WebSphere software

IBM

IBM WebSphere Everyplace Access V5 Handbook for Developers and Administrators

Volume I: Installation and Administration

- Extend your e-business applications to PDAs, phones, and other device types
- Install WebSphere Everyplace Access on AIX and Windows
- Deploy online portlet applications for PDAs

Juan Rodriguez
Anna Gangitano
Christian Kirsch
Marty Lassiter
Manuel Rodriguez
Gianfranco Rutigliano
Gregg Sanders
Guillermo Villavicencio

Redbooks

ibm.com/redbooks

Petitioner has added letters to pages (a)-(c) and numbers to pages 441-442. Otherwise, it leaves the original page numbering.

SAP AMERICA, INC.
EXHIBIT 1006

International Technical Support Organization

IBM WebSphere Everyplace Access V5 Handbook for Developers and Administrators Volume I: Installation and Administration

May 2005

SG24-6462-00

Note: Before using this information and the product it supports, read the information in "Notices" on page ix.

First Edition (May 2005)

This edition applies to Version 5 of IBM WebSphere Everyplace Access for multiplatforms.

© Copyright International Business Machines Corporation 2005. All rights reserved.
Note to U.S. Government Users Restricted Rights -- Use, duplication or disclosure restricted by GSA ADP Schedule Contract with IBM Corp.

Contents

Notices ix
Trademarks x

Preface xi
The team that wrote this redbook xi
Become a published author xiv
Comments welcome xiv

Chapter 1. Overview 1
1.1 The big picture 2
1.2 Inside the product 4
1.3 WebSphere Everyplace Access 4
1.3.1 Portlets 6
1.3.2 WebSphere Everyplace Access services 6
1.4 Everyplace Client 14
1.4.1 Tested devices 16
1.4.2 Resource Checker 17
1.4.3 Everyplace Client features per platform OS 18
1.5 Everyplace Toolkit V5.0.1 19
1.6 New in WebSphere Everyplace Access V5.0 20
1.7 Component products 21
1.7.1 Featured components 21
1.7.2 Support components 22
1.7.3 Third-party components 23
1.8 System hardware and software requirements 24
1.9 Complementary products 24

Chapter 2. Enhanced portlets 27
2.1 Introduction 28
2.2 Enhanced portlets provided by Everyplace Access 28
2.2.1 Lotus Notes PIM and e-mail portlets 29
2.2.2 Microsoft Exchange PIM and e-mail portlets 33
2.2.3 Productivity portlets 37

Chapter 3. Administration 41
3.1 WebSphere Portal Server overview 42
3.1.1 Welcome to the portal 42
3.2 Starting WebSphere Everyplace Access services 45
3.3 Getting started 46

© Copyright IBM Corp. 2005. All rights reserved.

3.4 Portal user interface 48
3.4.1 Manage pages 48
3.4.2 Themes and skins 64
3.5 Portlets 67
3.5.1 Portlet Install 67
3.5.2 Manage applications 68
3.5.3 Manage Portlets 70
3.5.4 Web clipping 71
3.6 Access 74
3.6.1 Users and groups 74
3.6.2 Giving permissions to resources 81
3.7 Portal settings 91
3.7.1 Supported markup 91
3.7.2 Supported clients 94
3.8 Portal analysis 97
3.9 WebSphere Everyplace functions 97

Chapter 4. Basic WebSphere Everyplace Access installation 99
4.1 Overview 100
4.2 Domino server installation 100
4.2.1 Preparation 101
4.2.2 Install Lotus Notes 103
4.2.3 Installing Domino Server 104
4.2.4 Lotus Domino configuration for WebSphere Everyplace Access . . 106
4.3 Installing WebSphere Everyplace Access 113
4.3.1 Preparation 113
4.3.2 Installation of Lotus Notes 117
4.3.3 Installation of WebSphere Everyplace Access 118

Chapter 5. Component installation 125
5.1 Overview 126
5.2 Server 1 - Lotus Domino 127
5.2.1 Preparation 127
5.2.2 Install Lotus Notes 129
5.2.3 Installing Domino 130
5.2.4 Lotus Domino configuration 132
5.2.5 Summary 140
5.3 Server 2 - WebSphere Everyplace Access 141
5.3.1 Preparation 141
5.3.2 Install Lotus Notes 146
5.3.3 Installation of WebSphere Everyplace Access 149

Chapter 6. AIX component installation 221
6.1 Overview 222

6.2 Server 1 - Lotus Domino 223
6.2.1 Preparation 223
6.2.2 Install Lotus Notes. 225
6.2.3 Installing Domino. 226
6.2.4 Lotus Domino configuration 228
6.2.5 Summary. 236
6.3 Server 2 - WebSphere Everyplace Access 236
6.3.1 Requirements 237
6.3.2 Preparation 237
6.3.3 Install the Lotus Domino Server on AIX 240
6.3.4 Installation of WebSphere Everyplace Access 242

Chapter 7. WebSphere Everyplace Client installation and configuration 287
7.1 Overview 288
7.2 Everyplace Client for Palm OS 289
7.2.1 Everyplace Client V5.0.1 installation. 290
7.2.2 Everyplace Client configuration. 296
7.3 Everyplace Client for Pocket PC 303
7.3.1 Everyplace Client V5.0.1 installation. 303
7.3.2 Everyplace Client configuration. 309

Chapter 8. Everyplace Client secure connections 315
8.1 Introduction 316
8.2 Enabling SSL on IBM HTTP Server 316
8.2.1 Creating a key database 316
8.2.2 Create a self-signed key file 318
8.2.3 Setting up IBM HTTP Server. 320
8.2.4 Verifying if security is enabled on IBM HTTP Server 321
8.3 Enabling SSL in WebSphere Application Server. 321
8.3.1 Configuring WebSphere Application Server 322
8.3.2 Verifying if security is enabled in the Application Server. 326
8.4 Configure WEA files to support SSL 326
8.4.1 Verifying if security is enabled on IBM HTTP Server 327
8.5 Enabling security for Offline Portal Content 328
8.6 Enabling SSL in Everyplace Client 331
8.6.1 Enabling SSL in Pocket PC devices 331
8.6.2 Enabling SSL in Palm devices 333

Chapter 9. Device Services 339
9.1 Device Services overview 340
9.1.1 Architecture 340
9.1.2 Device Services 341
9.1.3 Device Services Agent 341
9.1.4 Device Services database. 341

9.1.5 Device Management portlets 342
9.1.6 Device Services console 342
9.2 Setting the stage 343
9.2.1 Creating a device management user group 343
9.2.2 Starting the Device Services console 343
9.3 Scenarios 345
9.3.1 Using Device Manager portlets to install the WebSphere Everyplace Access Client 345
9.3.2 Software distribution using Device Manager Console. 355
9.3.3 Configuring SSL on a Palm device 365
9.4 Troubleshooting. 373

Chapter 10. Instant messaging 375
10.1 Overview 376
10.1.1 Sametime messaging on Pocket PC. 377
10.1.2 Sametime messaging on Palm OS 383
10.1.3 Sample scenario 384

Chapter 11. Resource Checker 387
11.1 Introduction 388
11.2 Installation 388
11.3 Determining device resources. 389
11.4 Running the Resource Checker 390

Chapter 12. Bulk user loading from existing mail environments 395
12.1 Overview 396
12.1.1 Configure the Bulk Load Portlet 396
12.1.2 Customize e-mail notifications 400
12.1.3 Using the Bulk Load portlet 402
12.1.4 Other functionality 413

Appendix A. A sample Sametime installation 421
Installation and configuration 422
Installation 422
Configuration. 424
Setting up Sametime Everyplace (STEP) 425
Checking the installation 429

Related publications 431
IBM Redbooks 431
Other publications 432
Online resources 432
How to get IBM Redbooks 433
Help from IBM 433

Index 435

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.

© Copyright IBM Corp. 2005. All rights reserved.

Trademarks

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

AIX®	Everyplace®	Redbooks™
Cloudscape™	IBM®	Redbooks (logo) ™
Domino®	iSeries™	Sametime®
DB2®	Lotus Notes®	SecureWay®
DB2 Universal Database™	Lotus®	Tivoli®
@server®	Notes®	WebSphere®
@server®	pSeries®	z/OS®

The following terms are trademarks of other companies:

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.

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

Intel, Intel Inside (logos), and Pentium are trademarks of Intel Corporation in the United States, other countries, or both.

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

Linux is a trademark of Linus Torvalds in the United States, other countries, or both.

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

Preface

This IBM® Redbook is part of a series of four volumes related to WebSphere® Everyplace® Access V5.0. These Redbooks™ will help you plan, install, administer, and develop mobile applications to run in a WebSphere Everyplace Access V5.0 environment. The information provided in these Redbooks target business-to-employee (B2E) enterprise applications, but most of the scenarios presented will apply to business-to-consumer (B2C) applications as well. In these Redbooks, you will find step-by-step examples and scenarios showing ways to integrate your enterprise applications into a WebSphere Everyplace Access environment using the WebSphere Studio Site Developer and the Everyplace Toolkit, as well as extending your online and offline application capabilities to use other advanced functions.

In this redbook, you will also find step-by-step sample installation and administration procedures to help you get online and access your enterprise applications from PDAs, such as Pocket PCs and Palm devices. The redbook includes topics such as product installation, administration, instant messaging implementation, device management, and how to establish secure connections.

A basic knowledge of Java™ technologies, such as servlets, JavaBeans, EJBs, JavaServer Pages (JSPs), as well as XML applications and the terminology used in Web publishing, is assumed.

The following IBM WebSphere Everyplace Access V5 Redbooks are part of this offering:

- *IBM WebSphere Everyplace Access V5 Handbook for Developers and Administrators Volume I: Installation and Administration*, SG24-6462
- *IBM WebSphere Everyplace Access V5 Handbook for Developers and Administrators Volume II: Application Development*, SG24-6463
- *IBM WebSphere Everyplace Access V5 Handbook for Developers and Administrators Volume III: E-Mail and Database Synchronization*, SG24-6676
- *IBM WebSphere Everyplace Access V5 Handbook for Developers and Administrators Volume IV: Advanced Topics*, SG24-6677

The team that wrote this redbook

This redbook was produced by a team of specialists from around the world working at the International Technical Support Organization, Raleigh Center.

© Copyright IBM Corp. 2005. All rights reserved.

Juan Rodriguez is a Consultant at IBM ITSO, Raleigh Center. He received his M.S. degree in Computer Science from Iowa State University. He writes extensively and teaches IBM classes worldwide on such topics as networking, pervasive computing, Web technologies, and information security. Before joining the IBM ITSO, he worked at IBM Research Triangle Park, North Carolina as a designer and developer of networking products.

Anna Gangitano holds a M.S. in Computer Science Engineering from Catania University, Italy. She is currently an IT Wireless Infrastructure Specialist working at the IBM SEMEA Sud, Mobile Technology Centre in Italy. Anna has a strong background in wireless solutions and has developed Digital Media solutions with collaboration at the IBM Boca Raton laboratory. She has experience with GPRS networks and a good knowledge of IBM Pervasive Computing products.

Christian Kirsch is an IT Specialist at IBM Global Services, Germany. He has been involved in several projects using pervasive computing technology. His areas of expertise include workforce mobility, remote access, and device management solutions. He holds a degree in Information Technology. In 2004, he moved to the Wireless Broadband and Sensing Solutions EBO.

Marty Lassiter works in the IBM Global Services Wireless PilotCenter in Charlotte, North Carolina. He is primarily responsible for the design and implementation of wireless middleware pilots and production systems for IBM's strategic outsourcing customers. He specializes in WebSphere Everyplace Access, WebSphere Everyplace Connection Manager, and BlackBerry Enterprise Server. He holds a Masters of Business Administration from the University of North Carolina at Charlotte, North Carolina.

Manuel Rodriguez has nine years of experience working in the wireless and pervasive e-business arena. Currently, he is working in the Wireless Broadband and sensing solutions department at IBM Spain Global Services as an IT Architect Solution Area Leader in RFID. His responsabilities include the development of new emerging business around Wireless solutions in innovative projects. Prior to working for IBM, Manuel worked for the European Space Agency in real time development projects.

Gianfranco Rutigliano holds a degree in Systems Engineering from the University of Lima (Peru) and has been a member of IBM Global Services for four years. He has strong experience designing and implementing pervasive and Java-based Web solutions. He is currently a Software Architect for Avatar e-Business Solutions, an IBM Business Partner, and has participated in several ITSO residencies for pervasive computing and WebSphere technologies.

Gregg Sanders is responsible for Pervasive Technical Sales for South and Central Africa, working with the WebSphere Pervasive product set, which includes Portal, Voice, and Connection Management. He has fulfilled a number of roles in his 5-year IT career, ranging from IT Technician, Systems and Network Administrator, Lotus® Domino® Developer, Java (J2EE) Developer, Architecture and Software Tester, and Consultant. He is also part of a South African Wireless initiative involving cutting-edge IBM tools and concepts.

Guillermo Villavicencio holds a degree in Informatics Engineering from the Pontifical Catholic University of Peru and works as a Software Architect for Avatar e-Business Solutions, an IBM Business Partner. He has been the architect for several e-business projects including wireless and Portal solutions. His current area of expertise is centered around Web technologies and pervasive computing.

Thanks to the following people for their contributions to this project:

Margaret Ticknor
International Technical Support Organization, Raleigh Center

Robert Sundstrom
IBM Research Triangle Park, North Carolina, USA

Mary Fisher
IBM Boca Raton, Florida, USA

Wade Wallace
International Technical Support Organization, Austin 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 customers.

Your efforts will help increase product acceptance and client 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 Redbooks to be as helpful as possible. Send us your comments about this 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 e-mail to:

  redbook@us.ibm.com

- Mail your comments to:

  IBM Corporation, International Technical Support Organization
  Dept. HZ8 Building 662
  P.O. Box 12195
  Research Triangle Park, NC 27709-2195

1

Overview

As the popularity of mobile computing grows, mobile workers are realizing the value of having access to information and resources held by the enterprise. Access to this information and the enterprise resources allows them to work more effectively and stay up to date with changing events and new information while away from the office. Likewise, enterprises are seeing real benefit from providing their mobile work force with mobile devices and giving access to enterprise information and applications.

In this chapter, we introduce you to IBM WebSphere Everyplace Access V5.0, a key component to extend business applications to mobile users. WebSphere Everyplace Access is designed to address the complexity and diversity of providing and managing mobile computing solutions for the enterprise. This chapter provides a high-level overview of WebSphere Everyplace Access, including:

- The product architecture and how it supports the enterprise
- An overview of the main components of the product
- An introduction to the various services that are provided by WebSphere Everyplace Access

© Copyright IBM Corp. 2005. All rights reserved.

1.1 The big picture

WebSphere Everyplace Access (subsequently referred to as Everyplace Access) is a comprehensive product that provides end-to-end coverage for the enterprise mobile computing needs. Everyplace Access is middleware that enables the enterprise and business partners to create robust mobile computing solutions that extend enterprise resources such as business applications, business data, and business information to the mobile worker. Everyplace Access consists of both the *infrastructure* intended to reduce the complexity of providing mobile computing solutions and the *services* needed to create the right mobile solution for the mobile worker and their particular needs.

Everyplace Access provides the connection between the mobile client and the enterprise environment. Figure 1-1 on page 3 provides the logical view of the overall mobile computing runtime environment. The figure shows the following major areas:

- Mobile client devices: Everyplace Access supports a variety of mobile devices, including various personal digital assistants (PDAs) and cell phones. Everyplace Client, included with Everyplace Access, provides a device environment for creating robust mobile solutions.
- Network (connectivity): Everyplace Access provides service across the majority of mobile computing network models, such as a wired and wireless infrastructure and local or wide area wireless networks.
- Load Balancing: An optional complementary product provided by IBM (WebSphere Edge Server) or a third party that improves performance and scalability of the overall mobile computing environment. WebSphere Application Server (part of the infrastructure of Everyplace Access) provides additional capabilities to create multiple instances of the components to improve availability and scalability.
- WebSphere Everyplace Access: The server-based portion of the product that provides the access point to the enterprise resources, such as PIM and e-mail, data (through connected access or data synchronization), offline browsing and offline forms entry, and business data synchronization.
- Enterprise Resources: These include business applications, Web content, and business data and information that are used to run the business and support business processes. Access to these resources can help the mobile worker perform their business activities more efficiently and effectively.

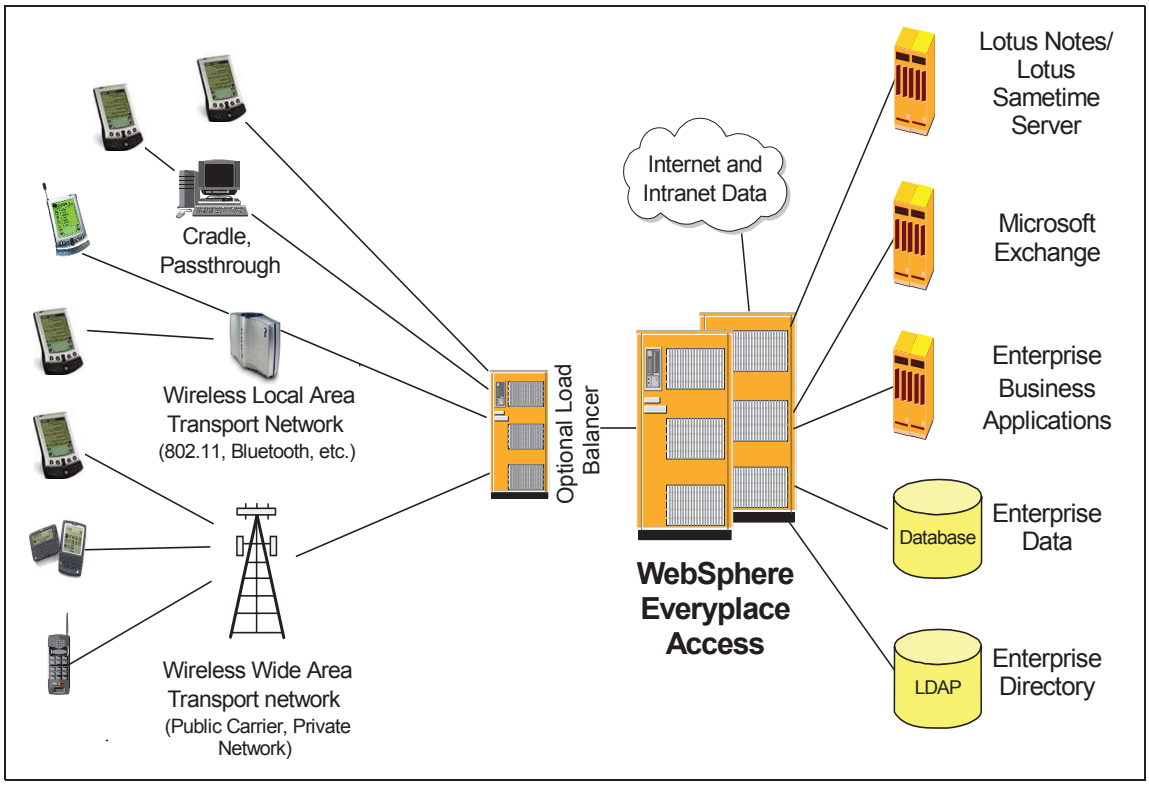

Figure 1-1 Logical view of mobile computing with WebSphere Everyplace Access

By being the access point to the enterprise, Everyplace Access addresses the complexity of mobile computing within the Enterprise environment and simplifies the overall runtime environment. The logical view in Figure 1-1 shows Everyplace Access in support of the enterprise and identifies it as providing the consistent access point for the mobile users regardless of the mobile device, the network, or the type of request or interaction with the enterprise that is needed.

Everyplace Access follows the IBM software development ground rules of incorporating open standards-based technology into the product and reusing existing technology wherever appropriate. Both IBM WebSphere Application Server and WebSphere Portal technologies provide the foundation for Everyplace Access. These products are built using open standards and open technology, such as XML and Java. Mobile computing technologies are changing fast and quickly evolving, which makes Everyplace Access the stabilizing factor in a very dynamic world. Everyplace Access accomplishes this by allowing the solution developer to write to its services, which minimizes the need to understand the details of the underlying technologies.

1.2 Inside the product

Everyplace Access comprises three major components necessary for delivering robust mobile computing solutions for the enterprise. The three components are:

1. WebSphere Everyplace Access: The server-based product that provides the infrastructure for interacting with the enterprise (from a mobile device) and the services that allow the enterprise to provide mobile solutions for mobile workers. It is the access point to the enterprise from the mobile device.
2. Everyplace Client: A mobile client environment that runs on the mobile device (PDA and cell phones), enabling mobile users to interact with WebSphere Everyplace Access components. Everyplace Client supports the mobile device when operating in a connected or occasionally connected mode.
3. Everyplace Toolkit: A plug-in for WebSphere Studio (WebSphere Studio Site Developer Advanced or WebSphere Studio Application Developer) that provides the developer with the tools needed to create mobile solutions. Associated with the Everyplace Toolkit and WebSphere Studio is WebSphere Studio Device Developer, which has the tools necessary to build a mobile device-based application, and the Mobile Application Builder, which is used to create DB2e-based applications.

These three components give Everyplace Access the ability to provide an end-to-end mobile computing solution environment by providing the runtime elements both at the server and at a mobile device, and the development tools necessary to create mobile solutions. Each of these components will be discussed in the following sections.

1.3 WebSphere Everyplace Access

As stated above, WebSphere Everyplace Access provides the access point to the enterprise for mobile devices. Figure 1-2 on page 5 shows the high-level architecture of WebSphere Everyplace Access (server side) and the services provided. Everyplace Access builds on the services provided by both WebSphere Application Server and WebSphere Portal technology and provides the additional services needed for mobile computing solutions. Everyplace Access uses many common services provided by the Portal technology, as shown in the Page Aggregation and Portlet Container & Services boxes within Figure 1-2 on page 5.

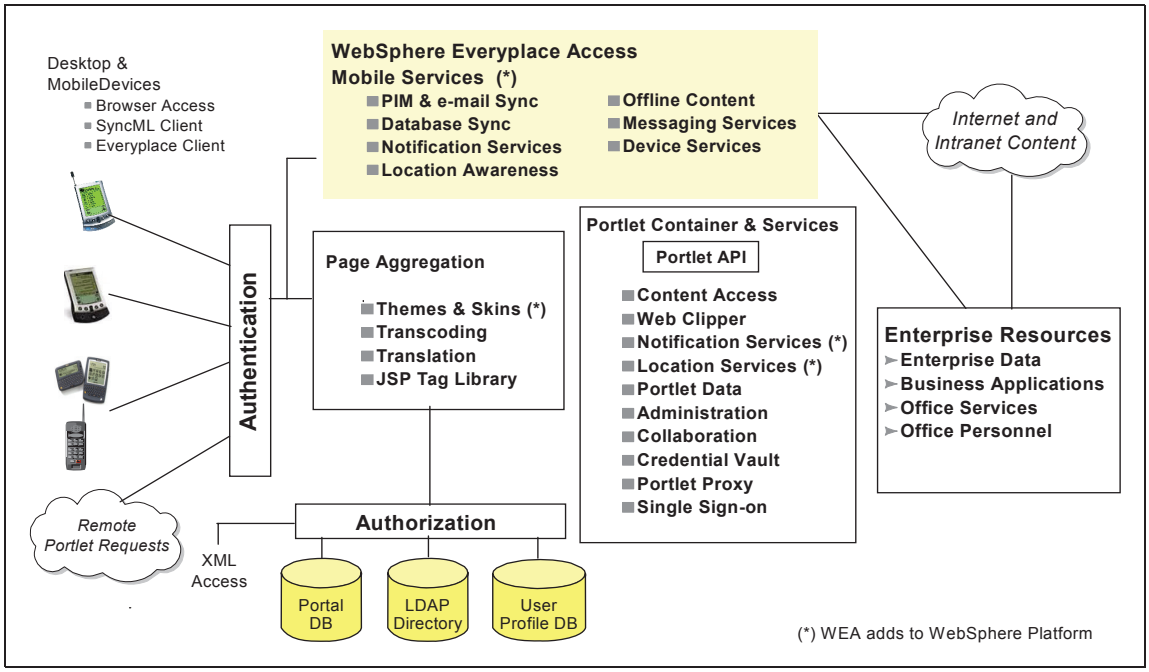

Figure 1-2 WebSphere Everyplace Access server

Everyplace Access provides a wide range of server-side functionality that includes:

- Basic Portal services for execution of mobile-enabled applications, including content access, Web clipper, portlet data, collaboration, Credential Vault, portlet proxy, and single sign-on.
- Administration that allows the management of mobile users (including their profiles and preferences), mobile devices, and the mobile solutions that make up the mobile computing environment.
- Services for connected or occasionally connected access to the enterprise.
- Browser-based access that is customized to the target device.
- Synchronization of PIM, e-mail, JDBC database data, Web content, and simple forms.
- Fundamental mobile enablement services that enhance the ability to deliver mobile computing solutions, such as:
  - Transcoding: Provides dynamic adaptation of Web and XML content to fit the device needs or user preferences
  - Themes and skins: Enhances the look and feel of the content and applications delivered to the device

  - Messaging Services: Support for mobile Sametime® and other messaging mechanisms
  - Device Services: Support for the management and maintenance of the mobile devices used within an enterprise environment
- Advanced mobile enablement services:
  - Intelligent Notification Services: Provides server-generated notifications when events occur that meet established criteria
  - Location Aware Services: An extension that can be incorporated into enterprise applications that provides device location and location-based service provider information access.

Everyplace Access relies on the authentication provided via the integrated Portal technology and the WebSphere Application Server (which is included in the software bundle). The integrated Portal technology provides authorization services such as users and groups management.

1.3.1 Portlets

Everyplace Access, much like WebSphere Portal, uses portlets as a fundamental building block for applications. Portlets are visual windows that organize content from different sources, such as Web sites, e-mail, and business applications, into a single interface for individual or group access. Portlets enable highly customized and productive work environments for projects, tasks, or organizational communities. They are applications that are based on the J2EE container model and run inside the Portal Container of the Portal, similar to the way servlets run within the Servlet Container for WebSphere Application Server.

Portlets are a special subclass of HTTPServlet that includes properties and functionality that allows them to run within the Portal Container. Even though portlets run as servlets, they do not interact with the browser directly. All communications back to the user from a portlet is accomplished through the aggregation modules.

For details about portlet applications, see *IBM WebSphere Everyplace Access V5 Handbook for Developers and Administrators Volume II: Application Development*, SG24-6463.

1.3.2 WebSphere Everyplace Access services

WebSphere Everyplace Access provides a wide variety of services that are available for creating robust mobile solutions that fit the enterprise and the mobile user's needs.

Administration

WebSphere Everyplace Access Administration provides centralized administration of information about the enterprise mobile environment. Administration is used to manage the overall environment, including users and groups, user customization, product administration, Portal content (online and offline Portal pages), Portal settings, security and access control, Web Clipping, and portlets.

Administration provides user and group definitions that include portlets for users to register and manage their own account information. User profile information includes a users's name and user ID, preference information such as news topics of interest, preferred language, and so on. A user may be a member of one or more groups. Group membership is used to determine the access rights to underlying services. For example, a user must belong to a group with permission to perform data synchronization in order to be authorized to use data synchronization on their PDA.

Note: For details about administration, see Chapter 3, "Administration" on page 41.

PIM and e-mail access

Everyplace Access supports both synchronization and online (connected) viewing of Personal Information Management (PIM) and e-mail information. Everyplace Access provides access to Lotus Domino Server Versions 5.0.12 to 6.5.3 and Microsoft® Exchange Servers 5.5, 2000, and 2003. For browser-based access, the information is tailored for the target device to improve the user experience.

Everyplace Access allows mobile users to have access to PIM and e-mail data from their company servers. It provides all the fundamental e-mail capabilities, including:

- Filtering: Allows the user to specify what e-mail gets delivered to the mobile device by selection criteria such as From, Subject, and Priority. Filtering helps limit the e-mail sent to the mobile device to those items that fit the selection criteria.
- Attachments: Allows the user to view and manage attachments on their mobile device. This includes adding attachments of any file type to new e-mail documents created on the mobile device. E-mail with attachments can also be forwarded from the mobile device. Updates to attachments are propagated in both directions during synchronization and it is possible to filter them out by type and size.
- Invitations: Allows the user to accept, decline, or reschedule meeting requests and initiate meeting requests on the mobile device.

- Recoverability: Allows interrupted synchronization to resume at the point of interruption when the connection is restored.
- Read status: Allows you to update the e-mail read status from both mobile clients and server.

PIM support includes access to contacts, tasks, to-do lists, calendars, and memos. PIM and e-mail are also available using native device mail and PIM services and is enabled on the Everyplace Client and SyncML compliant clients.

PIM and e-mail synchronization

The Everyplace Synchronization Service (ESS), a Everyplace Access server component, provides synchronization of PIM and e-mail data between the mobile device and the mail server. ESS interfaces with both Microsoft Exchange and Lotus Domino servers.

The Lotus Domino Adapter provides access to enterprise Lotus Domino server and supports e-mail, Address Book, Journals, and To Do and Calendar data types. The Microsoft Exchange Adapter provides access to Microsoft Exchange server and supports the following data types: e-mail, Contacts, Notes, Tasks, and Calendar.

ESS relies on SyncML data synchronization (DS), which is the standard for synchronization of remote data and personal information across different networks, platforms, and devices. SyncML, an XML-based protocol, defines the structure and format of SyncML messages exchanged between the mobile device and the server. Each SyncML message is a well-formed XML document that contains the business information and a set of related SyncML commands (add, delete, replace, and so on).

ESS supports the synchronization of e-mail data and PIM information, such as contacts, calendars, tasks, to do lists, and memos with the IBM Everyplace Client and other SyncML clients. Synchronization is profile driven. The profile defines the mail server the user intends to exchange data with, the user credentials to access that server, details on how conflicts are to be resolved during the synchronization process, data filtering, and any user synchronization preferences. A user may have multiple unique profiles for each device they wish to synchronize to the mail server.

E-Mail filters allow the user to determine which e-mail items will be delivered to their mobile device. The user can configure synchronization preferences to define the synchronization criteria. These preferences are used by ESS to determine what mail will be synchronized to your mobile device. By using the filters, a user can better control and manage the mail that is delivered to his or her mobile device.

ESS utilizes WebSphere Portal Server for security, administration, and user management purposes.

ESS and SyncML DS are covered in some detail in *IBM WebSphere Everyplace Access V5 Handbook for Developers and Administrators Volume III: E-Mail and Database Synchronization*, SG24-6676.

Data synchronization

Everyplace Access allows mobile users to have access and update enterprise data stored in a small footprint relational database and keep it synchronized with company database servers.

Everyplace Access enables data synchronization of JDBC-compliant database data to the DB2® Everyplace database, which is part of the Everyplace Client located on the mobile device. DB2 Everyplace has been incorporated into Everyplace Access. DB2 Everyplace is composed of three components:

- DB2 Everyplace Sync Server: Supports uni-directional and bi-directional synchronization of data between the mobile device and any server-based JDBC-compliant database, allowing both mobile device and enterprise database updating. It supports the following data sources: DB2 Universal Database™ for z/OS®, DB2 Universal Database for iSeries™, DB2 Universal Database for Linux®, UNIX® and Windows®, and any JDBC-compliant data source.
- DB2 Everyplace database: Provides a small footprint relational database located on the mobile device and is included as a part of the Everyplace Client.
- DB2 Everyplace SDK: Allows a faster and easier creation of DB2 Everyplace applications. For details about data synchronization, see *IBM WebSphere Everyplace Access V5 Handbook for Developers and Administrators Volume III: E-Mail and Database Synchronization*, SG24-6676.

Intelligent Notification Services (INS)

The Intelligent Notification Services are used to deliver information to users through different delivery channels (defined by the users) based on their preferences. This service allows the enterprise to proactively notify mobile workers (based on their subscription to particular notification applications) of important information and events. The notifications can be generated (when criteria is met) from a wide variety of sources, such as e-mail, news feeds, data management events, and directly from business applications. There are two general types of notifications:

1. Simple notifications: Messages that originate from other users or that come directly from applications. Examples would be personal messages or reminders.

2. Subscription-based notifications: Messages that are triggered by events to which users subscribe. For example, a subscriber could be notified when their favorite stock shifted five points.

To receive messages from the subscription-based notification, the user must request a subscription from the Subscription Manager. During the subscription process, the user specifies the information source, their notification criteria, any preferences, and subscription settings.

Figure 1-3 on page 11 shows the notification process. The figure is divided into three segments:

- Information sources: The originating sources of information that may cause the generation of a notification. This information may come from a variety of sources, such as Internet news services, the enterprise database, which is triggered when specific data changes occur, or business applications when certain criteria is met.
- Criteria: Once the information source sends the information, the Subscription Manager determines if that information meets the criteria established by the subscriber(s) and issues a message to the Notification Manager for further processing. Included in this section are a series of portlets used to define the user subscriptions, user preferences, and configuration information. This information is stored in a database.

  Simple notifications are sent directly to Notification Manager.
- Delivery: The Notification Manager is responsible for message formatting, using the subscriber's preferences to send the notification using the right delivery channel. A wide variety of delivery channels are supported, including Lotus Sametime, SMTP e-mail, Short Message Service (SMS), voice, Server-Initiated Actions and the Message Center portlet (which is part of Everyplace Access), or a custom-defined channel.

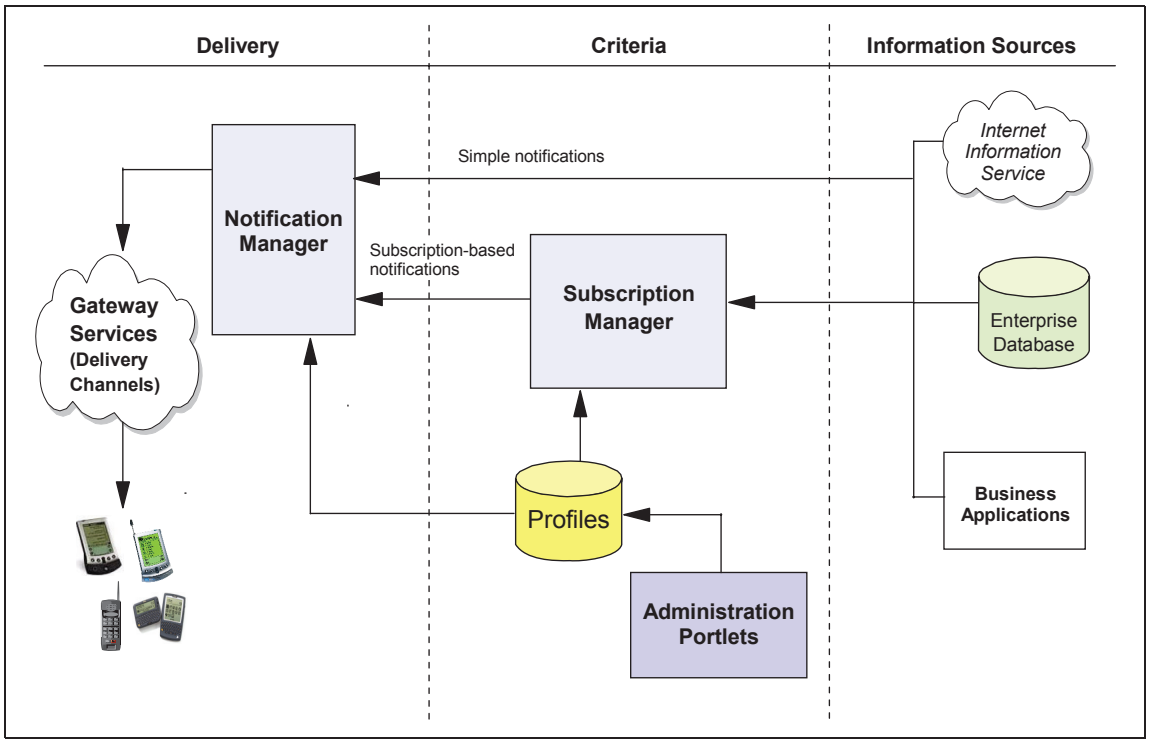

Figure 1-3 Notification services

Developers can extend the INS framework by adding more delivery channels and services.

The Intelligent Notification Services are detailed in *IBM WebSphere Everyplace Access V5 Handbook for Developers and Administrators Volume IV: Advanced Topics*, SG24-6677.

Location Aware Services

The Location Aware Services (LAS) enables the enterprise to take advantage of the location information provided by mobile devices and interpreted by the service provider of the location information. This service consists of a database, a set of mobile device-enabled portlets, and a rich set of Java APIs for accessing location-based services from enterprise or IBM Business Partner-written applications. These APIs isolate the developer from the underlying service provider details that may vary between providers.

LAS provides *transparency* to the developers, so they do not have to be worry about an individual's service provider (abstraction). Because services differ from different providers, LAS offers *provider differentiation*, allowing applications to

discern the service implementation that offers the desired capabilities. If service become unavailable, LAS provides the ability to roll over to another service provider if the primary provider fails (*dynamic service binding*), avoiding any interruption in the application.

The location services supported by LAS are:

- Geocoding: Using an address to determine its geographical coordinates
- Reverse geocoding: Converting geographical coordinates into the nearest address
- Mapping: Returning a map of a given location
- Routing: Returning directions in a road network from one point to another
- Directory: Finding points of interest and other entities around a given location
- Device position: Returning the location of a given subscriber's device

LAS enables dynamic balancing among several providers at runtime, helping to ensure that the applications get the most accurate information available. Location awareness includes the ability to select the best fit location provider at runtime based on the current situation, the ability to detect service availability, and the ability to roll over to another service provider if the primary provider fails.

The Location Aware Services is detailed in *IBM WebSphere Everyplace Access V5 Handbook for Developers and Administrators Volume IV: Advanced Topics*, SG24-6677.

Server Initiated Actions

Server Initiated Actions (SIA) relies on INS notification mechanisms to allow the server to send notifications to request the device to perform an action. Server Initiated Actions (SIA) is a means to notify the client device of events that drive client actions, such as e-mail synchronization.

SIA consists of two main parts: a SIA delivery channel and an administrative portlet. For more details, refer to *IBM WebSphere Everyplace Access V5 Handbook for Developers and Administrators Volume IV: Advanced Topics*, SG24-6677.

Device Services

Device Services provide the ability to maintain and deploy the Everyplace Client and software to the device. This server-based function provides support for IBM Everyplace Client. Device Services provides:

- Initial client deployment: Automating the deployment of Everyplace Client on mobile devices

- Device configuration: Maintains and manages the device configurations
- Software distribution: Ensures the mobile device has the right level of the application code by managing the software inventory on the device and delivering any new versions
- Inventory collection: Retrieves the current device inventory for review and reporting purposes

Also, the Everyplace Access device services can integrate with Tivoli® Configuration Manager for a complete enterprise-wide management solution. Device Services is covered in detail in Chapter 9, “Device Services” on page 339.

Offline Portal browsing and forms

Everyplace Access provides the ability to preselect Web content provided by the Portal technology for download to the mobile device. The Web content can be viewed on the device while disconnected from the network. The Everyplace Access Administration provides the ability to create a specific offline Portal page that contains user-selected portlets that generate Web content and Web forms. The Everyplace Access content adaptation (via Transcoding Technology) capabilities can be used to dynamically adapt the selected content for the target device. The content associated with an offline Portal page is synchronized to the user’s mobile device, where the user can perform:

- Offline viewing of the Web content
- Offline entry and submission of simple Web forms

Once the mobile device is connected to the server, the Web form data is sent to the server for processing by the server-based application.

For more details on offline content processing, refer to *IBM WebSphere Everyplace Access V5 Handbook for Developers and Administrators Volume II: Application Development*, SG24-6463.

Transcoding Technology

The Transcoding Technology included in Everyplace Access provides the ability to dynamically tailor and customize Web-based information to the needs of the mobile device and the mobile users. Transcoding is used to transform content based on the device’s characteristics and constraints, user preferences, and network bandwidth. Content adaptation may be as simple as automatically transforming an image to an alternate format or as involved as selecting specific Web content and converting that content to the markup required by the device. If the Transcoding Technology is used without any additional instruction, it will perform a “best-can-do” content adaptation of the original Web content.

To further customize the content sent to the mobile device, developers can use:

- Annotators: Instructions that direct the modification of the incoming HTML document. The annotation commands can be stored in a separate .ann file or embedded within the HTML document.
- The eXtensible Stylesheet Language (XSL): Stylesheets that can be used to format XML documents to another markup language.
- Transcoding plug-ins: Programs that modify the content of a document. Several transcoders (each with a specific task) can be invoked during the course of transforming a particular HTML or XML document.

Web Clipping

Web Clipping is the process of selecting specific content from an existing Web page for display on a mobile device. Web Clipping is a form of content adaptation that uses Transcoding Technology. The administrator or user creates a Web Clipping portlet and identifies the Web page associated with this particular clipper. As part of the creation process, the Web content is marked, indicating the content to be removed from the content displayed on the mobile device. Web Clipping uses Transcoding Technology to provide device-aware content tailoring and support for the major device markup languages.

Fragmentation

Fragmentation is another transcoding mechanism used to support pervasive devices. Large units of content may need to be broken down into smaller units for transmission to the mobile device, because the mobile device does not have the capacity to receive large chunks of data. The fragmentation support within the Transcoding Technology automatically splits the content, manages the generated decks, and delivers these decks to the mobile device. The first deck is delivered to the device with the remaining decks cached on the server. Each deck is delivered to the device as needed.

Transcoding Technology fragmentation support is illustrated in *IBM WebSphere Everyplace Access V5 Handbook for Developers and Administrators Volume II: Application Development*, SG24-6463.

1.4 Everyplace Client

Everyplace Client is an integrated complementary software package for personal digital assistants (PDAs) and cell phones that provides such functions as e-mail and PIM synchronization, database synchronization, device management, instant messaging, and offline portal browsing and forms submission. It is supported by a wide range of devices using such operating systems as Palm OS, eLinux, Symbian, Pocket PC 2002, and Windows Mobile 2003.

The Everyplace Access mobile environment, in relation to the Everyplace Access server environment, is shown in Figure 1-4. The mobile client shows three possible client environments: a SyncML client, the Everyplace Client, and a device browser (which allows browsing while in connected mode). The server environment reflects the Everyplace Access server. The enterprise includes the enterprise resources that are made available by using Everyplace Access services.

