB2 leave the default value, which is
COM.ibm.db2.jdbcd.B2ConnectionPoolDataSource

In the JDBC URL prefix field: Use the default.
For DB2 leave the default value, which is jdbc:db2

In the JDBC driver library field: Type /home/wasuser/sqllib/java12/db2java.zip
For DB2 it consists of:
<UNIX home directory of database user>/sqllib/java12/db2java.zip
A path like would present two mistakes:
/home/db2inst1/sqllib/java/db2java.zip
As we want to use the UNIX user wasuser to manage the databases, it would point to the wrong home directory, and as it states java instead of java12, it would point to the wrong version of the JDBC driver. A JDBC 2.0 driver is required for WebSphere Portal.

The correct path for our example would be:
/home/wasuser/sqllib/java12/db2java.zip

Click Next to go to the database option for Member Services.

---

Note: We highly recommend that you use the same user name that is used for the WebSphere Application Server. This will let you bypass potential problems.
10. On the Database option for WebSphere Member Services window, we are presented with two choices as shown in Figure 3-16. Select **Initialize an existing database** and click **Next**.

- **Initialize an existing database**
  Setup Manager will populate the tables and the appropriate data to the database that gets created for the WebSphere Portal database.

- **Use an existing and initialized database**
  Setup Manager assumes you have already set up and populated your databases correctly. It therefore will not touch it, as it should be ready to use.

As we chose to share a single database between WebSphere Portal and WebSphere Member Services (see Figure 3-14 on page 39), we do not get the option to create a database here. This additional option would have appeared if you had chosen not to share a single database.

### 3.1.7 Last configuration steps

In the last configuration steps you have to select a server machine as License Server and check your configuration settings as shown in Figure 3-17 and Figure 3-18.

![Figure 3-17 Select a valid License Server](image)

1. Select **Local License Server** install type.

License Use Management (LUM) is an IBM tool for managing and extending software licenses. If you choose to install LUM locally, the LUM installation program installs and configures LUM as a network license server, enrolls the WebSphere Portal product in the LUM database, and checks out the number of licenses corresponding to the number of processors you have online on the local server machine.

For example, as illustrated in Figure 3-17, a Local License Server is used for this sample installation.
Click Next and you will see the Summary of the Installation Information window.

2. Figure 3-18 shows our Configuration Summary window.

*Make very sure that each value displayed is spelled correctly and all values were issued correctly.*

**Note:** This is window is the last opportunity for you to go back and make changes to installation settings.

![Figure 3-18 Installation Information summary](image)

Click Next to start the installation process.

### 3.2 WebSphere Portal installation process

The WebSphere Portal Setup Manager installation process will prompt you to insert proper CDs, during its installation of the various products.

Each time you get prompted for inserting a new CD, do the following:
Click **Unmount** on the popup window (shown in Figure 3-19). You will not be able to remove the disk from the CD-ROM drive unless you unmount it. Make sure you use the popup window instead of a UNIX Shell to mount and unmount your disks.

**Note:** If you hit the mount button too quickly (and in other rare cases) the mount command of the Setup Manager might fail and the popup window might show you the wrong button, for example an Unmount button, even though the disk was already unmounted. Correct such a problem with a proper command from a shell.

It might also happen that the popup window appears to be underneath another window. If your installation seems to be stuck, check whether the popup window is just hidden.

If you decided to copy the CD-ROMs to a hard disk location, you will be prompted to change the path to the proper directory.

In our sample installation you will be asked for the following CDs:

- WebSphere Portal Family CD #2-3 (DB2 Universal Database)
- WebSphere Portal Family CD #2-11 (DB2 Fixpack 5)
- WebSphere Portal Family CD #5 (SecureWay Directory Server)
- WebSphere Portal Family CD #3-1 (WebSphere Application Server)

Make sure that the WebSphere Application Server installation has enough time to finish. The popup window that prompts you to insert a new CD-ROM might appear before the installation of the WebSphere Application Server Fixpacks is finished.

After Setup Manager installed WebSphere Application Server for you, you should populate the LDAP Server with a valid LDIF file. Follow these instructions:

- Adding entries to the LDAP directory

  **Important:** The LDIF file must be imported to the SecureWay directory before the WebSphere Portal Core CD-ROM (#7 or #13) is inserted!

  If you do not manually import an LDIF file you risk having the installation fail. This happens frequently if you do not have an LDAP structure with `domainController` schemas only (`dc=blabla,dc=bla`).