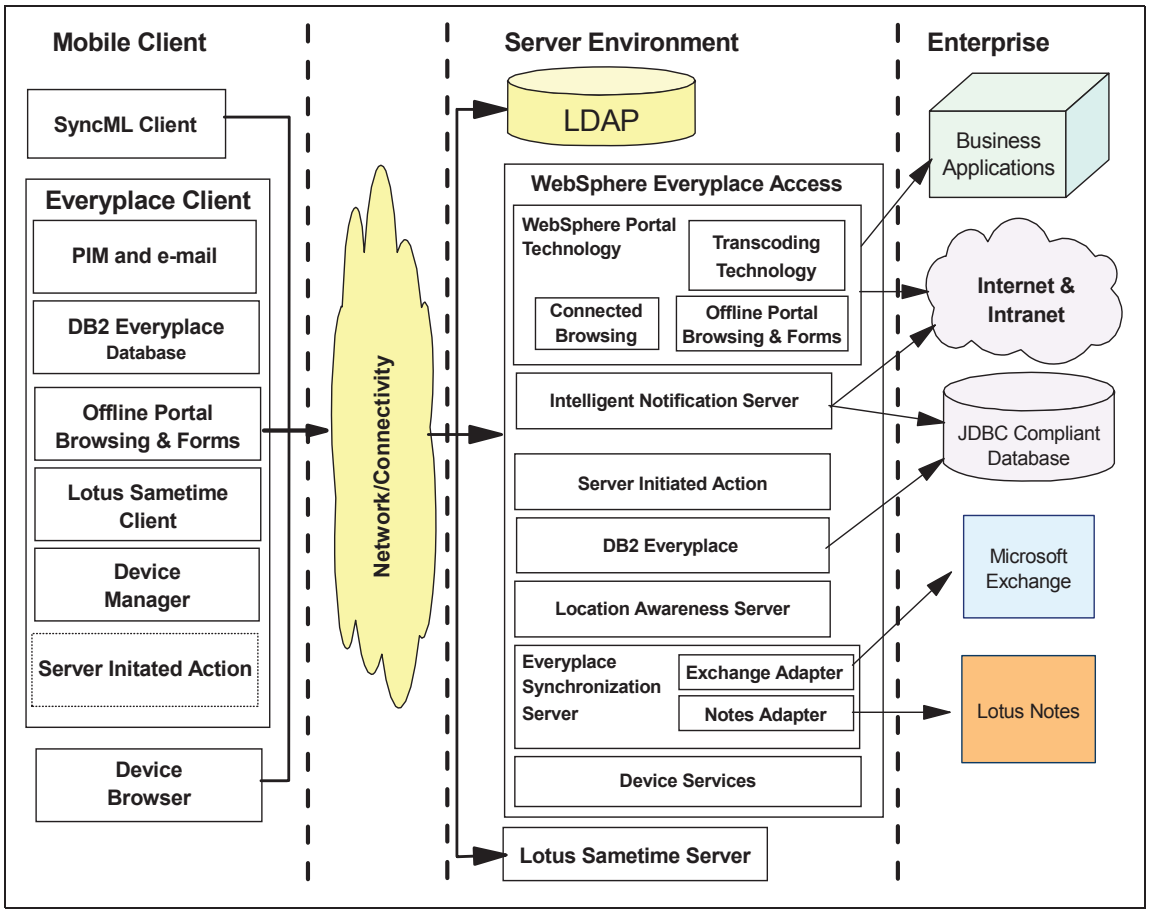

Figure 1-4 Mobile environment

Everyplace Client provides the following capabilities:

- Connected browsing: The native or installed device browser can be used to access the Internet or enterprise intranet Web content surfaced through portlets. These portlets can provide unique views for each device type.

- DB2 Everyplace database: Provides support for accessing the data within the local database by applications running on the device. Modifications and additions to the data in the local database can be synchronized with the enterprise database when a connection is available.
- PIM and e-mail functions: Allows the mobile worker to view and manage their e-mail and use the PIM applications on the local device. When a connection is available, synchronization is used to reflect any changes that have occurred both on the mobile device and on the server.
- Offline Portal browsing: The ability to view Portal content that has been downloaded to the mobile device. This allows the user to view Web content while disconnected from the enterprise.
- Offline Form submission: The ability to enter data and submit simple forms while disconnected from the network. The form data is held locally until the device can connect to the enterprise and transmit the form data for processing on the server.
- Sametime Connect: Provides mobile access to the server-based Lotus Sametime service. This allows mobile workers to communicate with colleagues in the office who are active on Sametime. This provides a transport-independent messaging capability. Sametime Server is a separately available product and is not included in the Everyplace Access product. The Sametime Server configuration and administration is provided by the Sametime product. The Sametime Server Extensions for Mobile Access are also required.
- IBM Device Manager: Provides device management services. The IBM device agent is used to report, inventory, carry out configuration activities, and perform installation activities on the mobile device.

1.4.1 Tested devices

To ensure a particular device works with the Everyplace Client per the product's specification, the mobile devices are tested. As of this writing, the list of tested and certified devices are:

- Pocket PC 2002 and Windows Mobile 2003 based devices:
  - Hitachi G1000
  - HP iPAQ 3760
  - HP iPAQ 1935
  - HP iPAQ 4150
  - HP iPAQ 5550
  - HP iPAQ 6315

  - Symbol 8800
  - MMO2 XDA II
  - Toshiba e405
  - Dell Axim X3
  - Siemens LOOX 610
- Palm OS based devices
  - PalmOne Tungsten C
  - PalmOne Tungsten W
  - PalmOne Treo 600
  - PalmOne Treo 300 (Web download only)
  - Kyocera 7135 (Web download only)
- Symbian OS based devices
  - Sony Ericsson P900
  - Nokia 9500 Communicator
- e-Linux OS based devices:
  - Sharp Zaurus SL-6000 (Japanese only)
- KDDI BREW Business Profile (BBP)
- DoCoMo P900i,N900i and F900i

Note: Everyplace Client for Treo 300, Kyocera 7135, and Sharp Zaurus SL-6000 devices is WEA R4.3 FP5 based code.

Note: To obtain more information about new Everyplace Client supported devices, refer to the WEA support page:

`http://www.ibm.com/software/pervasive/ws_everyplace_access/support`

1.4.2 Resource Checker

The WebSphere Everyplace Access Resource Checker is a tool that allows you to determine whether a Pocket PC 2002 or a Windows Mobile 2003 based device may be used with Everyplace Client. Resource Checker is a stand-alone device compatibility application that analyzes available resources (memory and processor) to determine if some or all of the Everyplace Client 5.0 components will work on any supported Windows CE platform device.

For more details on Resource Checker, refer to Chapter 11, “Resource Checker” on page 387.

1.4.3 Everyplace Client features per platform OS

Table 1-1 details the Everyplace Client features available on the various platforms that are supported as of this writing.

Table 1-1 Everyplace Clients feature support per device

Operating System	PPC 2002 / WM 2003	Palm OS	Symbian OS	e-Linux OS
Integrated shell	Yes	Yes (in WEA Client 5.0.1)	Yes (in Nokia 9500)	Yes
E-mail and PIM sync	Yes	Yes	Yes	Yes
E-mail attachment support	Yes	Yes	No	Yes
Invitation support	Yes	Yes	No	No
DB2 Everyplace	V8.1.4	V8.1.4 (in WEA Client 5.0.1)	V8.1.4	V8.1.2
Offline browsing	Yes	Tungsten C only	No	No
Offline forms	Yes	No	No	No
Device Manager Agent	V1.6	V1.6 (in WEA Client 5.0.1)	DM application provided by Nokia	V1.3
Lotus Sametime	Yes	Yes	Yes (in Nokia 9500)	Yes
Server Initiated Action	Yes	No	Yes	No

1.5 Everyplace Toolkit V5.0.1

The Everyplace Toolkit is a set of tools that provides developers the functionality to build wireless and mobile applications in WebSphere Everyplace Access platform. This toolkit is integrated into WebSphere Studio (Site Developer and Application Developer) and the Eclipse workbench. The IBM WebSphere Studio offering provides an integrated development environment (IDE) built on Eclipse, which supports WebSphere/J2EE application designing, development, testing and deploying (such as Web services), Web applications, XML applications, portlets, and much more.

The Everyplace Toolkit adds the following tools:

- Multi-Device Authoring Tools
- ERP/CRM portlet wizard
- Database Access portlet wizard
- Offline forms validations and Reusable forms
- Device emulator support
- Everyplace Toolkit examples
- Micro Environment tools
- Multimodal enablement

The Everyplace Toolkit includes various samples to speed the developers understanding and use of the toolkit and the application artifacts it creates.

Associated with Everyplace Access are other tools that provide additional developer support. These tools include WebSphere Studio Device Developer (which can plug in to WebSphere Studio), which provides developers with an IDE for creating Java applications that run on the mobile device and use the WebSphere Micro Environment. Also included in this group is the DB2 Everyplace's Mobile Application Builder, which is used to create form-based applications that access and update the local (on the mobile device) DB2 Everyplace database.

For details on the Everyplace Toolkit, see 1.5, "Everyplace Toolkit V5.0.1" on page 19.

1.6 New in WebSphere Everyplace Access V5.0

The following is a summary of the new features included in WebSphere Everyplace Access V5.0. For more information, review the product documentation.

- Improved performance
- Everyplace Access currency with WebSphere Application Server V5.0 and WebSphere Portal V5.0
- Improved Device Management (DM) portlets
- Enhancements to Everyplace Synchronization Server (ESS)
- Enhancements to Location Aware Services (LAS)
- Enhancements to Intelligent Notification Services (INS), including new notifications channels and capabilities
- Offline browsing and offline forms enhancements
- Support for new devices and browsers
- Additional support for XHTML and landscape displays
- Installation enhancements
  - For more flexibility, the installation process was divided in two phases (installation and configuration).
  - Installation scenarios have been provided to help product installation and configuration.
  - Two kinds of installation: *basic installation* in a single box and *component installation* supporting any combination of Everyplace Access components distributed across a variety of platforms.
- Multi-device Authoring Technology for Toolkit, to help automatically generate device-specific applications from a generic example
- Support for AIX® 5L V5.2
- Lotus Domino PIM and e-mail synchronization support on AIX
- Single-server Lotus Domino authentication
- Lotus Notes® and Microsoft Exchange portlet enhancements
- Enhancements to client and server user interfaces

1.7 Component products

In this section, we list the various products and components that comprise WebSphere Everyplace Access. There are three types of components:

1. Featured components: The primary services and components that make up Everyplace Access proper. This includes the server and client components.
2. Support components: Components that provide underlying support for the featured components.
3. Third-party components: Third-party software that is required to support some of the featured components. These components are not included in the packaging and must be purchased separately.

1.7.1 Featured components

The following products are featured in the product:

- Server components
  - Everyplace Access Services V5.0: Provides the core functionality.
  - Everyplace Synchronization Server V5.0: Enables synchronizing data between the mobile device and the server, which includes data from Microsoft Exchange and Lotus Notes.
  - DB2 Everyplace V8.1.4: Enables synchronizing relational database data stored in any JDBC-compliant database.
  - Intelligent Notification Services V2.2: Allows users to subscribe to notification services and define the delivery channel, the selection criteria, and message sending criteria.
  - Device Manager V1.6: Device management service that helps the enterprise manage the various mobile devices connecting to the enterprise. Device Manager is used to identify, configure, inventory, and distribute software to any device supported by the enterprise.
  - Location Aware Service V2.0: Provides a set of portlets that interact with location-based providers to obtain location information and provide a consistent interface for solution developers who need to incorporate this information into their mobile solutions.
  - WEA InfoCenter V5.0.
- Client components
  - Everyplace Client V5.0.1: Provides device security and a single user interface to a series of capabilities, such as PIM and e-mail synchronization, database synchronization, device management, instant messaging, and offline browsing.

- Application Development Components
  - Everyplace Toolkit V5.0.1: A plug-in for WebSphere Studio Site Developer or WebSphere Studio Application Developer. The toolkit provides support for building mobile applications into a WEA environment.
  - WebSphere Studio Site Developer V5.1.1: An integrated tool set built on Eclipse, which supports Web site development and management activities. It supports the J2EE specification and delivers integrated support for open Web standards, including Java, JSP, servlets, XML, HTML, DHTML, JavaScript, rich media, and Web services tools.
  - WebSphere Studio Device Developer V5.7.1: An integrated development environment (IDE) for the creation and testing of applications deployed on mobile devices.
  - DB2 Everyplace Mobile Application Builder V8.1.4: Provides the tools necessary for developing mobile device applications using the DB2 Everyplace product.

1.7.2 Support components

The following products are support components included in the product:

- IBM Java Toolkit: Required to complete product installation. The installation process will install it if it is not already present.
- DB2 Universal Database Workgroup V8.1.6: A relational database management system used by Everyplace Access that stores component-specific data.
- IBM HTTP Server V1.3.26: An IBM-enhanced version of the Apache Web server that supports both the Secure Sockets Layer (SSL) V2 and SSL V3 protocols for secure connections.
- IBM Directory Services V5.1: A Lightweight Directory Access Protocol (LDAP) that runs as a stand-alone daemon. It is based on a client/server model that provides client access to an LDAP server. It provides an easy way to maintain directory information in a central location.
- WebSphere Application Server V5.0: Enables Web transactions and interactions with the deployment environment for e-business applications. It provides the foundation for WebSphere Portal technology and Everyplace Access.
- WebSphere Portal Server V5.0.2.1: Provides a platform for WEA component portlets.

1.7.3 Third-party components

The following third-party products are associated with Everyplace Access and can be ordered separately as needed:

- Operating systems:
  - Windows 2000 Server with Service Pack 4 (32-bit version)
  - Windows 2000 Advance Server with Service Pack 4 (32-bit version)
  - AIX V5.2 (32-bit version)
- Desktop Web browser support:
  - Windows:
    - Microsoft Internet Explorer V5.5, 5.5 SP2, or 6.0 SP1
    - Mozilla 1.0.2, 1.2.1, 1.3, or 1.4
    - Netscape Communicator V6.2 or 7.0
    - Opera 7.11 or later
  - AIX:
    - Netscape Communicator V6.2 or 7.0
- Handheld device browser support:
  - Pocket Internet Explorer (on Pocket PC 2002 and Windows Mobile 2003)
  - Web Pro browser V2 (on Palm Tungsten)
  - Opera 7.25 and 6.02
  - Netfront browser
  - Blazer 3.0 (on Treo 600)
- Microsoft Exchange 5.5, 2000 and 2003 for PIM and e-mail synchronization with Exchange data
- Lotus Domino Server V5.0.12 to 6.5.3 or later for Lotus Notes PIM and e-mail synchronization
- LDAP server (other than IBM Directory Server that is provided), such as:
  - Lotus Domino V5 and V6
  - Microsoft Active Directory 2000 and 2003

1.8 System hardware and software requirements

The Everyplace Access server runs on these operating systems:

- Windows 2000 Server or Advanced Server with Service Pack 4
- AIX 5L V5.2

The Everyplace Access server requires at least the following hardware:

- Intel® Pentium® 4 (2 GHz or higher) or IBM @server® pSeries® (1 GHz or higher).
- 2 GB of memory at a minimum.
- The disk space will vary, depending the Everyplace Access components to be installed.

For more information, refer to the product documentation.

1.9 Complementary products

IBM provides a set of complementary products that can be used in conjunction with Everyplace Access to fulfill the requirements for a particular enterprise environment. We have included a list of complementary IBM products. Some of these products could be replaced by third-party products that provide similar services, if so desired. The commonly used IBM complementary products are:

- WebSphere Everyplace Connection Manager: Fortifies Everyplace Access by providing the underlying network connectivity for the enterprise. WebSphere Everyplace Connection Manager can be used to extend the number of network choices by providing secure data access to both WAP and non-WAP clients over a wide range of international wireless network technologies, as well as local area network (LAN) and wide area network (WAN) wire-line networks. WebSphere Everyplace Connection Manager is often used with Everyplace Access to provide a secure VPN-like connection to the enterprise. It also provides seamless roaming across different networks and different network types. It extends Everyplace Access's ability to handle large numbers of subscribers, improves response time on low bandwidth networks, and lowers network fees by providing data compression and header reduction. WebSphere Everyplace Connection Manager also protects the data with bi-directional user and server authentication and data encryption, ensuring that the mobile data is protected and secure.
- WebSphere MQ Everyplace (MQe): Extends Everyplace Access by providing secure and dependable messaging between the mobile device and the enterprise. Applications written for the mobile device can create messages that are handled by MQe and sent to the server for processing. It is often used

in conjunction with the DB2 Everyplace capability that is part of the Everyplace Client. MQe delivers once-only messaging so transactions are not lost and not duplicated between the mobile applications. MQe also provides peer-to-peer synchronous and asynchronous support, local and remote queue access, direct and indirect routing, encryption, non repudiation and authentication features that can be used to extend the existing capabilities within Everyplace Access. MQe interacts seamlessly with the WebSphere MQ family of products and provides any-to-any communication and business process integration. MQe is often used in situations where WebSphere MQ is already used as part of the enterprise solution architecture.

- WebSphere Edge Server: Can be used with Everyplace Access to distribute the application processing to the edge of the network while at the same time ensuring centralized administration and application control. It provides both load balancing and caching functions. With its enhanced load balancing features, it can improve server selection, load optimization, and fault tolerance.
- IBM SecureWay® Firewall: For a production Everyplace Access deployment, firewalls are required. Usually two firewalls are included within the solution architecture. One is between the Internet (or third-party gateway) and all servers that communicate outside the enterprise (these are the edge of network servers). The second one is normally between these edge of network servers and all the back-end system servers in the enterprise that contain all the business databases, applications, directories, and so forth. The area between these two firewalls is called the demilitarized zone (DMZ).
- WebSphere Portal offering: Even though Everyplace Access relies on Portal technology to provide mobile solutions, to create a robust Portal for the enterprise, a WebSphere Portal product should be used to support the connected users. There are three unique WebSphere Portal offerings, each of which can work in conjunction with Everyplace Access. The WebSphere Portal offerings deliver a single, universal point of access that is integrated, highly customizable and scalable. A Portal can be created to interact with various enterprise resources, such as business applications, existing content, people, and business processes. The WebSphere Portal offering can be used to support the always connected employees while Everyplace Access can be used to support mobile employees who may operate either in a connected or in an occasional connection mode.

2

Enhanced portlets

Everyplace Access extends the functionality of the Portal offering by providing specialized portlets for mobile devices. In this chapter, we introduce you to the enhanced portlets provided in Everyplace Access.

© Copyright IBM Corp. 2005. All rights reserved.

2.1 Introduction

WebSphere Everyplace Access includes many enhancements that extend limited base Portal functions to mobile devices. WebSphere Everyplace Access provides device-viewing enhancements for online viewing, offline Portal content viewing, selected portlet enhancements, and a custom WebSphere Everyplace Access page group.

Portlets are visual windows that organize content from different sources, such as Web sites, e-mail, and business applications, into a single interface for individual or group access. Portlets enable highly customized and productive work environments for projects, tasks, or organizational communities.

Everyplace Access provides a set of productivity and personal information manager (PIM) portlets that have been enhanced for viewing on mobile devices using either WML, HTML, or text-based browsers. Everyplace Access selected these particular portlets to focus on personal information management and enterprise-related functionality. These selected portlets have been enhanced for Palm browsers, such as WebPro or Blazer, and for Pocket PC browsers, such as Pocket Internet Explorer.

2.2 Enhanced portlets provided by Everyplace Access

Table 2-1 shows the list of enhanced PIM portlets provided in the Everyplace Access package. Portlets may have additional functions beyond View, including Configure, Edit, Create, Delete, Forward, Reply, Reply All, and so on. The table shows the functions available by portlet for the specific markup: PDA, PDA text-only, and WML. This function is provided for online browsing only.

Table 2-1 PIM portlets

Portlets	PDA markup	PDA text-only markup	WML markup
Lotus Notes Mail	All functions available	All functions available	View, Forward, Reply, and Reply All
Lotus Notes Calendar	All functions available	View, Create, and Delete	View only
Lotus Notes ToDo	All functions available	View, Create, and Delete	View only
Lotus Notes Contacts	All functions available	View, Create, and Delete	View only

Portlets	PDA markup	PDA text-only markup	WML markup
Lotus Notes Journal	All functions available	View, Create, and Delete	View only
Microsoft Exchange Mail	All functions available	All functions available	View, Forward, Reply, and Reply All
Microsoft Exchange Calendar	All functions available	View, Create, and Delete	View only
Microsoft Exchange Tasks	All functions available	View, Create, and Delete	View only
Microsoft Exchange Contacts	All functions available	View, Create, and Delete	View only
Microsoft Exchange Notes	All functions available	View, Create, and Delete	View only

Table 2-2 shows the productivity portlets provided by Everyplace Access.

Table 2-2 Productivity portlets

Portlets	PDA markup	PDA text-only markup	WML markup
World Clock	Edit and View	View only	View only
Bookmarks	Edit and View	View only	View only
LDAP Search	Edit and View	View only	View only

2.2.1 Lotus Notes PIM and e-mail portlets

These portlets provide access to the PIM and e-mail functions of Lotus Notes. You have to configure the Lotus Domino Server in order to access it from the PIM and e-mail portlets. For information about configuring the Lotus Domino Server, refer to Chapter 4, “Basic WebSphere Everyplace Access installation” on page 99.

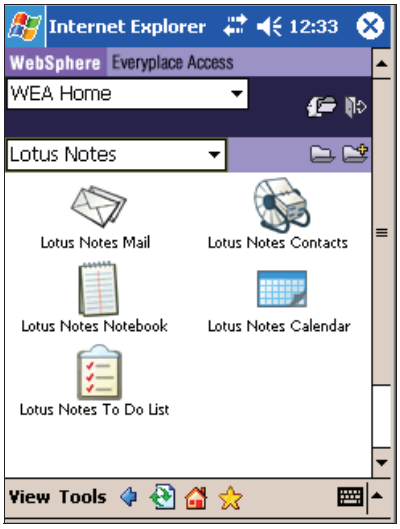

Figure 2-1 Lotus Notes PIM and e-mail portlets

Lotus Notes Mail portlet

Lotus Notes Mail portlet provides access to your Lotus Notes mail database using a Web browser or Web-enabled wireless phone. Before you can access your mail database, you must first edit the settings and enter the name of your mail server, user name, and password.

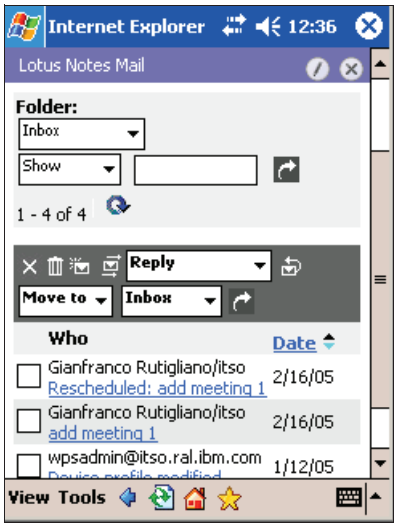

Figure 2-2 Lotus Notes Mail portlet

Lotus Notes Contacts portlet

Lotus Notes Contacts provides access to your Lotus Notes contacts using a Web browser. Before you can access your contacts, you must first edit the settings and enter the name of your mail server, user name, and password.

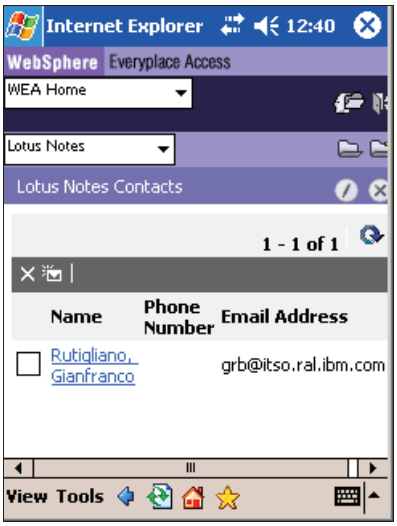

Figure 2-3 Lotus Notes Contacts portlet

Lotus Notes Journal (Notebook) portlet

Lotus Notes Notebook provides access to your Lotus Notes notebook using a Web browser. Before you can access your notebook, you must first edit the settings and enter the name of your mail server, user name, and password.

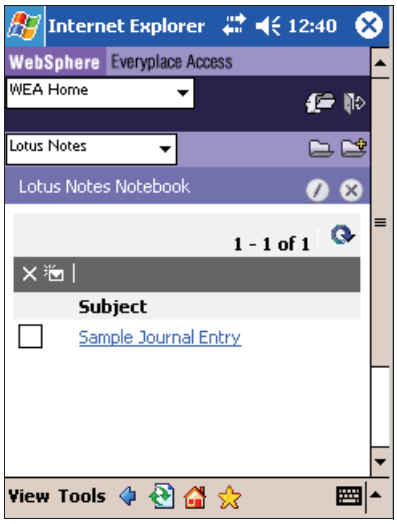

Figure 2-4 Lotus Notes Notebook portlet

Lotus Notes Calendar portlet

Lotus Notes Calendar provides access to your Lotus Notes calendar using a Web browser. Before you can access your calendar, you must first edit the settings and enter the name of your mail server, user name, and password.

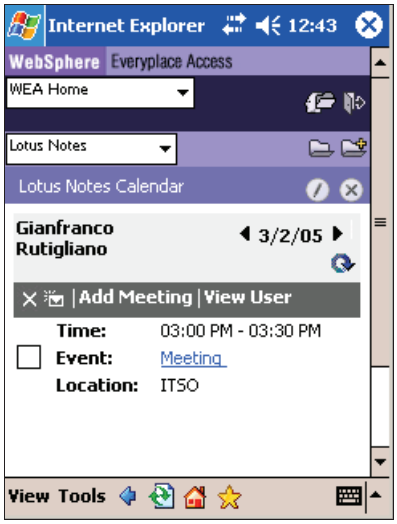

Figure 2-5 Lotus Notes Calendar portlet

Lotus Notes ToDo portlet

Lotus Notes ToDo provides access to your Lotus Notes to-do list using a Web browser. Before you can access your to-do list, you must first edit the settings and enter the name of your mail server, user name, and password.

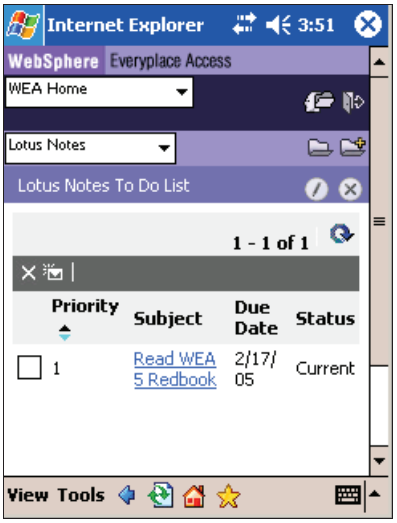

Figure 2-6 Lotus Notes ToDo portlet

2.2.2 Microsoft Exchange PIM and e-mail portlets

The Microsoft Exchange PIM portlets provides access to Exchange 5.5/2000/2003 servers. Before using these portlets, you have to configure them by setting a credential slot to store the users' passwords. The credential slot can be created using the Credential Vault administration page in the WebSphere Everyplace Access server.

For information about configuring Microsoft Exchange to work with Everyplace Access, refer to *IBM WebSphere Everyplace Access V5 Handbook for Developers and Administrators Volume III: E-Mail and Database Synchronization*, SG24-6676.

Figure 2-7 Microsoft Exchange PIM portlets

Microsoft Exchange Mail portlet

Exchange mail connects to an Exchange Server. You can perform standard mail functions, such as compose, reply, forward, and delete mail.

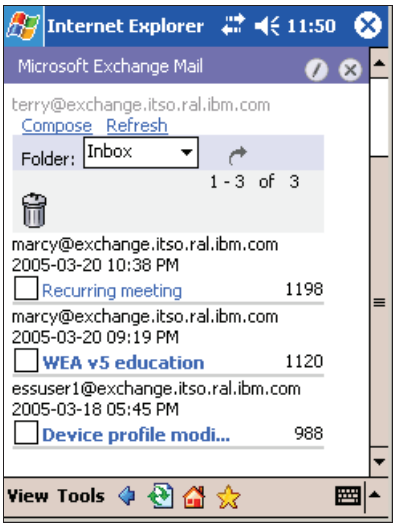

Figure 2-8 Microsoft Exchange Mail portlet

Microsoft Exchange Calendar portlet

Exchange Calendar connects to an Exchange Server. You can perform standard calendar functions, such as creating, editing, deleting, and viewing appointments.

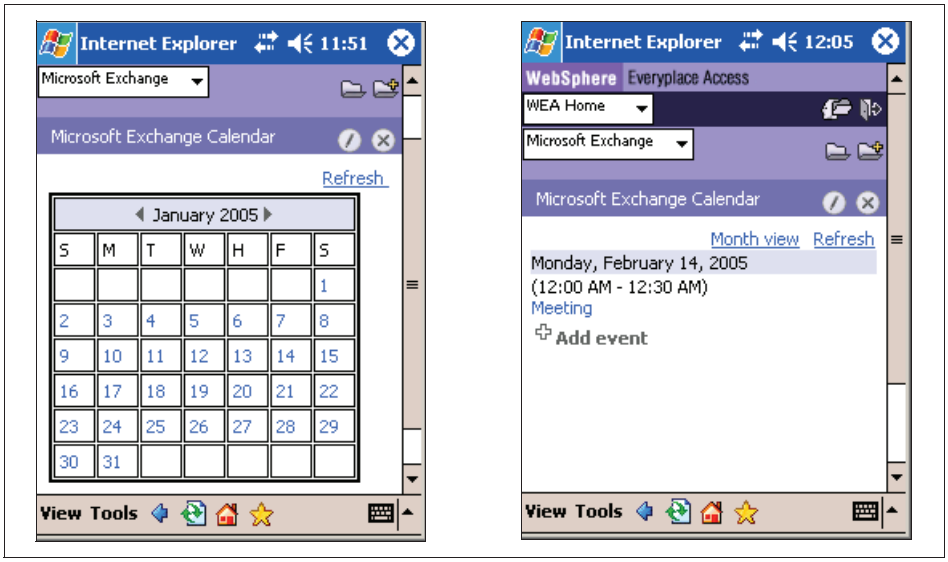

Figure 2-9 Microsoft Exchange Calendar portlet

Microsoft Exchange Tasks portlet

Exchange Tasks connects to an Exchange server. You can perform standard task functions, such as creating, editing, deleting, and viewing tasks.

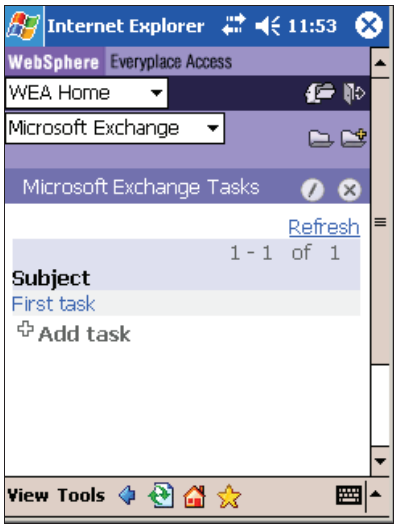

Figure 2-10 Microsoft Exchange Tasks portlet

Microsoft Exchange Contacts portlet

Exchange Contacts connects to an Exchange server. You can perform standard contact list functions, such as creating, editing, deleting, and viewing contacts.

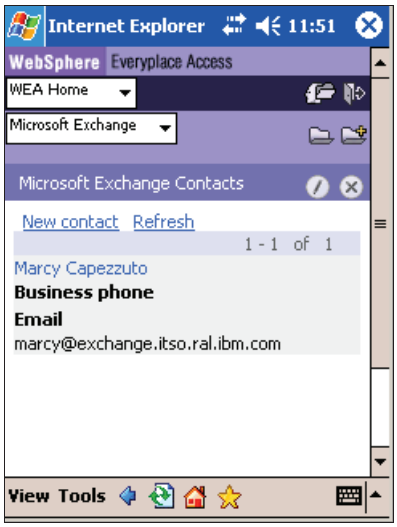

Figure 2-11 Microsoft Exchange Contacts portlet

Microsoft Exchange Notes portlet

Exchange Notes connects to an Exchange server. You can perform standard note functions, such as creating, editing, deleting, and viewing notes.

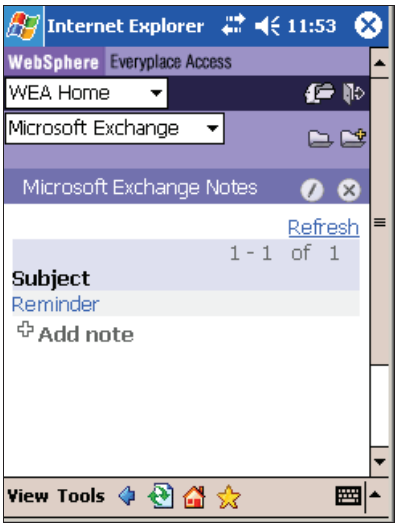

Figure 2-12 Microsoft Exchange Notes portlet

2.2.3 Productivity portlets

WebSphere Everyplace Access provides a set of productivity portlets enhanced for mobile access.

World Clock portlet

World Clock allows you to set your local time zone and view the current time in that time zone. It also allows you to view the current local time in several time zones around the world at one time. You can also do a quick search for the current local time in an individual time zone.

With World Clock you can:

- Set a local time zone and view the current time.
- Set a list of time zones around the world and view their current times.
- Do a quick search for the current time in an individual time zone.

Note: Be careful that you select the correct time zone. Even though a time zone has the same GMT, the actual local time may differ, so you need to select the time zone with the correct cities. For example, GMT 7:00 has two options, Arizona and Mountain Time, because of Daylight Savings Time.

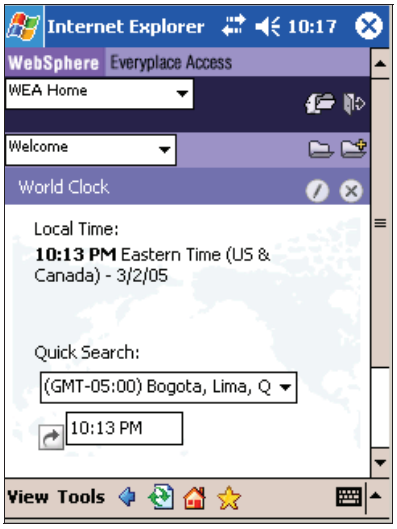

Figure 2-13 World Clock portlet

Bookmarks portlet

The Bookmarks portlet allows you to bookmark internal information and external sites. You can then use these bookmarks to access regularly visited sites. You can add, delete, and edit your bookmarks as well as organize them into folders.

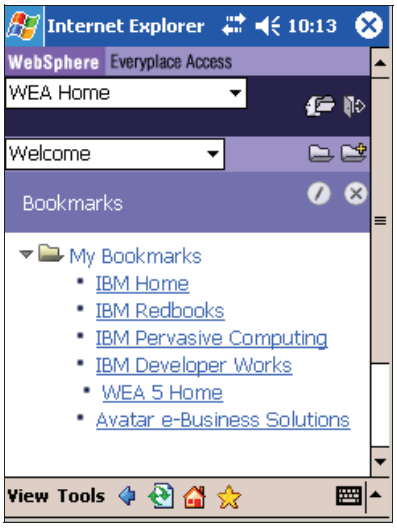

Figure 2-14 Bookmarks portlet

LDAP Search portlet

The LDAP Search portlet allows you to contact an LDAP server and perform a search based on parameters set. Before you can use this portlet, you must first edit the settings and enter a display name for the search, the LDAP server name, the directory name, and some other parameters.

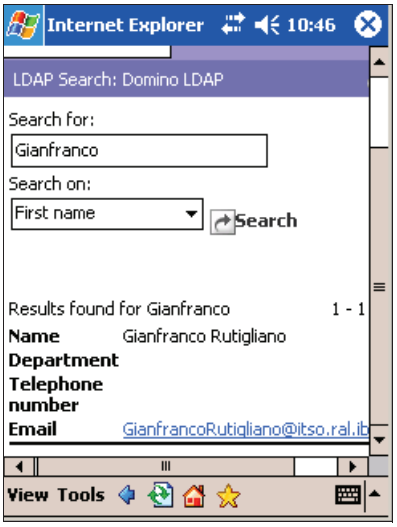

Figure 2-15 LDAP Search portlet

3

Administration

WebSphere Everyplace Access provides administration services that allow administrator and users to maintain the Everyplace Access runtime environment that supports the enterprise mobile environment. Administration consists of a centralized administration environment that supports activities such as managing Portal user interface, managing portlet applications, maintaining the mobile security environment (access control), and configuration of different parts of the WebSphere Everyplace Access.

In this chapter, we describe the main features of administration and show how to use it to accomplish many common activities. This chapter covers the following:

- Portal User Interface (selection of themes and skins)
- Installing and configuring portlets
- Managing secure access control
- Managing access control
- Portal settings

WebSphere Everyplace Access administration is based on portlets, which are running on top of WebSphere Portal Server, which is installed with WebSphere Everyplace Access.

© Copyright IBM Corp. 2005. All rights reserved.

3.1 WebSphere Portal Server overview

Before starting with WebSphere Everyplace Access administration, you must be able to understand some of terms included in WebSphere Portal Server.

This section gives you a brief overview of the portal in order to help you to understand how WebSphere Everyplace Access administration actually works.

3.1.1 Welcome to the portal

A portal is a centralized point for accessing applications, information, and other resources in your enterprise or on the Internet. The portal provides a view of applications and information aggregated from either the Internet or from a corporate network or intranet.

Portal content is divided into modules called *portlets*. Each portlet provides a view of certain types of information, such as weather, remainders, or to applications such as e-mail or calendar. Portlets are displayed with a little bar that provides the name of the portlet and display controls that allow you to minimize, maximize, edit the portal settings, or to obtain help information.

WebSphere Portal proves an easy way to customize the look and feel of the portal through the use of *themes* and *skins*. Themes define the visual appearance of the portal pages while skins define the visual appearance surrounding each portlet.

A theme determines the global appearance of all pages within a specific top-level page. Themes define the overall layout of the page. The theme for the Welcome page (shown in Figure 3-2 on page 44) defines:

- The banner at the top of the page
- Navigation elements under the banner, which includes:
  - Labels to group nodes. A label is a type of node that has a name and is used to hold other nodes.

    Note: Node is a level of hierarchy in the portal that includes the pages, labels, and URLs used to navigate in the portal structure.

  - Tabs to select a specific page.

    Note: Pages display content in the form of portlets.

– Links / shortcuts to create, edit, and grant access for the page that you are located at (that is, New page, Edit page, and Assign Permissions).

– Links for the portal controls (such as Sign up, Login and Help).

– The rest of the page displays the available portlets.

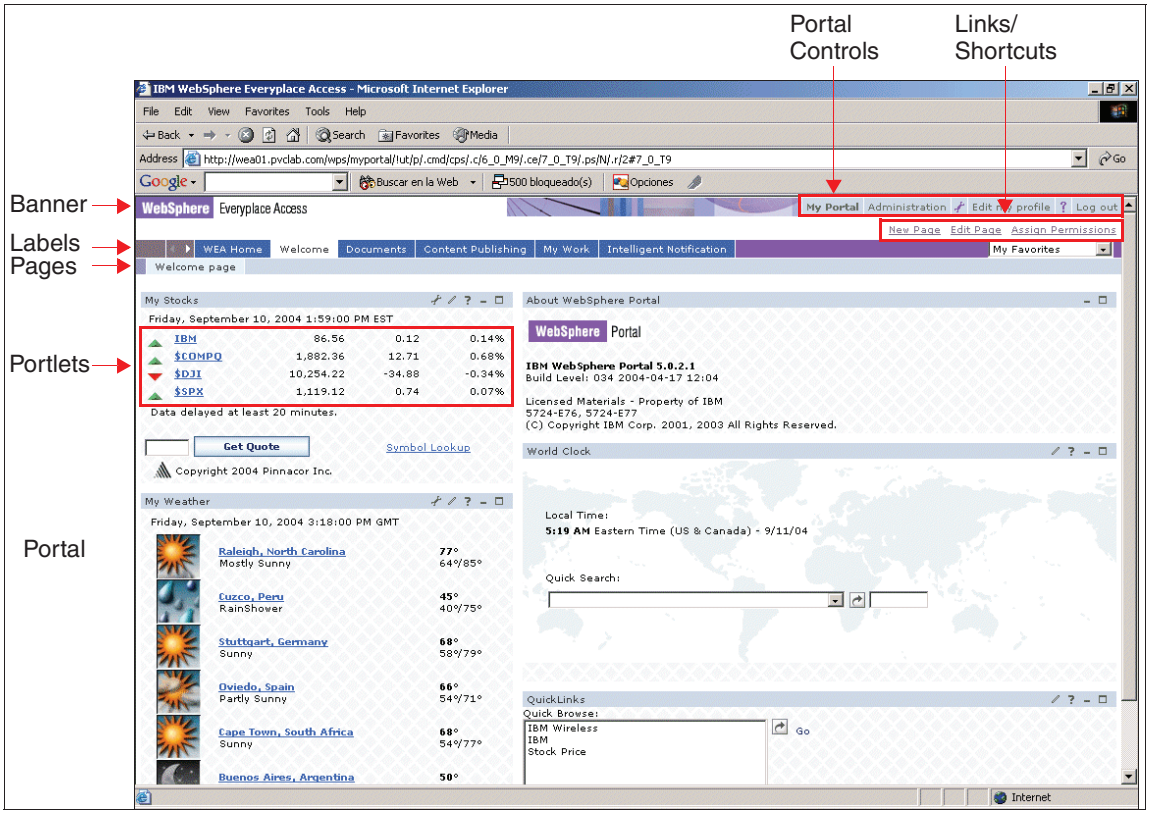

Figure 3-1 Welcome page example

A skin refers to the visual appearance of the area surrounding an individual portlet. A skin can include the tittle bar and portlet controls, such as minimize, maximize, edit, and help. Each portlet has its own skin (or it can inherit it from the default skin defined in the administration area of WebSphere Portal), which may be different from other portlets on the same page. See the different examples of skins in Figure 3-2 on page 44.

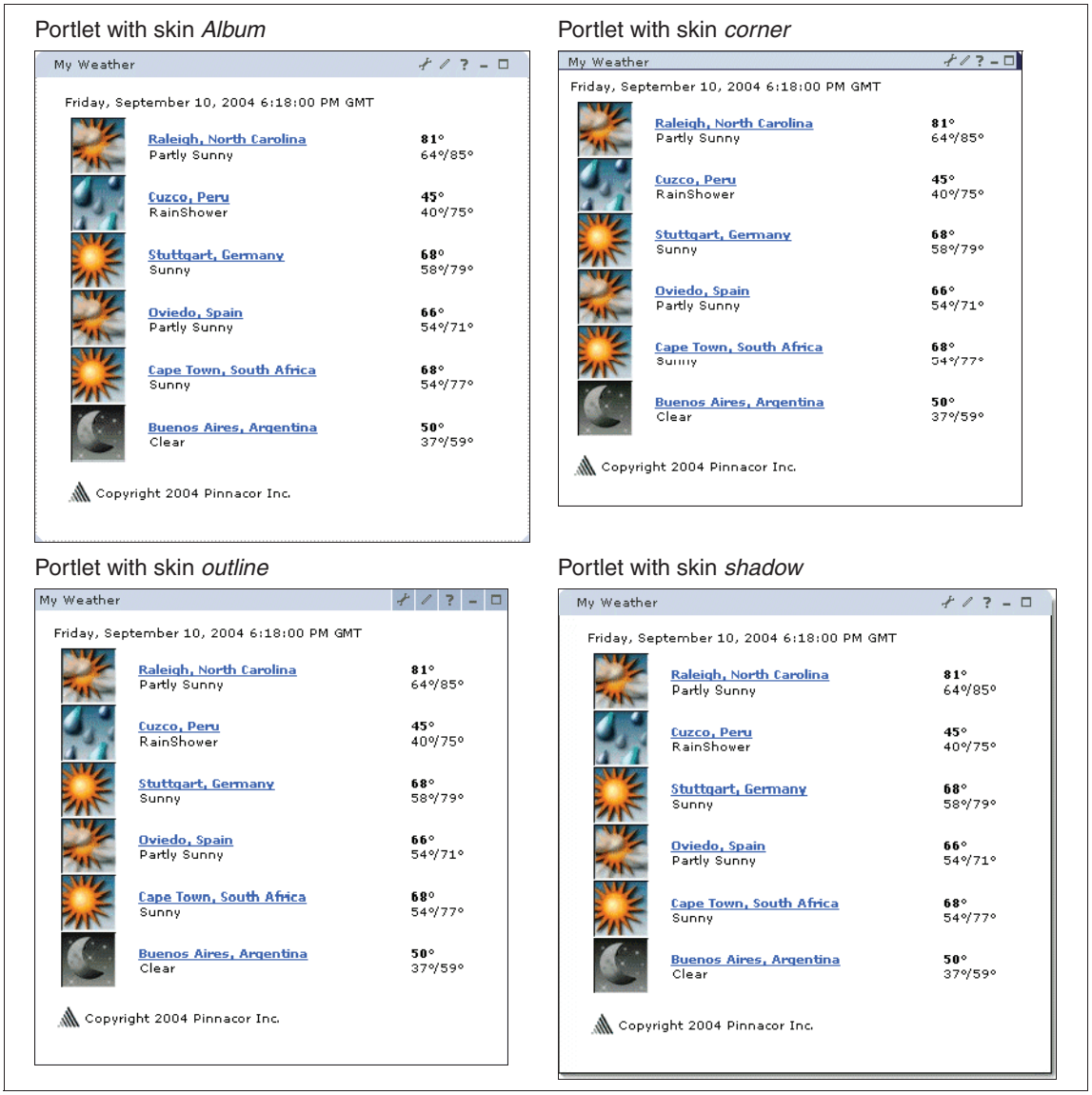

Figure 3-2 Skin examples

The WebSphere Portal (the initial version) provides the following root nodes:

1. My Portal: Displays pre-packaged portlets for the end user for different business proposals, by default, the first page displayed after login
2. Administration: Allows the administrators to install and manage portlet applications on the portal, configure the portal, define the users and user

groups for the portal, and control which portal resources user groups can access.

3. New Page, Edit Page and Assign permissions links: Enables the user and administrators to quickly create and edit pages and give resource permissions to the users exactly for the page that the user is located.

3.2 Starting WebSphere Everyplace Access services

Before logging in to WebSphere Everyplace Access, you have to start Everyplace Access services. You can run the following command lines procedure to start WebSphere Everyplace Access:

1. Start the WebSphere Application Server.
   - Windows: Run the command **`startServer server1 -user`** ***`was_admin`*** **`-password`** ***`password`*** from the *was_home*\bin directory.
   - AIX: Run the command **`./startServer.sh server1 -user`** ***`was_admin`*** **`-password`** ***`password`*** from the *was_home*\bin directory.
2. Start the WebSphere Portal Server.
   - Windows: Run the command **`startServer WebSphere_Portal -user`** ***`was_admin`*** **`-password`** ***`password`*** from the *was_home*\bin directory.
   - AIX: Run the command **`./startServer.sh WebSphere_Portal -user`** ***`was_admin`*** **`-password`** ***`password`*** from the *was_home*\bin directory.
3. Start the Everyplace Access Services.
   - Windows: Run the command **`startServer WEA_Server -user`** ***`was_admin`*** **`-password`** ***`password`*** from the *was_home*\bin directory.
   - AIX: Run the command **`./startServer.sh WEA_Server -user`** ***`was_admin`*** **`-password`** ***`password`*** from the *was_home*\bin directory.
4. Start the Everyplace Synchronization Server.
   - Windows: There are two ways to start the service:
     - Select **Start** → **Control Panel** → **Administrative Tools** → **Services**, select **IBM Everyplace Synchronization Server** and click **Start Service**.
     - Select **Start** → **Programs** → **IBM WebSphere** → **Everyplace Synchronization Server** → **Start server**.
   - AIX: Run the command **`./esscmd init`** from the Everyplace Synchronization Server bin directory.

5. Start the DB2 Everyplace server.
   - Windows: Run the command **startServer IBMDB2eServer -user *was_admin* -password *password*** from the *was_home*\bin directory.
   - AIX: Run the command **./startServer.sh IBMDB2eServer -user *was_admin* -password *password*** from the *was_home*\bin directory.
6. Start the Device Manager server.
   - Windows: Run the command **startServer DMS_AppServer -user *was_admin* -password *password*** from the *was_home*\bin directory.
   - AIX: Run the command **./startServer.sh DMS_AppServer -user *was_admin* -password *password*** from the *was_home*\bin directory.
7. Start the Location Aware Services.
   - Windows: Run the command **startServer LasAppServer -user *was_admin* -password *password*** from the *was_home*\bin directory.
   - AIX: Run the command **./startServer.sh LasAppServer -user *was_admin* -password *password*** from the *was_home*\bin directory.
8. Start the Intelligent Notification Services.
   - Windows: Run the command **startServer INSServer -user *was_admin* -password *password*** from the *was_home*\bin directory.
   - AIX: Run the command **./startServer.sh INSServer -user *was_admin* -password *password*** from the *was_home*\bin directory.

Note: In Windows environments, WebSphere Everyplace Access services can be started from the Windows Services interface.

3.3 Getting started

We will be performing a variety of administration tasks. To log in, click the **Log in** icon shown in Figure 3-3. Log in with a user ID with the appropriate administration rights.

Figure 3-3 Log in

WebSphere Everyplace Access Administration navigation is very similar to Portal Administration. Everyplace Access Administration (subsequently called Administration) provides a multi-tiered menu with the top-level tab menu bar controlling the overall navigation and selection process. This menu bar (top level) then determines the second-level menu options displayed.

Once the administrator of the system is logged on, click **Administration** and the page shown in Figure 3-4 will appear.

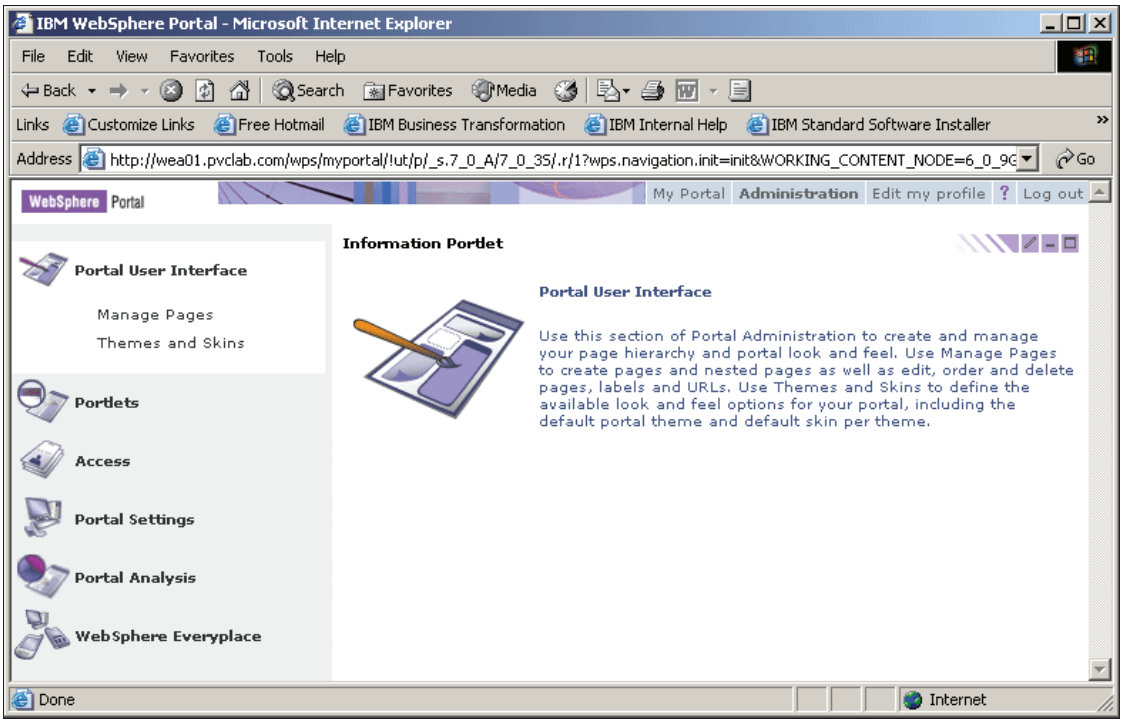

Figure 3-4 Administration page

The left panel (shown in Figure 3-4) contains the categories and the associated activities (based on portlets):

- Portal User Interface: Manage Pages and Themes and Skins
- Portlets: Install, Manage Applications, Manage Portlets, and Web Clipping
- Access: Users and Groups, Resource Permissions, User and Group Permission, and Credential Vault
- Portal Settings: Global Settings, URL Mapping, Custom Unique Names, Supported Markup, Supported Clients, and Search Administration
- Portal Analysis: Frequent Users and Enable Tracing
- WebSphere Everyplace: Device Management, Offline Browsing, Everyplace Synchronization Server Administration, Intelligent Notification Services, and Location Aware Services

3.4 Portal user interface

As stated before, a portal consists of labels that have one or more pages, and each page contains one or more portlet applications. Think of a label as a collection of portal pages. From the Administration portal control, it is possible to configure the Portal User Interface. Administrators can manage pages (create new pages, modify pages, and include/delete portlets) and modify the Themes and Skins. In order to do so, click **Portal User Interface** portlet on the left panel of the Administration Portal controls link, as shown in Figure 3-5.

As you can see, there are two different options on the page: Manage pages and Themes and Skins.

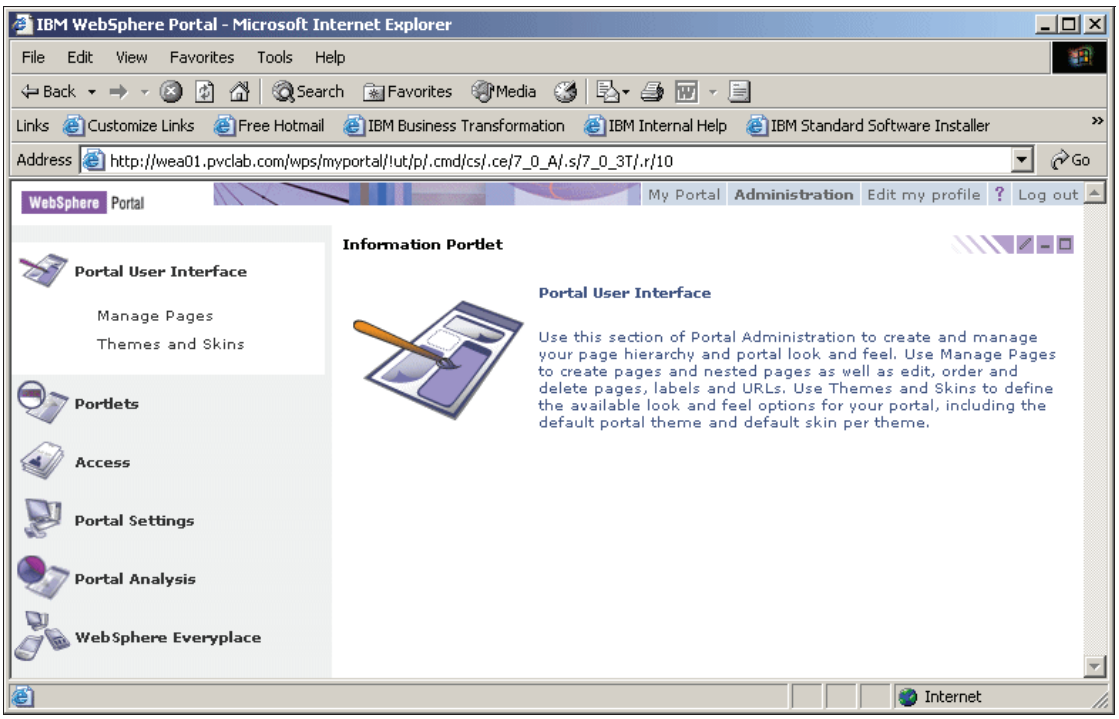

Figure 3-5 Portal user interface

3.4.1 Manage pages

One of the features WebSphere Portal Server offers to WebSphere Everyplace Access is the possibility of managing pages, giving you the ability of:

- Create and Modify: Labels, pages, and links.

- Change the properties of Labels/Pages (Title, Theme, supported markup languages, and so on).
- Reorder labels and pages on the portal.
- Lock / Unlock labels, pages and portlets.
- Include new portlets on pages.

To start managing pages, click **Manage Pages** under the Portal User Interface portlet, as shown in Figure 3-6.

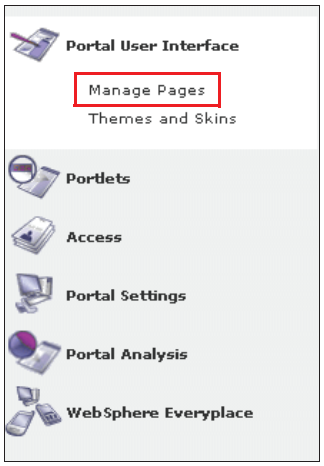

Figure 3-6 Selecting Manage Pages tab

Once you have clicked **Manage Pages**, the portlet shows all the Labels and Pages that hang from the *Content Root*, as seen in Figure 3-7 on page 50.

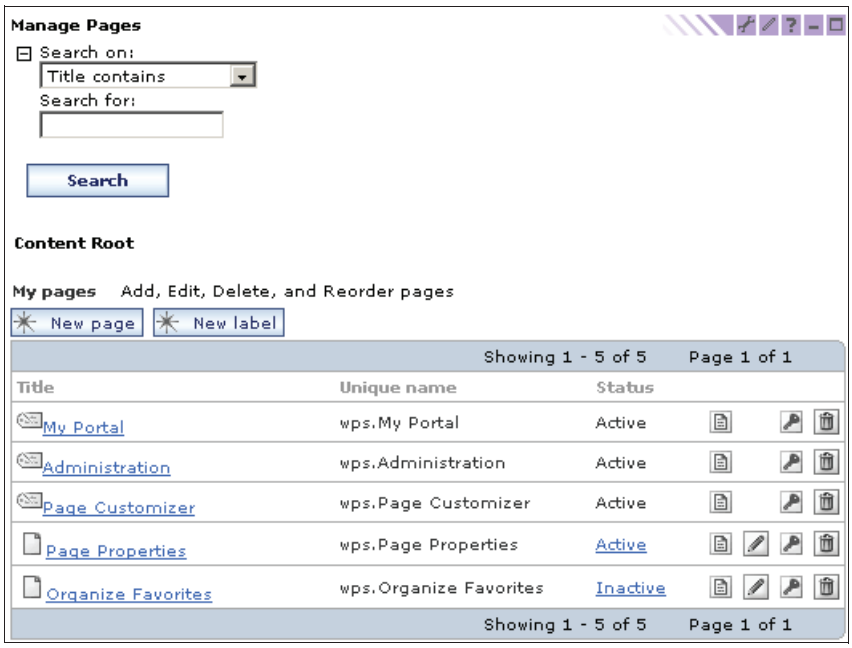

Figure 3-7 Content of Manage Pages

Content Root is the first node the system shows when the WebSphere Everyplace Access is reached. All labels, pages, links will drill down from the Content Root (see Figure 3-7).

From that page, you can search from pages and labels based on:

- Contents of the title (`Title contains`).
- Content of the description (`Description contains`).
- Content of the markup (`Markup contains`).
- Last Modification (`Last Modified`). In this case, a new form appears asking for year, month, and day.
- Name Uniqueness (`Unique name`).
- All available pages and labels (`All available`).

Create New Pages

You can create a new page under an existing page, reference an existing page, apply a layout, and select supported markups. For public pages, you must have the Administrator, Manager, or Editor role assignment (see 3.6.1, “Users and groups” on page 74).

When you create a page, you always have the option to create a new page with a new layout. You may create a derived page to a derivation parent page if you have the Editor and Privileged User role assignment. If you have Editor role on the derived page, you may change anything except markups. If you have Privileged User role on the derived page, you may change the title, skins, or layout on the derived page (see 3.6.1, “Users and groups” on page 74).

For layout, this is restricted by the derivation parent page. If you reference an existing page, this layout, supported markups, locks, skins, portlet list, and locale specific titles are predetermined by the existing page you reference. Any changes to the original page results in the same change to all pages that are referenced.

When creating a new page, you must click the **New Page** button, as shown in Figure 3-8.

Figure 3-8 New page button

The window illustrated in Figure 3-9 appears.

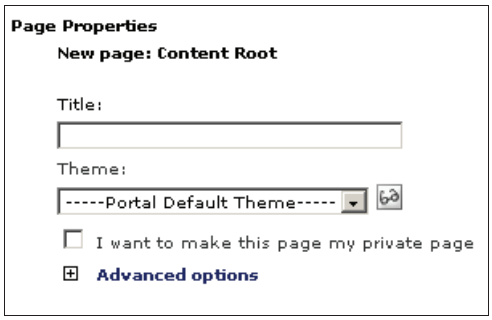

Figure 3-9 Creating a new page

On this page, you may give it a title. All the other settings are optional.

To create a new page, perform the following steps:

1. Type the title of the new page in **Title**. This is the title for the default locale.
2. Select **Theme** to determine the look of the new page. A root page is considered a level 0 page. This option is only available on a level 1 or 2 page.
3. Continue to the next step to set advanced options. If you do not want to set advanced options, click **OK** to save the new page and begin adding content or **Cancel** to discard the new page settings and return to Manage Pages.

Click **Advanced options** to view the optional settings in this section. The window shown in Figure 3-10 will appear.

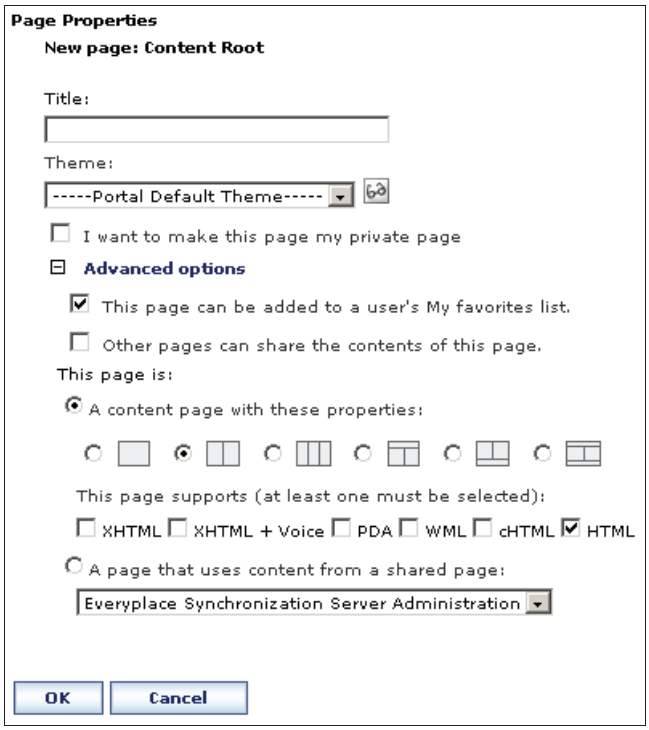

Figure 3-10 Creating a new page - advanced features

If you want to allow this page to be bookmarked by other users, check **This page can be added to a user's My favorites list**. If a user bookmarks this page, it will be available from **My favorites** in the banner.

Check **The contents of this page can be shared by other pages** if you want this page to be shared by others. If checked, users can reference this page when they create a new page.

Determine the page layout by selecting an option from **A content page with these properties**.

Check a supported markup from **This page supports**.

> **Note:** You must select at least one supported markup to create the page. The default is HTML.

If you want the new page to reference an existing page, check **A page which uses content from a shared page** and choose a shared page to reference.

Click **OK** to save these settings for the new page and add new content. A web page similar to Figure 3-11 will appear.

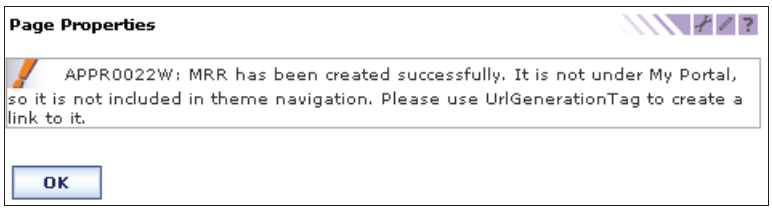

Figure 3-11 A new page has been created

Click **Cancel** if you want to return to Manage Pages without creating the new page.

Create new label

You can create a label to act as a separator. Labels can be used to help organize groups of pages, places, and URLs into categories. For example, if you have a Media place, you can create a Music label to separate your music pages and URLs from other media URLs.

To create a new label, perform the following steps:

1. Click **New label** to create a new label (Figure 3-12). You will leave Manage Pages to create the new label.

Figure 3-12 New label button

After clicking **New Label**, the window shown in Figure 3-13 on page 54 appears.

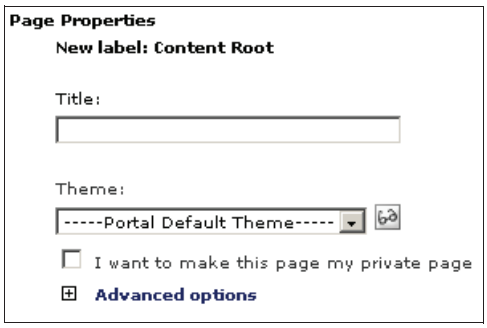

Figure 3-13 New label page

2. Type the title of the new label in **Title**. This is the title for the default locale. Select **Theme** to determine the look of the new label.

   Note: This option is only available when creating a root page.

3. Continue to the next step to set the advanced options. If you do not want to set advanced options, click **OK** to save the new label or **Cancel** to discard the label settings and return to Manage Pages. Click **Advanced options** to view optional settings in this section. The page shown in Figure 3-14 on page 55 will appear.

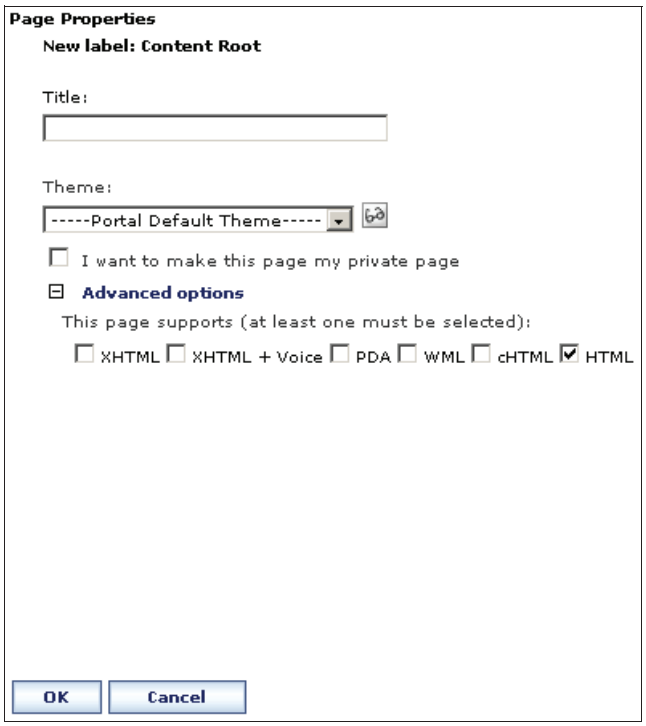

Figure 3-14 New label page - advanced features

4. Check the supported markup in **This page supports**.

> **Note:** You must select at least one supported markup to create the label. The default is HTML.

5. Click **OK** to save these settings for the new label. Click **Cancel** if you want to return to Manage Pages without creating the new label.

Create a new link

As the WebSphere Portal Server is an entry point for all the information you need, you can add external URLs to your portal navigation (even if those links take you outside the portal infrastructure)

To create a new URL, perform the following steps:

1. Click **New Url** to create a new URL (Figure 3-15 on page 56). You will leave Manage Pages to create the new URL.

Figure 3-15 New url button

2. Check that, depending on the page you are on, you will have or will not have the access for creating a new URL button. In this case, from the Content Root, as the default, you do not have permission to create URLs.

   Once you have clicked on the **New url** button, it takes you to the following page (Figure 3-16).

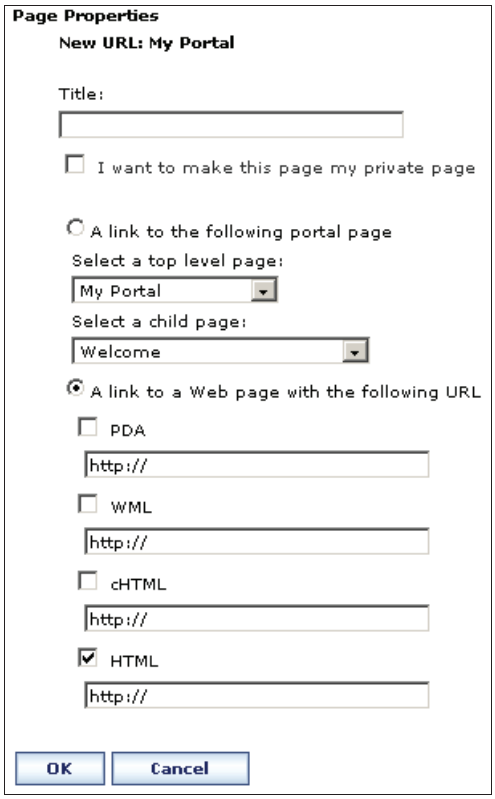

Figure 3-16 Creating a new URL

3. Type the title of the new URL in **Title**. This is the title for the default locale. You may create an internal or external URL.
   - If you select an internal URL (A link to the following portal page), you must select a bookmarkable page. In order to so, you have to select the top level page (starting from the Content Root) and a child page.

– If you select an external URL (A link to a Web page with the following URL), you should provide the URL for at least one markup language, but several URLs can be provided for different markup languages.

4. Click **OK** to save these settings for the new URL. Click **Cancel** if you want to return to Manage Pages without creating the new URL.

   From then on, the URL created will appear as though a Page inside a Label were created and if you click it, it jumps to the page you selected in the same window.

   Once the link is created, you can modify the link clicking the **Edit Property** button (see Figure 3-17).

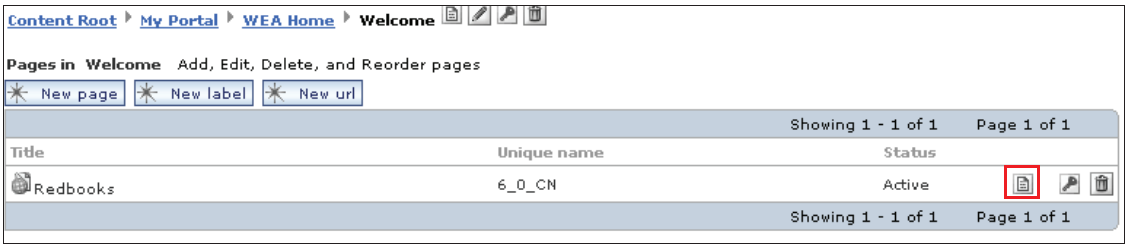

Figure 3-17 Editing a created link

You can change the Title name of the link by clicking **I want to select titles and description**, as shown in Figure 3-18 on page 58.

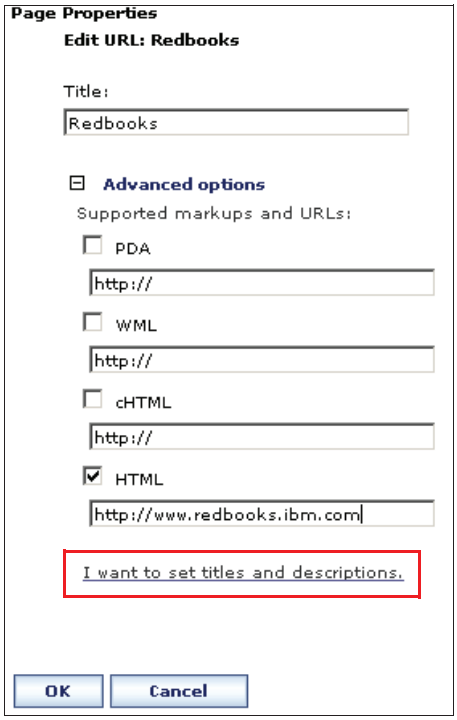

Figure 3-18 Setting titles and descriptions for different languages

That link will take you to a screen where you can change the titles and descriptions for different pages (see Figure 3-19).

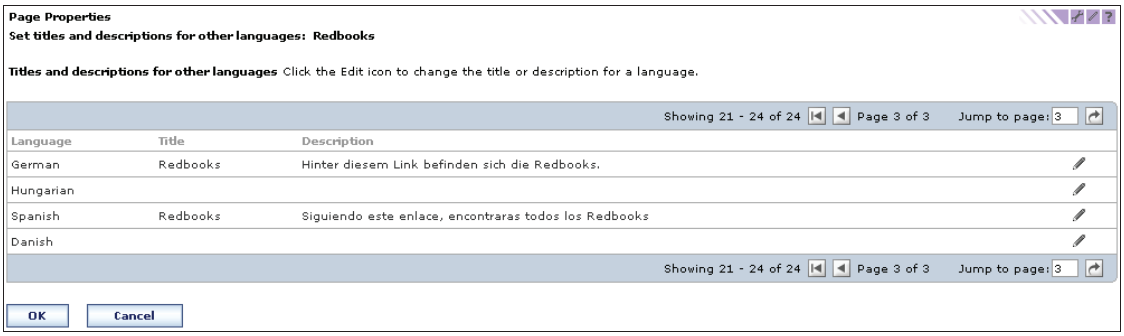

Figure 3-19 Changing titles and descriptions for different languages (II)

Editing pages

Once a page is created, it can be modified in several aspects, such as content, appearance, and lock containers.

For modifying an already created page, go to the Manage Places and navigate until you reach the page you want to change, clicking the **pencil** icon that reads Edit Page Layout (Figure 3-20).

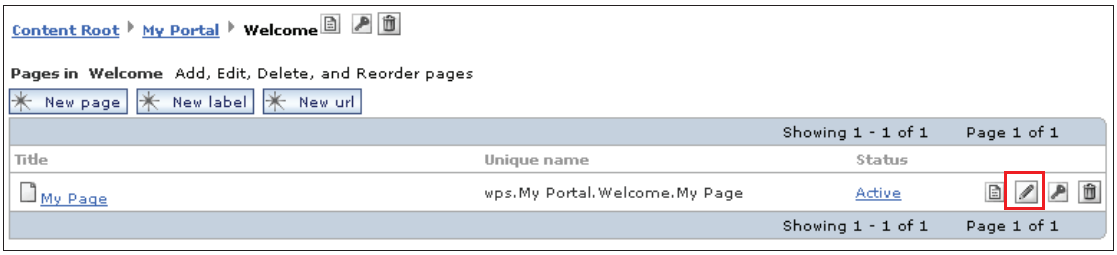

Figure 3-20 Editing pages

You can modify the Layout in three different ways:

- Content

  From here on, you can select the number of columns you have in your page by selecting one of the following graphs in Figure 3-21.

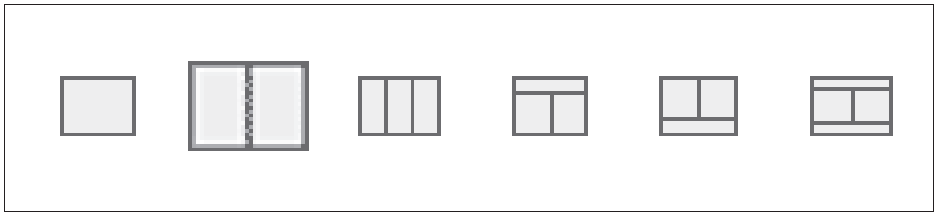

Figure 3-21 Different page layouts

Each graph shows a different way of arranging the page: 1 column, 2 columns (this is the one selected in Figure 3-21), 3 columns, and so on.

The second part of the page takes care of portlet arrangements on the layout defined in the previous section (Figure 3-22 on page 60).

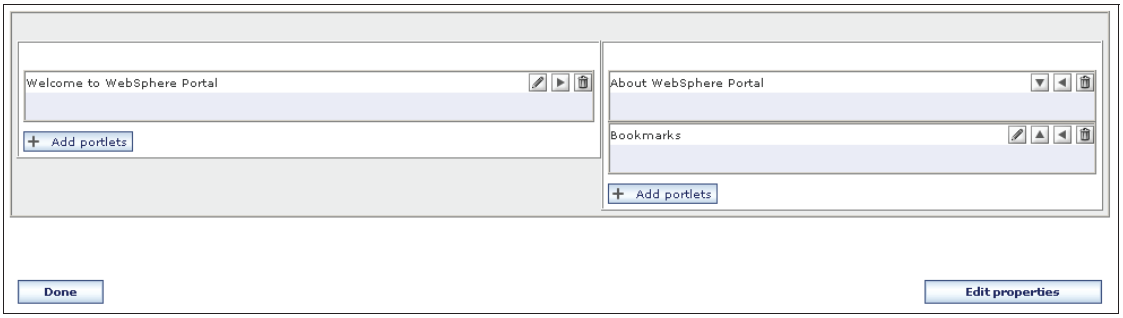

Figure 3-22 Modifying the content of a page

For each portlet, you can (Figure 3-23):

- Edit Portlet: Clicking the **pencil** icon that reads Edit Portlet.
- Delete Portlet: Clicking the **trash** icon that reads Delete Portlet.
- Move Portlets: Inside a page, you can move portlets to a different column (clicking **left arrow** or **right arrow**) or reorder then inside the same column (clicking the **up arrow** or **down arrow**).
- Add new portlets to the page: It appears as one **+ Add portlet** sign for each column.

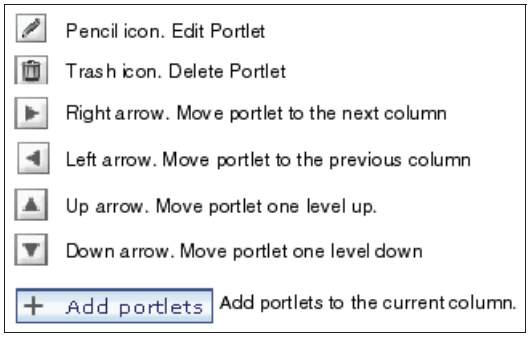

Figure 3-23 Icons in the Content Layout page

Clicking **+ Add portlets**, it takes you to the following screen (see Figure 3-24 on page 61), where you can search and select the portlets you want to include in the page. When finished, click **OK**.

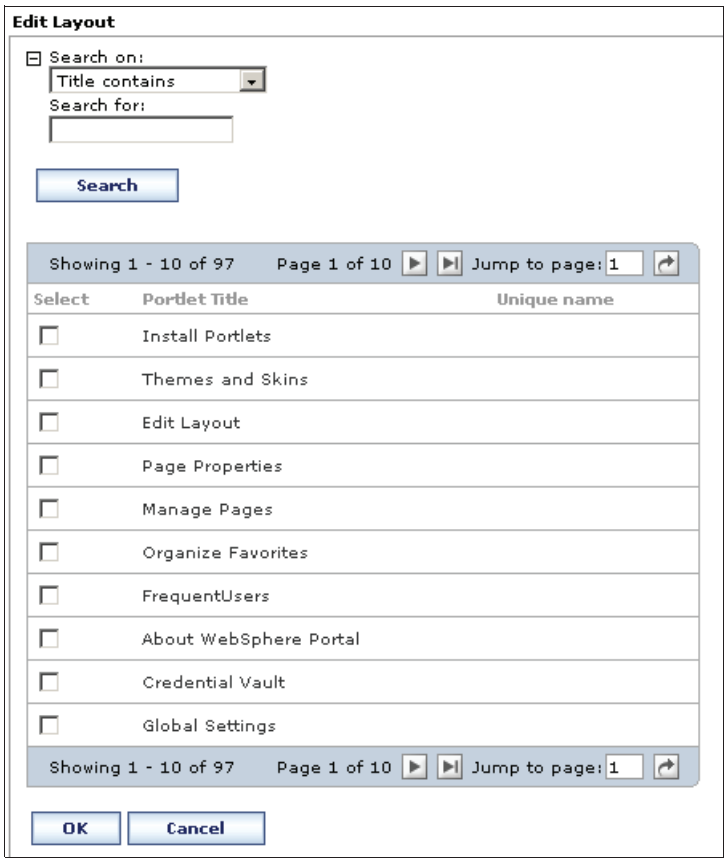

Figure 3-24 Adding portlets to a page

When you have selected the format of the page (number of columns), which portlets are needed, and where they should be located, click **Appearance** at the top of the page (see Figure 3-25).

Figure 3-25 Changing Appearance

- Appearance

  Once the content is already in place, you can, from the Appearance tab, change the skin of a portlet by selecting the correct skin from the combo box. Once selected, you can see a preview of the selected skin by clicking the **preview button** at the right of the combo box. The preview button is highlighted in Figure 3-26 on page 62.

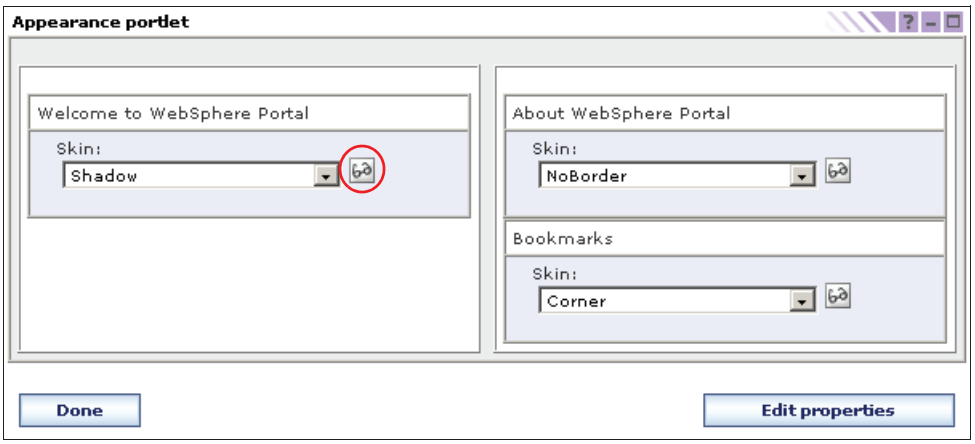

Figure 3-26 Appearance portlet

You can also select the default skin defined for the entire portal (see more on skins at 3.4.2, “Themes and skins” on page 64).

- Locks

  Once you have finished with the Appearance, you should click the next tab call **locks** (see Figure 3-27).

Figure 3-27 Changing the locks

With the Page Locks portlet, you can lock and unlock container content and containers by clicking the corresponding lock icon. You can lock and unlock the delete option for portlets by checking the check box on the title bar of the portlet. The Page Locks settings are hereditary to children portlets.

As seen in the following example (see Figure 3-28 on page 63), there is a hierarchy of locks.

At the first level, you have two different locks: The one on the left is called a container content lock and the following one is called a container lock.

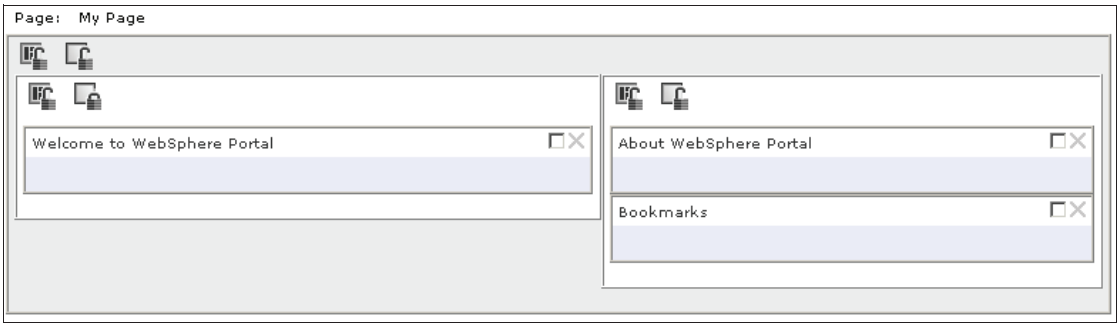

Figure 3-28 Locks page

If the first lock (container content) is locked, it means that the content of that layout cannot be changed, therefore, the child contents of the page will be locked automatically. That means that you cannot change the layout of the page (if you go back to the content tab, you will see that graphs showing the possible layouts do not show up (see Figure 3-21 on page 59).

In this example, the page has two columns defined in the Content tab. If you click any of the container content of one of the columns defined in the Content tab, you will see that it is not possible to add new portlets to that column (see Figure 3-29) or delete the portlet from the lock tab (the X arrow is disabled).

Also note that, as one of the content of a column is blocked, portlets cannot be moved from the other column (in our example) to that locked column. Note that some left arrow buttons are dismissed (see differences between Figure 3-22 on page 60 and Figure 3-29).

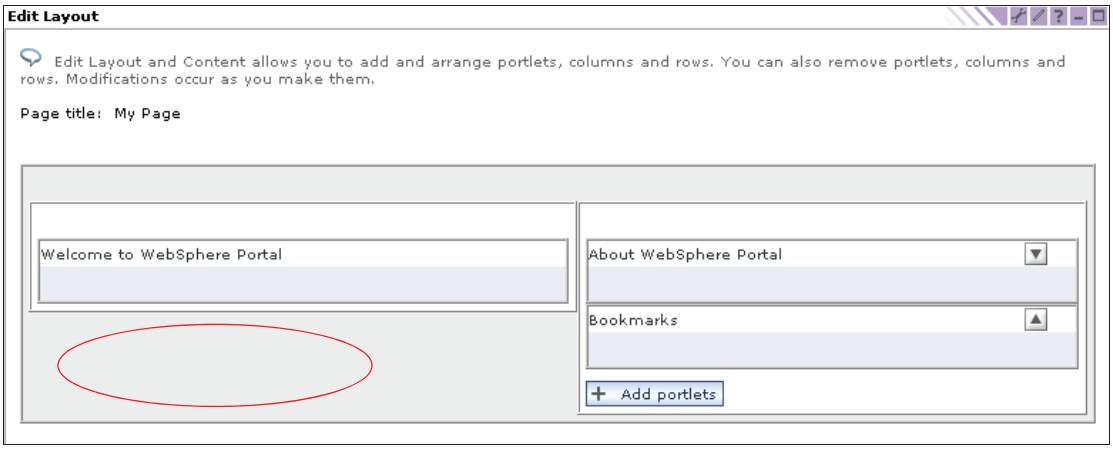

Figure 3-29 Add portlet button is removed

Note: Note that when the container content lock is unlocked, it will seem that you cannot delete a portlet. However, as soon as you click the **X** you are actually marking that portlet for deletion and it will effectively be deleted when you will click **Done**.

3.4.2 Themes and skins

A theme is an interchangeable front end for a portal node or group of nodes. A theme controls elements such as the banner, navigation, colors, and look and feel for a node. The option to set a theme is only available when creating a node and that node has nodes nested immediately beneath. For example, if the node, sports, has a nested page, baseball, which has a nested page home runs, only the sports and baseball pages can be assigned a theme.

From the Administration Portal control, you can access the Portal User Interface, and just after that, if you click Themes and Skins, you will get the following page (Figure 3-30).

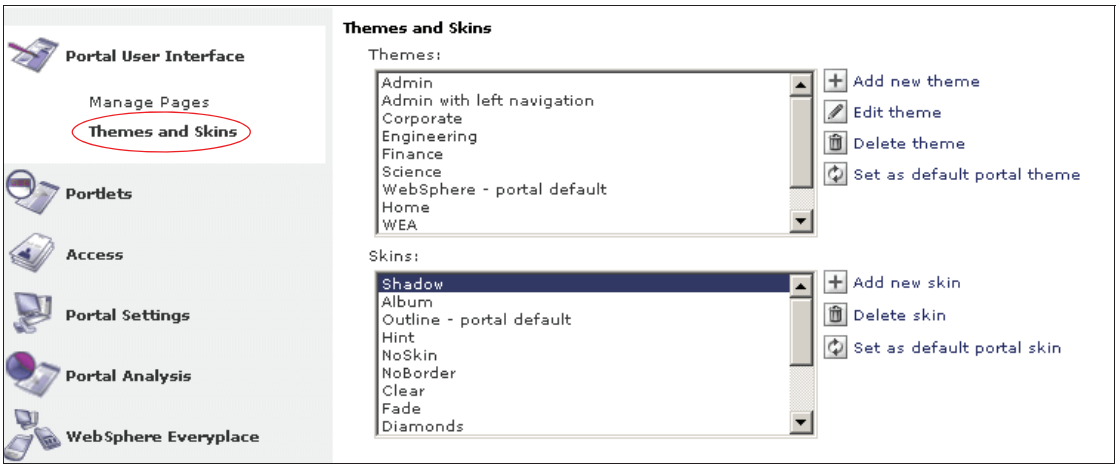

Figure 3-30 Themes and Skins portlet

On the Themes dialog box, you could:

- Add a new Theme by clicking the **+** sign next to **New Theme**, which takes you to the following page (Figure 3-31 on page 65).