  See 2.5.1, “Creation of a Lightweight Directory Interchange Format (LDIF) file” on page 19 for instructions on creating a proper LDIF file.
Do not close any of the install windows, but open a new Terminal as root user and execute the following command:

```
ldif2db -i WPSconfig_itso.ldif
```

If you added the entries of your LDIF file successfully to the SecureWay Directory Server, you can close that Terminal and continue with the installation process.

The popup window prompting you for the next CD should still be open. So continue with the same procedure as described above for the following upcoming CDs:

- WebSphere Portal Family CD #4 (WebSphere Personalization Server)
- WebSphere Portal Family CD #13 (WebSphere Portal Extend Edition)

During installation of the WebSphere Portal core component, applications are imported and configuration changes are made to the WebSphere Application Server. WebSphere Application Server will also be restarted several times by WebSphere Portal Setup Manager during this process.

If a popup window appears as shown in Example 3-20 and prompts you for identification do the following:

- Enter wpsbind in both fields and click OK.

![Figure 3-20  Login window for the WebSphere Application Server Administration Console](image)

Finally an information window with the title “Configuring for Admin Role” will appear.

**Setup of Admin Role**

The information window will guide you through the following process:

**Important:** Do not close this information window for the following process! After finishing that process you will need to click OK in this window.

1. Restart your HTTP Server
   
   Without closing any of the windows open a new Terminal window as root user and issue the commands:
   
   ```
   /usr/HTTPServer/bin/apachectl stop
   /usr/HTTPServer/bin/apachectl start
   ```
   
   Do not close the Terminal window.

2. Start the WebSphere Application Server Administration Console (AdminConsole)
   
   In the Terminal window enter the command:
   
   ```
   /usr/WebSphere/AppServer/bin/adminclient.sh
   ```
If the AdminConsole does not start, your graphical environment might not be set up correctly (see “Remote display” on page 10) or your WebSphere Application Server might not be running (see “WebSphere Application Server” on page 54).

3. Open the AdminConsole Security Center. Click Console menu tab and then on the entry named Security Center.

4. In the Security Center window, as shown in Figure 3-21, make sure that Security is enabled in the General tab. If Security is enabled, continue with the next step.

If Security is not enabled, do the following:

a. Check the Enable Security box.

b. Change to the Authentication tab and supply appropriate values. Consult your WebSphere Application Server Expert about appropriate values or check the IBM WebSphere V4.0 Advanced Edition Handbook, SG24-6176.

c. Click the Apply button and then continue with the next step.

5. Click the Administrative Role tab, select AdminRole in the Roles list.
6. Click **Select**. You will see a window similar to Figure 3-23.

![Figure 3-23 Selecting wpsadmin out of the users and wpsadmins out of the groups](image)

7. In the Select Users/Groups - AdminRole window, insert an * in the Search field and click **Search**. At least two users and one group will appear in the Available Users/Groups list.
   
   a. Select uid=wpsadmin and click **Add >>**
   b. Select cn=wpsadmins and click **Add >>**

   Do this so that both the wpsadmin user and the wpsadmins group will appear in the right list of the Selected Users/Groups as shown in Figure 3-23. Click **OK** to leave this window.

8. Click **Apply** button of the Security Center. If no error occurs, close the Security Center.

   In case you get an error, usually it is that the binding to your LDAP Server did not work correctly.

9. Stop the WebSphere Application Server by stopping its node. Do this by opening the Nodes folder, right-click the node name (for example, m10df55f), and click **Stop** (see Figure 3-24).
10. As you stop your WebSphere Application Server node, your AdminConsole will close automatically. Restart WebSphere Application Server by issuing this command from the directory /usr/WebSphere/AppServer/bin:

```
./startupServer.sh &
```

If WebSphere Application Server has successfully restarted (see 4.2, “WebSphere Application Server” on page 54 on how to start WebSphere Application Server), open the AdminConsole again.

11. Open the Nodes folder and then the node name of your Application Server. After that, open the Application Server folder and check to see if the WebSphere Portal application has restarted (see Figure 3-25).

If not, select WebSphere Portal and start it manually (for example, right-click on the name and then click Start).

![Figure 3-24 Stopping the Administration Server](image)

![Figure 3-25 Make sure WebSphere Portal application is running](image)
12. As soon as WebSphere Portal is started you can close the AdminConsole and continue with the installation process by clicking **OK** in the information window. Setup Manager will now import the Portlets into WebSphere Portal.