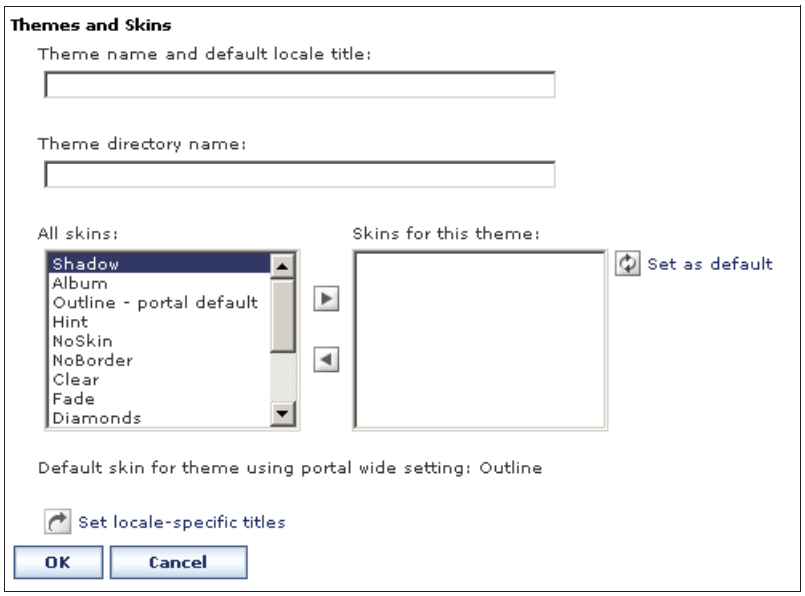

Figure 3-31 Creating a new theme

When the **Add new theme** page is displayed, you have to:

- Name the theme. Specify the name with which you would like to refer to the new theme. This is the default locale title.
- Specify the location of the theme files. Specify the name of the directory in which the theme files are located. This value will be equivalent to one of the directories located in:

  <portal_server_directory>/app/wps.ear/wps.war/themes/<markup_language>

  where <portal_server_directory> is the install location of the portal server and <markup_language> is the type of markup language you are using.
- Specify which portlet skins the theme will use.
- Set a default skin. Select a skin from the list of skins for the new theme. Then click the **Set as default** button to set the selected skin as the default skin for the theme. If no skin is selected as the theme default, the portal-wide skin default is used.
- You can also specify titles for different languages.

Click **OK** when you are done to create the theme. Click **Cancel** to go back to the Manage Themes and Skins page without creating the theme.

- Edit an existing theme. When editing a theme, you can modify the skins the theme uses.
- Delete a Theme. You can delete a theme from the portal, but the real files are not removed from the system.
- Set a default portal theme. You can select a default portal theme for the whole system. If another theme is selected instead, this is the one the system uses. If no theme has been selected for selected pages, the default theme will be used.

Changing themes does not only apply to the Web browser interface from the PC, but it could change the interface of the mobile device. The only thing needed for that is that the theme selected has to have themes developed for mobile devices.

The following page (Figure 3-32) shows the same page when different themes have been chosen.

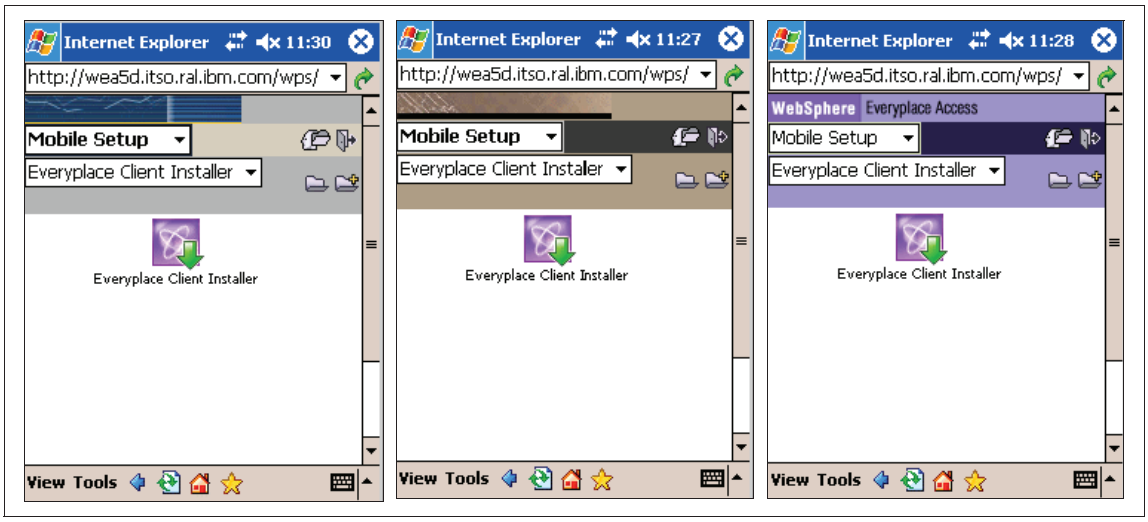

Figure 3-32 Different themes on the PDA

A skin is an interchangeable front end for a portlet. A skin controls elements such as the minimize and maximize icons, the title bar, and the background color or pattern.

From the same page where the theme is selected (see Figure 3-30 on page 64), several actions can be taken on skins:

- Add new skin
- Delete skin
- Set as default portal skin

The components are handled are the same as themes, with the same menus but related to skins.

3.5 Portlets

All portal based applications (as WebSphere Everyplace Access) are based in labels, pages, and eventually in portlets.

This section will show you how to install, uninstall, and modify portlets, as well as how to manage applications and a special case of a portlet: the Web clipping portlet.

3.5.1 Portlet Install

In addition to the existing portlets in WebSphere Portal, other portlets can be installed, configured, and added to pages. Following the J2EE specifications, WebSphere Portal installs portlets via Web ARchives or *WAR* files. The WAR file contains one or more portlets, the portlet initial configuration, deployment descriptors, and associated files, such as images. The portlet developer is responsible for building the portlet and delivering it in a WAR file for installation to the WebSphere Portal administrator. Installing a WAR file is a simple process.

Perform the following steps to install a portlet:

1. Enter the portlet's location in the **Directory** field (the Directory field is located where your browser is running. It does not have to be in WebSphere Everyplace Access). You can also use the **Browse** button to navigate your file system (see Figure 3-33 and Figure 3-34 on page 68).

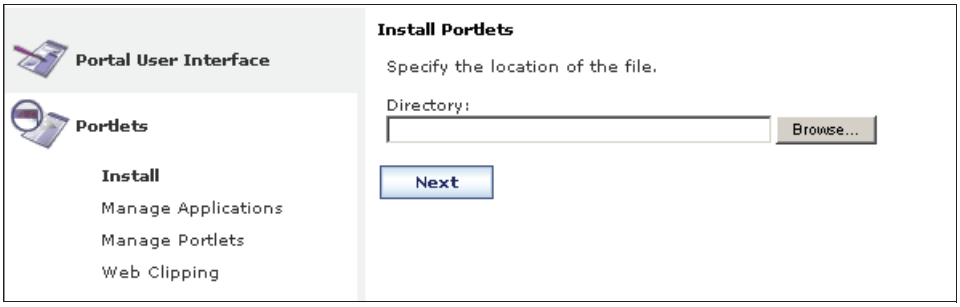

Figure 3-33 Installing a portlet

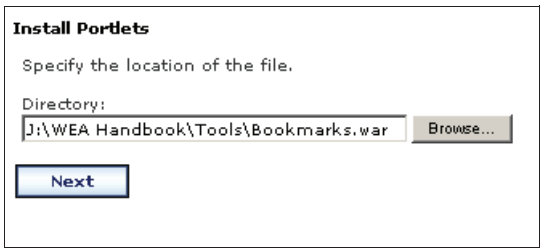

Figure 3-34 Installation process

2. Select the portlet WAR file you want to install.
3. Click **Next** to begin the installation process.
4. A confirmation appears that lists the portlets included in the WAR file. Click **Install** to begin the installation. Click **Cancel** to return to Install Portlets.
5. When installation is complete, you are returned to Install Portlets, and a message confirming success or failure is displayed. A successful installation indicates that the portlet has been added to the portlet catalog and activated. To allow others to use this portlet, you must set the access rights for it (see 3.6.2, “Giving permissions to resources” on page 81).

Note: You must be assigned a Manager or Administrator role to install portlets.

3.5.2 Manage applications

When installing portlets on the WebSphere Portal, these portlets come in a Web Archive file (WAR file). These files are much more than containers, because they could contain portlets (one or more than one), html pages, jsp pages, gif files, and much more.

Therefore, each WAR file works as a complete application from a WebSphere Portal point of view.

In this section, you will learn how you can manage those applications.

Under the **Administration** portal control, click **Portlets** → **Manage Applications**, as shown in Figure 3-35 on page 69.

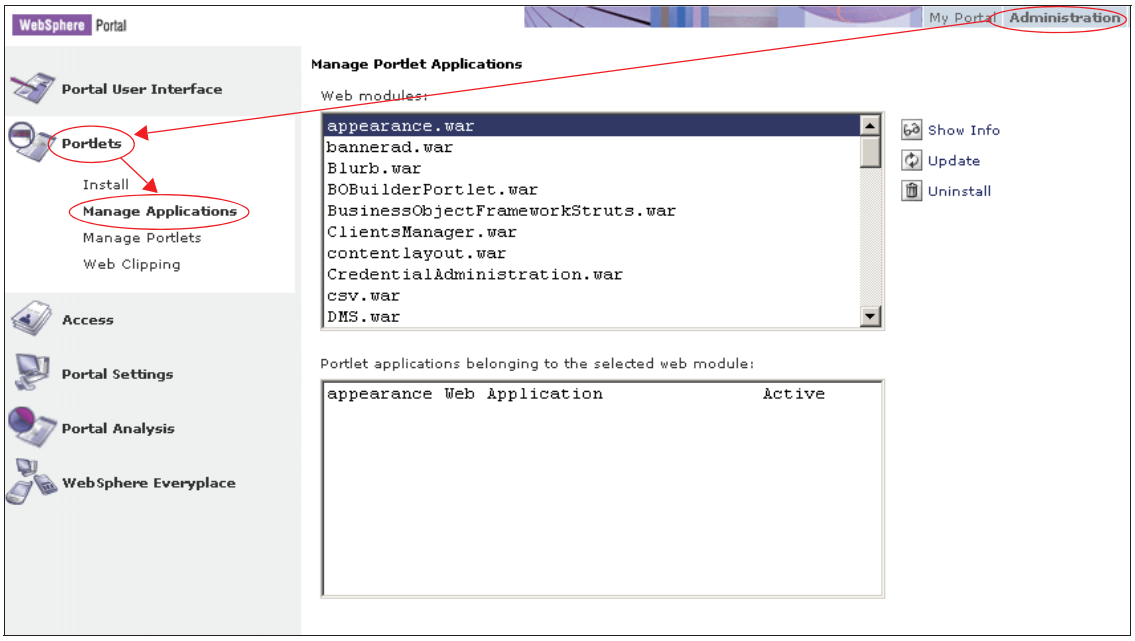

Figure 3-35 Manage Applications portlet

All Web archives installed on WebSphere Portal will appear in the first box. If you select an application, you will see the related portlets that it contains and if you select the portlet, some icons will appear in order to manipulate those portlets.

This way of working with portlets works in the same way that the Manage Portlets portlet works, which will be explained in 3.5.3, “Manage Portlets” on page 70.

Going back to the WAR files, different actions can be done on every application.

Show information about applications

To show information about applications, you have to select the application you want to see information about and click the **Show Info** button next to it (the icon is represented as a small pair of glasses).

Once you click the pair of glasses, you can see information about the selected web module, the portlet applications belonging to the Web module, the name of the portlets, and so on. Just click **Done** to go the previous page.

Update installed application

When you are in the middle of a portlet development, and you install the same war files several times, it could be useful to not install and uninstall now and then.

There is the option to update an existing war file, which works basically how it was shown in 3.5.1, “Portlet Install” on page 67.

Uninstalling applications

Once one application is not used anymore, it can be removed from the system. In order to do so, the application must be selected and then you must click the **trash bin icon** on the right. The system will ask for confirmation. If you answer **OK**, the application will be deleted from the server (and all the related files)

> **Note:** Keep in mind that if you delete an application that has several portlets associated, all of them will disappear from the system, so they will not be accessible to it anymore.

3.5.3 Manage Portlets

This section of the administration is used to administer each portlet installed in the WebSphere Portal.

To get to the Manage portlets page, you have to follow the steps shown in Figure 3-36.

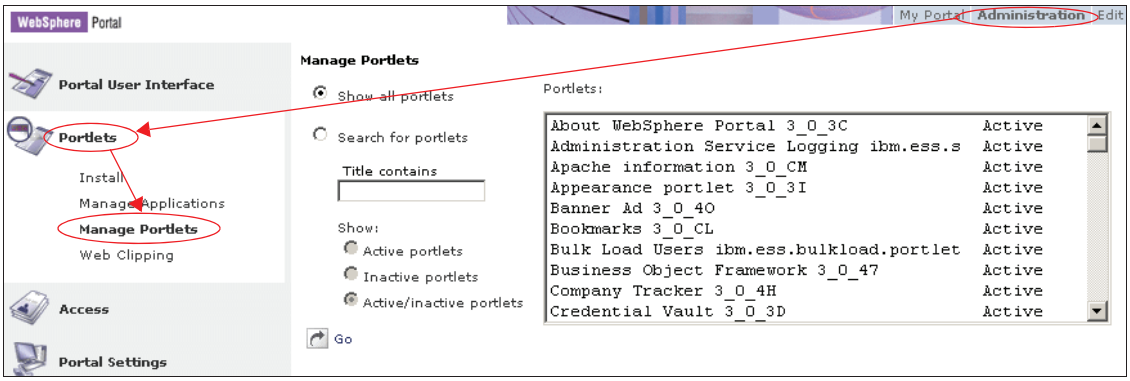

Figure 3-36 Manage Portlets portlet

On this page you will be able to:

- See all the available portlets
- Search for a portlet (Title Contains) between the active, inactive, or active/inactive portlets.

The result (as seen in Figure 3-36) is valid for both options.

On the first column, you will see the name of the portlet (unique name) and the second one will give you information about whether the portlet is active or inactive.

Keep in mind that the same portlet could have several instances, so the name will be the same, but the end of the portlet name will be different. In the following example (see Figure 3-37), you see a portlet with the same name but with a different ending. Also, one of the portlets is active and the other one is inactive.

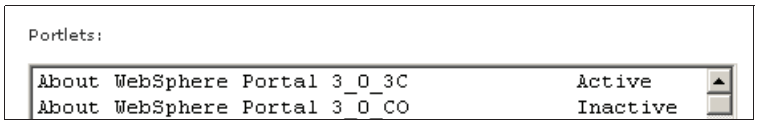

Figure 3-37 Two cloned portlets

Once you have selected a portlet, several actions could be done:

- Activate / Deactivate. With this option, you can activate a portlet, and given the right permissions, use it in pages. Or you can deactivate the portlet, and it cannot be incorporated in any page, and in those pages where it is used, from then on, it will not appear again. You can access this option by clicking the **Activate / Deactivate** button on the right hand side.
- Copy: With this option, you can create an exact copy of a portlet, but it will be registered in the system as a different portlet. You can access this option by clicking **Copy**. This option can have many different uses, such as:
  - Assign an instance of a portlet to each person.
  - Those portlets that are not prepared to work with authenticated uses (that is, there are some portlets where the configuration applies just to all the users, so a particular user cannot change the parameters for himself/herself). In this scenario, if there are not many users using this portlet, copying the portlet could be a solution.
- Modify parameters. You can modify the parameters of each portlet by clicking the **wrench** (Modify Parameters). Each portlet has a different set of parameters such as language configuration, icon location for each markup language, location of the jsp pages, and so on.
- Show info. If you click the **Show Info** link, you will see information relative to the portlet you are working on, such title and description.

3.5.4 Web clipping

Web clipping allows you to perform Web clipping to identify and extract specific portions of an HTML document for display in a type of portlet called a Web clipping portlet (see Figure 3-38 on page 72). Using the Web Clipping Editor, you

can tailor the content of the portlet to better suit the needs of your users and any display constraints that might be associated with the device displaying the portlet.

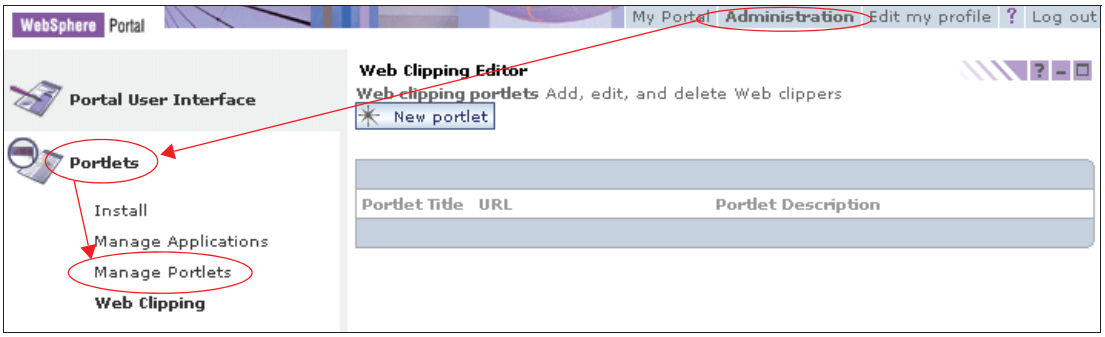

Figure 3-38 Accessing the Web Clipping editor

Note: You can click the URL of a Web clipping portlet listed in the table to use as a reference, and the site will open in a new window. For example, if `http://wea5d.itso.ral.ibm.com/manual/index.html` is the URL from where you want to clip, click the URL in the table to view that site in a separate window.

Creating Web Clipping content

To create Web clipping content, follow these steps:

1. Click **New portlet**.
2. Type the name of the Web clipping portlet in the **Name and default locale title** field. This value is used both as a name to identify the portlet and as the default locale title. Enter a description for the Web clipping portlet in the **Description** field. To specify titles and descriptions for the Web clipping portlet in other languages, click **Set locale-specific titles and descriptions**. Enter the fully qualified URL (for example, `http://wea5d.itso.ral.ibm.com/manual/index.html`) of the HTML document that the Web clipping portlet is associated within the **URL to clip** field (see Figure 3-39 on page 73).

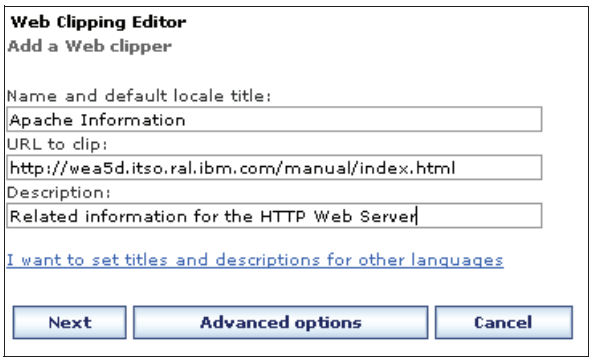

Figure 3-39 Creating a Web Clipping portlet

3. Click **Advanced options**. If you want to modify the default values for the clipping type, authentication options, URL rewriting rules, or firewall options, click the appropriate link. Make your changes, and click **OK** to return to this page.

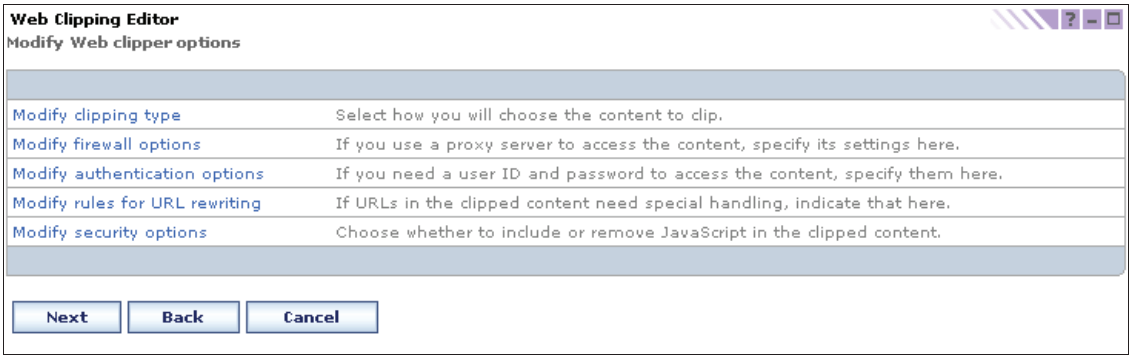

Figure 3-40 Advanced options for Web Clipping

4. Click **Next**. Select the content to keep and preview the resulting output. While previewing the resulting output, if you selected to follow the links, you can use **Back** to navigate through the pages you selected for the Web clipping portlet.
5. Click **Done** to save the Web clipping portlet.

Using that portlet in a page inside the portal, you can search the portlet using the text you used in the Name and Default locale title.

Keep in mind that this portlet does not give access to anybody (but administrators), so you must give access to other users if you want to use it.

Using the Web Clipping editor portlet, you can create new portlets. Portlets created this way are registered in the system with the name in the Name field and a default locale. You can see if the portlet has been installed by following the procedure in 3.5.3, “Manage Portlets” on page 70.

3.6 Access

Use this section of Portal Administration to control who has access to your portal. Define your user group and user hierarchy using Users and Groups. Use Resource Permissions to assign user groups and users to specific roles for a resource. Use User and Group Permissions to view the level of access a user group or user has for a given resource. Use Credential Vault to manage and maintain the secure storage of credentials within your portal.

3.6.1 Users and groups

Manage Users and Groups allows you to view, create, and delete users and user groups. You can also change group memberships. Before you can modify user and group information, you must have the appropriate level of authorization. See the Access Rights topic in the WebSphere Portal InfoCenter for more information.

Creating users

There are two different ways of creating a user:

1. Click **Sign up Portal Control** (when nobody is connected to the WebSphere Portal). This is used for self-care registration. See Figure 3-41 on page 75 for details.

Figure 3-41 Self-care user creation

All the fields with a preceding star are mandatory. All the fields are self-explanatory.

In this case, the user is created and it can be seen in the Lotus Domino Administrator tool (see Figure 3-42 on page 76).

Note: In this example, we are using Lotus Domino as a LDAP directory.

Something that you have to keep in mind is that the user just created belongs only to the All authenticated portal users group (see “Creating groups” on page 78).

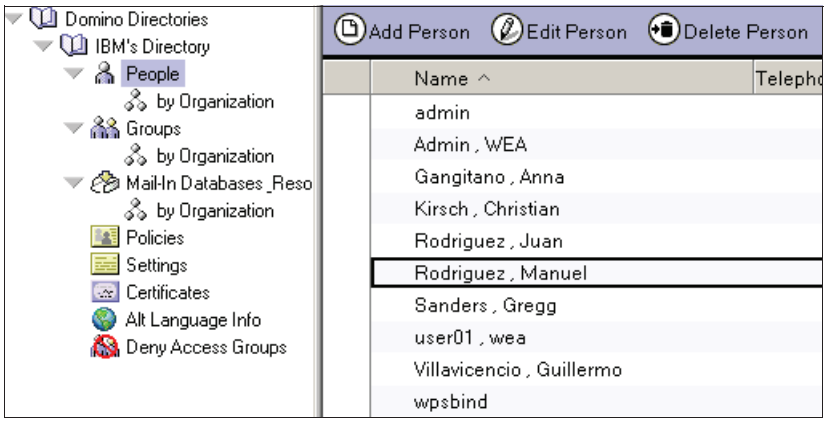

Figure 3-42 Lotus Domino Administrator tool

2. Within the Portal Administration (see Figure 3-43 on page 77), you have to select **Administration** → **Access** → **User and Groups** and search **All available** in the drop-down list **Users Groups**.

   At this point, you have to select one of the already created groups and click it (for example, wpsadmins).

   Once you have selected a user group (clicking the name), you will be able to create a new user, and that user will belong to that group (and the group called All authenticated portal users).

   The process of creating a user is exactly the same as shown in Figure 3-41 on page 75.

Figure 3-43 Creating a user

Editing user information

Once the user is created, its information can be modified at any time. In order to do so, there are two different ways of doing it:

1. The user can change his information by clicking the portal control **Edit my profile** once the user is logged in (see Figure 3-44).

Figure 3-44 Modifying user information

Changing information about the user is as easy as creating it.

2. The user can be modified from the Users and Groups tab. The first thing to do is to select **Users** from the **Search for** drop-down, select **uid** from the **Search on** drop-down (there are many different criteria for selecting a user, so please feel free to check all the possible values) and write the user name you are looking for (see Figure 3-24 on page 61 for more details).

   Once you have narrow down the search and you have the user on the screen, you have to click the **pencil** on the right (it is marked on the picture with a red circle). Changing that information is as easy as creating it.

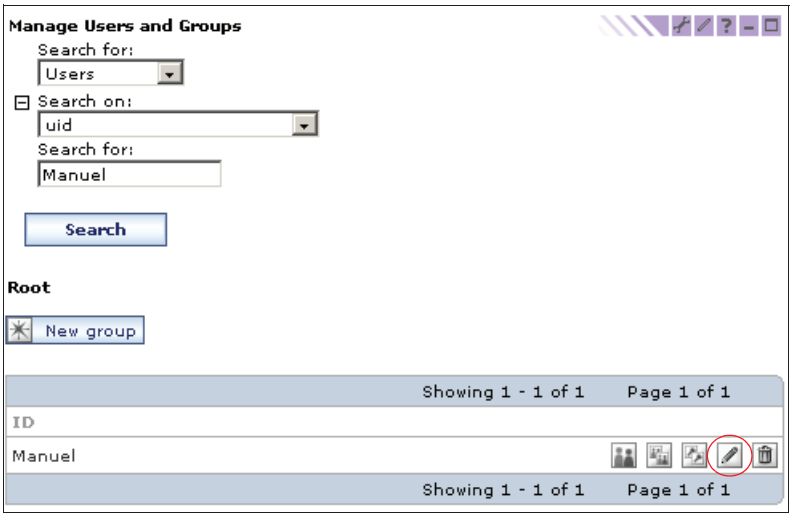

Figure 3-45 Modifying user details from the Administration tab

Note: There is a special user called the anonymous portal user that allows access to the portal without a user ID. As a user, it has rights to access resources, so keep in mind which resources are available to the special user.

Creating groups

As a best practice, all the users created in WebSphere Portal must be under one or more groups. This makes management of the access control list and the management of users easier.

There are many predefined user groups when you install the WebSphere Everyplace Server, depending on what is installed (basic installation versus component installation). These are some of the groups you could find:

- All portal users group: This group contains all the groups that are available in the system.

- All authenticated portal users: This group contains all registered users available in the system.
- LocalDomainsServers & LocalDomainAdmins: Users which can manage the Domain Servers (in our case, Domino servers).
- dmadmins: In this group, we can find all the users with admin rights to manage the device management services (known as Device services).
- essusers: All the users that have the rights of synchronize data from the server to the mobile device and the other way around (ess stands for Everyplace Synchronization Server).
- essusers_nonlock: In the previous group, essusers, they are able to synchronize, but they cannot modify the settings. Users included in this group can change the settings.
- essadmins: Privileged users to administrate and manage the synchronization settings.
- wpsadmins: Users which have admin rights to manage all parts of the portal.

Please note that some users can belong to more than one group.

There are many ways of creating a group: as a stand-alone group, as a group inside another group, and so on. Depending on your requirements, each option has some benefits and drawbacks.

From the Administrator portal control, click **Access** → **User and groups** → **New group** button, as shown in Figure 3-46 on page 80.

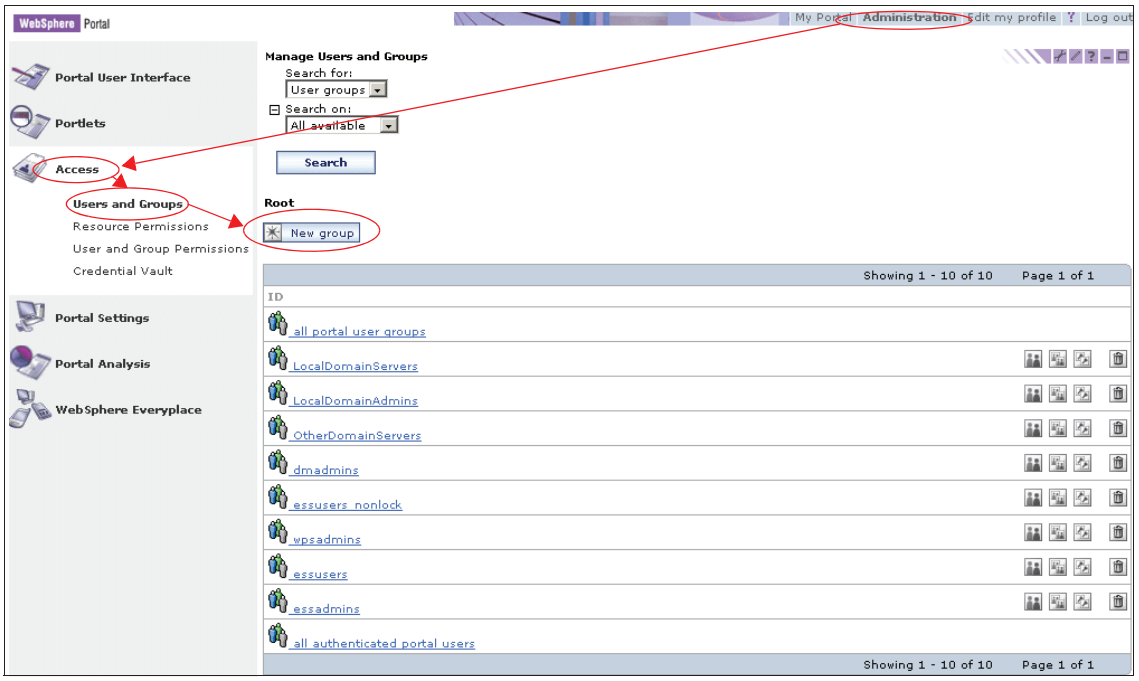

Figure 3-46 Creating a group

When clicking **New Group**, you just have to input the Name of the group and click **OK**.

From now on, you can:

- Include users into the group. Click the name of the group and click **Add member**. Keep in mind that a member could be any group or any user. You navigate until you find the user(s)/group(s) you want to include, mark the box next to the name(s), and click **OK**.
- Include groups into a new group. As stated before, you could include a group as a member of an existing group. You follow the same steps as the previous paragraph and you include the groups you need.
- Create a new user. Follow the same steps shown in “Creating users” on page 74.
- Create a new group.

3.6.2 Giving permissions to resources

In a WebSphere Portal environment, all the pages, labels, portlets, and so on are called resources. To access, modify, or administrate these resources, users (and groups) must have the rights to do so.

WebSphere Portal includes several types of resources. For a detailed description of these resources and the resource hierarchy, refer to the “Securing your portal” section of the InfoCenter, which is included with the product.

Resource types are broad categories that contain resource instances. Resource instances are specific resources, such as a single portlet or page. Each resource instance belongs to only one resource type. For example, the resource instance Market News Page would belong to the Page resource type.

You can assign roles on virtual resources and on resource instances. Assigning roles on virtual resources reduces the time needed to administer access control, because all child resources inherit roles that are assigned to the parent resource. Assigning roles to specific resource instances offers more granular access control. Refer to the “Securing your portal” section of the InfoCenter for more detailed information about the relationship between virtual resources and resource types.

Table 3-1 provides a brief description of resource types.

Table 3-1 Resource types

Resource Type	Description
Web Modules	Portlet WAR files that are installed on WebSphere Application Server. Web modules can contain multiple portlet applications.
Portlet Applications	Parent containers for portlets.
Portlets	The portlet objects. Multiple instances of the portlet object can exist on multiple pages in the portal. Users have the same access to all instances of a portlet.
Pages	The content that determines the portal navigation hierarchy.
User Groups	Groups of portal users.
URL Mapping Contexts	User-defined definitions of URL spaces that map to portal content.

Resource Type	Description
Virtual Resources	Virtual resources have two functions: They protect sensitive operations that affect the entire portal. For example, the XmlAccess virtual resource protects the ability to execute XmlAccess scripts. They group resources of the same resource type. For example, the Web Modules virtual resource is the root node of all Web Modules within the portal. Role assignments on the Web Modules virtual resource permit access to all Web Modules in the portal.

Unlike WebSphere Everyplace Access V4.3, this new version of WebSphere Everyplace Access V5.0 has defined *roles* for each task.

Roles on a resource propagate to all of its child resources. For example, if a user has the Editor role on the Market News Page, then by default that user also has the Editor role on all pages that are children of the Market News Page.

Users and user groups may be assigned different roles for each resource. Roles determine the level of access and can be assigned in one of three ways:

1. Explicitly assigned by someone with the necessary authorization. Use the User and Group Permissions portlet or the Resource Permissions portlet to assign roles explicitly. Explicit role assignments override role blocks. For more information about role blocks, see the “Securing your portal” section of the InfoCenter.
2. Implicitly assigned through membership in a user group. Use the Manage Users and Groups portlet to administer group membership.
3. Inherited through a role assignment on a parent resource. Use the Resource Permissions portlet to administer role blocks that affect inherited role assignments. You can also use the User and Group Permissions portlet to administer the role assignments that a user or group has on a parent resource.

Table 3-2 on page 83 summarizes roles and how they affect user interaction with resources.

Table 3-2 Roles definition

Role	Permissions
Administrator	Unrestricted access on resources. This includes creating, configuring, and deleting resources. Administrators can also change the access control configuration
Security Administrator	Creating and deleting role assignments for roles tied to specific resources.
Delegator	No actual access to resource, but allows creating and deleting role assignments. Delegator roles allow assigning specific users or user groups to roles.
Manager	Creating new resources as well as configuring and deleting existing resources that are used by multiple users.
Editor	Creating new resources and configuring existing resources that are used by multiple users.
Privileged user	Viewing portal content, personalizing portlets and pages, and creating new private pages.
User	Viewing portal content. For example, viewing a specific page or user profile.
No role assigned	Cannot interact with resource.

There are two different perspectives where you can assign roles to a resource:

- Resource permission: Starting from the perspective of a resource, you can navigate until you get the resource you want to work on. Then you can assign users/groups to different roles.
- User and Groups Permission: Starting from a user or group, you can select afterwards the resource what you want to work on.

Resource Permissions

Starting from the Administration portal controls, you can get to the Resource Permission portlet, as shown in Figure 3-47 on page 84.

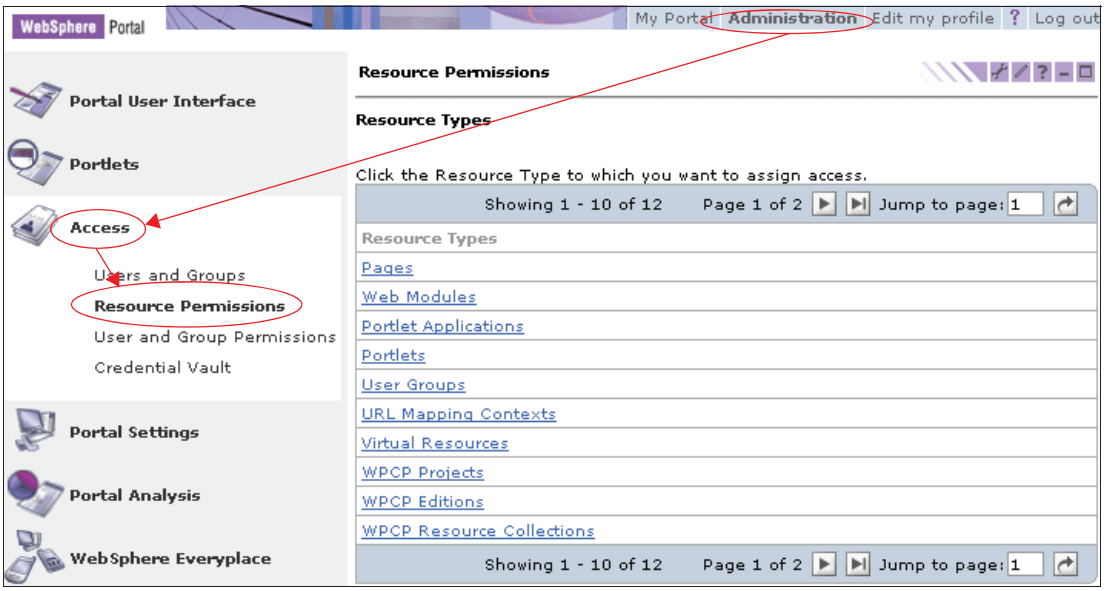

Figure 3-47 Assigning permissions to a resource

Once you have decided what resource you need to modify, you must navigate to the end resource.

For example, if you want to change the page called My page from the Welcome label, you have to select **Pages** → **Content Root** → **My portal** → **Welcome**, and you will end up in the page shown in Figure 3-47.

By clicking the **key** (highlighted with a circle), you will be able to see all the features relative to the resource permission (see Figure 3-49 on page 86).

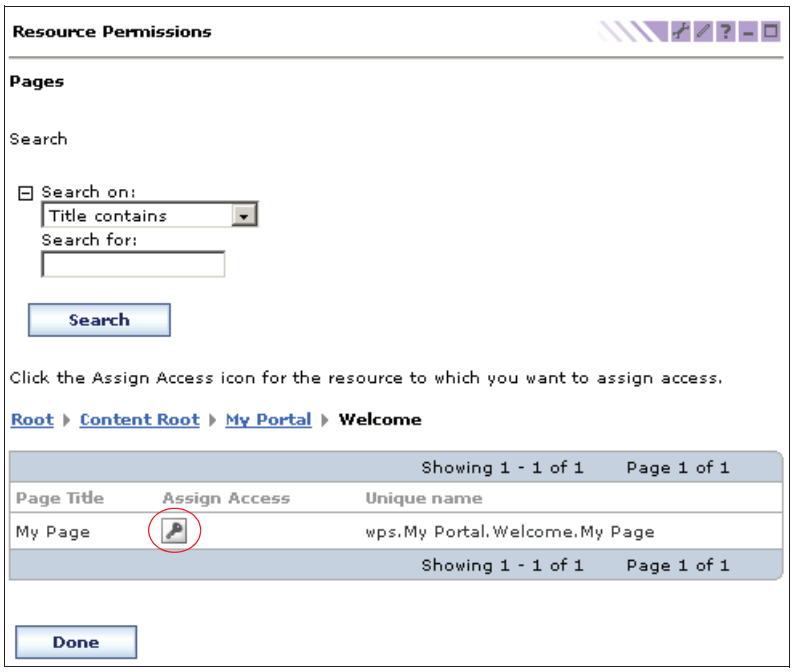

Figure 3-48 Assigning permissions to a resource (I)

In Figure 3-49 on page 86, there are four different columns:

1. Roles: Specifies each role that can be applied to the resource.
2. Allow Propagation: This information can be inherited from another resource or it can be specified by a user who needs a role. In our example, number 1 shows how the permissions given to this window are propagated to the rest of resources that are dependant on this page (just for the Administrator and Security Administrator profiles). The rest of roles have the same permissions, but they have been given explicitly.
3. Allow Inheritance: Allows child resources to inherit permissions from parent resources. You can see the flag activated in number 3 because it has been granted permission already, and in number 4, you see that the permission is given manually.
4. Edit Role: In this column, you can see a pencil for each role. Clicking this **pencil** allows the administrator to members grant access to the roles (either users or groups).

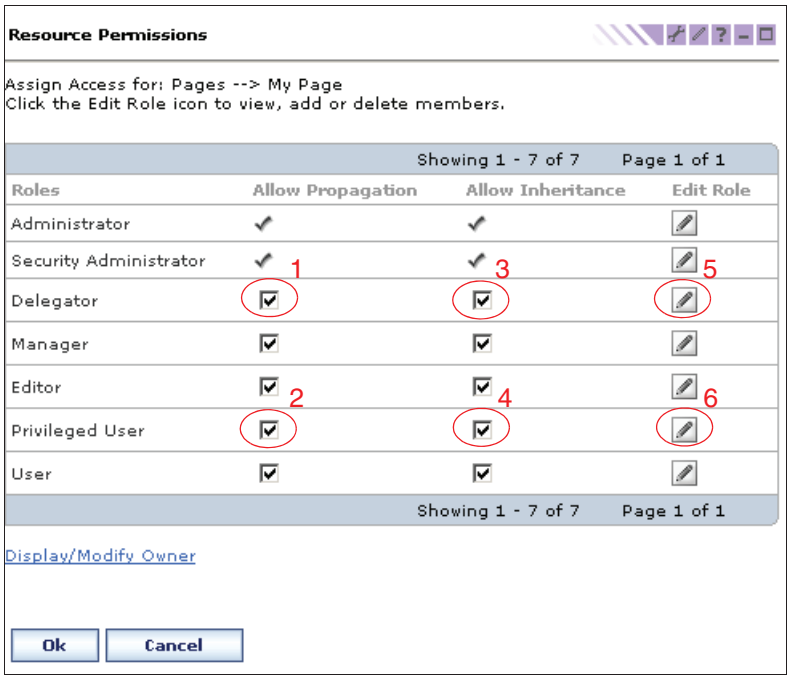

Figure 3-49 Assigning permissions to a resource (II)

If you click number 5, you will see that no member is assigned to this role (see Figure 3-50 on page 87). On the other hand, if you click the icon that is located on the administrator role, you will find that weaadmin (WebSphere Everyplace Access Administrator user) and wpsadmin have access to this role (see Figure 3-51 on page 87).

If you click number 6 (see Figure 3-49), you will see that just the anonymous user portal user has access to this role. So keep in mind that, if a portal contains important information, this must be kept in the portal and not exported to non-validated users (see Figure 3-52 on page 88).

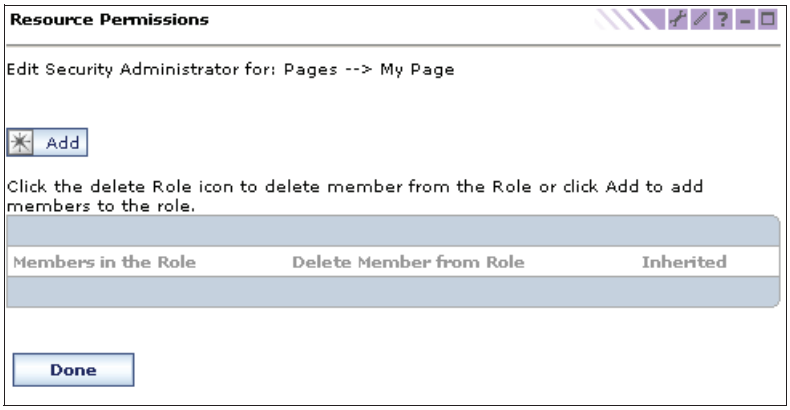

Figure 3-50 Users and Groups assigned to the Security Administrator role

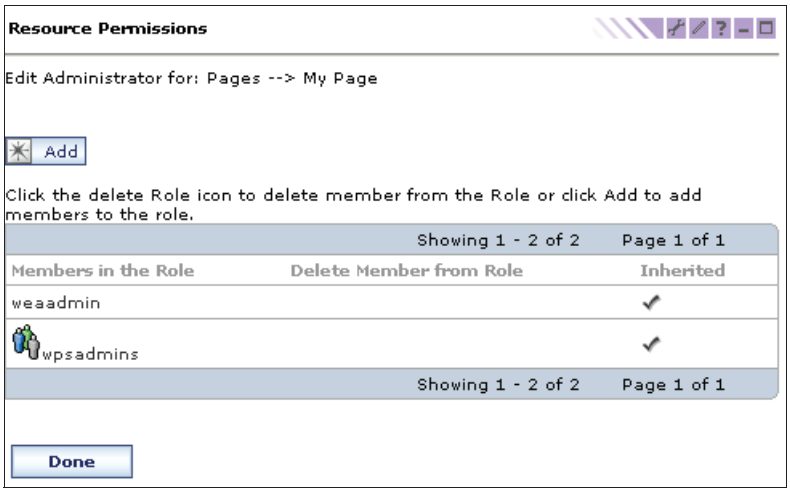

Figure 3-51 User and groups assigned to the Administrator role

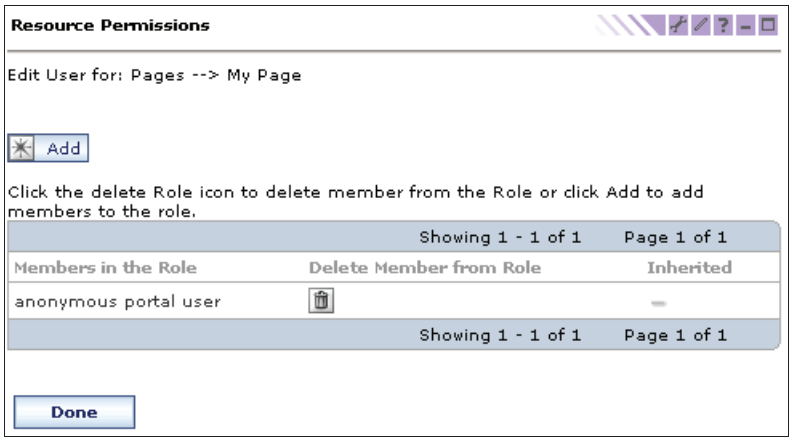

Figure 3-52 Users and groups assigned to the User role

User and Group Permissions

As stated above, there are two different perspectives of the same thing. So far, we have used the Resource Permissions view.

With the User and Group Permissions view, instead of focusing on what to give permissions to, we focus on who should have permissions.

Therefore, we start looking at groups / users and once we select them, we should be able to allocate a resource and give permissions to that resource to the specific user or group we had selected before.

So, in our example, if we want to give permissions to My page to a user called Manuel, we should follow these steps:

1. Select Users on the first page we found after clicking **User and Group Permission** and search for the user you are looking for (see Figure 3-53).

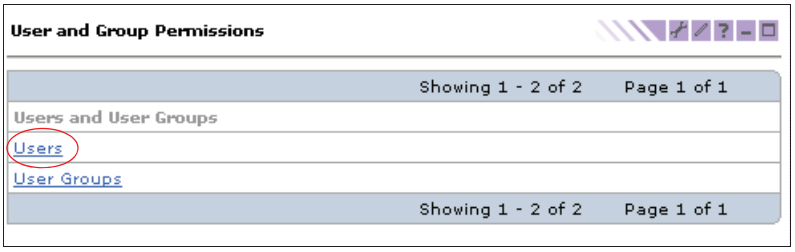

Figure 3-53 Selecting User Permissions

2. Once you find the user (in our example, Gregg Sanders), click the **pencil** icon (highlighted with a circle) (see Figure 3-54).

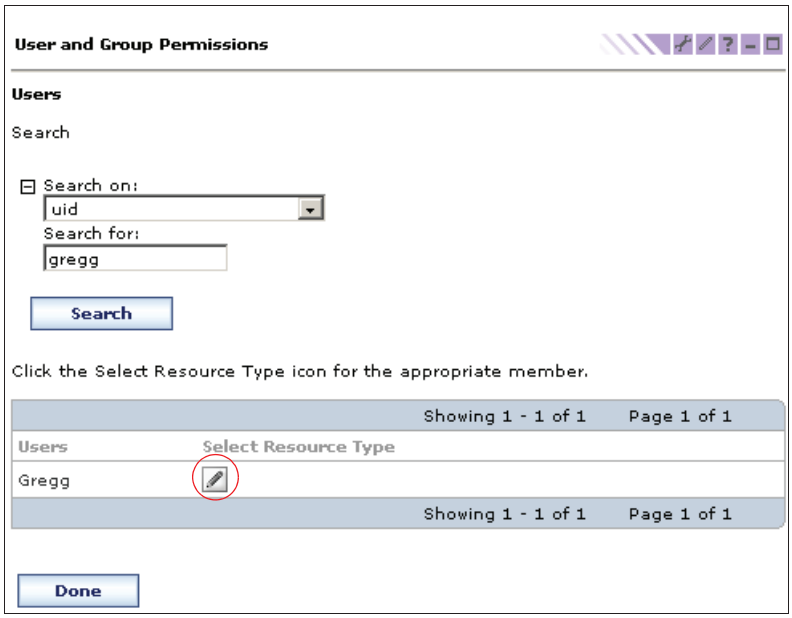

Figure 3-54 Selecting the user

3. Select the Resource you want to give access to by selecting the route where the resource is or searching for it. In our example, we are going to give access to the resource My Page (see Figure 3-55 on page 90).

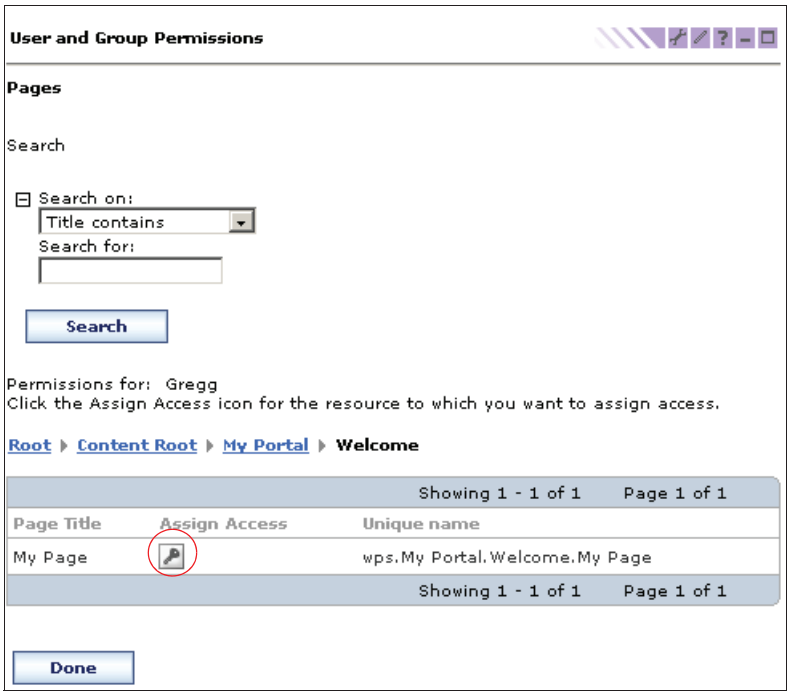

Figure 3-55 Selecting the resource for the selected user

4. Once you click the **key** icon, you can give any access to the user (see Figure 3-56 on page 91).

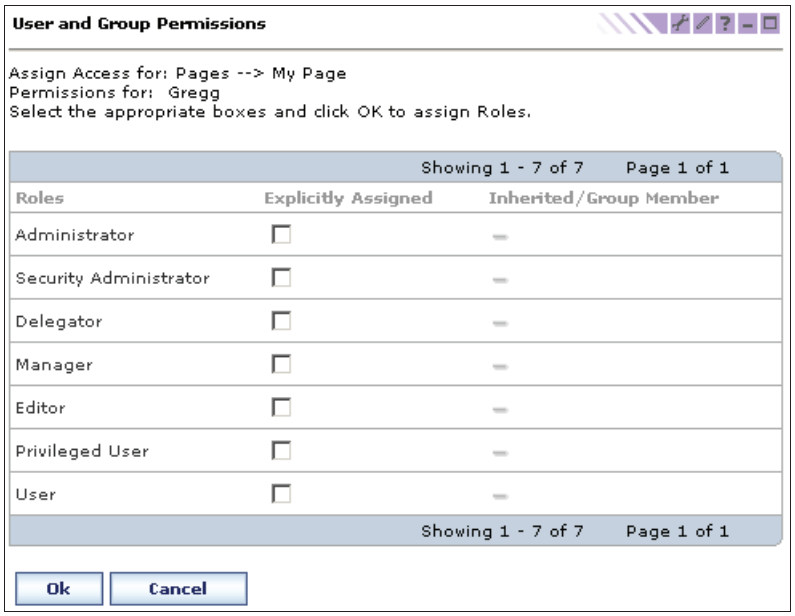

Figure 3-56 Giving explicit access to the selected user

If what you want is to give access to specific resources to a specific group instead of a user, select **User Groups** instead of Users, as shown in Figure 3-53 on page 88. From then on, the configuration is exactly the same for all the users in the group.

As a best practice recommendation, try to give access to groups instead of individual users. For management purposes, it is much easier to keep a system when everything is based on groups.

3.7 Portal settings

As WebSphere Everyplace Access administration relies on WebSphere Portal, there are a few options that are specific for WebSphere Portal. Also, under Portal settings, some options are not directly used in WebSphere Everyplace Access.

3.7.1 Supported markup

One of the important options for WebSphere Portal is the ability to show content for different devices and in different ways. Therefore, markup languages must be created in order to differentiate between all kind of devices. For accessing the supported markup, see Figure 3-57 on page 92.

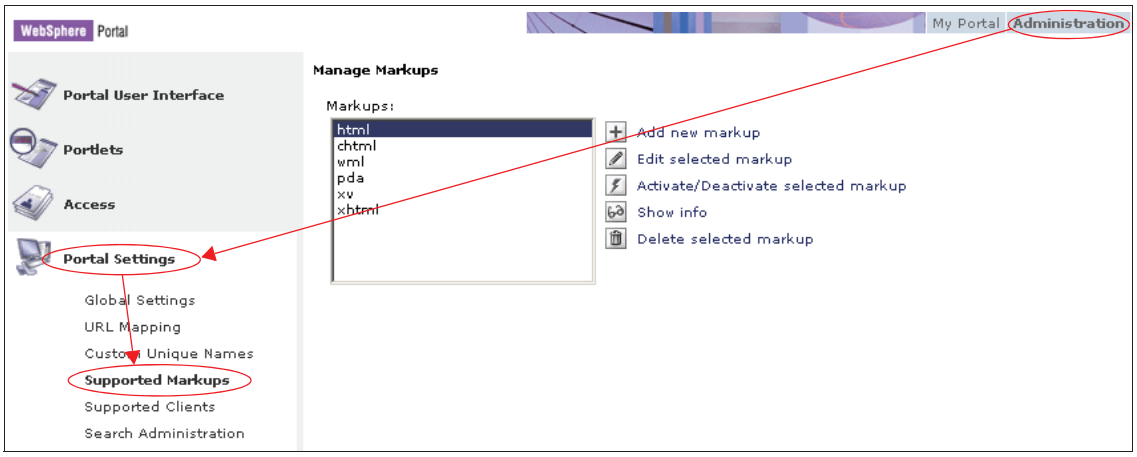

Figure 3-57 Accessing Supported Markup portlet

By default, a few markups already exist (the most commonly used ones), but you can perform several actions on these markups (or create a new one if you need it):

- Add a new Markup: Although the markup languages you see here are the most commonly used ones, it is always possible to create a new one. Clicking **Add new markup** (or the sign **+**) will take you to the following page (see Figure 3-58).

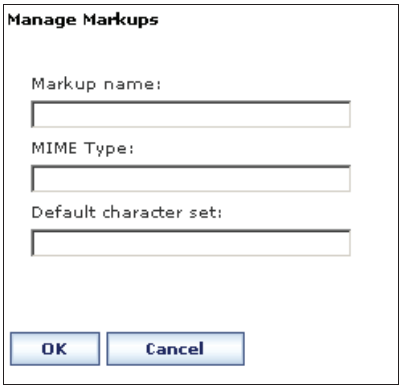

Figure 3-58 Adding a markup language

The following fields must be filled:

  - Markup name: Required. Indicates the name of the markup. Directories of this name also have to be created to support the aggregation of the portal

for clients that support this markup. For example, to add the markup MathML, the following directories have to be created:

was_root/installedApps/*hostname*/wps.ear/wps.war/MathML

was_root/installedApps/*hostname*/wps.ear/wps.war/themes/MathML

was_root/installedApps/*hostname*/wps.ear/wps.war/skins/MathML

was_root/installedApps/*hostname*/wps.ear/wps.war/screens/MathML

For this reason, avoid characters in the markup name that might cause conflicts inside file or path names, such as /, \, ., or &. The markup name also acts as a default title for those languages where no locale-specific title has been set.

– MIME type: Required. Enter the MIME type associated with this markup (that is, text/html).

– Default character set: Indicates the character encoding to be used for this markup unless not specified in the locale-specific settings. If this field is left empty, UTF-8 is used as the default character set.

- Edit selected markup: You can change the values you specified previously and you can modify the Set locale-specific settings:

  – Set locale-specific settings: Click this button to open markup settings for different languages.

- Activate / Deactivate selected markup: You can make one markup language not available for the portal. This option is useful when it is clear what kind of content you are going to supply (for example, if the only content you want to supply is html, just deactivate the rest of the markup languages).

- To display detailed information about all of the markups defined to WebSphere Portal, click **Show info**. The Markup Info list is displayed, showing the properties defined for each markup from the Markup fields. See Figure 3-59 on page 94 to see what kind of information is provided.

- Delete selected markup: If you select a markup language, you can delete it. If your WebSphere Portal is just going to be used for html, you could remove all the different markups.

> **Note:** Do not delete the html markup language because otherwise you will not be able to administer the portal (using the Web interface).

Manage Markups

Name	Title	MIME type	Default character set	Created	Last Modified
html	HTML	text/html	UTF-8	May 31, 2002	Sep 16, 2004
chtml	cHTML	text/html	UTF-8	Sep 10, 2004	Sep 10, 2004
wml	WML	text/vnd.wap.wml	UTF-8	Sep 10, 2004	Sep 10, 2004
pda	PDA	text/html	UTF-8	Sep 10, 2004	Sep 10, 2004
xv	XHTML + Voice	application/xhtml+voice+xml	UTF-8	Sep 10, 2004	Sep 10, 2004
xhtml	XHTML	application/xhtml+xml	UTF-8	Sep 10, 2004	Sep 16, 2004

OK

Figure 3-59 Information about all supported markup language

3.7.2 Supported clients

Every new device normally comes with a predefined browsing interface (either Web, WAP, and so on) or in some cases, for different applications or business needs, a new browser is installed.

Each different browser has a means of communicating with the server it is connecting to, which browser it is, and what capabilities it has.

The standard way of communicating with the server about this information is sending it in a header (if using html based browser) known as a *user-agent*. This header provides a name to the server that is unique to that browser and provides the version.

Unfortunately, each browser's provider is providing its own user-agent content, and it is not standarized anyway.

Therefore, when a device wants to get content from the WebSphere Everyplace Access, it send its user-agent header to the system. These are the steps taken by the system in order to provide the right capabilities to the client:

1. It extracts the user-agent header from the request (normally an HTTP request)
2. It checks against the supported clients list (see Figure 3-60 on page 95) to see if that user-agent exists. That check goes from the top to the bottom and it stops at the first match.
3. When it finds a proper supported client entry, it goes to the supported markup and it forwards that request to the appropriate page.

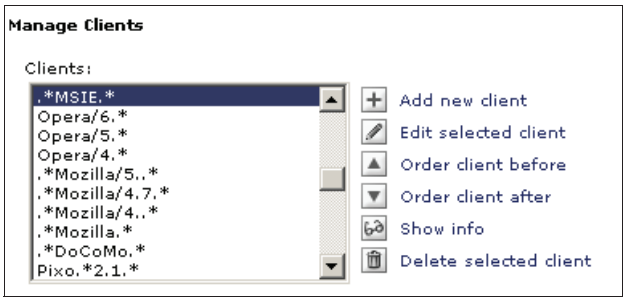

Figure 3-60 Supported clients portlet

From the supported clients portlet, you can select different options:

- Add new client.

  When a new browser client comes into the marketplace and its user-agent is not known, it must be defined here. The following form must be filled in:

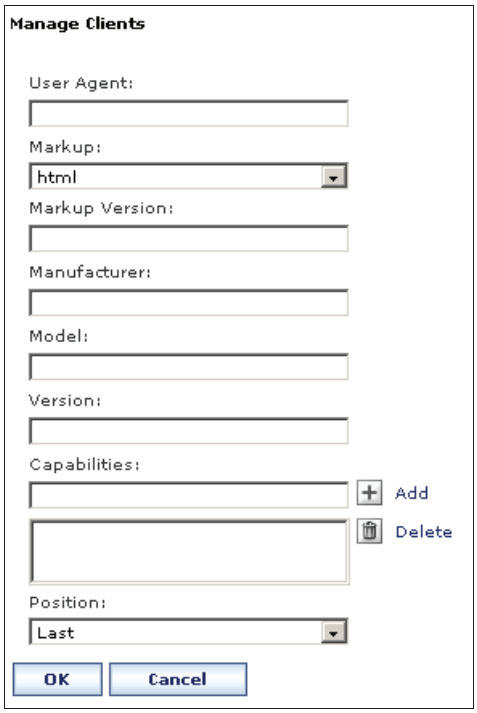

Figure 3-61 Creating a new client

The following items are used to define a client:

– User agent: Required. Enter the name of the client. This should match as close as possible the user agent string that the client sends in its request header. You might need to enter several string patterns for a single client. In addition, surround the name with a period plus asterisk combination, for example:

```
.*useragent.*
```

This wild card string is used and resolved according to the wild card resolution rules of the Apache foundation. Keep the following in mind:

- Some user agent strings contain locale information about the language of the client browser. The portal uses the language definition in the HTTP request header for its language selection. It usually is not necessary to define user agent patterns on certain browser languages.
- Some client browsers include information about the operating system. In most cases, the client detection should work independently of this setup.
- Some browsers allow the user to customize the user agent patterns.

– Markup: Required. Indicate the type of markup the client supports. The markup must already be defined to the portal from Manage Markup.

– Markup Version: Optional. Indicate more specific information about the markup supported by the client. This markup version is used to identify deviations of a standard markup. For example, WebSphere Portal includes the markup version in the registry to correctly handle HTML deviations of the Microsoft Internet Explorer.

– Manufacturer: Optional. Enter the name of the company that manufactured the client.

– Model: Optional. Indicate the model number or name of the client.

– Version: Optional. Indicate any version associated with the model.

– Capabilities: Enter specific capabilities of this client. If the client is a Web browser, for example, you could list specific capabilities in HTML that it supports, such as frames or JavaScript. Click **Add** to add it to the capabilities list. To delete a capability, select it from the list and click **Delete**.

– Position: Indicate the order in which you want this client entered in the client registry. The WebSphere Portal Server matches the user agent string in the client's request header to patterns in the client registry. For example, if the user agent sends 'Microsoft Internet Explorer 5.5' and the portal server finds '*Internet Explorer 5*', then that registry entry is used to determine markup sent to the client. For this reason, it is recommended to

place the most specific User Agent patterns at the top of the list. The default user agent pattern (*), if included in the list, should be placed in the last position.

- Edit selected client: When a client is selected, you can modify any of the fields explained in the previous section (Add a new client).
- Order client before: As stated earlier, the position of a user agent can determine which characteristics can be used. It is highly recommended that more specific (or newer user agents) go as close to the top as possible, if there are more than one related to the same browser (for example, Internet Explorer 6 should be before than Internet Explorer 5). If it is not related to the same browser, it is not critical where the user agent is.

  Clicking **Order client before** moves the agent one position up.
- **Order client after**: It moves the agent one position down.
- **Delete selected client**: It deletes the user-agent from the list.

Note: A user-agent is always associated to a browser type and not to devices. Therefore, it some cases, you might be using just one device with two different user-agents when using different browsers. For example, you could be using Internet Explorer and Netscape browsers in your workstation.

3.8 Portal analysis

Use this section of Portal Administration to gather data about your portal. Frequent Users gives you user statistics. Enable Tracing allows you to turn on portal logging features.

3.9 WebSphere Everyplace functions

Specific Everyplace Access functions, such as Everyplace Synchronization Server, Intelligent notification Services, Location Aware Services, Device services, and so on, can be seen in the following resources:

- Everyplace Synchronization Server: For details, see *IBM WebSphere Everyplace Access V5 Handbook for Developers and Administrators Volume III: E-Mail and Database Synchronization*, SG24-6676.
- Intelligent Notification Services: For details, see *IBM WebSphere Everyplace Access V5 Handbook for Developers and Administrators Volume IV: Advanced Topics*, SG24-6677.

- Location Aware Services: For details, see *IBM WebSphere Everyplace Access V5 Handbook for Developers and Administrators Volume IV: Advanced Topics*, SG24-6677.
- Device Services: For details, see Chapter 9, “Device Services” on page 339.

4

Basic WebSphere Everyplace Access installation

This chapter describes how to use the Basic Installation to install WebSphere Everyplace Access and configure it to use a Domino Directory. It provides step-by-step instructions to install and configure the Domino LDAP as well as WebSphere Everyplace Access and its requirements.

© Copyright IBM Corp. 2005. All rights reserved.

4.1 Overview

Websphere Everyplace Access V5 has two installation options: the Basic Install and the Component Install. The Basic Install option includes everything that is needed for PIM and e-mail synchronization, including all the prerequisite software. A configuration wizard is available that allows for the rapid setup of proof-of-concepts with the Personal Information Manager (PIM) and e-mail synchronization solution.

In our sample environment, we will install WebSphere Everyplace Access on a single computer. Lotus Domino, which acts as mail server and LDAP Directory, is on another machine.

It is important that each machine has a host and domain name, which is registered in the DNS Server, so that both machines can be accessed by its name. In our example, the server with WebSphere Everyplace Access is called wea5d.itso.ral.ibm.com and the server containing Lotus Domino is wea5e.itso.ral.ibm.com.

On wea5e, we will install Lotus Domino and Lotus Notes. The Notes client is needed to configure Lotus Domino. This server is only an example for a mail and LDAP server, because in a given environment, for example, at a client, you would generally use existing installations.

On the machine wea5d, we will install all components of WebSphere Everyplace Access and its requirements:

- DB2 Workgroup
- WebSphere Application Server
- WebSphere Portal Server
- Everyplace Access Services without Offline functionality
- Device Management Services
- Everyplace Synchronization Server

4.2 Domino server installation

This section describe the installation of the Domino machine. It includes the preparation of the machine, the installation of the Notes Client to administer and configure Domino, as well as the Domino installation and configuration for WebSphere Everyplace Access.

In our example, we will install Lotus Domino V6.5.1 and Lotus Notes V6.5.1 on the machine. As described above, the machine name is wea5e.itso.ral.ibm.com. This name is registered in DNS so that the machine is accessible with this name.

Note: If you consider installing Lotus Sametime Everyplace on Domino, be sure to use the supported Domino Version:

- Sametime V3.1 is supported on Domino V6.0.3.
- Sametime V3.0 is supported on Domino V5.x.

4.2.1 Preparation

Before installing Lotus Domino, you should check, that the computer has all the prerequisites.

Check the Service Pack version

WebSphere Everyplace Access requires Service Pack 4 for Windows 2000 Server and Advanced Server. Service Pack 4 must be installed before the WebSphere Everyplace Access installation. To verify that the correct service pack version is installed:

1. Select **Start** → **Run**.
2. Type `winver` and press **Enter** to display information about Windows.
3. Verify that Service Pack 4 is installed.
4. If Service Pack 4 is not installed, refer to the Microsoft support site or Windows Update for Windows 2000 to download and install the service pack.

Check for static IP address

WebSphere Everyplace Access requires that the computer has a static IP address.

1. Select **Start** → **Settings** → **Network and Dial-up Connections**.
2. Right-click the LAN connection for your network adapter and click **Properties**.
3. On the network adapter properties window, select **Internet Protocol (TCP/IP)** from the list of components used by the connection and click **Properties**. The Internet Protocol (TCP/IP) will display.
4. Verify that **Use the following IP address** is selected. If **Obtain an IP address automatically** is selected, the computer has a dynamic IP address. If this is the case, contact your network administrator to obtain and configure a static IP address.

Check for a fully-qualified host name

WebSphere Portal also requires the use of a fully qualified host name (this is typically the host name of the server) along with its fully-qualified domain name (FQDN). For a basic installation, the Domino and the WebSphere Everyplace Access Server should have access to each other. Follow these step to check that your computer has a host name and a FQDN:

1. Select **Start** → **Settings** → **Control Panel** → **System** and click **Network Identification**.
2. Click **Properties**. In our example, the computer name should be wea5e and the full computer name wea5e.itso.ral.ibm.com.
3. If there is only a host name, contact your system administrator or change the host name and FQDN. To do that, enter a host name in the field **Computer name**.
4. To specify a FQDN, click **More** and enter it into the field **Primary DNS suffix of this**. Click **OK**.
5. Click **OK**. If you changed any settings, reboot your computer.
6. Try to ping yourself:

   ```
   ping wea5e.itso.ral.ibm.com
   ```

7. You should see a reply.

Check port bindings

Specific ports are required to install Lotus Domino. If two applications attempt to use the same port, a port conflict results. To ensure that the required port bindings are available, the netstat utility can be used.

1. Select **Start** → **Programs** → **Accessories** → **Command Prompt** to launch a command prompt.
2. Type `netstat -an` at the command prompt.
3. Look at the numbers listed in the Local Address column. The number after the colon is the port number. For example, in the IP address 1.2.3.4:80, 80 is the port number.
4. Verify that Port 80, required by Lotus Domino, is not in use. If it is in use you may experience port conflicts.

If port 80 is in use, it is possible that IIS is installed. If the Microsoft Internet Information Services (IIS) Web server is running, you will have a port conflict with IBM HTTP Server. Both of these Web servers listen on port 80, unless otherwise configured. To prevent this conflict, disable the Microsoft IIS Web server.

Follow these steps to verify that IIS is enabled:

1. Select **Start** → **Settings** → **Control Panel** → **Add/Remove Programs**.
2. Select **Add/Remove Windows Components**.
3. If IIS is listed, it has been installed on the computer.
4. To disable IIS:
   a. Select **Start** → **Programs** → **Administrative Tools**.
   b. Open **Services**.
   c. Locate and highlight **IIS Admin Service**.
   d. Select the **Action** menu and click **Properties**. A window opens.
   e. Change the **Startup type** to **Disabled** and click **Stop** to stop the server.
   f. Click **Yes** to stop any services that are stopped as a result.
   g. Locate the **World Wide Web Publishing Service**. Disable it at startup using the steps listed above.

4.2.2 Install Lotus Notes

Follow these steps to install Lotus Notes:

1. Start the installation either by using an installation CD or a file, which contains the installation files. For a CD installation, skip to step 3.
2. Specify where the installation files should be extracted and click **Next** (see Table 4-1).

Table 4-1 Lotus Notes 6 directory

Field	Value
Directory	C:\Program Files\Lotus Notes 6

3. The Lotus Notes Installation window will appear. Click **Next**.
4. Select **I accept the terms in the license agreement** and click **Next**.
5. Enter a name and company and click **Next**.
6. Accept the default folders (see Table 4-2) and click **Next**.

Table 4-2 Lotus Notes directory

Field	Value
Directory	C:\Program Files\Lotus\Notes

7. Be sure to select **Domino Administrator** and click **Next**.

8. Accept the default and click **Install**.
9. Click **Finish**.

Note: After finishing the Lotus Notes installation, the directory (including all the files) created in Step 2 can be deleted.

4.2.3 Installing Domino Server

Follow these steps to install Domino Server:

1. Start the installation either by using an installation CD or a file, which contains the installation files. For CD installation, go to step 3.
2. Specify where the installation files should be extracted and click **Next** (see Table 4-3).

Table 4-3 Lotus Domino 6 directory

Field	Value
Directory	C:\Program Files\Lotus Domino 6

3. The Lotus Domino Installation window will appear. Click **Next**.
4. Accept the License by clicking **Yes**.
5. Enter a name and company. Leave Partitioned Installation unchecked and click **Next**.
6. Accept the default folders and click **Next**.
7. Choose **Domino Enterprise Server** and click **Next**.
8. Accept the default and click **Next**.
9. Click **Finish**.
10. Start the configuration wizard by clicking **Start** → **Programs** → **Lotus Applications** → **Lotus Domino Server**.
11. Select **Start Domino as a Windows service** and **Don't ask me again** and click **OK**.
12. Select a different font if you want and click **Next**.
13. Choose **Set up the first server or a stand-alone server** and click **Next**.
14. The server name should be already set (see Table 4-4 on page 105). A server description and title is optional. Leave the check box unchecked and click **Next**.

Table 4-4 Server name

Field	Value
Server name	wea5e

15. Choose a Organization name and a password (see Table 4-5) and click **Next**.

Table 4-5 Organization name and password

Field	Value
Organization name	ITSORaleigh
Certifier password	passw0rd

16. Choose a Domino Domain Name (see Table 4-6) and click **Next**.

Table 4-6 Domino Domain Name

Field	Value
Domino Domain Name	IBM

17. Specify an administrator name and password. Select **Also save a local copy of the ID File** and click **Next** (see Table 4-7).

Table 4-7 Administrator name and password

Field	Value
First name	
Initials	
Last name	admin
Password	dpnadm

18. Select **Web Browsers (HTTP services)**, **Directory services (LDAP services)**, and click **Next**.
19. Click **Next**.
20. Select both check boxes and click **Next**.
21. Review the summary and click **Setup**.
22. When the configuration is finished, click **Finish**.

4.2.4 Lotus Domino configuration for WebSphere Everyplace Access

Here we discuss the Lotus Domino configuration for WebSphere Everyplace Access.

Initial setup of Lotus Notes

1. Start the Lotus Domino Server if it is not already started by selecting **Start** → **Programs** → **Lotus Applications** → **Lotus Domino Server**.
2. Start the Lotus Domino Administrator by selecting **Start** → **Programs** → **Lotus Applications** → **Lotus Domino Administrator**.
3. If this is the first start of Lotus Domino Administrator or Lotus Notes on this computer, it has to be configured. Click **Next**.
4. Type in the Lotus Domino Administrator name and the appropriate server (see Table 4-8). Click **Next**. If the server cannot be found, a screen will appear to specify the server, for example, by its host name, including the fully-qualified domain name.

Table 4-8 Administrator name and password

Field	Value
User name	admin
Domino Server	wea5e

5. Provide your password and click **OK**.
6. Do not select **Setup Instant Messaging**. Click **Next**.
7. Leave all check boxes unchecked. Click **Next**.
8. The Notes setup should be complete. Click **OK**.

LDAP configuration

The features of the portal require that LDAP users access specific attribute types in Domino. For example, within the edit mode of some collaborative portlets, a pick list of available servers displays if the user has access to the attributes shown in the steps below. The following instructions provide steps that enable anonymous LDAP users to access these attributes.

For a complete information, refer to the Domino documentation on the Lotus Web site at `http://www.lotus.com/ldd/doc`. The guide, *Lotus Domino 6 Administering the Domino System, Volume 1*, provides details about setting up the LDAP service and methods for extending the schema.

To allow anonymous users to query LDAP, follow these steps:

1. Open the Schema database (schema.nsf) by selecting **File** → **Database** → **Open**, choose your Domino Server (in our example, wea5e/ITSORaleigh), and choose Domino LDAP Schema.
2. Select the **All Schema Documents** view, and then click **New Document - Add Attribute Type**.
3. Complete the fields shown in Table 4-9 on the **Basic** tab.

Table 4-9 Basic tab fields and values

Field	Value
LDAP Name	HTTP-HostName.
OID	2.16.840.1.113678.2.2.2.2.461.
Syntax Name	**Directory String**.
Description	(Optional) Enter a description for the attribute.
Equality match	Leave as is.
Ordering match	Leave as is.
Substrings match	Leave as is.
Single valued Choose one	Leave as is.
Collective	Leave as is.
No user modification	Leave as is.

4. Click **Save & Close**. The document is saved as a draft and needs to be approved.
5. From the Domino LDAP schema view, select the **Draft Documents** → **Draft Attribute Types** view. Select the HTTP-HostName draft document and select **Approve** → **Approve Selected Drafts**.
6. Open the names.nsf file by selecting **File** → **Database** → **Open**, choose your Domino Server (in our example, wea5e/ITSORaleigh), and choose *Domino_Domain*'s Directory (in our example, it is IBM Directory).
7. Navigate to the view **Configuration** → **Servers** and highlight **Configurations**.
8. If there is already a configuration document open it. Otherwise, click **Add Configuration** to create a new Configuration Settings document.

9. On the Basic tab, for the option **Use these settings as the default settings for all servers**, click **Yes**. This is required for the LDAP tab to appear for use in the next step.
10. On the LDAP tab, click **Select Attribute Types**.
11. The LDAP Attribute Type Selection dialog box will appear. Select ***** in the Object Classes drop-down list and click **Display Attributes**.
12. From Selectable Attribute Type box, select the following fields, and then click **Add** to add them to the Queriable Attribute Types box:
    - AltFullName
    - dominoCertificate
    - givenName
    - HTTP-Hostname
    - Location
    - mail
    - mailaddress
    - MailDomain
    - MailFile
    - MailServer
    - member
    - NetAddresses
    - PublicKey
    - Sametime
    - sn
    - uid
    - userCertificate
13. Click **OK** to close the LDAP Attribute Selection dialog box, and return to the Configuration Settings document.
14. Check that all the attributes selected in the previous steps are included in the **Anonymous users can query field**.
15. Select the option **Allow LDAP users write access** and click **Yes**. This setting ensures that Portal users can use the self-care and self-registration features of Portal.
16. Keep all the other default LDAP settings and click **Save & Close**.

17. Open the Schema database (schema.nsf). This can be done by either selecting **File** → **Database** → **Open** and then selecting the appropriate Domino Server and opening **Domino LDAP Schema** or by selecting the **Files** tab and opening **schema.nsf**.
18. In the left navigation area, expand **All Schema Documents** and select **LDAP Attribute Types** and click **Add Attribute Type**.
19. Complete the fields (see Table 4-10) in the **Basic** tab.

Table 4-10 Basic tab fields

Field	Value
LDAP Name	ibm-appUUID.
OID	1.3.18.0.2.4.2323.
Notes mapping	Should be filled with ibm-appUUID.
Syntax name	Select **Directory String**.
Schema	Should be filled with **IBM SecureWay Directory,** after you save it!
Syntax type	Should be filled with 1.3.6.1.4.1.1466.115.121.1.15.
Description	(Optional) Enter a description.
Usage	Should be filled with **User Applications**.
Equality match	Select **Case Exact IA5 Match**.
Ordering match	Select **Case Ignore Ordering Match**.
Substrings match	Select **Case Ignore Substring Match**.
Single valued	Choose **Yes**.
Collective	Choose **Yes**.
No user modification	Choose **No**.

20. Click **Save & Close**.The document is saved as a draft and needs to be approved.
21. Select the **Draft Documents** → **Draft Attribute Types** view. Select the ibm-appUUID draft document, and click **Approve** → **Approve Selected Drafts**.
22. Click **LDAP Object Class** and click **Add Object Class**.

23. Enter the following information in the **Basic** tab (see Table 4-11).

Table 4-11 Basic tab

Field	Value
LDAP Name	ibm-appUUIDAux.
OID	1.3.18.0.2.6.475.
Notes mapping	Should be filled with ibm-appUUID.
Object Class Type	Select **Auxiliary Object Class**.
Schema	Should be filled with **IBM SecureWay Directory**.
Superior Object Class	top.
Description	(Optional) Enter a description.
Mandatory Attribute Types	
Optional Attribute Types	Select **ibm-appUUID**.

24. Click **Save & Close**.The document is saved as a draft and needs to be approved.
25. Select the **Draft Documents** → **Draft Object Classes** view. Select the ibm-appUUIDAux draft document and select **Approve** → **Approve Selected Drafts**.

Adding portal administrators to the Domino Directory

If you do not have a user to administer your portal or you do not have an existing LDAP, you should create a new user to act as the portal administrator. The following steps should be followed if the portal administrative user does not exist in the directory.

1. Navigate to the **People & Groups** tab and select the **People** view. From the action bar, click **Add Person**.
2. Enter the following values in the fields (Table 4-12).

Table 4-12 Add Person fields

Field	Value
Last Name	wpsbind
User Name	wpsbind/<DominoDomainName> wpsbind
Short name/UserID	wpsbind

Field	Value
Internet password	wpsbind

In our scenario, the DominoDomainName is ITSORaleigh, so the user name is:

```
wpsbind/ITSORaleigh
wpsbind
```

3. Click **Save & Close**.
4. Click **Add Person** again.
5. Enter the following values into the fields (see Table 4-13).

Table 4-13 Add Person fields

Field	Value
Last Name	weaadmin
User Name	weaadmin/<DominoDomainName> weaadmin
Short name/UserID	weaadmin
Internet password	weaadmin

In our scenario, the DominoDomainName is ITSORaleigh, so the user name is:

```
weaadmin/ITSORaleigh
weaadmin
```

6. Click **Save & Close**.
7. Navigate to the **Groups** view and, from the action bar, click **Add Group**.
8. Enter the following values in the fields (see Table 4-14).

Table 4-14 Add Group fields

Field	Value
Group name	wpsadmins
Group type	Multi-purpose
Members	wpsbind/<DominoDomainName> weaadmin/<DominoDomainName>

In our scenario, the DominoDomainName is ITSORaleigh, so the members are:

```
wpsbind/ITSORaleigh
weaadmin/ITSORaleigh
```

9. Click **Save & Close**.

Updating the Access Control List of the Domino Directory

You must be sure that the wpsadmins group we created has the right permissions and roles in the Domino directory.

1. Open the names.nsf file by selecting **File** → **Database** → **Open**, select the appropriate Domino Server, and open the *Domino_Domain*'s Directory (in our example, it is IBM's Directory) or by selecting the **Files** tab and opening **names.nsf**.
2. From main menu, select **File** → **Database** → **Access Control**.
3. Select **Access Control List** → **Basic**, click **Add** and choose the just created wpsadmins group.
4. The wpsadmins group requires either Author or Editor access. Select the following Role Types for the wpsadmin group:
   - GroupCreator
   - GroupModifier
   - UserCreator
   - UserModifier
5. Click **OK** to save these settings and close the Domino Administrator.

4.3 Installing WebSphere Everyplace Access

In this section, a sample WebSphere Everyplace Access installation is presented.

4.3.1 Preparation

Follow these steps to verify the machine before installation.

Check the Service Pack Version

WebSphere Everyplace Access requires Service Pack 4 for Windows 2000 Server and Advanced Server. Service Pack 4 must be installed before the WebSphere Everyplace Access installation. To verify that the correct service pack version is installed:

1. Select **Start** → **Run**.
2. Type `winver` and press **Enter** to display information about Windows.
3. Verify that Service Pack 4 is installed.
4. If Service Pack 4 is not installed, refer to the Microsoft support site or Windows Update for Windows 2000 to download and install the service pack.

Check for static IP address

WebSphere Everyplace Access requires the computer have a static IP address.

1. Click **Start** → **Settings** → **Network and Dial-up Connections**.
2. Right-click the LAN connection for your network adapter and click **Properties**.
3. On the network adapter properties window, select **Internet Protocol (TCP/IP)** from the list of components used by the connection and click **Properties**. The Internet Protocol (TCP/IP) will display.
4. Verify that **Use the following IP address** is selected. If **Obtain an IP address automatically** is selected, the computer has a dynamic IP address. If this is the case, contact your network administrator to obtain and configure a static IP address.

Check for a fully-qualified host name

WebSphere Portal also requires the use of a fully qualified host name, which is typically the host name of the server, along with its fully-qualified domain name (FQDN). For a Basic Installation, the Domino and the WebSphere Everyplace Access Server should have access to each other. To check that your computer has a host name and a FQDN:

1. Select **Start** → **Settings** → **Control Panel** → **System** and click **Network Identification**.

2. Click **Properties**. In our example, the computer name should be wea5d and the full computer name wea5d.itso.ral.ibm.com.
3. If there is only a host name, contact your system administrator or change the host name and FQDN. To do that, enter a host name in the field **Computer Name**.
4. To specify a FQDN, click **More** and enter it in the field **Primary DNS suffix of this**. Click **OK**.
5. Click **OK**. If you changed any settings, reboot your computer.
6. After rebooting, try to ping yourself and the Domino Server to prove that the connection is working:

   ```
   ping wea5d.itso.ral.ibm.com
   ```

7. You should see a reply.
8. Try to ping the Domino Server:

   ```
   ping wea5e.itso.ral.ibm.com
   ```

9. You should see another reply.

Check port bindings

Specific ports are required to install WebSphere Everyplace Access. If two applications attempt to use the same port, a port conflict results. To ensure that the required port bindings are available, the netstat utility can be used.

1. Click **Start** → **Programs** → **Accessories** → **Command Prompt** to launch a command prompt.
2. Type `netstat -an` at the command prompt.
3. Look at the numbers listed in the Local Address column. The number after the colon is the port number. For example, in the IP address 1.2.3.4:80, 80 is the port number.
4. Verify that the following list of port numbers, required by WebSphere Portal, are not in use. If any of these port numbers are in use, you may experience port conflicts. The following ports are required by default for WebSphere Portal and its related applications:
   - 80 (standard HTTP port)
   - 443 (standard HTTPS port)
   - 523 (DB2 Administration Server)
   - 8008 (IBM HTTP Server Administration port)
   - 9081 (existing WebSphere Portal)
   - 50000 (DB2 instance connection port)

- 50001 (DB2 instance interrupt port)
- 50002 (DB2 Control Server)
- 55555 (WebSphere Application Server database port)

If port 80 is in use, it is possible that IIS is installed. If the Microsoft Internet Information Services (IIS) Web server is running, you will have a port conflict with IBM HTTP Server. Both of these Web servers listen on port 80, unless otherwise configured. To prevent this conflict, disable the Microsoft IIS Web server.

To see if IIS is enabled:

1. Select **Start** → **Settings** → **Control Panel** → **Add/Remove Programs**.
2. Select **Add/Remove Windows Components**.
3. If IIS is listed, it has been installed on the computer.
4. To disable IIS:
   a. Select **Start** → **Programs** → **Administrative Tools**.
   b. Open **Services**.
   c. Locate and highlight **IIS Admin Service**.
   d. Select the **Action** menu and click **Properties**. A window opens.
   e. Change the **Startup type** to **Disabled** and click **Stop** to stop the server.
   f. Click **Yes** to stop any services that are stopped as a result.
   g. Locate the **World Wide Web Publishing Service**. Disable it at startup using the steps listed above.

Create the WebSphere Everyplace Access Administrator IDs

Before installing, an Administrator ID for WebSphere Everyplace Access needs to be created. During a Basic Install, the administrator ID, which is a local Windows operating system administrator ID that is shared by all components, is used to create WebSphere Everyplace Access databases and Windows services. The ID is required to have system administrator permissions, in other words, it must be a member of the Administrators group.

Another ID is created for installing WebSphere Everyplace Access. This ID is used to log on to the computer and is only needed during the installation.

These IDs must conform to the following list of requirements for a basic installation:

- Can contain characters a-z, A-Z, or 0-9
- Cannot begin with a numeric character

- Cannot be longer than 12 characters
- Cannot include spaces, non-ASCII characters, or diacritics (such as umlauts)
- Cannot be *users*, *admins*, *guests*, *public*, *local*, or any SQL reserved word list in SQL Reference.
- Cannot start with *SQL*, *SYS*, or *IBM* (This also applies to the password.)