A popup window will prompt you for another CD. So continue with the unmounting/mounting procedure as described in the beginning of this section for the following CD:

- WebSphere Portal Family CD #7 (WebSphere Transcoding Publisher)

**Note:** Depending on the configuration of the setup, you might get prompted for more or less CDs.

If Setup Manager completes the steps successfully it will show a final window as shown in Figure 3-26 and you can continue with verifying your installation.

![Figure 3-26 Information Window of a successful installation](image)

**Verify whether installation process was successful**

Use any machine on the network that has access to the installed server and has a Web browser installed to check if WebSphere Portal was installed correctly.

For this example, enter the Web address `http://m10df55f.itso.ibm.com/wps/portal` into the browser URL address field.

If you can log on and enroll a new user, you have proven that your installation was successful.

**Note:** Understand that the first request to each page takes a while to process and appear, as the JSPs require compilation at the moment of the first access.
Post-installation instructions

Even though it appears that you now have a ready-to-use WebSphere Portal installation, we recommend some manual post-installation steps.

4.1 DB2 Universal Database

In this section, we discuss some suggested activity you should perform for your DB2 Universal Database.

4.1.1 Updating WebSphere Portal database configuration

If you decided to share a single database for WebSphere Portal database tables and WebSphere Member Services database tables, you have to update the database configuration of the database that was created by Setup Manager.

Important: Make sure all applications are disconnected from the databases before you issue the *db2stop* command. That means WebSphere Application Server needs to be stopped.

Log in as your database user and issue the commands as shown in Example 4-1 to update your WebSphere Portal database settings. In this example, we list the databases and the catalogs that were created, connect to the *xwpsdb* database, and then update its configuration.

Important: These steps are required if you chose to share a database, due to a flaw in an installation script.

Note: In case you chose not to share a database (see Figure 3-14 on page 39) between WebSphere Portal and WebSphere Member Services, you do not need to update your database settings.
Example 4-1  Updating database configuration for WebSphere Portal

# su - wasuser
$ cd
$ id
uid=8(wasuser) gid=13(wasgrp) groups=0(system),103(db2asgrp)
$ db2 list db directory

System Database Directory

Number of entries in the directory = 4

Database 1 entry:
  Database alias                  = WPSDB
  Database name                   = XWPSDB
  Node name                       = XWPSNODE
  Database release level          = 9.00
  Comment                         =
  Directory entry type            = Remote
  Catalog node number             = -1

Database 2 entry:
  Database alias                  = XWPSDB
  Database name                   = XWPSDB
  Local database directory        = /home/wasuser
  Database release level          = 9.00
  Comment                         =
  Directory entry type            = Indirect
  Catalog node number             = 0

Database 3 entry:
  Database alias                  = WASDB
  Database name                   = WASDBL
  Node name                       = LOOPBACK
  Database release level          = 9.00
  Comment                         =
  Directory entry type            = Remote
  Catalog node number             = -1

Database 4 entry:
  Database alias                  = WASDBL
  Database name                   = WASDBL
  Local database directory        = /home/wasuser
  Database release level          = 9.00
  Comment                         =
  Directory entry type            = Indirect
  Catalog node number             = 0

$ db2 connect to xwpsdb user wasuser using wasuser

Database Connection Information

  Database server        = DB2/6000 7.2.3
  SQL authorization ID   = WASUSER
  Local database alias   = XWPSDB
$ db2 update db cfg for xwpsdb using applheapsz 16384
$ db2 update db cfg for xwpsdb using stmheap 60000
$ db2 update db cfg for xwpsdb using app_ctl_heap_sz 8192
$ db2 update db cfg for xwpsdb using locklist 400
$ db2 update db cfg for xwpsdb using indexrec RESTART
$ db2 update db cfg for xwpsdb using logfilsiz 1000
$ db2 update db cfg for xwpsdb using logprimary 12
$ db2 update db cfg for xwpsdb using logsecond 10

$ db2set DB2_RR_TO_RS=yes
$ db2set
DB2ENVLIST=EXTSHM
DB2_RR_TO_RS=yes
DB2COMM=tcpip
$

### 4.1.2 Removing unnecessary databases

During installation, the DB2 instance owner db2inst1 was created and a sample database (DWCNTRL) inside that instance was created. As those are not used by WebSphere Portal, they can be deleted as shown in Example 4-2.

In this example, we remove the dwcntrl database and then delete the db2inst1 instance in the DB2 environment. In the AIX environment we remove the db2inst1 user and appropriate group and then remove the entry in the /etc/services file that was created for this DB2 instance.

The db2fenc1 user is not removed in this example, because it takes almost no resources and might be helpful for future usage.