To create the IDs, do the following:

1. Select **Start** → **Programs** → **Administrative Tools** → **Computer Management**.
2. Under System Tools, expand **Local Users and Groups**.
3. Right-click **Users** and select **New User**.
4. On the New User dialog, enter a user name, password, and confirm the password (see Table 4-15).

Table 4-15 New User dialog fields

Field	Value
User name	instwea
Password	lpiwea

5. Deselect **User must change password at next logon**.
6. Select **Password never expires**.
7. Click **Create**.
8. Enter the a User name, password for the WebSphere Everyplace Access user ID.

Table 4-16 User name and password fields

Field	Value
User name	weaadmin
Password	lpuwea

9. Deselect **User must change password at next logon**.
10. Select **Password never expires**.
11. Click **Create** and then click **Close**.

Both IDs need to have system administrator permissions. Therefore, they must be members of the Administrators group:

1. Right-click the instwea user you just created and select **Properties**.

2. Click the **Member Of** tab and click **Add**.
3. Select **Administrators** from the Name column and click **Add**. Click **OK**.
4. Click **Apply** and then click **Close**.
5. Right-click the weaadmin you just created and select **Properties**.
6. Click the **Member Of** tab and click **Add**.
7. Select **Administrators** from the Name column and click **Add**. Click **OK**.
8. Click **Apply** and then click **Close**.

The ID that is used to log on to the computer, in our example, instwea, must be a local user that is 12 characters or less. To be an administrative user, it must belong to the Administrators group defined in Windows. A domain user ID cannot be used. In addition, it must have the following rights:

- Act as part of the operating system
- Create a token object
- Increase quotas
- Log on as a Service
- Replace a process level token

To access the interface for editing user rights, do the following:

1. Select **Start** → **Programs** → **Administrative Tools** → **Local Security Policy**.
2. Expand **Local Policies** and click **User Rights Assignment**.
3. Locate each Policy listed above and verify that the logon ID is listed in the **Local Setting** column.
4. To add the user, right-click the policy and select **Security**.
5. Log off and log in as the user just created.

4.3.2 Installation of Lotus Notes

To be able to synchronize PIM and e-mail data, a Lotus Notes Client must be installed and configured, because Everyplace Synchronization uses the Notes Client to communicate with the Domino Server.

1. Copy Admin ID file from Domino Server to the WEA Server.
2. Use CD 9-1, and open the command prompt by selecting **Start** → **Programs** → **Accessories** → **Command Prompt**. Go to the CD drive in directory \win\en and invoke the following command:

   ```
   installnotes.bat "c:\program files\websphere\"
   ```

3. When the Notes client is installed, the configuration will automatically be loaded. Click **Next** and specify the user name and Domino server name in the screen that appears (see Table 4-17) and click **Next**.

Table 4-17 User name and Domino server name fields

Field	Value
Your name	admin
Domino server	wea5e

4. If the Notes configuration returns with the message that the ID file cannot be found on the server, specify the location of the ID File.
5. Enter your password and click **OK**.
6. Leave all the check boxes blank on the Additional Services screen and click **Next**.
7. Finish the Notes client configuration click **OK**.

4.3.3 Installation of WebSphere Everyplace Access

This section describes all the steps that are necessary to install WebSphere Everyplace Access. At first, all software, including the needed Fix Packs, are installed. After that, the configuration wizard will appear and guide you through the configuration.

1. Start install.bat from the first WebSphere Everyplace Access CD labeled Setup.
2. Select **English** and click **OK**.
3. Click **Next** or view the Infocenter.
4. View the license agreement and select **I accept the terms in the license agreement** and click **Next**.
5. Select **Basic Install** and click **Next**.

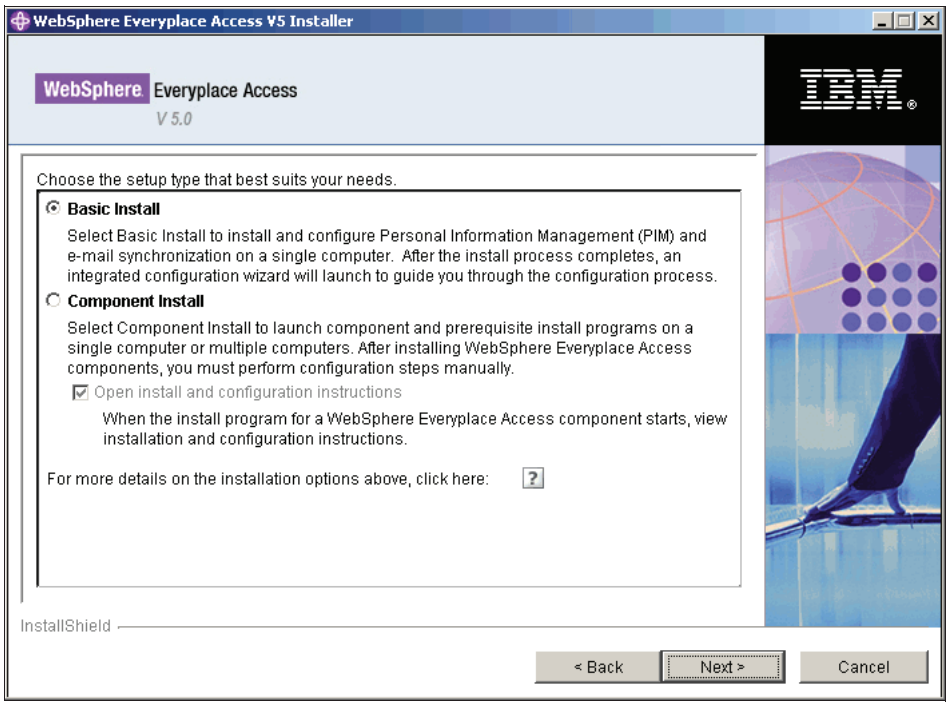

Figure 4-1 Basic installation

6. Click **Next** to continue or review a planning worksheet.
7. Leave the default path and enter the Administrator ID on which WebSphere Everyplace Access will run and the appropriate password (see Table 4-18). Click **Next**.

Table 4-18 Administrator and password fields

Field	Value
Administrator ID	weaadmin
Password	lpuwea

> **Note:** This is the user ID on the local system, not on the LDAP Server.

8. Check the host name and domain name and click **Next** (see Table 4-19 on page 120).

Table 4-19 Host name sample value

Field	Value
Host name	wea5d.itso.ral.ibm.com

9. Review the summary and click **Next** to start the installation.

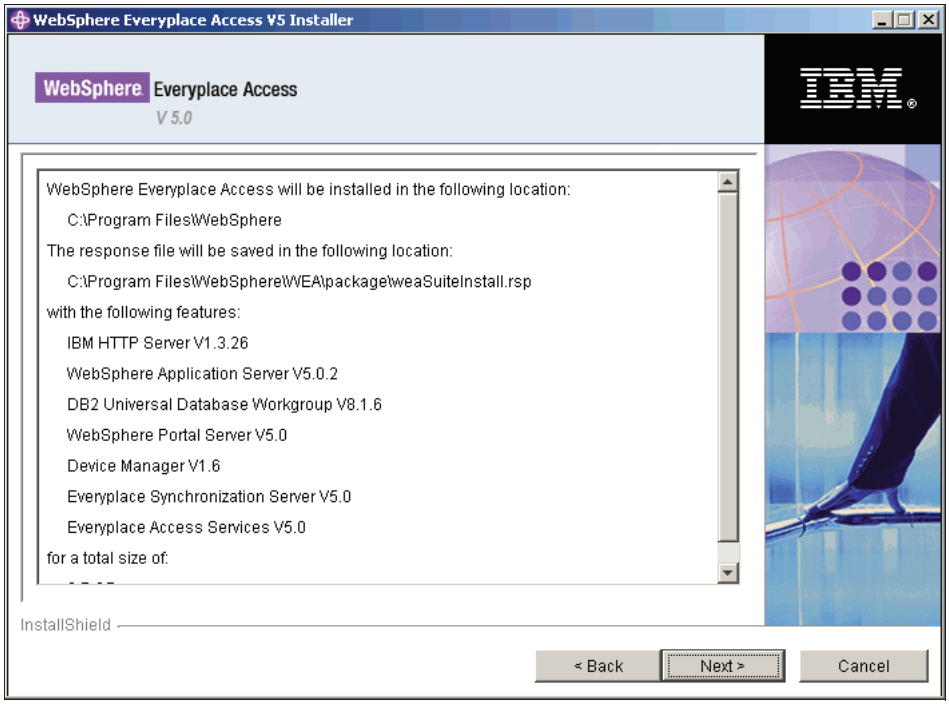

Figure 4-2 Summary

10. Follow the on-screen instructions to install the CDs in the correct sequence.
11. After all the components are installed, the Install Complete screen appears. Click **Next** to begin configuring WebSphere Everyplace Access.
12. Choose **English** and click **OK**.
13. Select **Existing Directory Server** and click **Next**.

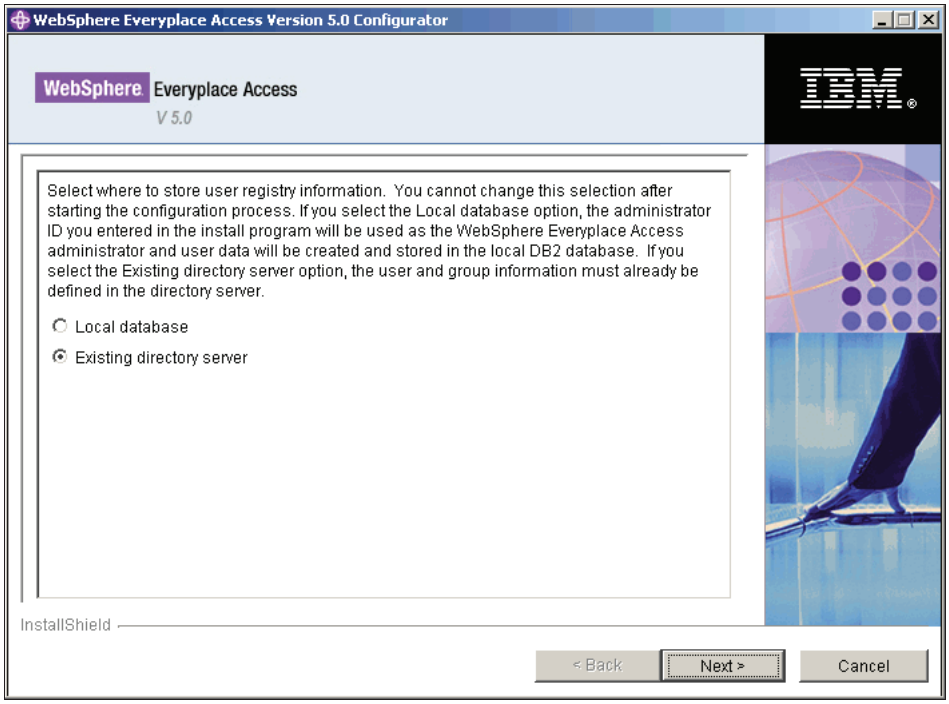

Figure 4-3 Selecting a directory server

14. Select **Lotus Domino Directory Server 6** and click **Next**.
15. Enter the following information and click **Next** (see Table 4-20).

Table 4-20 Lotus Domino Directory Server 6 fields

Field	Value
Host name	wea5e.itso.ral.ibm.com
Port	389
Administrator ID	admin/ITSORaleigh
Password	dpnadm

16. Enter the following information and click **Next** (see Table 4-21 on page 122).

Table 4-21 Additional fields

Field	Value
User prefix	cn
User container	o=ITSORaleigh
Administrative group name	wpsadmins
Group prefix	cn
Bind user	wpsbind
Bind password	wpsbind
WEA Admin ID	weaadmin
WEA Admin password	weaadmin

17. Before selecting a mail server, Lotus Notes must be installed.
18. Select **Lotus Domino 5, 6, or 6.5** as the mail server. Click **Next** (see Figure 4-4).

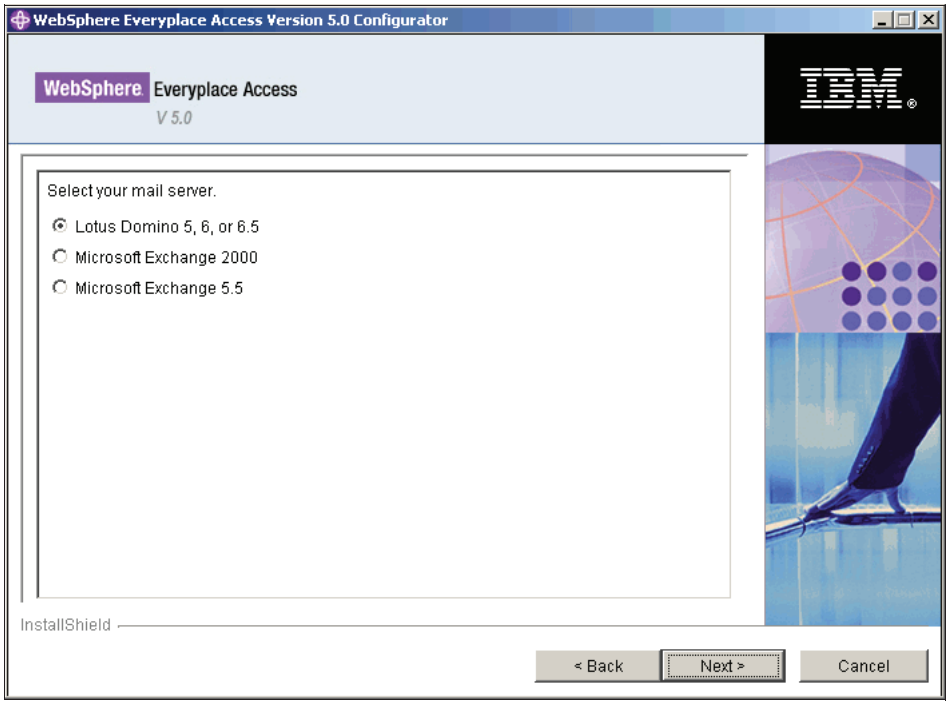

Figure 4-4 Selecting a mail server

19. Enter the host name of the Domino Server and the appropriate Administrator ID and password (see Table 4-22). Click **Next**.

Table 4-22 Host name and administrator user ID and password

Field	Value
Host Name	wea5e.itso.ral.ibm.com
Administrator ID	admin
Password	dpnadm

20. Review the summary and click **Next**. The configuration of WebSphere Everyplace Access will begin.

5

Component installation

This chapter describes how to install all the components of WebSphere Everyplace Access and configure it to use a Domino Directory. It provides step-by-step instructions to install and configure the Domino LDAP as well as WebSphere Everyplace Access and its requirements on two Windows machines.

© Copyright IBM Corp. 2005. All rights reserved.

5.1 Overview

Websphere Everyplace Access V5 has two installation options: the Basic Install and the Component Install. The Component Install provides a flexible install path for distributing and scaling components. It gives the choice to install only the component that you need to implement WebSphere Everyplace Access in a given environment, including the prerequisite software.

In our sample environment, we will install all the components of WebSphere Everyplace Access on a single computer. Lotus Domino, which acts as mail server and LDAP Directory, will be installed on another machine.

It is important that each machine has a host and domain name, which is registered in a DNS Server, so that both machines can be accessed by its name. In our example, the server with WebSphere Everyplace Access is called wea5d.itso.ral.ibm.com and the server containing Lotus Domino is wea5e.itso.ral.ibm.com.

On wea5e, we will install Lotus Domino and Lotus Notes. The Notes client is needed to configure Lotus Domino. This server is only an example for a mail and LDAP server, because in a given environment, you would generally use existing installations.

On wea5d, we will install all components of WebSphere Everyplace Access and its requirements. First, we will install the prerequisite software:

- DB2
- WebSphere Application Server
- WebSphere Portal Server

After the prerequisite software is in place, we will install all WebSphere Everyplace Access features:

- Everyplace Access Services
- Device Management Services
- Everyplace Synchronization Server
- Intelligent Notification Services
- DB2e
- Location Aware Services

5.2 Server 1 - Lotus Domino

This section describes the installation of the Domino machine. It includes the preparation of the machine, the installation of the Notes Client to administer and configure the Domino, as well as the Domino installation and configuration for WebSphere Everyplace Access.

In our example, we will install Lotus Domino V6.5.1 and Lotus Notes V6.5.1 on the machine. As described above the machine name is wea5e.itso.ral.ibm.com. This name is registered in DNS so that the machine is accessible with this name.

5.2.1 Preparation

Before installing Lotus Domino, check that the computer is prepared.

Check the Service Pack version

WebSphere Everyplace Access requires Service Pack 4 for Windows 2000 Server and Advanced Server. Service Pack 4 must be installed before the WebSphere Everyplace Access installation. To verify that the correct service pack version is installed:

1. Select **Start** → **Run**.
2. Type `winver` and press **Enter** to display information about Windows.
3. Verify that Service Pack 4 is installed.
4. If Service Pack 4 is not installed, refer to the Microsoft support site or Windows Update for Windows 2000 to download and install the service pack.

Check for a static IP address

WebSphere Everyplace Access requires that the computer have a static IP address.

1. Select **Start** → **Settings** → **Network and Dial-up Connections**.
2. Right-click the LAN connection for your network adapter and click **Properties**.
3. On the Network Adapter Properties window, select **Internet Protocol (TCP/IP)** from the list of components used by the connection and click **Properties**. The Internet Protocol (TCP/IP) will display.
4. Verify that **Use the following IP address** is selected. If **Obtain an IP address automatically** is selected, the computer has a dynamic IP address. If this is the case, contact your network administrator to obtain and configure a static IP address.

Check for a fully-qualified host name

WebSphere Portal also requires the use of a fully qualified host name, which is typically the host name of the server, along with its fully-qualified domain name (FQDN). The Domino and the WebSphere Everyplace Access Server should have access to each other. To check that your computer has a host name and a FQDN:

1. Select **Start** → **Settings** → **Control Panel** → **System** and click **Network Identification**.
2. Click **Properties**. In our example, the computer name should be wea5e and the full computer name wea5e.itso.ral.ibm.com.
3. If there is only a host name, contact your system administrator or change the host name and FQDN. To do that, enter a host name in the field **Computer Name**.
4. To specify a FQDN, click **More** and enter it in the field **Primary DNS suffix of this**. Click **OK**.
5. Click **OK**. If you changed any settings, reboot your computer.
6. Try to ping yourself:

   ```
   ping wea5e.itso.ral.ibm.com
   ```

7. You should see a reply.

Check port bindings

Specific ports are required to install Lotus Domino. If two applications attempt to use the same port, a port conflict results. To ensure that the required port bindings are available, the netstat utility can be used.

1. Click **Start** → **Programs** → **Accessories** → **Command Prompt** to launch a command prompt.
2. Type `netstat -an` at the command prompt.
3. Look at the numbers listed in the Local Address column. The fifth number is the port number. For example, in the IP address 1.2.3.4:80, 80 is the port number.
4. Verify that port 80, required by Lotus Domino, is not in use. If it is in use, you may experience port conflicts:

If port 80 is in use, it is possible that IIS is installed. If the Microsoft Internet Information Services (IIS) Web server is running, you will have a port conflict with IBM HTTP Server. Both of these Web servers listen on port 80, unless otherwise configured. To prevent this conflict, disable the Microsoft IIS Web server.

To see if IIS is enabled:

1. Click **Start** → **Settings** → **Control Panel** → **Add/Remove Programs**.
2. Select **Add/Remove Windows Components**.
3. If IIS is listed, it has been installed on the computer.

To disable IIS:

1. Click **Start** → **Programs** → **Administrative Tools**.
2. Open **Services**.
3. Locate and highlight **IIS Admin Service**.
4. Click the **Action** menu and click **Properties**. A window opens.
5. Change the **Startup type** to **Disabled** and click **Stop** to stop the server.
6. Click **Yes** to stop any services that are stopped as a result.
7. Locate the **World Wide Web Publishing Service**. Disable it at startup using the steps listed above.

5.2.2 Install Lotus Notes

The Notes Client is required to configure Lotus Domino. Therefore, the Domino Administrator has to be installed (not only the Lotus Notes Client).

1. Start the installation either by using an Installation CD or a file, which contains the installation files. For CD installation, go to Step 3.
2. Specify where the installation files should be extracted and click **Next** (see Table 5-1).

Table 5-1 Extracted installation files directory

Field	Value
Directory	C:\Program Files\Lotus Notes 6

3. The Lotus Notes Installation window will appear. Click **Next**.
4. Select **I accept the terms in the license agreement** and click **Next**.
5. Enter a name and company and click **Next**.
6. Accept the default folders and click **Next** (see Table 5-2 on page 130).

Table 5-2 Installation default folders

Field	Value
Install program files to	C:\Program Files\Lotus\Notes
Install data files to	C:\Program Files\Lotus\Notes\NotesData

7. Be sure to select **Domino Administrator** and click **Next**.
8. Accept the default and click **Install**.
9. Click **Finish**.

Note: After finishing the Lotus Notes installation, the Directory created in Step 2 can be deleted, including all the files.

5.2.3 Installing Domino

This section describes how to install Lotus Domino so that it can be configured later for WebSphere Everyplace Access.

1. Start the installation either by using an Installation CD or a file, which contains the installation files. For CD installation, go to step 3.
2. Specify where the installation files should be extracted and click **Next** (see Table 5-3).

Table 5-3 Installation files

Field	Value
Directory	C:\Program Files\Lotus Domino 6

3. The Lotus Domino Installation window will appear. Click **Next**.
4. Accept the license by clicking **Yes**.
5. Enter a name and company. Leave **Partitioned Server Installation** unchecked and click **Next**.
6. Accept the default folders and click **Next** (see Table 5-4).

Table 5-4 Default folders

Field	Value
Program folder	C:\Lotus\Domino
Data folder	C:\Lotus\Domino\Data

7. Choose **Domino Enterprise Server** and click **Next**.

8. Accept the default and click **Next**.
9. Click **Finish**.
10. Start the configuration wizard by selecting **Start** → **Programs** → **Lotus Applications** → **Lotus Domino Server**.
11. Select **Start Domino as a Windows service** and **Don't ask me again** and click **OK**.
12. Select a different font if you want and click **Next**.
13. Choose **Set up the first server or a stand-alone server** and click **Next**.
14. The Server name should be already set (see Table 5-5). A server description is optional. Leave the check box unchecked and click **Next**.

Table 5-5 Server name

Field	Value
Server name	wea5e

15. Choose an Organization name and a password and click **Next** (see Table 5-6).

Table 5-6 Organization name

Field	Value
Organization name	ITSORaleigh
Certifier password	certpwd

16. Choose a Domino Domain Name and click **Next** (see Table 5-7).

Table 5-7 Domino Domain Name

Field	Value
Domino Domain Name	IBM

17. Specify an administrator name and password (see Table 5-8). Select **Also save a local copy of the ID File** and click **Next**.

Table 5-8 Administrator user ID and password

Field	Value
First name	
Middle	
Last name	admin

Field	Value
Password	dpnadm

18. Select **Web Browsers (HTTP services)** and **Directory services (LDAP services)** and click **Next**.
19. Click **Next**.
20. Select both check boxes and click **Next**.
21. Review the summary and click **Setup**.
22. When the configuration finishes, click **Finish**.

Note: After finishing the Lotus Domino installation, the Directory created in step 2 can be deleted, including all the files.

5.2.4 Lotus Domino configuration

After installing Lotus Domino it needs to be configured so that WebSphere Everyplace can use it as its LDAP Directory. First, Lotus Notes is set up to connect to Lotus Domino. Then the Domino LDAP is configured to match the needs of WebSphere Everyplace. Finally, the required users in Domino LDAP are created.

Initial setup of Lotus Notes

1. Start the Lotus Domino Server if it is not already started by selecting **Start** → **Programs** → **Lotus Applications** → **Lotus Domino Server**.
2. Start the Lotus Domino Administrator by selecting **Start** → **Programs** → **Lotus Applications** → **Lotus Domino Administrator**.
3. If this is the first start of Lotus Domino Administrator or Lotus Notes on this computer, it has to be configured. Click **Next**.
4. Type the Lotus Domino Administrator name and the appropriate server. Click **Next**. If the server cannot be found, a screen will appear to specify the server, for example, by its host name, including the fully-qualified domain name.

Table 5-9 Lotus Domino Administrator

Field	Value
User name	admin
Domino Server	wea5e

5. Provide the password (for our example, dpnadm) and click **OK**.

6. Do not select **Setup Instant Messaging** and click **Next**.
7. Leave all check boxes unchecked and click **Next**.
8. The Notes setup should be complete. Click **OK**.

LDAP configuration

The features of the portal require that LDAP users access specific attribute types in Domino. For example, within the edit mode of some collaborative portlets, a pick list of available servers displays if the user has access to the attributes shown in the steps below. The following instructions provide steps that enable anonymous LDAP users to access these attributes.

For complete information, refer to the Domino documentation on the Lotus Web site at `http://www.lotus.com/ldd/doc`. The guide, *Lotus Domino 6 Administering the Domino System, Volume 1* provides details about setting up the LDAP service and methods for extending the schema.

To allow anonymous users to query LDAP, follow these steps:

1. Open the Schema database (schema.nsf). This can be done by either selecting **File** → **Database** → **Open** and then selecting the appropriate Domino Server and opening **Domino LDAP Schema** or by selecting the **Files** tab and opening **schema.nsf**.
2. Select the All Schema Documents view and then click **New Document - Add Attribute Type**.
3. Complete these fields on the **Basic** tab (see Table 5-10).

Table 5-10 Basic tab

Field	Action
LDAP Name	Enter `HTTP-HostName`.
OID	2.16.840.1.113678.2.2.2.2.461.
Syntax Name	Select **Directory String**.
Description	(Optional) Enter a description for the attribute.
Equality match	Leave as is.
Ordering match	Leave as is.
Substrings match	Leave as is.
Single valued Choose one	Leave as is.
Collective	Leave as is.

Field	Action
No user modification	Leave as is.

4. Click **Save & Close**. The document is saved as a draft and needs to be approved.
5. From the Domino LDAP schema view, select the **Draft Documents** → **Draft Attribute Types** view. Select the HTTP-HostName draft document, and select **Approve** → **Approve Selected Drafts**.
6. Open the names.nsf file. This file is called *domino_domain*'s directories, where *domino_domain* is, in our example, IBM.
7. Select **Configuration** → **Servers** and highlight **Configurations**.
8. If there is already a configuration document, open it. Otherwise, click **Add Configuration** to create a new Configuration Settings document.
9. On the Basic tab, for the option **Use these settings as the default settings for all servers**, click **Yes**. This is required for the LDAP tab to appear for use in the next step.
10. On the LDAP tab, click **Select Attribute Types**.
11. The LDAP Attribute Type Selection dialog box will appear. Select ***** in the Object Classes drop-down list and click **Display Attributes**.
12. From Selectable Attribute Type box, select the following fields, and then click **Add** to add them to the Queriable Attribute Types box:
    - AltFullName
    - dominoCertificate
    - givenName
    - HTTP-Hostname
    - Location
    - mail
    - mailaddress
    - MailDomain
    - MailFile
    - MailServer
    - member
    - NetAddresses
    - PublicKey
    - Sametime

- sn
- uid
- userCertificate

13. Click **OK** to close the LDAP Attribute Selection dialog box, and return to the Configuration Settings document.
14. Check that all the attributes selected in the previous steps are included in the **Anonymous users can query field**.
15. For the option **Allow LDAP users write access**, click Yes. Maybe you have to scroll down in order to see this field.
16. Keep all other default LDAP settings and click **Save & Close**.
17. Open the Schema database (schema.nsf). This can be done by either selecting **File** → **Database** → **Open** and then selecting the appropriate Domino Server and opening **Domino LDAP Schema** or by selecting the **Files** tab and opening **schema.nsf**.
18. In the left navigation area, expand **All Schema Documents**, select **LDAP Attribute Types**, and click **Add Attribute Type**.
19. Complete these fields on the **Basic** tab (see Table 5-11).

Table 5-11 Basic tab values

Field	Action
LDAP Name	Enter `ibm-appUUID`.
OID	1.3.18.0.2.4.2323.
Notes mapping	should later be filled with ibm-appUUID.
Syntax name	Select **Directory String**.
Schema	Should filled with **IBM SecureWay Directory**, after closing.
Syntax type	Should later filled with 1.3.6.1.4.1.1466.115.121.1.15.
Description	(Optional) Enter a description.
Usage	Should be filled with User Applications.
Equality match	Select **Case Exact IA5 Match**.
Ordering match	Select **Case Ignore Ordering Match**.
Substrings match	Select **Case Ignore Substring Match**.
Single valued	Choose **Yes**.

Field	Action
Collective	Choose **Yes**.
No user modification	Choose **No**.

20. Click **Save & Close**. The document is saved as a draft and needs to be approved.
21. Select the **Draft Documents** → **Draft Attribute Types** view. Select the ibm-appUUID draft document and select **Approve** → **Approve Selected Drafts**.
22. Click **LDAP Object Class** and click **Add Object Class**.
23. Enter the following information in the **Basic** tab (see Table 5-12).

Table 5-12 Basic tab values

Field	Action
LDAP Name	Enter `ibm-appUUIDAux`.
OID	1.3.18.0.2.6.475.
Notes mapping	Should be filled with **ibm-appUUID** after closing.
Object Class Type	Select **Auxiliary Object Class**.
Schema	Should be filled with **IBM SecureWay Directory** after closing.
Superior Object Class	top.
Description	(Optional) Enter a description.
Mandatory Attribute Types	
Optional Attribute Types	Select **ibm-appUUID**.

24. Click **Save & Close**. The document is saved as a draft and needs to be approved.
25. Select the **Draft Documents** → **Draft Object Classes** view. Select the ibm-appUUIDAux draft document and click **Approve** → **Approve Selected Drafts**.

Adding portal administrators to the Domino Directory

If you do not have a user to administer your portal or you do not have an existing LDAP, you should create a new user to act as the portal administrator. The following steps should be followed if the portal administrative user does not exist in the directory.

1. In the Domino Administrator, navigate to the **People & Groups** tab and select the **People** view. From the action bar, click **Add Person**.
2. Enter the following values in the fields (see Table 5-13).

Table 5-13 Portal administrator

Field	Value
Last Name	wpsbind
User Name	wpsbind/<Organization name> wpsbind
Short name/UserID	wpsbind
Internet password	wpsbind

In our scenario, the Organization name is ITSORaleigh, so the user name is:

```
wpsbind/ITSORaleigh
wpsbind
```

3. Click **Save & Close**.
4. Click **Add Person** again.
5. Enter the following values in the fields (see Table 5-14).

Table 5-14 Everyplace Access administrator

Field	Value
Last Name	weaadmin
User Name	weaadmin/<Organization name> weaadmin
Short name/UserID	weaadmin
Internet password	weaadmin

In our scenario, the Organization name is ITSORaleigh, so the user name is:

```
weaadmin/ITSORaleigh
weaadmin
```

6. Click **Save & Close**.

Because the users for Intelligent Notification Service and Everyplace Synchronization Server need to connect from a Lotus Notes Client to Domino, we have to register them in Domino so that they will have an user ID file.

1. In the Domino Administrator, navigate to the **People & Groups** tab. Select **Tools** → **People** → **Register** on the right side.

2. Click **Certifier ID...**.
3. Navigate to your domino\data folder, which is, in our example, C:\Lotus\Domino\Data.
4. Select cert.id and click **Open**.
5. Click **OK**.
6. Specify the password for the Certifier ID and click **OK**. In our example, the password is certpwd.
7. Click **OK**.
8. In the **Register Person - New Entry** window, specify the following information (see Table 5-15).

Table 5-15 Everyplace Synchronization Server administration

Field	Value
Last Name	essadmin
Short name/UserID	essadmin
password	dpessadm

9. Click **Password Options...**.
10. Set the **Password Quality Scale** to 7, check both check boxes, and click **OK**.
11. Click the green check mark to add the person to the registration queue.
12. Specify the following information for the Intelligent Notification Service user ID (see Table 5-16).

Table 5-16 Intelligent Notification Services administrator

Field	Value
Last Name	insadmin
Short name/UserID	insadmin
password	dpinsadm

13. Click **Password Options...**.
14. Set the **Password Quality Scale** to 7, check both check boxes, and click **OK**.
15. Click the green check mark to add the person to the registration queue.
16. Click **Register all**.
17. After both user IDs are successfully created, click **Done**.

Creating required groups

1. In the Domino Administrator, navigate to the **People & Groups** tab and select the **Groups** view and, from the action bar, click **Add Group**.
2. Enter the following values in the fields (see Table 5-17).

Table 5-17 Groups

Field	Value
Group name	wpsadmins
Group type	Multi-purpose
Members	wpsbind/<Organization name> weaadmin/<Organization name>

In our scenario the Organization name is ITSORaleigh, so the members are:

```
wpsbind/ITSORaleigh
weaadmin/ITSORaleigh
```

3. Click **Save & Close**.
4. Click **Add Group**.
5. Enter the following values in the fields (see Table 5-18).

Table 5-18 Other groups

Field	Value
Group name	essadmins
Group type	Multi-purpose

6. Click **Save & Close**. Repeat steps 4 - 6 for the following groups:
   - essusers
   - essuser_nonlock
   - dmadmins
   - insadmins
   - insusers
   - lasadmins
   - SyncGroup

Updating the Access Control List of the Domino Directory

You must be sure that the wpsadmins group we created has the right permissions and roles in the Domino directory.

1. Open the names.nsf file by clicking **File** → **Database** → **Open**, and select the appropriate Domino Server, and open **names.nsf** or by selecting the **Files** tab and opening **names.nsf**.
2. From main menu, select **File** → **Database** → **Access Control**.
3. Select **Access Control List** → **Basic**, click **Add**, and choose the just created **wpsadmins** group.
4. The wpsadmins group requires either Author or Editor access. Select the following Role Types for the wpsadmin group:
   - GroupCreator
   - GroupModifier
   - UserCreator
   - UserModifier
5. Click **OK** to save these settings and close the Domino Administrator.

5.2.5 Summary

After you finish the installation of the Domino Server, you should have a setup that is similar to the following. Remember your user IDs and passwords.

- The computer has a host and domain name, such as wea5e.itso.ral.ibm.com.
- Lotus Notes Administrator Client and Lotus Domino are installed.
- The organization name is ITSORaleigh and the Domino Domain is IBM.
- The certifier password is certpwd. This password is used for creating users.
- The Lotus Domino administrative user is admin with dpnadm as the password.
- LDAP is configured as described in “LDAP configuration” on page 133.
- WebSphere Portal users and their passwords weaadmin and wpsbind are created in the Domino directory.
- The wpsadmins group is created in the Domino directory. Members of this groups are weaadmin and wpsbind.
- The users insadmin using dpinsadm as a password and essadmin using dpessadm as a password are created in the Domino directory.
- The groups essadmins, essusers, essuser_nonlock, dmadmins, insadmin, insusers, lasadmins and SyncGroup are created.

- The wpsadmins group has the right permissions on the names.nsf.

5.3 Server 2 - WebSphere Everyplace Access

This section describe the installation of the WebSphere Everyplace Access machine. It includes the preparation of the machine, the installation of the Notes Client connected to Domino, as well as the WebSphere Everyplace Installation.

The Component Install of WebSphere Everyplace Access does not include a configuration tool. After you install a component, you must run configuration tasks to configure the feature.

As described before, the machine name is wea5d.itso.ral.ibm.com. This name is registered in DNS so that the machine is accessible with this name.

5.3.1 Preparation

Before installing WebSphere Everyplace Access, you should check to see if the computer is prepared. That means the network is configured, including the host and domain name as well as all necessary users are created on the system.

Check the Service Pack version

WebSphere Everyplace Access requires Service Pack 4 for Windows 2000 Server and Advanced Server. Service Pack 4 must be installed before the WebSphere Everyplace Access installation. To verify the correct service pack version is installed:

1. Click **Start** → **Run**.
2. Type `winver` and press **Enter** to display information about Windows.
3. Verify that Service Pack 4 is installed.
4. If Service Pack 4 is not installed, refer to the Microsoft support site or Windows Update for Windows 2000 to download and install the service pack.

Check for static IP address

WebSphere Everyplace Access requires the computer have a static IP address.

1. Click **Start** → **Settings** → **Network and Dial-up Connections**.
2. Right-click the LAN connection for your network adapter and click **Properties**.
3. On the network adapter properties window, select **Internet Protocol (TCP/IP)** from the list of components used by the connection and click **Properties**. The Internet Protocol (TCP/IP) will display.

4. Verify that **Use the following IP address** is selected. If **Obtain an IP address automatically** is selected, the computer has a dynamic IP address. If this is the case, contact your network administrator to obtain and configure a static IP address.

Check for a fully-qualified host name

WebSphere Portal also requires the use of a fully qualified host name, which is typically the host name of the server, along with its fully-qualified domain name (FQDN). The Domino and the WebSphere Everyplace Access Server should have access to each other. To check, that your computer has a host name and a FQDN:

1. Select **Start** → **Settings** → **Control Panel** → **System** and click **Network Identification**.
2. Click **Properties**. In our example, the computer name should be wea5d and the full computer name wea5d.itso.ral.ibm.com.
3. If there is only a host name, contact your system administrator or change the host name and FQDN. To do that, enter a host name in the field **Computer Name**.
4. To specify a FQDN, click **More** and enter it in the field **Primary DNS suffix of this**. Click **OK.**
5. Click **OK**. If you changed any settings, reboot your computer.
6. Try to ping yourself:

   ```
   ping wea5d.itso.ral.ibm.com
   ```

7. You should see a reply.
8. Try to ping the Domino Server:

   ```
   ping wea5e.itso.ral.ibm.com
   ```

9. You should see another reply.

Check port bindings

Specific ports are required to install WebSphere Everyplace Access. If two applications attempt to use the same port, a port conflict results. To ensure that the required port bindings are available, the netstat utility can be used.

1. Click **Start** → **Programs** → **Accessories** → **Command Prompt** to launch a command prompt.
2. Type `netstat -an` at the command prompt.
3. Look at the numbers listed in the Local Address column. The fifth number is the port number. For example, in the IP address 1.2.3.4:80, 80 is the port number.

4. Verify that the following list of port numbers, required by WebSphere Portal, are not in use. If any of these port numbers are in use, you may experience port conflicts. The following ports are required by default for WebSphere Portal and its related applications:
   - 80 (Standard HTTP port)
   - 443 (Standard HTTPS port)
   - 523 (DB2 Administration Server)
   - 8008 (IBM HTTP Server Administration port)
   - 9081 (Existing WebSphere Portal)
   - 50000 (DB2 instance connection port)
   - 50001 (DB2 instance interrupt port)
   - 50002 (DB2 Control Server)
   - 55555 (WAS database port)

If port 80 is in use, it is possible that IIS is installed. If the Microsoft Internet Information Services (IIS) Web server is running, you will have a port conflict with IBM HTTP Server. Both of these Web servers listen on port 80, unless otherwise configured. To prevent this conflict, disable the Microsoft IIS Web server.

To see if IIS is enabled:

1. Select **Start** → **Settings** → **Control Panel** → **Add/Remove Programs**.
2. Select **Add/Remove Windows Components**.
3. If IIS is listed, it has been installed on the computer.
4. To disable IIS:
   a. Select **Start** → **Programs** → **Administrative Tools**.
   b. Open **Services**.
   c. Locate and highlight **IIS Admin Service**.
   d. Select the **Action** menu and click **Properties**. A window opens.
   e. Change the **Startup type** to **Disabled** and click **Stop** to stop the server.
   f. Click **Yes** to stop any services that are stopped as a result.
   g. Locate the **World Wide Web Publishing Service**. Disable it at startup using the steps listed above.

Create the WebSphere Everyplace Access Administrator IDs

Before installing Everyplace Access, an Administrator ID for it needs to be created. During a Component Install, the administrator ID, which is a local Windows operating system administrator ID that is shared by all components, is used to create WebSphere Everyplace Access databases and Windows services. The ID is required to have system administrator permissions, in other words, it must be a member of the Administrators group.

Another ID is created for installing WebSphere Everyplace Access. This ID is used to log on to the computer and to install WebSphere Everyplace Access.

These IDs must conform to the following list of requirements for a component installation:

- Can contain characters a-z, A-Z, 0-9, - (dash), _ (underscore), and . (dot).
- Cannot be longer than 12 characters.
- Cannot include spaces, NON-ASCII characters, or diacritics (such as umlauts).

To create the IDs, do the following:

1. Click **Start** → **Programs** → **Administrative Tools** → **Computer Management**.
2. Under System Tools, expand **Local Users and Groups**.
3. Right-click **Users** and select **New User**.
4. On the New User dialog, enter a user name, password, and confirm the password (see Table 5-19).

Table 5-19 Installation user

Field	Value
User name	instwea
Password	lpiwea

5. Deselect **User must change password at next logon**.
6. Select **Password never expires**.
7. Click **Create**.
8. Enter the user name and password for the WEA user ID (see Table 5-20 on page 145).

Table 5-20 Everyplace Access administrator

Field	Value
User name	weaadmin
Password	lpuwea

9. Deselect **User must change password at next logon**.
10. Select **Password never expires**.
11. Click **Create** and then click **Close**.

Both IDs need to have system administrator permissions. Therefore, they must be members of the Administrators group:

1. Right-click the instwea you just created and select **Properties**.
2. Click the **Member Of** tab and click **Add**.
3. Select **Administrators** from the Name column and click **Add**. Click **OK**.
4. Click **Apply** and then click **Close**.
5. Right-click the weaadmin you just created and select **Properties**.
6. Click the **Member Of** tab and click **Add**.
7. Select **Administrators** from the Name column and click **Add**. Click **OK**.
8. Click **Apply** and then click **Close**.

The ID that is used to log on to the computer, in our example, instwea, must be a local user that is 12 characters or less. To be an administrative user, it must belong to the Administrators group defined in Windows. A domain user ID cannot be used. In addition, it must have the following rights:

- Act as part of the operating system
- Create a token object
- Increase quotas
- Log on as a Service
- Replace a process level token

Note: The user weaadmin needs the right to **Create a token object**; otherwise the installation will fail during the Intelligent Notification Service component.

To access the interface for editing user rights, do the following:

1. Select **Start** → **Programs** → **Administrative Tools** → **Local Security Policy**.
2. Expand **Local Policies** and click **User Rights Assignment**.
3. Locate each Policy listed above and verify that the ID is listed in the **Local Setting** column.
4. To add the user, right-click the policy and select **Security**.
5. Log off and log in as the user just created (instwea).

5.3.2 Install Lotus Notes

To be able to synchronize PIM and e-mail data or to receive e-mail notifications, a Lotus Notes Client must be installed and configured, because Everyplace Synchronization and Intelligent Notification Services use the Notes Client to communicate with the Domino Server. Do the following:

1. Insert CD 9-1 and navigate to the win directory and open the en directory.
2. Run setup.exe.
3. Click **Next** on the welcome panel.
4. Accept the terms of the license agreement and click **Next**.
5. Specify a User Name and Organization.
6. Select **Only for me (Single User Install)** and click **Next**.
7. Accept the default folders and click **Next** (see Table 5-21).

Table 5-21 Installation default folders

Field	Value
Install program files to	C:\Program Files\Lotus\Notes
Install data files to	C:\Program Files\Lotus\Notes\NotesData

8. Accept the default features to install on the Custom Setup panel. Click **Next**.
9. On the **Ready to Install the Program** panel, click **Install**.
10. Click **Finish**.

To configure Lotus Notes so that Everyplace Synchronization and Intelligent Notification Services can use it, the Notes Data directory has to be copied.

1. For Everyplace Synchronization Services, create the following directory, *ess_home*\NotesData, where ess_home is the location where you will install

the Everyplace Synchronization Server. The default location is C:\Program Files\WebSphere\IBMSyncServer.