Removing the user and the associated sample database is not required, but reasonable if you do not have any additional use for them.

**Example 4-2 Removing unnecessary DB2 instance db2inst1**

```bash
# cd
# id
uid=0(root) gid=0(system) groups=101(db2iadm1),103(db2asgrp),400(dbsysadm)
# su - db2inst1
$ db2start
SQL1063N  DB2START processing was successful.
$ db2 drop db dwcntrl
DB20000I  The DROP DATABASE command completed successfully.
$ db2 list db directory
SQL1057W  The system database directory is empty.  SQLSTATE=01606
$ db2stop
SQL1064N  DB2STOP processing was successful.
$ exit
# cd /usr/lpp/db2_07_01/instance
#. /db2ilist
db2inst1
ldapdb2
wasuser
#. /db2idrop db2inst1
DB110701 Program db2idrop completed successfully.

# /db2ilist
wasuser
```
ldapdb2
# userdel -r db2inst1
# rmgroup db2iadm1
# cd /etc
# cp -p services services.old
# grep 50000 services
db2cdb2inst1 50000/tcp # Connection port for DB2 instance db2inst1
# sed -e 's/^db2cdb2inst1.*$//' < services.old > services
#

4.1.3 Starting and stopping DB2 Universal Database

Only the instances used by WebSphere Portal are required to be started. The DB2 admin
user (db2as) is only required for certain tasks, such as using the DB2 Graphical
Administration Interface (db2cc). Therefore, the admin instance is optional.

To start DB2 for WebSphere Portal:

su - db2as -c 'db2admin start'
su - ldapdb2 -c 'db2start'
su - wasuser -c 'db2start'

To stop DB2 processes again (all applications must be disconnected):

su - ldapdb2 -c 'db2stop'
su - wasuser -c 'db2stop'
su - db2as -c 'db2admin stop'

4.2 WebSphere Application Server

In this section, we discuss some actions you might need to perform for your WebSphere
Application Server.

4.2.1 Updating sas.client.props

If you frequently use the Administration Console, it might be worth getting rid of the window
(see Figure 3-20 on page 45) that asks for username and password. To do so, the
sas.client.props file in /usr/WebSphere/ApplicationServer/properties requires an update.

Search for each of the following three lines:

com.ibm.CORBA.loginSource=prompt
com.ibm.CORBA.loginTimeout=300

com.ibm.CORBA.securityEnabled=true
com.ibm.CORBA.loginUserId=
com.ibm.CORBA.loginPassword=

Change the values for those three lines to:

com.ibm.CORBA.loginSource=properties
com.ibm.CORBA.loginTimeout=300

com.ibm.CORBA.securityEnabled=true
com.ibm.CORBA.loginUserId=wpsbind
com.ibm.CORBA.loginPassword=wpsbind
4.2.2 Starting and stopping applications from the command line

Even if you are able to use a graphical administration tool like the WebSphere Administration Console, it is helpful if you are able start and stop the WebSphere Application Server and WebSphere Portal from the command line.

**Note:** *All actions need to be done as user root!*

Always replace the sample node name (m10df55f) with your node name.

Make sure you updated the sas.client.props file as described above before using the XMLConfig.sh tool, that is used in this section.

- To start WebSphere Application Server use the command:
  ```
  /usr/WebSphere/AppServer/bin/startupServer.sh &
  ```
  With the command `tail -f /usr/WebSphere/AppServer/logs/tracefile` you can see the progress of program start. As soon as the line “... open for e-business” appears, WebSphere Application Server is started.

- To stop WebSphere Application Server create a file as shown in Example 4-3. You will need to replace the value of name in section node with the appropriate node name.

  You know the name of the node from the AdminConsole (see Figure 3-24 on page 48) and this name is usually equal to your hostname. To get your hostname, type:
  ```
  uname -n
  ```
  **Note:** These examples use the node name m10df55f. Make sure you replace this value with your own node name!