2. For Intelligent Notification Services, create the following directory, *ins_home*\NotesData, where ins_home is the location where you will install Intelligent Notification Services. The default location is C:\Program Files\WebSphere\INS.
3. Copy the content of the Notes Client data directory (C:\Program Files\Lotus\Notes\Data) to both directories.

In order to work correctly, Everyplace Synchronization and Intelligent Notification Services need the Notes client directory to be in the system PATH variable. Do the following

1. Select **Start** → **Settings** → **Control Panel** → **System**.
2. Select the **Advanced** tab.
3. Click **Environment Variables**.
4. In the System variables region, select the **Path** variable and click **Edit**.
5. In the Variable Value field, add the Notes client installation directory to the end of the variable. Remember to type a semicolon at the end of the Variable Value before adding the Notes client path. For example, add the following:

   ```
   ;C:\Program Files\Lotus\Notes
   ```

6. Click **OK** to close the Environment Variables dialog box.
7. Click **OK** to close the System Properties dialog box.

Because Intelligent Notification Service and Everyplace Service need Lotus Notes in different configurations, we have to adjust it.

1. Rename the notes.ini file to notes.save. You will find the notes.ini file in the following location: C:\Program Files\Lotus\Notes.
2. Copy C:\Program Files\Lotus\Notes\notes.save to *ess_home*\NotesData\notes.ini and to *ins_home*\NotesData\notes.ini.
3. Open the *ess_home*\NotesData\notes.ini in a Editor and edit the Directory parameter to point to the *ess_home*\NotesData, for example:

   ```
   Directory=C:\Program Files\WebSphere\IBMSyncServer\NotesData
   ```

4. Open the *ins_home*\NotesData\notes.ini in a Editor and edit the Directory parameter to point to the *ins_home*\NotesData, for example:

   ```
   Directory=C:\Program Files\WebSphere\INS\NotesData
   ```

5. Open a command prompt.
6. Within this command prompt, from the *ess_home*\NotesData directory, launch the Notes Client by typing `notes.exe`.

7. The Notes Client Configuration Wizard will appear.
8. At the Welcome screen, click **Next**.
9. Enter the Notes ID created for the Everyplace Synchronization Service in the Your name field (see Table 5-22).

Table 5-22 Notes ID

Field	Value
Your name	essadmin

10. Enter the Domino server and check the **I want to connect to Domino Server** check box and click **Next**. In our installation, we entered `wea5e/ITSORaleigh`.
11. Enter your Password and click **OK** (see Table 5-23).

Table 5-23 Password

Field	Value
password	dpessadm

12. In the Additional Services panel, leave the default selections as is and click **Finish**.
13. Close the Notes Client after configuring.

Now ESS is configured to use the Lotus Notes Client to access the Domino. The INS configuration is similar:

1. In the command prompt, go to the *ins_home*\NotesData directory and launch the Notes Client by typing `notes.exe` again.
2. The Notes Client Configuration Wizard will appear.
3. At the Welcome screen, click **Next**.
4. Enter the Notes ID created for the Intelligent Notification Service in the Your name field (see Table 5-24).

Table 5-24 Notes ID for Intelligent Notification Services

Field	Value
Your name	insadmin

5. Enter the Domino server and check the **I want to connect to Domino Server** check box and click **Next**. In our installation, we entered `wea5e/ITSORaleigh`.
6. Enter your Password and click **OK** (see Table 5-25 on page 149).

Table 5-25 Password

Field	Value
password	dpinsadm

7. In the Additional Services panel, leave the default selections and click **Finish**.
8. Close the Notes Client after configuring.
9. Close the command prompt.

5.3.3 Installation of WebSphere Everyplace Access

This section describes all the steps that are necessary to install WebSphere Everyplace Access. At first, all the required software packages, such as DB2, WebSphere Application Server, WebSphere Portal Server, and all the needed Fix Packs are installed. After that, the components of WebSphere Everyplace Access are installed. Each component installation is split into two parts. First, the component is copied to the computer and the system registry information is configured. Then the component has to be configured by running configuration tasks to set up the needed features. The configuration tasks include editing configuration files and invoking commands from the command line to set up the component.

DB2 Universal Database Workgroup installation

1. Make sure you are logged in as the administrative user you created, in our example, instwea.
2. Start install.bat from the WebSphere Everyplace Access Setup CD.
3. Select **English** and click **OK**.
4. Click **Next** or launch the InfoCenter (see Figure 5-1 on page 150).

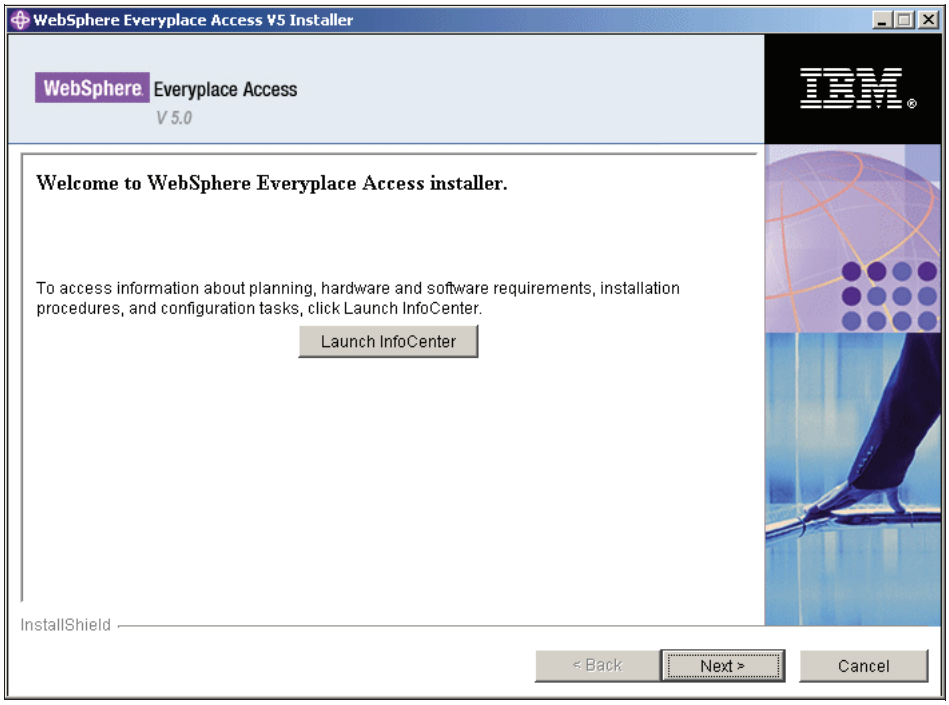

Figure 5-1 Everyplace Access installer welcome window

5. View the license agreement and select **I accept the terms in the license agreement** and click **Next**.
6. Select **Component Installation** and click **Next** (see Figure 5-2 on page 151).

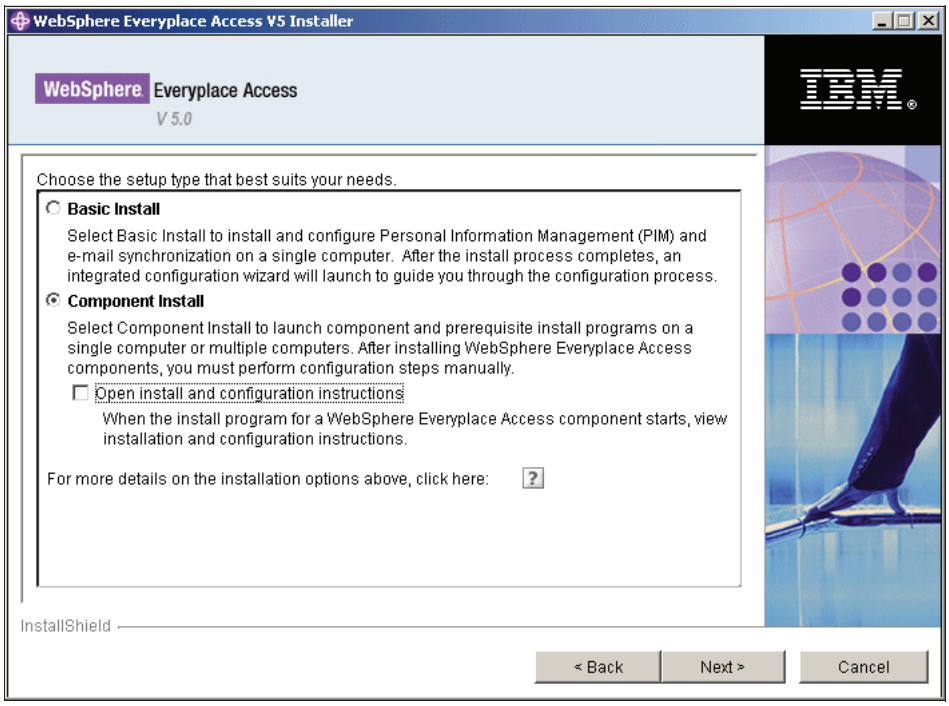

Figure 5-2 Setup types

7. Select **DB2 Universal Database Workgroup V8.1.6** and click **Next** (see Figure 5-3 on page 152).

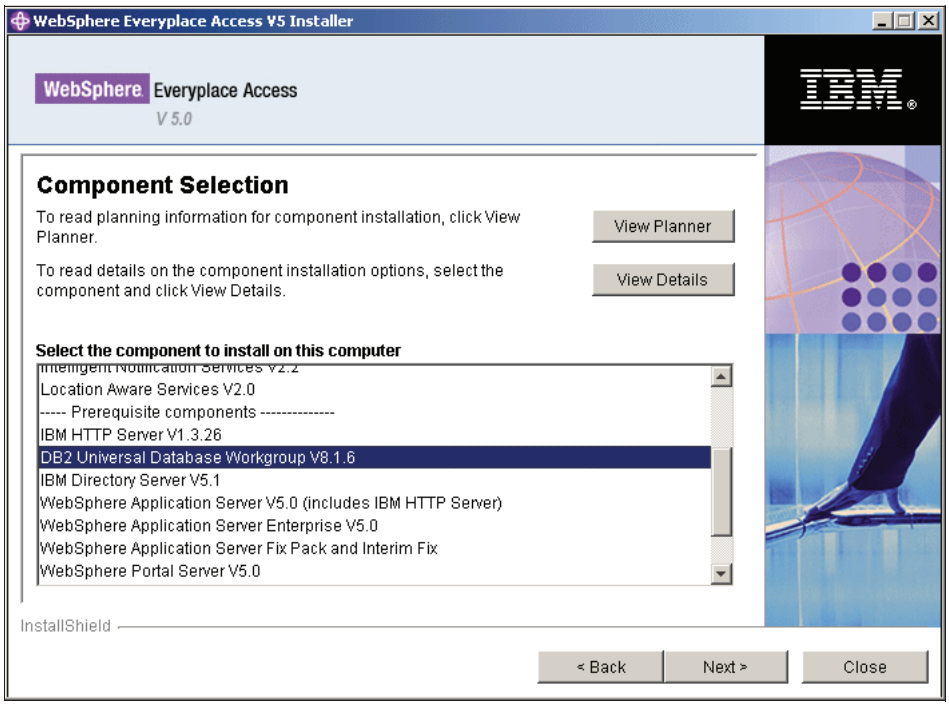

Figure 5-3 Component selection: DB2 UDB Workgroup V8.1.6

8. Insert the CD (labeled as CD 1-1) when prompted and click **Next**.
9. Click **Installation Prerequisites** if you want to review the requirements for DB2. Close the browser when you are finished.
10. Click **Install Product** (see Figure 5-4 on page 153).

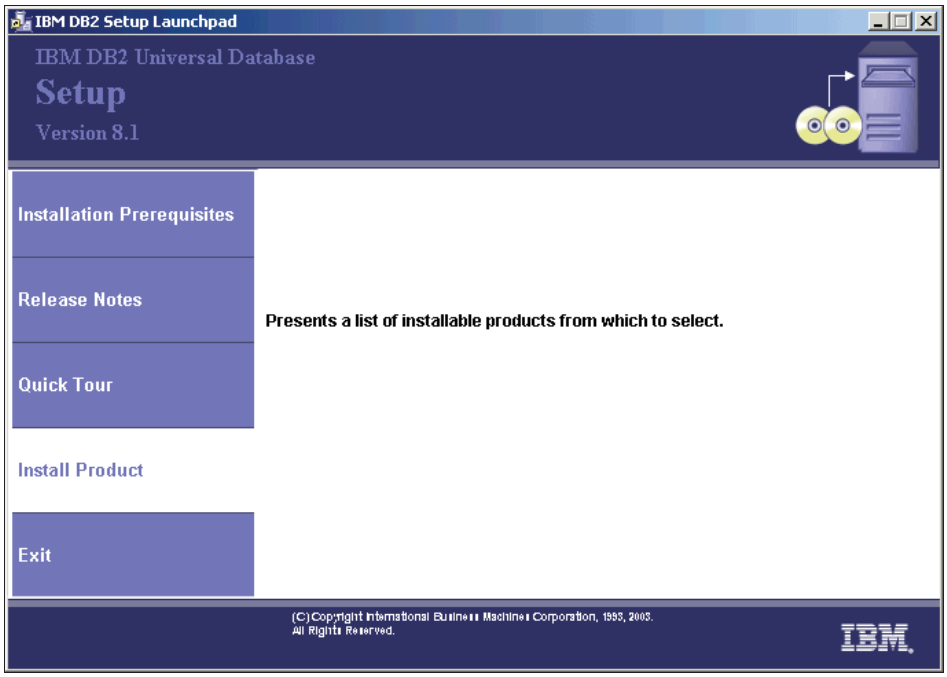

Figure 5-4 Install Product option

11. On the product selection panel, click **Next** (see Figure 5-5 on page 154).

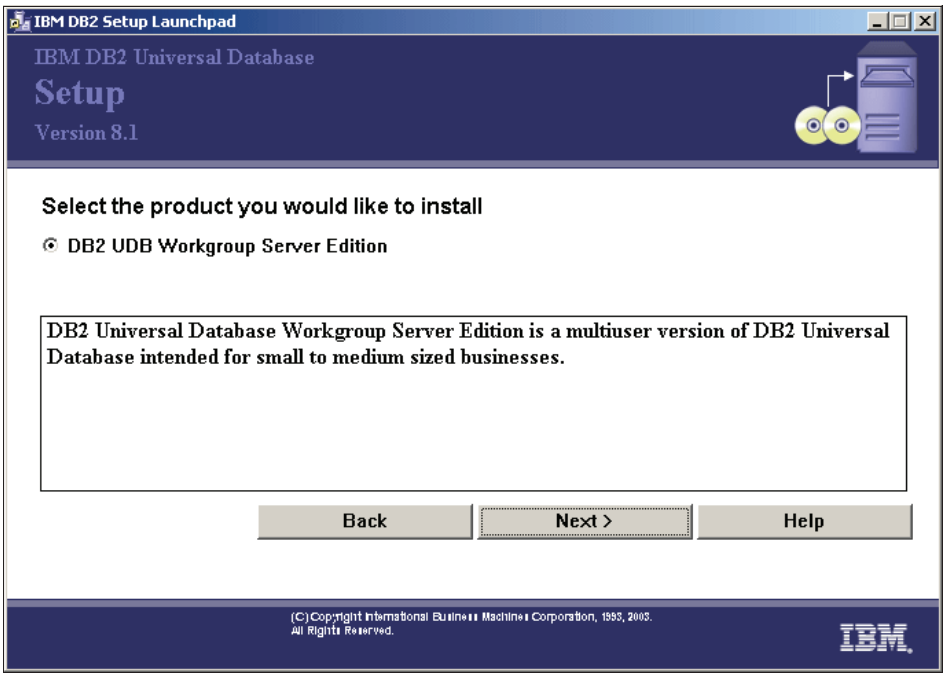

Figure 5-5 Product selection panel

12. Click **Next** on the welcome panel.
13. Review the license agreement and select **I accept the terms in the license agreement** and click **Next**.
14. Select **Typical** as the installation type and click **Next** (see Figure 5-6 on page 155).

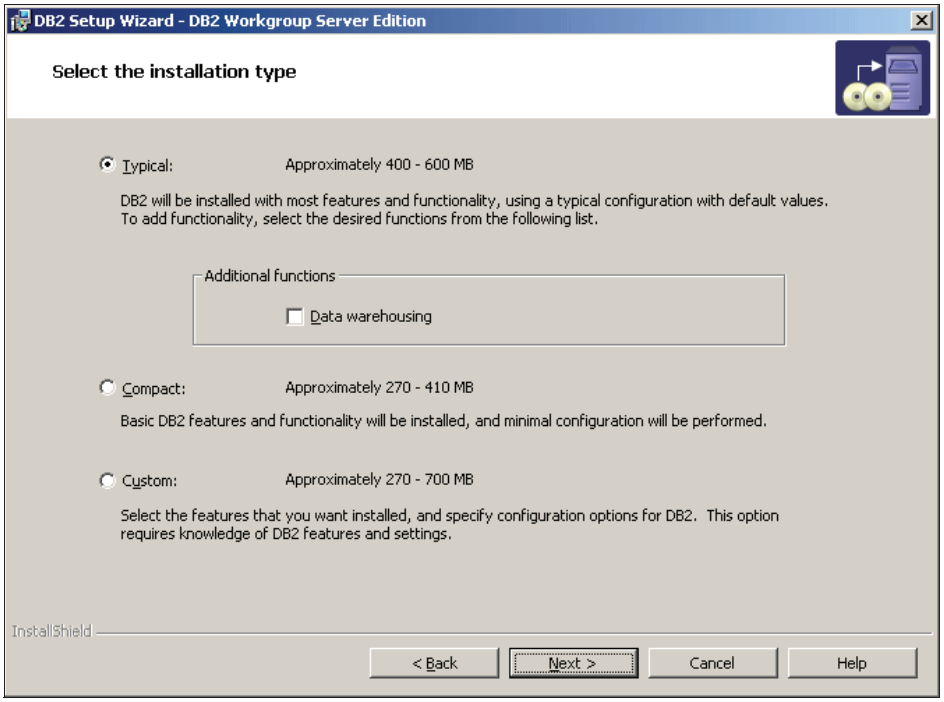

Figure 5-6 Installation type

15. Select the **Drive** and change the **Directory** location if needed and click **Next** (see Table 5-26).

Table 5-26 Drive and directory

Field	Value
Drive	C
Directory	C:\Program Files\IBM\SQLLIB

16. Enter the DB2 Administrator **User name** and **Password**. This should be a local user. If the user does not exist, the install program will create the local user with the appropriate access rights. In our example, the user will be created. Select **Use the same user name and password for the remaining DB2 services** and click **Next** (see Table 5-27 on page 156).

Table 5-27 User name and password

Field	Value
User name	db2admin
Password	lpudbase

17. When a database needs attention, DB2 use a contact list to send messages. In our installation, we do not need a contact list. Select **Local** and click **Next**.
18. A warning will appear alerting you with the notification `SMTP server has not been specified`. Ignore it and click **OK**.
19. Leave DB2 as default instance and click **Next**.
20. Select **Do not prepare the DB2 tools catalog on this computer** and click **Next**.
21. In the **Specify a contact for health monitor notification** window, select **Defer the task until after installation is complete** and click **Next**.
22. Review the summary and click **Install** to start copying files (see Figure 5-7).

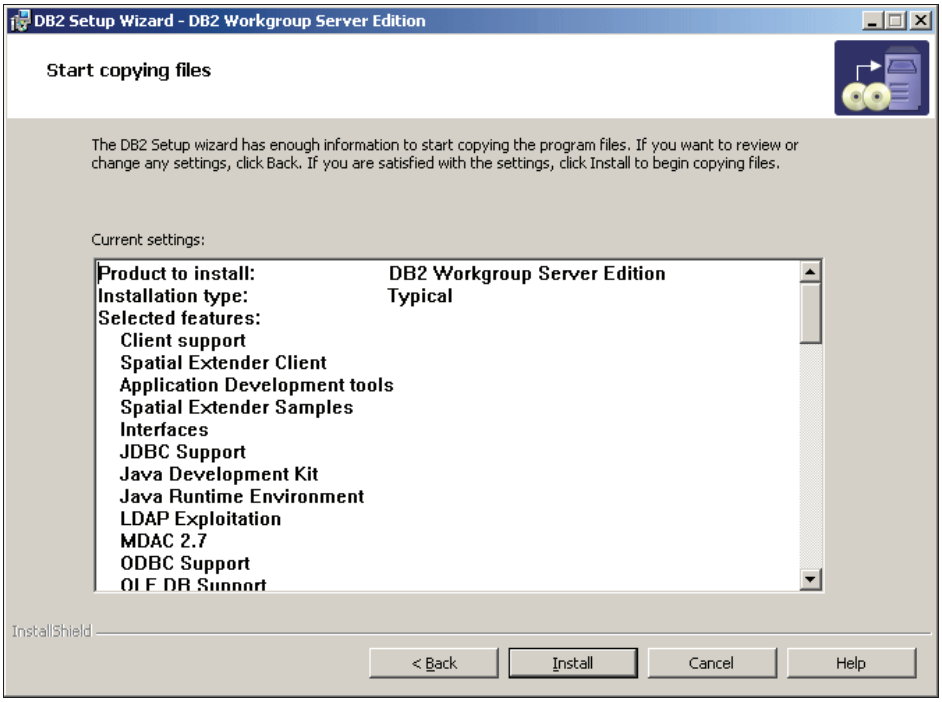

Figure 5-7 Installation summary

23. Click **Finish** to exit the DB2 install program (see Figure 5-8).

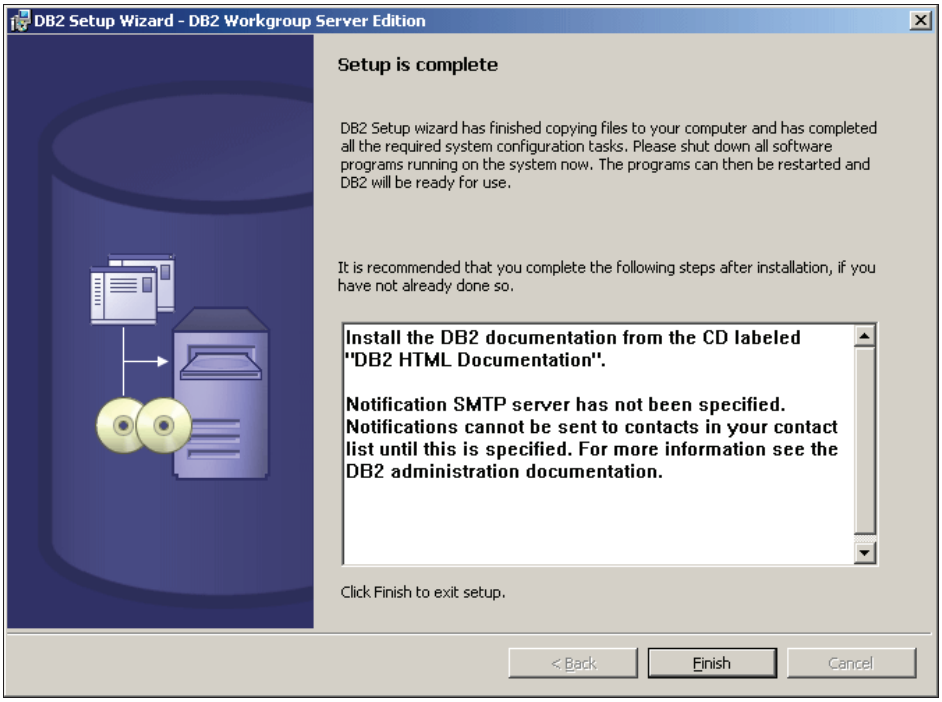

Figure 5-8 Setup finish

24. The DB2 Universal Database First Steps interface will open. Click **Exit First Steps**.
25. You will be returned to the WebSphere Everyplace Access install program. Leave it open. Select **Start** → **Programs** → **IBM DB2** → **General Administrations Tools** → **Control Center**.
26. Expand **All Cataloged System**, the current node (in our example, wea5d), and then **Instances**.
27. Right-click **DB2** and select **Configure Parameters**.
28. Scroll down to the Diagnostic section and select the **NOTIFYLEVEL** parameter.
29. Change the **NOTIFYLEVEL** value to 1 (Errors Only).
30. Scroll down to the Environment section and select the **NUMDB** parameter.
31. Change the NUMDB Value to 25.
32. Click **OK** to close the configuration window

33. You need to restart the DB2 Instance. Therefore right-click **DB2** and choose **Stop**. After it is stopped, right-click **DB2** and choose **Start**.
34. Close the Control Center and leave the WebSphere Everyplace Access install program open.

WebSphere Application Server installation

1. Assuming the WebSphere Everyplace Access install program is still open, choose **WebSphere Application Server 5.0 (includes IBM HTTP Server)** and click **Next** (see Figure 5-9).

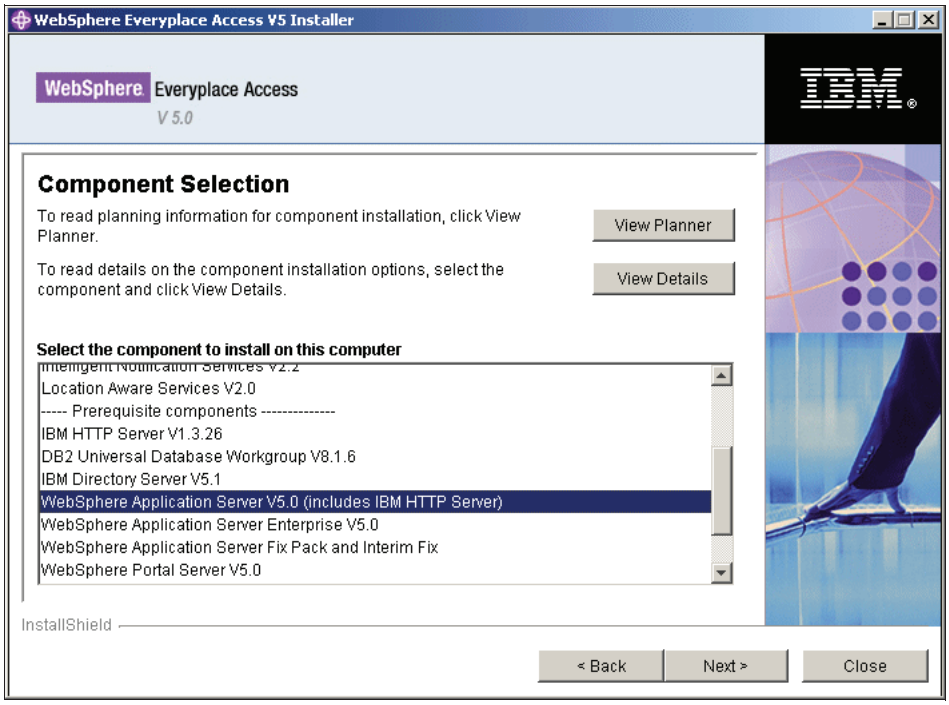

Figure 5-9 Component selection: WebSphere Application Server V5.0

2. Insert the CD when prompted and click **Next**.
3. Select **English** as the language and click **OK**.
4. Click **Next** on the welcome panel.
5. Review the license agreement and select **I accept the terms in the license agreement** and click **Next**.

Note: You might see a message that indicates that the install program cannot detect a supported operating system. If you are using Windows Server 2000 SP 4 or Windows Advanced Server 2000 SP 4, you can ignore this message.

6. Select the **Full** install type and click **Next** (see Figure 5-10).

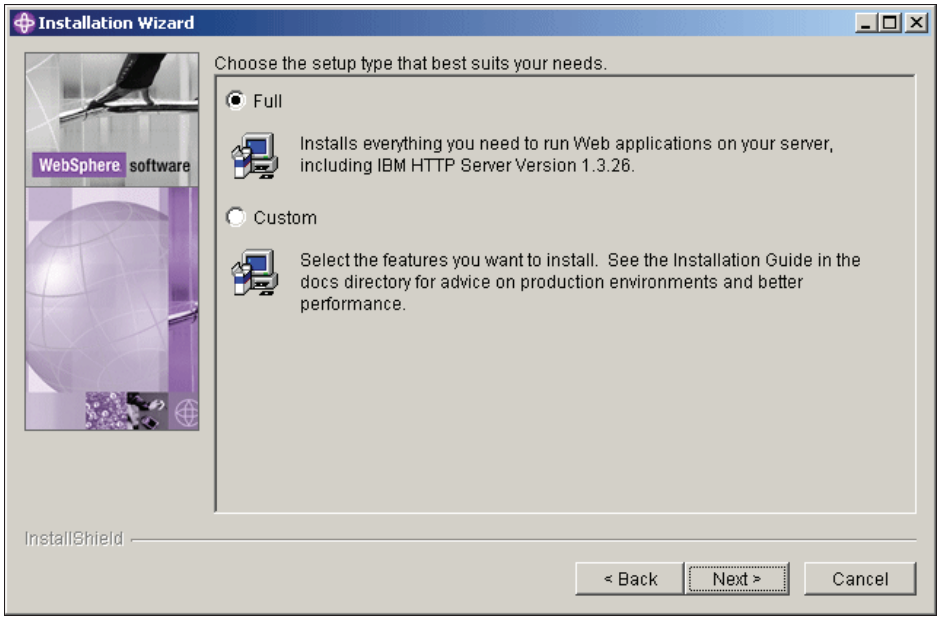

Figure 5-10 Setup types

7. Enter the install directory for IBM WebSphere Application Server V5, IBM HTTP Server V1.3.26, and Embedded Messaging Server and Client and click **Next** (see Table 5-28).

Table 5-28 Install directories

Field	Value
IBM WebSphere Application Server V5	C:\Program Files\WebSphere\AppServer
IBM HTTP Server V1.3.26	C:\Program Files\IBMHttpServer
Embedded Messaging Server and Client	C:\Program Files\IBM\WebSphere MQ

8. The install program should detect the Node Name and Host Name or IP Address. If it does not, enter those values (see Table 5-29). When entering the host name, be sure to enter the fully-qualified host name. Click **Next**.

Table 5-29 Node and host names

Field	Value
Node name	wea5d
Host name or IP Address	wea5d.itso.ral.ibm.com

9. Enter the administrative user ID created in "Create the WebSphere Everyplace Access Administrator IDs" on page 144 and the password. Select both check boxes and click **Next.**

   As the default, the installation provides the user name as instwea, because that is the user you are currently logged on with. Change it to your created administrative user ID (see Table 5-30).

Table 5-30 User ID

Field	Value
Run WebSphere Application Server as a service	Selected
Run IBM HTTP Server as a service	Selected
User ID	weaadmin
Password	lpuwea

10. Review the summary panel and click **Next** to start the install (see Figure 5-11 on page 161).

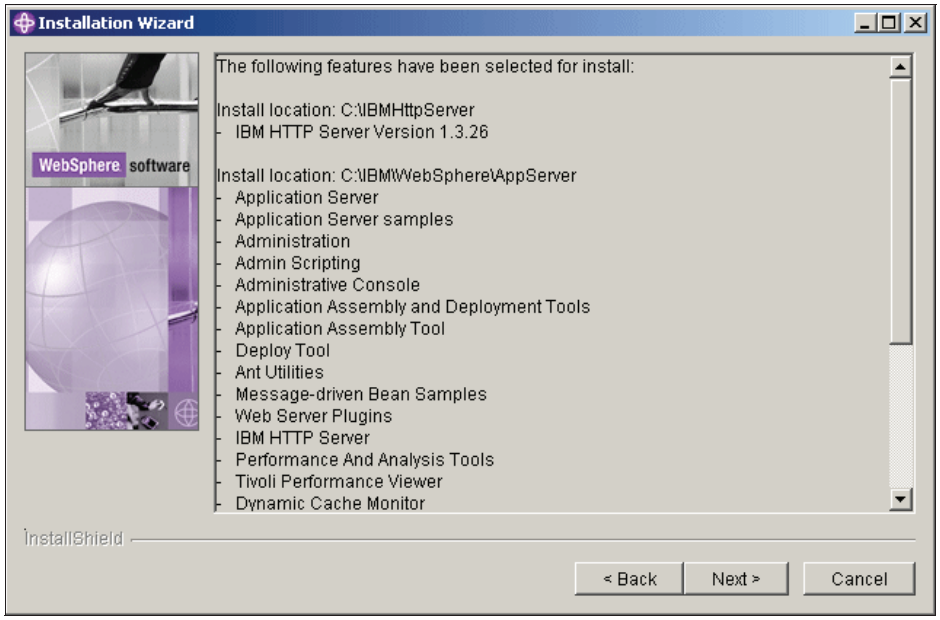

Figure 5-11 Installation summary

11. On the registration panel, uncheck **Register this product now** and click **Next**.
12. WebSphere Application Server First Steps will open. Click **Verify Installation**. If the server installed successfully, you will see a message similar to the following message:

    ```
    IVTL0070I: IVT Verification Succeeded
    IVTL0080I: Installation Verification is complete
    ```

13. Click **Stop the Server**.
14. Click **Exit** when you are finished reviewing First Steps. Click **Finish** on the WebSphere Application Server install program.

WebSphere Application Server Enterprise installation

1. Assuming the WebSphere Everyplace Access install program is still open, choose **WebSphere Application Server Enterprise V5.0** and click **Next** (see Figure 5-12 on page 162).

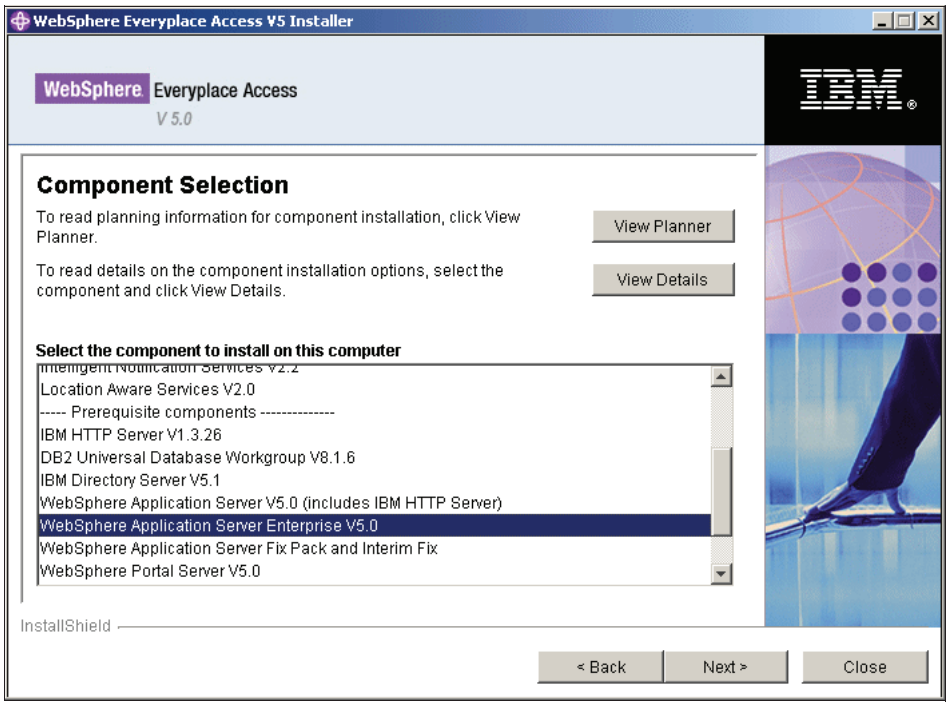

Figure 5-12 Component selection: WebSphere Application Server Enterprise V5.0

2. Insert the CD 3-1 when prompted and click **Next**.
3. Select **English** as the language and click **OK**.
4. Click **Next** on the welcome panel.
5. Review the license agreement, select **I accept the terms in the license agreement**, and click **Next**.
6. Select **Add to existing copy of WebSphere Application Server, v5.0** and click **Next** (see Figure 5-13 on page 163).

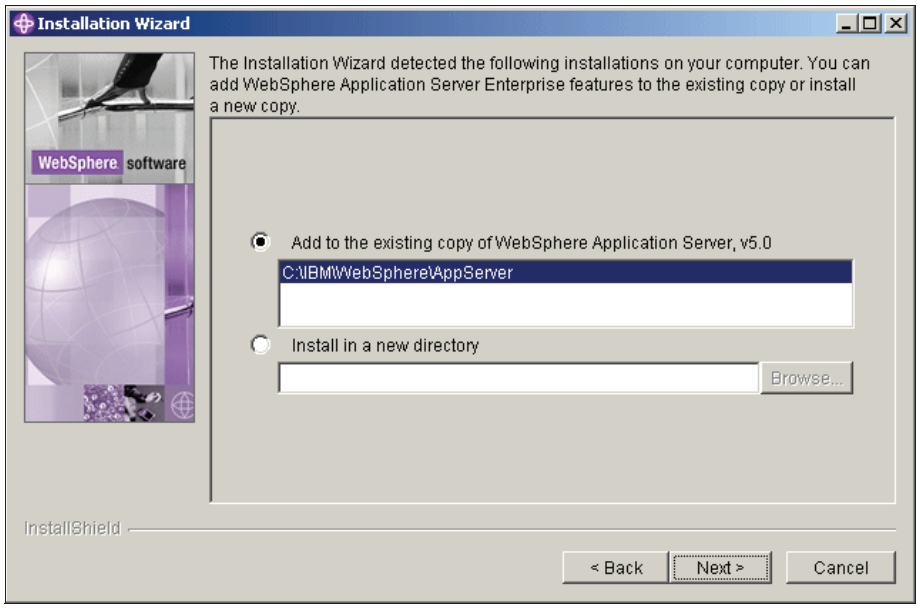

Figure 5-13 Add to existing copy of WebSphere Application Server V5.0

7. Select **Typical** install type and click **Next** (see Figure 5-14).

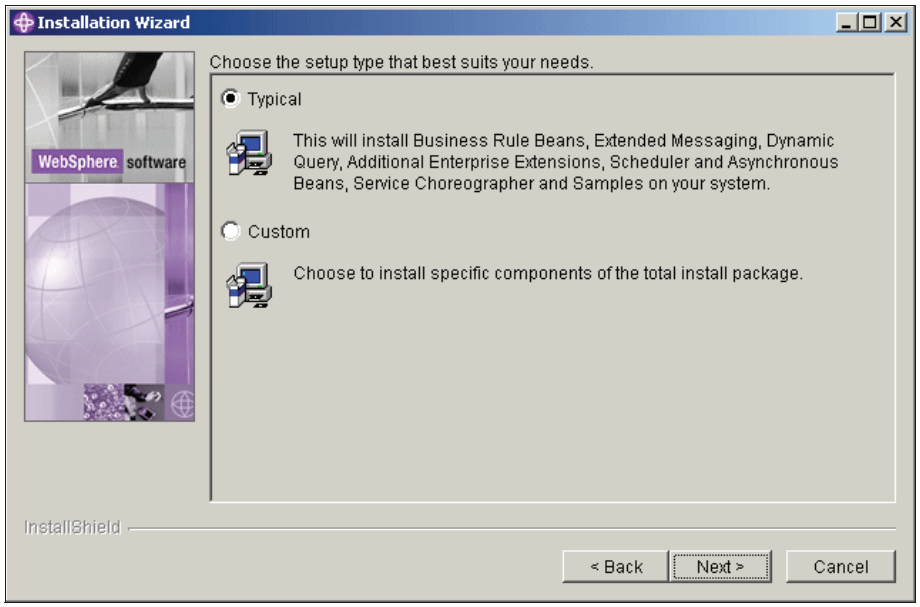

Figure 5-14 Setup types

8. Review the summary panel and click **Install** to start the install (see Figure 5-15).

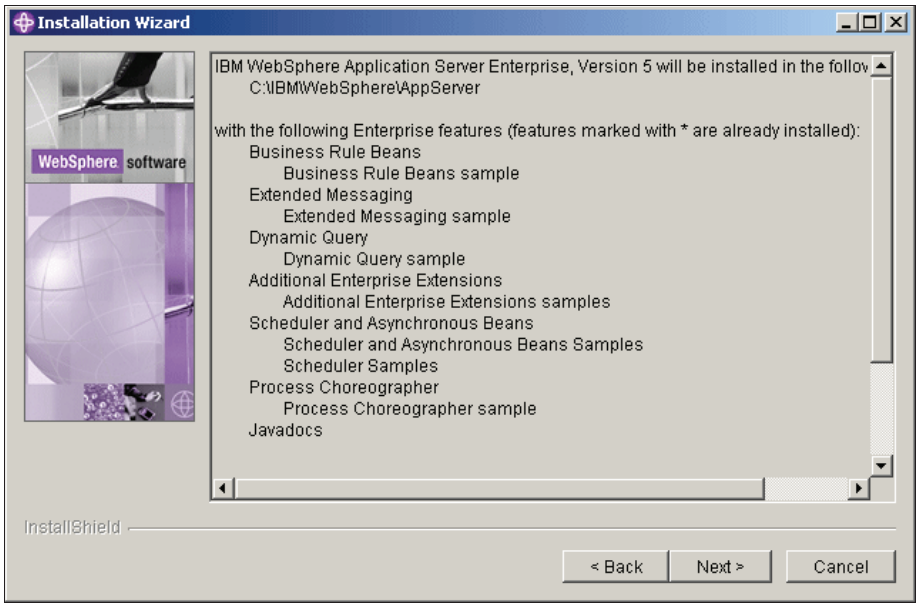

Figure 5-15 Installation summary

9. After finishing the installation, uncheck **Register this product now** and click **Next** on the registration panel.
10. Click **Finish** to exit the WebSphere Application Server install program.

WebSphere Application Server Fix Pack installation

Make sure that WebSphere Application Server, IBM HTTP Server, and IBM HTTP Administration Server are stopped.

1. To test if the WebSphere Application Server is stopped, open a command prompt and run the **`serverstatus server1`** command in the *was_home*\bin directory:

   ```
   cd \program files\websphere\appserver\bin
   serverstatus server1
   ```

2. If it is started, stop it with the **`stopserver`** command from the same directory:

   ```
   stopserver server1
   ```

3. To stop both IBM HTTP Servers, select **Start** → **Settings** → **Control Panel** → **Administrative Tools** → **Services.** Right-click **IBM HTTP Server** and select **Stop**. Right-click **IBM HTTP Administration Server** and select **Stop**.

4. Assuming the WebSphere Everyplace Access install program is still open, choose **WebSphere Application Server fix pack and interim fix** and click **Next**.
5. Insert the CD 3-3 when prompted and click **Next**.
6. Select **English** as the language and click **OK**.
7. Click **Next** on the welcome panel.
8. The next panel should display the currently installed version of WebSphere Application Server. If it does not, click the empty text box and the information should appear.
9. Select **IBM WebSphere Application Server v5.0.0 + Enterprise v5.0.0**, accept the default install location of the Application Server, and click **Next**.