  To use the newly created file that we call stopwas.xml, change to the directory
  `/usr/WebSphere/AppServer/bin` and enter the command:
  ```
  # ./XMLConfig.sh -import stopwas.xml -adminNodeName m10df55f
  ```

  **Example 4-3 Sample XML file to stop the WebSphere Application Server node**

  ```xml
  <?xml version="1.0"?>
  <!DOCTYPE websphere-sa-config SYSTEM "file:///$XMLConfigDTDLocation$$dsep$xmlconfig.dtd" >
  <websphere-sa-config>
  <node name="m10df55f" action="stop">
  </node>
  </websphere-sa-config>
  ```

  Even though processing of the command is finished, WebSphere Application Server and the dependent processes of WebSphere Portal might not be stopped completely. Check the operating system for remaining java processes:
  ```
  ps -ef | grep java
  ```

  - To start WebSphere Portal as an application inside WebSphere Application Server use the command (with the XML file as shown in Example 4-4):
    ```
    ./XMLConfig.sh -import wps.xml -adminNodeName m10df55f -substitute "paction=start"
    ```
To stop WebSphere Portal without stopping WebSphere Application Server use the same XML file as before, but import it with:

```
./XMLConfig.sh -import wps.xml -adminNodeName m10df55f -substitute "paction=stop"
```

**Example 4-4 Sample XML file (wps.xml) to start WebSphere Portal**

```xml
<?xml version="1.0"?>
<!DOCTYPE websphere-sa-config SYSTEM "file:///$XMLConfigDTDLocation$$dsep$xmlconfig.dtd" >
<websphere-sa-config>
  <node name="m10df55f" action="update">
    <application-server action="$paction$" name="WebSphere Portal">
    </application-server>
  </node>
</websphere-sa-config>
```

### 4.3 SecureWay Directory

In this section, we discuss suggested activity you should perform for your SecureWay Directory.

#### 4.3.1 Apply SecureWay 3.2.2 eFix 2

You must apply eFix 2, that is included on CD-ROM #1 in the subdirectory /swd-eFix/aix. Carefully, read the installation instructions (AIX-128-2.txt) and apply the fix as described.

**Note:** Stop all processes, including WebSphere Portal and WebSphere Application Server that might access the LDAP Server before applying the eFix.

#### 4.3.2 Stopping and starting SecureWay Directory

Follow these procedures to stop and start the SecureWay Directory:

**Stop SecureWay Directory Server**

The recommended way to stop SecureWay Directory from a Shell is to send the main process a terminate task signal (TERM):

```
kill -15 'cat /etc/slapd.pid'
```

**Note:** *Use backticks, not single-quotes for this command!*

**Start SecureWay Directory Server**

The SecureWay Directory daemon process can be started issuing the command `slapd` from any directory. It comes with some command line tools, such as `ldapsearch`, `ldapxcfg`, `ldapadd`, `ldapdelete`, etc. Those programs can all be found in the `/usr/bin` directory and are therefore in the default PATH.

### 4.4 Changing passwords

This section is intended to show how to change some passwords after installation.
4.4.1 Change password for wpsadmin

In this section, we show how to change the password for the wpsadmin user, which is by default wpsadmin. We highly recommend that you change it. Therefore, complete the following instructions:

1. Use any Web browser to go to the WebSphere Portal page. In our sample setup that would be:
   http://m10df55f.itso.ral.ibm.com/wps/myportal
2. Log in as wpsadmin user.
3. Click **Edit my profile**, that is placed on the upper right corner of the Portal Web page. You will see a window similar to Figure 4-1.

![Figure 4-1](image)

*Figure 4-1 Personal Setup of any user can be change, including the wpsadmin user*

4. Enter your new password in the Password and Confirm Password fields. Click **Continue** to set the new password.

4.4.2 Change password for wpsbind

In this section, we show how to change the password wpsbind user. To change it, complete the following instructions:

1. Start AdminConsole.
2. Go to Security Center.
3. Go to the Authentication tab and change the value of the field Security Server Password as seen in Figure 4-2.

**Note:** The password change was applied to the users that was installed during this sample installation. Even though your users might be named differently, the same rules apply.
Figure 4-2  Setting a new password for the Security Server ID

4. Start the Directory Management Tool (DMT). You will see a window similar to Figure 4-3.
Figure 4-3  Open the LDAP directory tree, find and select the wpsbind user

**Tip:** You can start the DMT on a remote machine, such as a Linux or Windows PC and then connect to the machine where SecureWay Directory Server is installed. To do this, click **Add Server** button in the lower left corner.

DMT does not support usage at a Remote Display.

5. Rebind as Administrative User, which would be in our sample installation `cn=ldapadmin`

6. Browse in the directory tree to the user wpsbind, select it and click **Edit** (see red circle in Figure 4-3). Next, you will see a window similar to Figure 4-4.
7. Go to the end of the list in the window and change the value in the userPassword field. Click OK to set the new value. You can close the DMT, as it is not required any more.

8. Change back to the window of the Security Center in the AdminConsole (see Figure 4-2). Click Apply to set and validate the new password.

9. Stop the WebSphere Application Server node.

10. Update your sas.client.props, if you have ever changed it manually.

11. Start the WebSphere Application Server and the WebSphere Portal, for example, as described in 4.2.2, “Starting and stopping applications from the command line” on page 55.

### 4.4.3 Change password for DB2 user wasuser

In this section, we provide an example changing the wasuser password. The user, wasuser, was used during installation as the DB2 instance for all databases. Complete the following instructions:

1. Change the user password on the AIX operating system.
   
   Open a Terminal as root user and change the password of the wasuser as shown below:
   
   ```
   # su - wasuser
   $ passwd
   Changing password for "wasuser"
   wasuser's Old password: 
   wasuser's New password: 
   Enter the new password again: 
   $ exit
   #
   ```

   **Note:** This will not only change the UNIX password of this user, but also alter the password used to connect to the databases.
2. Change the database password for WebSphere Application Server.

   This procedure includes two steps, changing the admin.config file of WebSphere Application Server and changing the password in the appropriate DataSources inside WebSphere Application Server.

   a. Make sure WebSphere Application Server is not running.

   b. Create a file (for example /tmp/filename) with a single line:

   ```
   com.ibm.ejs.sm.adminServer.dbpassword=newpassword
   ```

   c. Run the following command:

   ```
   java -classpath /usr/WebSphere/AppServer/lib/security.jar
   com.ibm.ws.security.util.PropFilePasswordEncoder /tmp/filename
   com.ibm.ejs.sm.adminServer.dbpassword
   ```

   d. Replace the line that starts with com.ibm.ejs.sm.adminServer.dbpassword in the file /usr/WebSphere/AppServer/bin/admin.config with the line in the changed file /tmp/filename

   e. Start the WebSphere Application Server.

   f. Start the AdminConsole of WebSphere Application Server.

   g. To change the password for the Pers DataSource that is required by WebSphere Personalization Server, open the folder Resources, then the folder JDBC Providers and then the Pers DB Driver folder. Click **Data Sources** folder to view a window similar to Figure 4-5.

![WebSphere Advanced Administrative Console](image)

*Figure 4-5 Changing the password for the Personalization Data Source*
h. To change the password of the Pers DataSource.
   Change the value in the field password and click **Test Connection** button (see Figure 4-5). If you issued the correct password a popup window will tell you that the connection was successful.

i. Click **Apply**.

j. You might want to do the same procedure for the Sample DB Driver, even though this is not required to run WebSphere Portal.

k. Close the AdminConsole.

3. Change the database password for WebSphere Portal.

   The primary source that WebSphere Portal uses to lookup the password is the property file `<was_home>/lib/app/config/services/DataStoreService.properties`, where `<was_home>` is the home directory of the WebSphere Application Server. In our sample installation that would be `/usr/WebSphere/AppServer`.

   The values for `datasource.userid` and `datasource.password` are by default empty. We do not recommend changing this default setting.

   – If the values are not empty, you have to change them in this property file.
   – If the values are empty, you have to change the password setting in the wps40DS DataSource of WebSphere Application Server.

   To do so, follow these steps:

   i. Start the AdminConsole of WebSphere Application Server.

   ii. Make sure, the WebSphere Portal application is not started.

   iii. Open the folder Resources, then the folder JDBC Providers and after that the wps40JDBC folder. Click **Data Sources** and you will see a window similar to Figure 4-6.
iv. Select the wps40DS and change the value in the field password and click on the Test Connection button. If you issued the correct password a popup window will tell you that the Connection was successful.

v. Click Apply.

vi. Close the AdminConsole.

**Note:** If WebSphere Member Services uses the same database user, as we have it in our sample installation, make sure you also change the passwords for WebSphere Member Services as described below before starting the WebSphere Portal application.


You cannot change the password for the database, WebSphere Member Services uses, by updating the database properties in the proper WebSphere Application Server Data Resource.

The password for the database is an encrypted value in the field DBUserPwd that can be found in the file <was_home>/lib/app/xml/wms.xml, where <was_home> is the home directory of WebSphere Application Server.

Accidentally, the database userid and password is also defined in the deployed Enterprise Java Bean. To make the password change happen, you will need to remove these entries.

There are three steps required to update the password:
a. Create a new encrypted value by using a command as root user as shown here:

```
# cd /usr/WebSphere/PortalServer/bin
# ./wms_encrypt.sh newpassword
```

b. Replace the old value of DBUserPwd in wms.xml with the new generated ASCII value. Use an editor like vi to do this. The commands might look like the following:

```
# cd /usr/WebSphere/AppServer/lib/app/xml
# vi wms.xml
-> use Editor to replace the old value with the new one and save
# grep DBUser wms.xml
DBUserID="wasuser"
DBUserPwd="o78nO8D0o8nfEdlaGcU9fw=="
```

c. Remove the username/password entries in the installed Enterprise Java Beans (EJB) of WebSphere Member Service.

i. Start the WebSphere Application Server AdminConsole.

ii. Open the Enterprise Applications folder, then the WebSphere Member Subsystem folder and click EJB Modules folder.

iii. Click WCSCommon EJB and select General tab. A window will appear similar to Figure 4-7.

iv. Remove the UserId and Password, that is stated there and click Apply.

v. Click WCSServer EJB, remove the UserId and Password and click Apply.

vi. Click WCSUser EJB, remove the UserId and Password and click the Apply button.
vii. Ensure the wmsDS has the correct password.

Open the folder Resources, then the folder JDBC Providers, and after that the wps40JDBC folder. Click **Data Sources** to get to a window as shown in Figure 4-6 on page 63.

Select **wmsDS**, retype the password for the database user in the field password and click on the Test Connection button. If you issued the correct password a popup window will tell you that the Connection was successful.

viii. Click **Apply** and close the AdminConsole.

### 4.4.4 Change password for LDAP Admin user cn=ldapadmin

In this section, we provide an example changing the ldapadmin password.

Two steps are required to change the password of your Administrative Distinguished Name (DN) of your SecureWay Directory Server. First is to update the password in the LDAP Server itself, then second to update that password in the settings of WebSphere Member Service.

**Note:** If you do not have SecureWay Directory, but another LDAP Server, refer to the documentation of this product on how to change the password for the Administrative user.

Make sure WebSphere Portal is not running during configuration change.

1. Change Administrative DN password in SecureWay Directory Server:
   a. Start as root user the IBM SecureWay Directory Configuration Utility by using the command `ldapxcfg`. If you are unable to use graphical tools, use `ldapcfg` instead.

   ![Figure 4-8 Set or change the Administrative DN for SecureWay Directory](image)

   **Figure 4-8  Set or change the Administrative DN for SecureWay Directory**

   b. Select **Set the directory administrator name and password** as shown in Figure 4-8 and click **Next**.
WebSphere Portal V4.1 AIX 5L Installation

Figure 4-9 Insert a new password for the LDAP Administrative DN

c. Figure 4-9 has the current Administrative user inserted in the Administrative DN field. Make sure the field includes what you expect. For our example, the correct value is cn=ldapadmin.

d. Insert your new password in both the Administrator Password field and the Type the password again to confirm field as shown in Figure 4-9. Click Next to continue.

e. A summary of the actions you intend to set up will appear. Click Configure to execute the changes.

Figure 4-10 Information window in LDAP Configuration Utility about the setup change

f. A window as shown in Figure 4-10 informs you if your setup changes were applied successfully.


Note: The change of the Administrative DN password will take effect when you start the SecureWay Directory Server again.
2. Change Administrative DN password for WebSphere Member Services.

To change the password of the Administrative DN user in the WebSphere Member Service configuration you will need to update the file <was_home>/lib/app/xml/wms.xml, where <was_home> is the home directory of WebSphere Application Server.

The password for the database is an encrypted value in the field LdapAdminPW.

There are two steps required to update this password value:

a. Create a new encrypted value by issuing a command as root user as shown below:

```
# cd /usr/WebSphere/PortalServer/bin
# ./wms_encrypt.sh newpassword
IBM*
Licensed Materials - Property of IBM
5697-A16
(C) Copyrights by IBM and by other(s) 1978, 1997. All Rights Reserved.
* Trademark of International Business Machines Corp.
ASCII encrypted string : o78nO8D0o8nfEdlaGcU9fw==
HEX encrypted string : 6F37386E4F3844306F386E6645646C614763553966773D3D
```

b. Replace the old value of LdapAdminPW in wms.xml with the new generated ASCII value. Use an editor like vi to do this. The commands might look like the following:

```
# cd /usr/WebSphere/AppServer/lib/app/xml
# vi wms.xml
-> use Editor to replace the old value with the new one and save
# grep LdapAdmin wms.xml
LdapAdminDN="wasuser"
LdapAdminPW="o78nO8D0o8nfEdlaGcU9fw=="
```

4.4.5 Change password for the users ldapdb2, ldap

These users currently have no password and they are not allowed to log in. This is a secure and reasonable default value. Setup of a password with the standard UNIX command passwd does not hurt functionality.

4.4.6 Change password for the users db2as, db2fenc1, db2inst1

The default password of these automatically generated users is ibmdb2. We highly recommend that you change these values. To do so, log in as the appropriate user and change the password as shown in the example below:

```
# su - db2as
$ passwd
Changing password for "db2as"
db2as's Old password:
db2as's New password:
Enter the new password again:
$ exit
```

4.4.7 Change password for the user httpd

To change the password for the IBM HTTP Server (IHS) user you have to do two configuration changes. One is to change the UNIX user password, and the other is to change the IHS Administrator password. The changes can be done independently of each other.
Change password in the UNIX environment.

Log in as httpd user and use the passwd command as shown in the example below:

```
# su - httpd
$ passwd
Changing password for “httpd”
httpd’s Old password:
httpd’s New password:
Enter the new password again:
$ exit
```

Change password for the IHS Administrator.

Use the following command as root user to change the password for the Administrator, that is in our example the user httpd:

```
# /usr/HTTPServer/bin/htpasswd -m /usr/HTTPServer/conf/admin.passwd httpd
New password:
Re-type new password:
Updating password for user httpd
```

4.4.8 Change LTPA password of WebSphere Application Server Security

Keep in mind that if you change the LTPA password, your exported LTPA Security keys are no longer valid. That is because changing the LTPA password requires regenerating the Security keys.

![Figure 4-11 Setting a new LTPA Password by generating new security keys](image)

To change the LTPA Password, complete the following steps:

1. Open the AdminConsole and from there, open the Security Center.
2. Click the Authentication tab to get a window as shown in Figure 4-2 on page 58.
3. Click the Generate Keys button that is located in the center of the window.
4. You will get a popup window as shown in Figure 4-11. Insert a new LTPA password, confirm it, and click OK.
5. Restart WebSphere Application Server by stopping the node.
Related publications

The publications listed in this section are considered particularly suitable for a more detailed discussion of the topics covered in this Redpaper.

IBM Redbooks

For information on ordering these publications, see “How to get IBM Redbooks” on page 70.

- *IBM WebSphere V4.0 Advanced Edition Handbook*, SG24-6176
- *WebSphere Solution Bundles: Implementation and Integration Guide*, SG24-6550
- *IBM WebSphere V4.0 Advanced Edition Security*, SG24-6520
- *IBM WebSphere V4.0 Advanced Edition Scalability and Availability*, SG24-6192
- *WebSphere Application Server V4 for Linux, Implementation and Deployment Guide*, REDP0405

Referenced Web sites

These Web sites are also relevant as further information sources:

- WebSphere Application Server Advanced Edition 4.0-PTF and FixPaks
- WebSphere Software Platform
  http://www.ibm.com/websphere
- IT and Professional Training
  http://www.ibm.com/services/learning
- WebSphere Portal for Multiplatforms
- Portlet Development Guide
- InfoCenter
  http://www.ibm.com/software/webservers/portal/library/enable/InfoCenter
- WebSphere Portal planning sheet
- Introduction to custom registries
  http://www-3.ibm.com/software/webservers/appserv/doc/v40/ae/infocenter/was/0502.html
How to get IBM Redbooks

You can order hardcopy Redbooks, as well as view, download, or search for Redbooks at the following Web site:

ibm.com/redbooks

You can also download additional materials (code samples or diskette/CD-ROM images) from that site.

IBM Redbooks collections

Redbooks are also available on CD-ROMs. Click the CD-ROMs button on the Redbooks Web site for information about all the CD-ROMs offered, as well as updates and formats.
Install and administer WebSphere Portal in an AIX environment

Understand options and implications of Setup Manager

AIX considerations for WebSphere Portal

This IBM Redpaper will help you plan, install and administer the IBM WebSphere Portal Version 4.1.2 Enable offering product in an IBM AIX 5L environment, so that existing enterprise applications can be accessed from portlets using the IBM WebSphere Portal product.

This Redpaper provides easy, step-by-step examples allowing you to rapidly deploy IBM WebSphere Portal Version 4.1.2 on AIX 5L — therefore, providing you with a solid foundation to begin importing and using existing portlets to access your enterprise applications. You will find the recommended process of using Setup Manager to install WebSphere Portal 4.1.2. In addition, you will find an in-depth description of the available options during the Setup Manager process.

A basic knowledge is assumed for AIX, LDAP Directory Services, WebSphere Portal, Java technologies such as servlets, as well as HTML and XML markup languages, and the terminology used in Web publishing.