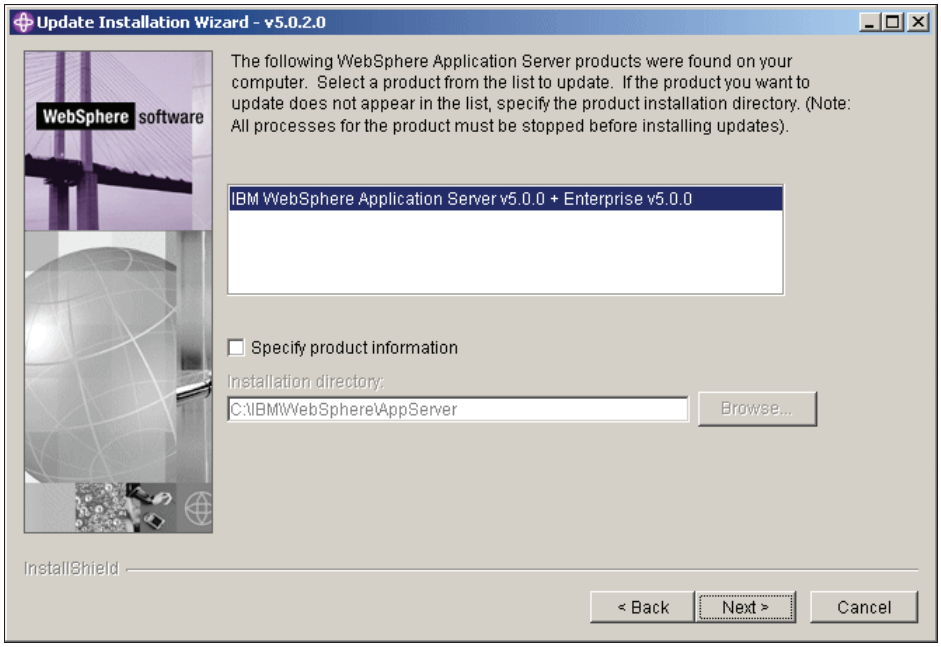

Figure 5-16 Update WebSphere Application Server

10. Select **Install fix packs** and click **Next**.
11. Click **Browse** to specify the fix pack location. Go to the CD 3-3, select **WAS502BASE**, and click **Open**. Click **Next**.
12. Select **was50_fp2_win** and click **Next** (see Figure 5-17 on page 166).

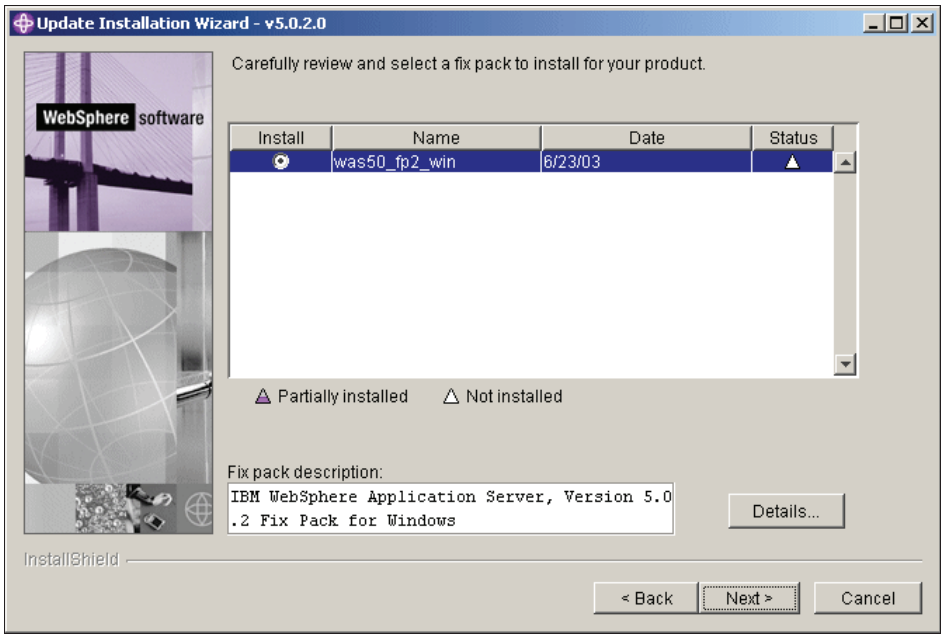

Figure 5-17 Fix Pack selection

13. In the external components to update window, select **IBM HTTP Server** and **Embedded Messaging**, and accept the default values for the install directories. Click **Next** (see Figure 5-18 on page 167).

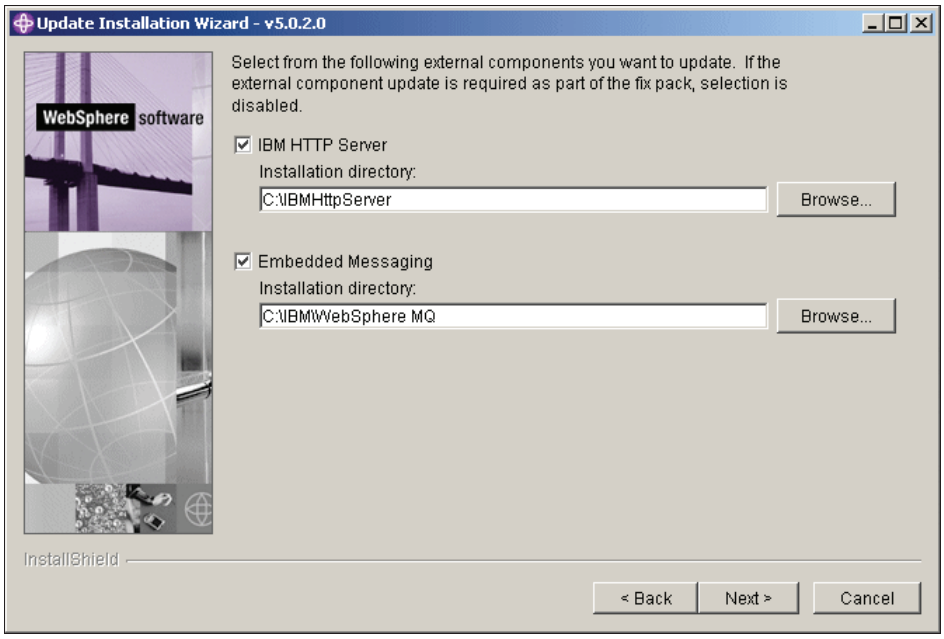

Figure 5-18 Select external components to update

14. Review the summary information and click **Next**.
15. The final install panel (see Figure 5-19 on page 168) should display the following message when it is complete:

    `The following fix pack was successfully installed: was50_fp2_win`

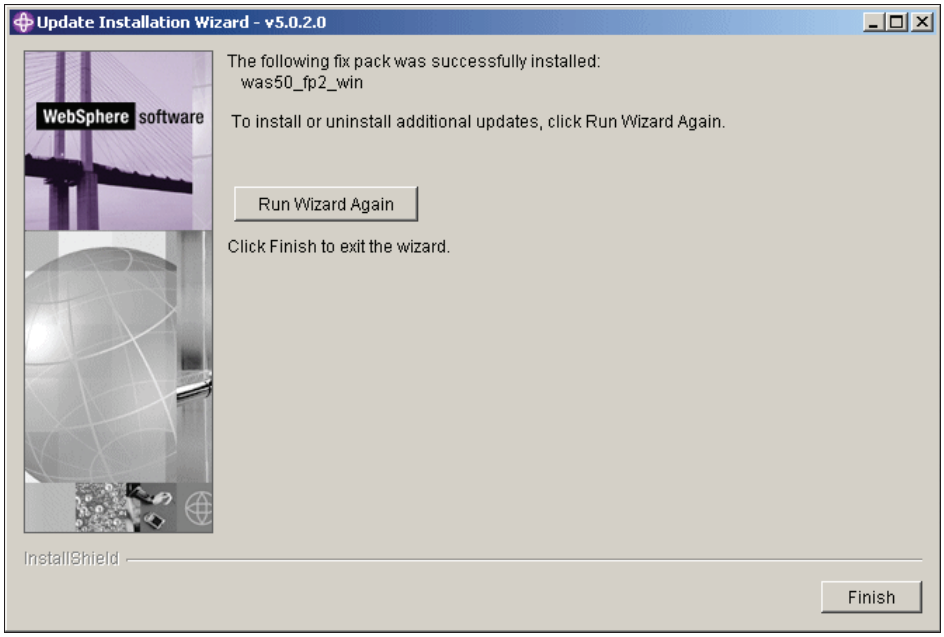

Figure 5-19 Final install panel

16. Click **Run wizard again** and repeat step 10 on page 165 - 15 on page 167 for was50_pme_fp2_win, which is located in the WAS502PME directory on CD 3-3.
17. Click **Run wizard again** to install the first set of WebSphere Everyplace Access Enterprise Fix Pack 2 eFixes.
18. Select **Install fixes** and click **Next**.
19. Click **Browse** to specify the Fix Pack location. Go to the CD 3-3, select **WAS502EFIX**, and click **Open**. Click **Next.**
20. Select all available fixes and click **Next**. If you get a message that indicates a specific fix is not supported, click **OK**, click **Back**, and deselect the specified fix. Click **Next** (see Figure 5-20 on page 169). (There might be multiple unsupported fixes, so repeat this deselect step as needed.)

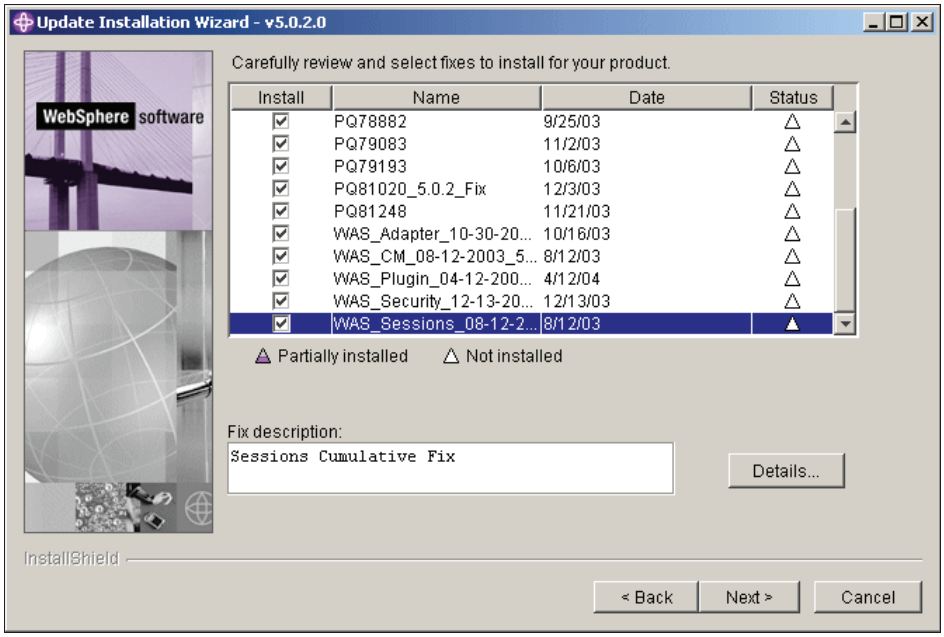

Figure 5-20 Fix Pack selection

21. Review the summary information and click **Next**.
22. The final install panel (see Figure 5-21 on page 170) should display the following message when it is complete:

    `The following fixes were successfully installed:`

    The fixes will appear in the field below the message.

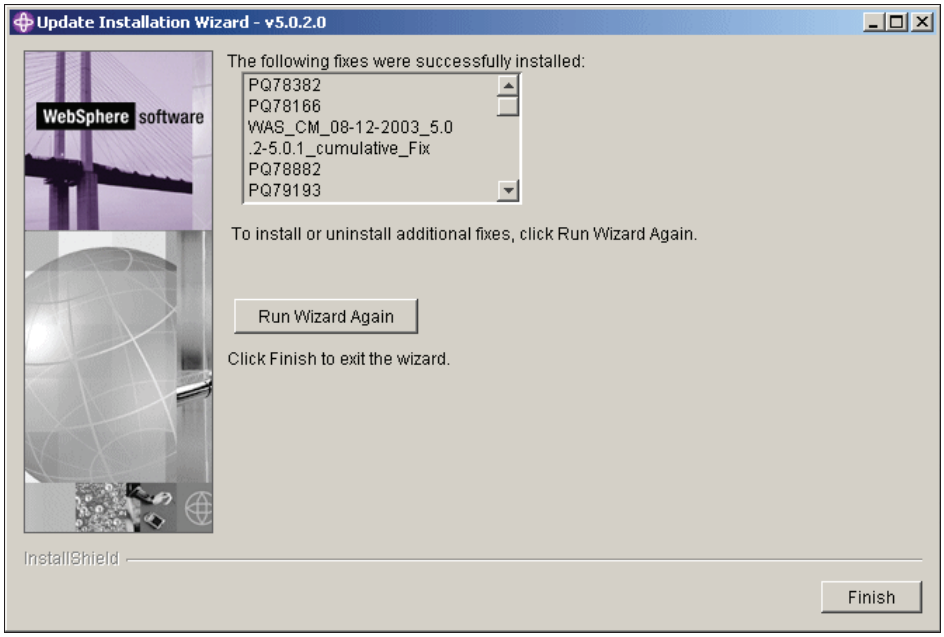

Figure 5-21 Final install panel

23. Click **Run wizard again** and repeat steps 18 on page 168 - 22 on page 169 to install the additional WebSphere Everyplace Access Enterprise Fix Pack 2 eFixes, which are located in the WAS502EFIX2 directory on CD 3-3.
24. Click **Finish**.
25. To verify the installation, select **Start** → **Programs** → **IBM WebSphere** → **Application Server V5.0** → **First Steps** and click **Verify Installation**. You should see a message similar to the following:

```
IVTL0070I: IVT Verification Succeeded
IVTL0080I: Installation Verification is complete
```

26. Click **Exit** to close First Steps.

WebSphere Portal Server installation

1. Assuming the WebSphere Application Server is still running and the WebSphere Everyplace Access install program is still open, choose **WebSphere Portal Server V5.0** and click **Next** (see Figure 5-22 on page 171).

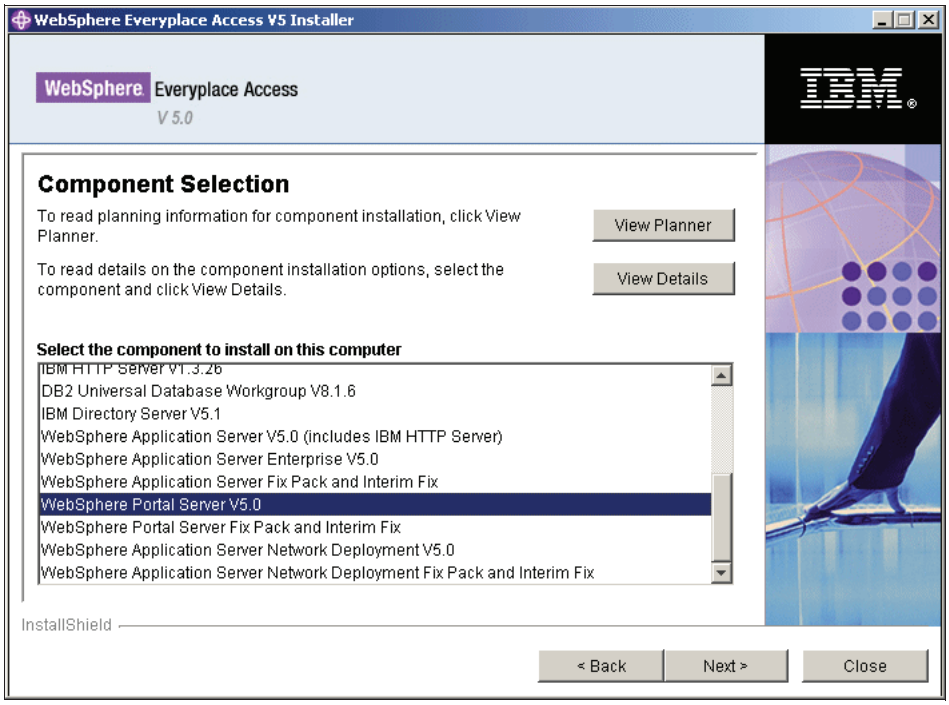

Figure 5-22 Component selection: WebSphere Portal Server V5.0

2. Insert the CD 2-1 when prompted and click **Next**.
3. Select **English** as the language and click **OK**.
4. Click **Next** on the welcome panel.
5. Review the license agreement, select **I accept the terms in the license agreement**, and click **Next**.
6. Verify the WebSphere Application Server install location. Correct the install location if needed and click **Next**.
7. Specify where you want to install WebSphere Portal and click **Next** (see Table 5-31).

Table 5-31 WebSphere Portal installation directory

Field	Value
Directory	C:\Program Files\WebSphere\PortalServer

8. Enter your Portal administrative user name and password (see Table 5-32 on page 172). This password is used to log on the Portal and configure the

Portal. It is temporary, because later we will move to the Domino Directory, where we created weaadmin in the Lotus Domino Preparation. Click **Next**.

Table 5-32 Portal administrator

Field	Value
User name	wpstemp
Password	wpstemp

9. Review the summary information and click **Next**.
10. After the install completes, click **Finish**.
11. Close the WebSphere Portal V5 Launcher.

To verify that the WebSphere Portal Server is successfully installed, check that it is running and try to go to the Portal Homepage and log in as the admin we have just created.

1. Check to see if WebSphere Portal has started (WebSphere Portal should be running after a successful install). To test if the WebSphere Portal Server is started, open a command prompt and run the **`serverstatus -all`** command in the *was_home*\bin directory:

   ```
   cd \program files\websphere\appserver\bin
   serverstatus -all
   ```

2. If it is stopped, start it with the **`startserver`** command from the same directory:

   ```
   startserver WepSphere_Portal
   ```

3. Open a browser and use the following URL to access the portal: http://*hostname*:9081/wps/portal, where hostname is the machine we installed the Portal Server (in our example, wea5d.itso.ral.ibm.com). The portal will open in your browser.
4. Log on to the portal with the administrator ID that you created.

WebSphere Portal Server Fix Pack installation

1. Open a command prompt, go to *was_home*/bin, and set up the Java environment for the update installer:

   ```
   cd \Program Files\WebSphere\AppServer\bin
   setupCmdLine.bat
   ```

2. Check that all WebSphere Application Server servers are stopped:

   ```
   serverstatus -all
   ```

3. If they are started, stop them with the **stopserver** command from the same directory:

```
stopserver server1
stopserver WebSphere_Portal
```

4. Create an update directory in *wps_home*:

```
mkdir \Program Files\WebSphere\PortalServer\update
```

5. Copy the contents of CD 2-2 to *wps_home*/update.
6. Create a fixpacks directory in the update directory:

```
mkdir \Program Files\WebSphere\PortalServer\update\fixpacks
```

7. Move WP_PTF_502.jar and WPCP_PTF_502.jar, which you previously copied from CD 2-2 to *wps_home*/update, to the *wps_home*/update/fixpacks directory.
8. Run the WebSphere Portal update installer to apply the Fix Pack by running the following commands (see Figure 5-23). (You have to change the directory to *wps_home*\update.)

```
cd C:\Program Files\WebSphere\PortalServer\update
updatePortal -fixpack -installDir "C:\Program Files\WebSphere\PortalServer"
-fixpackDir "C:\Program Files\WebSphere\PortalServer\update\fixpacks"
-install -fixpackID WP_PTF_502
```

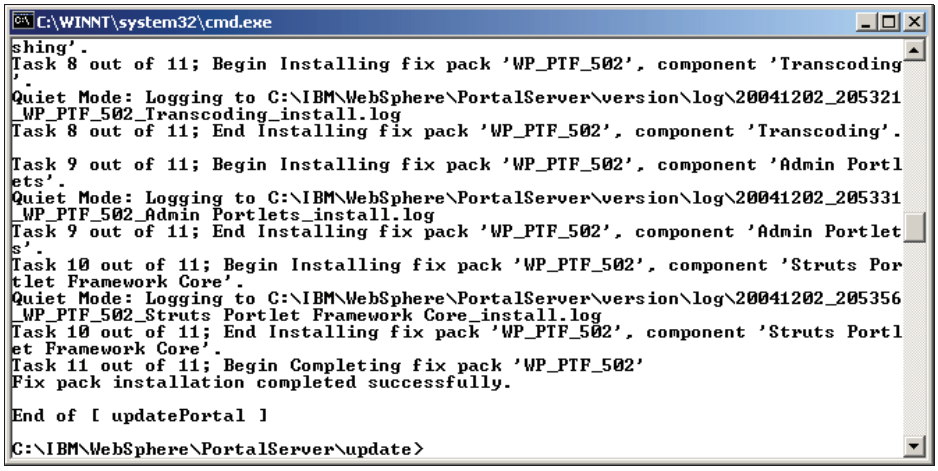

Figure 5-23 WebSphere Portal update installer command

Note: If you receive a message that indicates *WAS_HOME* is not set, the Java environment might not be properly set.

9. Run the following configuration task (see Figure 5-24). The password is used is the temporary administrative Portal user created in step 8 on page 171 during the WebSphere Portal Server Installation, in our example, wpstemp:

```
cd C:\program files\WebSphere\PortalServer\config\WPSconfig.bat WP-PTF-502
-DPortalAdminPwd=wpstemp
```

```
C:\WINNT\system32\cmd.exe
iseries-switch-to-was-user:

stop-portal-server:
     [echo] Executing  WP-PTF-502 task 50 of 50

set-instance-properties:

action-start-portal-server-iseries:

start-portal-server:
   [logmsg] 2004.12.02 21:50:15.484 start-portal-server
   [logmsg]   EJPC3060I Starting Server "WebSphere_Portal"

     [exec] ADMU0116I: Tool information is being logged in file
     [exec]            C:\IBM\WebSphere\AppServer\logs\WebSphere_Portal\startSer
ver.log
     [exec] ADMU3100I: Reading configuration for server: WebSphere_Portal
     [exec] ADMU3200I: Server launched. Waiting for initialization status.
     [exec] ADMU3000I: Server WebSphere_Portal open for e-business; process id i
s 2116

BUILD SUCCESSFUL
Total time: 57 minutes 31 seconds

C:\IBM\WebSphere\PortalServer\config>_
```

Figure 5-24 Running a configuration task

Note: If the WP-PTF-502 task fails for some reason, correct the cause of the failure and run the following configuration tasks from the *wps_home*/config directory:

```
WPSconfig.bat UNINSTALL-WP-PTF-502 -DPortalAdminPwd=wpstemp
```

If the WP-PTF-502 task failed at task 44 of 50 with the following error, `XMLC0009E: Invalid password for user wpsadmin`, verify the Portal Administrator password and run the WP-PTF-502 command again with a valid password. You do not need to run the UNINSTALL-WP-PTF-502 configuration task.

10. Check that all the servers are started:

```
cd \program files\websphere\appserver\bin
serverstatus -all
```

11. Check the status of the servers named server1 and WebSphere_Portal.

12. If any of the servers are stopped, start them:

```
startServer.bat server1
startServer.bat WebSphere_Portal
```

13. Open a browser and use the following URL to access the portal: http://hostname:9081/wps/portal, where hostname is the machine we installed the Portal Server (in our example, wea5d.itso.ral.ibm.com). The portal will open in your browser.
14. Log on to the portal with the administrator ID. In our example, it is wpstemp with wpstemp as the password
15. The fix installation is complete. The *wps_home*/update directory is no longer needed and can be deleted.

WebSphere Application Server Enterprise Fix Pack installation

Make sure that WebSphere Application Server, WebSphere Portal Server, IBM HTTP Server, and IBM HTTP Administration Server are stopped.

1. To test if the WebSphere Application Server servers are stopped, open a command prompt and run the **`serverstatus -all`** command in the *was_home*\bin directory:

   ```
   cd \program files\websphere\appserver\bin
   serverstatus -all
   ```

2. If they are started, stop them with the **`stopserver`** command from the same directory:

   ```
   stopserver server1
   stopserver WebSphere_Portal
   ```

3. To stop both IBM HTTP Servers, select **Start** → **Settings** → **Control Panel** → **Administrative Tools** → **Services**. Right-click **IBM HTTP Server 1.3.26** and select **Stop**. Right-click **IBM HTTP Administration Server 1.3.26** and select **Stop**.
4. Assuming the WebSphere Everyplace Access install program is still open, choose **WebSphere Application Server fix pack and interim fix** and click **Next** (see Figure 5-25 on page 176).

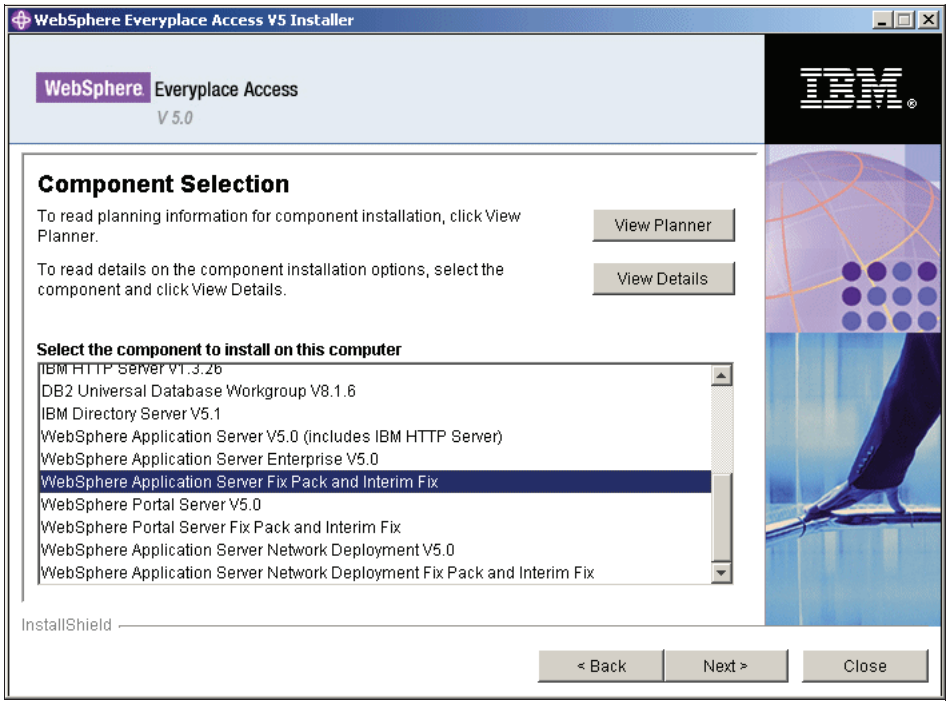

Figure 5-25 Component Selection: WebSphere Application Server Fix Pack

5. Insert the CD when prompted and click **Next**.
6. Select **English** as the language and click **OK**.
7. Click **Next** on the welcome panel.
8. The next panel should display the currently installed version of WebSphere Application Server. If it does not, click the empty text box and the information should appear.
9. Select **IBM WebSphere Application Server v5.0.2 + Enterprise v5.0.2**, accept the default install location of the Application Server, and click **Next**.
10. Select **Install fix packs** and click **Next**.
11. Click **Browse** to specify the Fix Pack location. Go to the CD 3-3, select **WAS5022BASE** and click **Open**. Click **Next**.
12. Select **was502_cf2_win** and click **Next** (see Figure 5-26 on page 177).

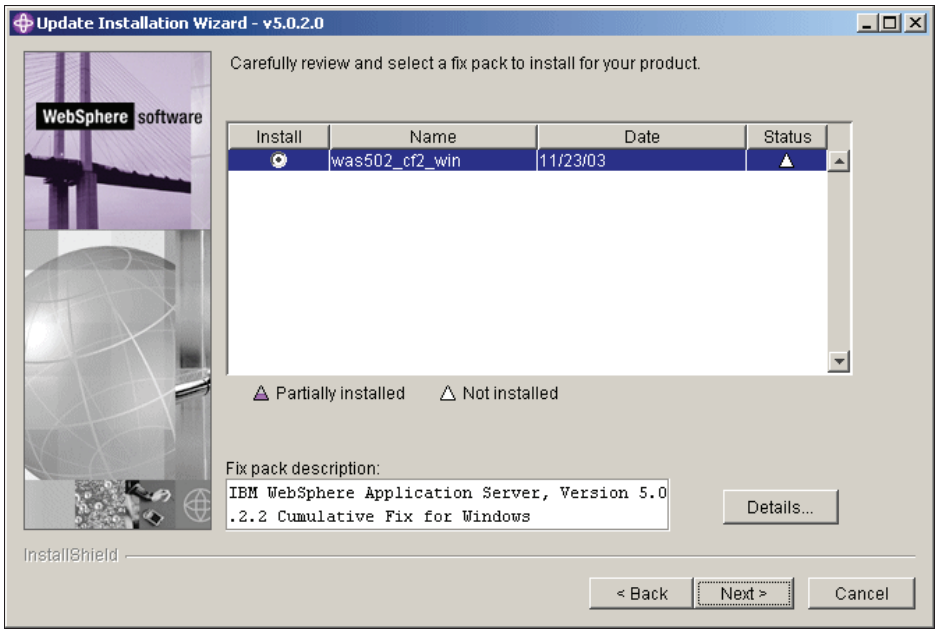

Figure 5-26 Fix Pack selection

13. Select the external components to update, IBM HTTP Server and Embedded Messaging, accept the default values for the install directories, and click **Next**.
14. Review the summary information and click **Next**.
15. The final install panel (see Figure 5-27 on page 178) should display the following message when it is complete:

    ```
    The following fix pack was successfully installed: was502_cf2_win.jar
    ```

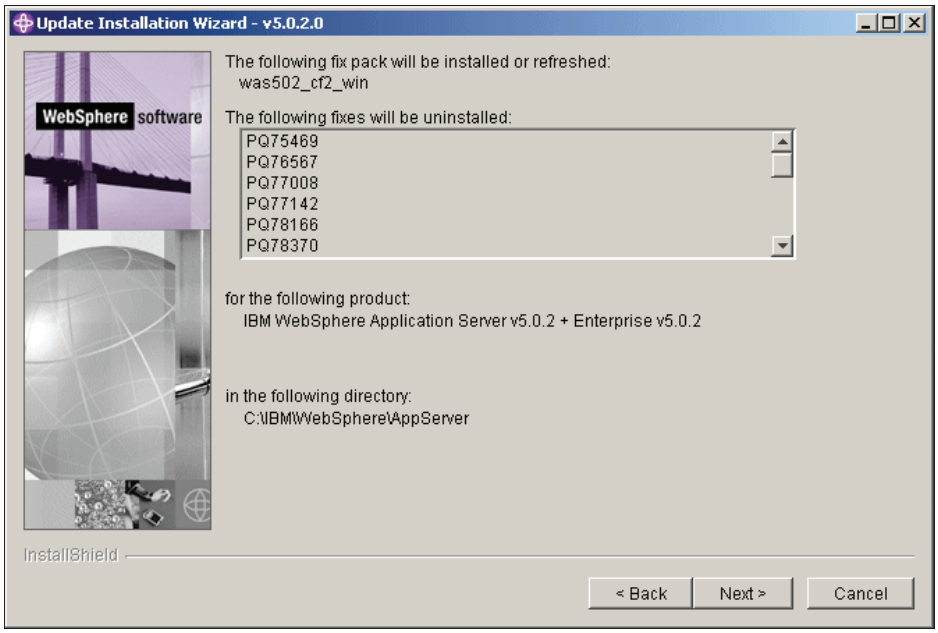

Figure 5-27 Final install panel

16. Click **Run wizard again** and repeat steps 10 on page 176 - 15 on page 177 for was502_pme_cf2_win, which is located in the WAS5022PME directory on CD 3-3.
17. Click **Run wizard again** and repeat steps 10 on page 176 - 15 on page 177 for was502_cf3_win.jar, which is located in the WAS5023BASE directory on CD 3-3.
18. Click **Run wizard again** to install interim fixes for WebSphere Application Server V5.0.2.3.
19. Select **Install fixes** and click **Next**.
20. Click **Browse** to specify the Fix Pack location. Go to the CD 3-3, select **WAS5023EFIX**, and click **Open**. Click **Next.**
21. Select all available fixes and click **Next**.(see Figure 5-28 on page 179).

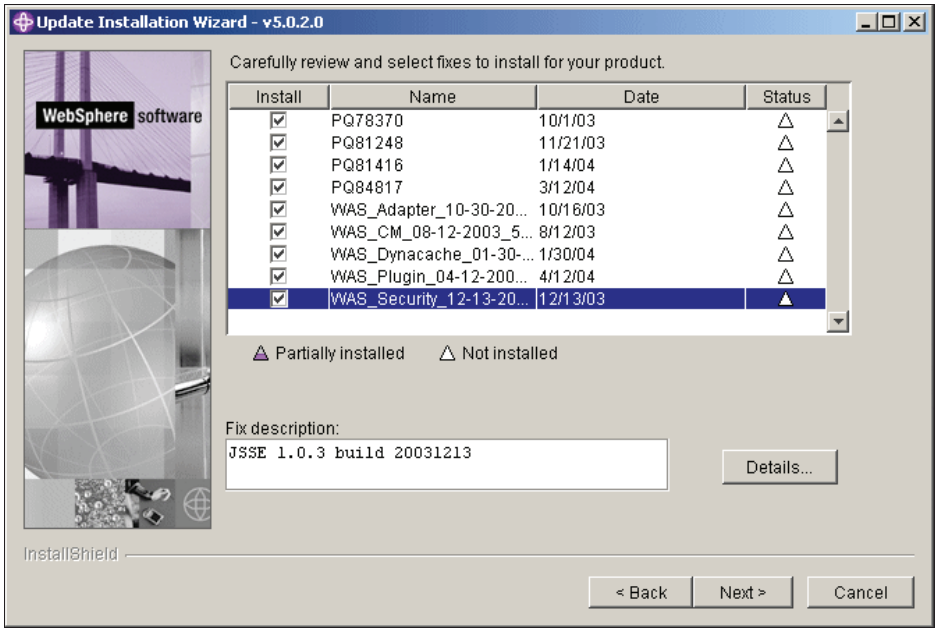

Figure 5-28 Fix Pack selection

22. Review the summary information and click **Next**.
23. The final install panel (see Figure 5-29 on page 180) should display the following message when it is complete:

    `The following fixes were successfully installed:`

    The fixes will appear in the field below the message.

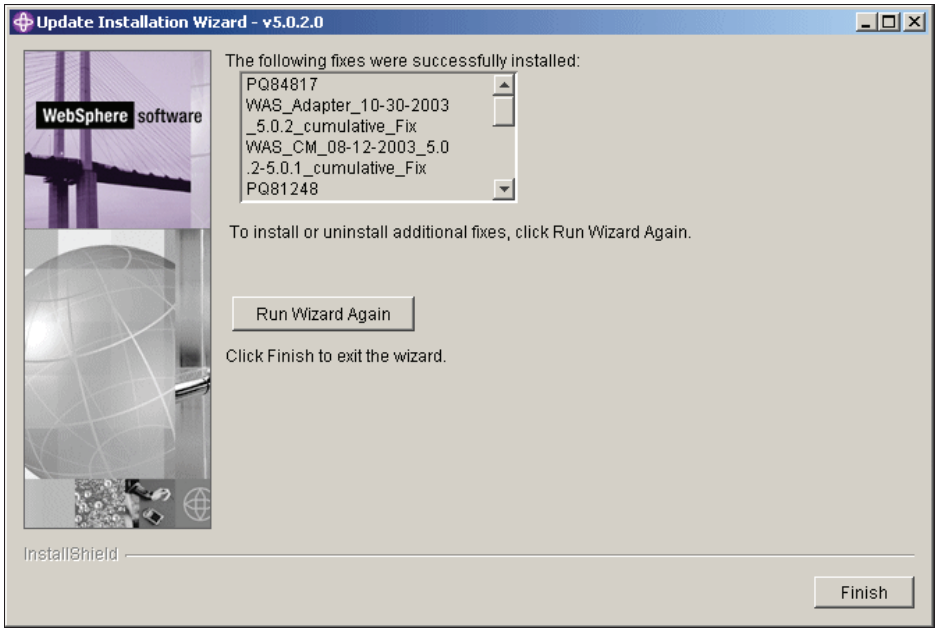

Figure 5-29 Final install panel

24. Click **Finish**.
25. To verify the installation, select **Start** → **Programs** → **IBM WebSphere** → **Application Server V5.0** → **First Steps** and click **Verify Installation**. You should see a message similar to the following:

```
IVTL0070I: IVT Verification Succeeded
IVTL0080I: Installation Verification is complete
```

26. Click **Stop the Server**. After the server stops, click **Exit** to close First Steps.

WebSphere Portal Server Fix Pack installation

1. Open a command prompt, go to *was_home*/bin, and set up the Java environment for the update installer:

```
cd \Program Files\WebSphere\AppServer\bin
setupCmdLine.bat
```

2. Check that all WebSphere Application Server servers are stopped:

```
serverstatus -all
```

3. If they are started, stop them with the **`stopserver`** command from the same directory:

```
stopserver server1
stopserver WebSphere_Portal
```

4. Create an update directory in *wps_home*:

   ```
   mkdir \Program Files\WebSphere\PortalServer\update
   ```

5. Copy the contents of CD 2-3 to *wps_home*/update.
6. Create a fixpacks directory in the update directory:

   ```
   mkdir \Program Files\WebSphere\PortalServer\update\fixpacks
   ```

7. Move WP_PTF_5021.jar and WPCP_PTF_5021.jar, which you previously copied from CD 2-2 to *wps_home*/update, to the *wps_home*/update/fixpacks directory.
8. Edit the soap.client.props file, which is located in *was_home*\properties. Change the timeout request for the Simple Object Access Protocol (SOAP) client. The default, in seconds, is 180. Change the line to:

   ```
   com.ibm.SOAP.requestTimeout=6000
   ```

9. Run the WebSphere Portal update installer to apply the Fix Pack by running the following commands (see Figure 5-30). You have to change the directory to *wps_home*\update:

   ```
   cd C:\Program Files\WebSphere\PortalServer\update
   updatePortal -fixpack -installDir "C:\Program Files\WebSphere\PortalServer"
   -fixpackDir "C:\Program Files\WebSphere\PortalServer\update\fixpacks"
   -install -fixpackID WP_PTF_5021
   ```

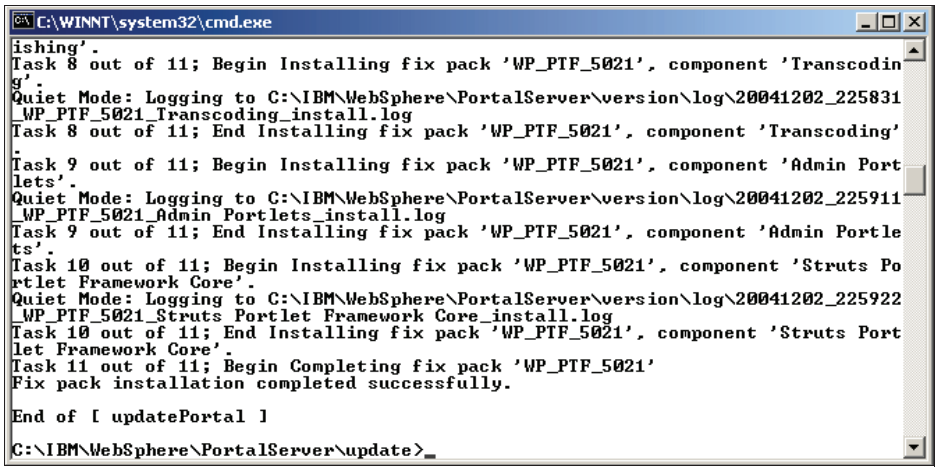

Figure 5-30 WebSphere Portal update installer command

Note: If you receive a message that indicates the *WAS_HOME* is not set, the Java environment might not be properly set.

10. Run the following configuration task (see Figure 5-31):

```
cd C:\program files\WebSphere\PortalServer\config\WPSconfig.bat
WP-PTF-5021 -DPortalAdminPwd=wpstemp
```

```
Select C:\WINNT\system32\cmd.exe

action-start-portal-server-iseries:

start-portal-server:
   [logmsg] 2004.12.03 00:03:10.500 start-portal-server
   [logmsg]   EJPC3060I Starting Server "WebSphere_Portal"

     [exec] ADMU0116I: Tool information is being logged in file
     [exec]            C:\IBM\WebSphere\AppServer\logs\WebSphere_Portal\startSer
ver.log
     [exec] ADMU3100I: Reading configuration for server: WebSphere_Portal
     [exec] ADMU3200I: Server launched. Waiting for initialization status.
     [exec] ADMU3000I: Server WebSphere_Portal open for e-business; process id i
s 1928
     [echo] Executing  WP-PTF-5021 task 33 of 33

action-create-history-event-WP-PTF-5021:
     [echo] Creating history event for config task WP-PTF-5021.
     [copy] Copying 1 file to C:\IBM\WebSphere\PortalServer\version\history

BUILD SUCCESSFUL
Total time: 60 minutes 27 seconds

C:\IBM\WebSphere\PortalServer\config>
C:\IBM\WebSphere\PortalServer\config>_
```

Figure 5-31 Running a configuration task

Note: If the WP-PTF-5021 task fails for some reason, correct the cause of the failure and run the following configuration tasks from the *wps_home*/config directory:

```
WPSconfig.bat UNINSTALL-WP-PTF-5021 -DPortalAdminPwd=wpstemp
```

If the WP-PTF-5021 task failed at task 30 of 33 with the following error, `XMLC0009E: Invalid password for user wpsadmin`, verify the Portal Administrator password and run the WP-PTF-5021 command again with a valid password. You do not need to run the UNINSTALL-WP-PTF-5021 configuration task.

11. Check that all servers are started:

```
cd \program files\websphere\appserver\bin
serverstatus -all
```

12. Check the status of the servers named server1 and WebSphere_Portal.

13. If any of the servers are stopped, start them:

```
startServer.bat server1
startServer.bat WebSphere_Portal
```

14. Open a browser and use the following URL to access the portal, http://*hostname*:9081/wps/portal, where hostname is the machine where we

installed the Portal Server (in our example, wea5d.itso.ral.ibm.com). The portal will open in your browser.

15. Log on to the portal with the administrator ID. In our example, it is wpstemp, with wpstemp as the password.

16. The fix installation is complete. The *wps_home*/update directory is no longer needed and can be deleted.

Configure Portal to use DB2 instead of Cloudscape™

1. Assuming WebSphere Application Server and WebSphere Portal Server are still running and the command prompt is open, go to *wps_home*/config:

```
cd \program files\websphere\portalserver\config
```

2. Export the current database (see Figure 5-32):

```
WPSconfig.bat database-transfer-export
```

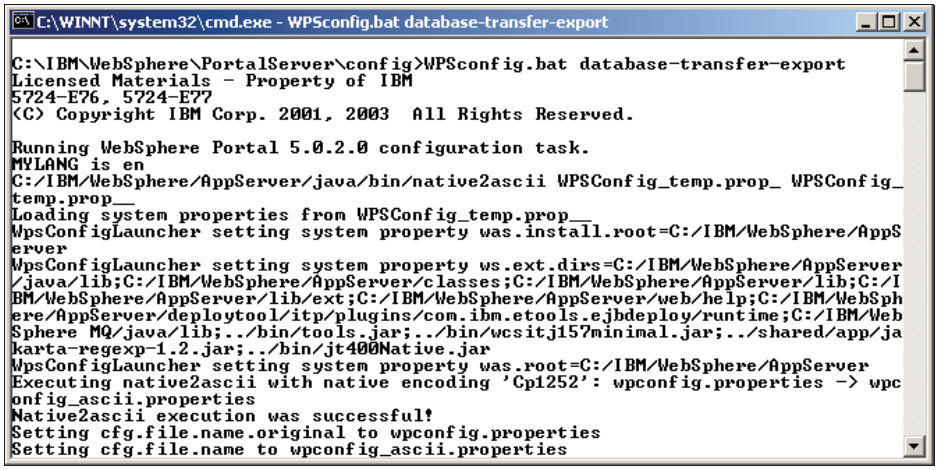

Figure 5-32 Exporting the current database

3. After successfully exporting the database, you should see a `BUILD SUCCESSFUL` message (see Figure 5-33 on page 184).

```
C:\WINNT\system32\cmd.exe
     [exec] Done Exporting DB Item 199
     [exec] Done Exporting DB Item 200
     [exec] Done Exporting DB Item 201
     [exec] Done Exporting DB Item 202
     [exec] Done Exporting DB Item 203
     [exec] Done Exporting DB Item 204
     [exec] Done Exporting DB Item 205
     [exec] Done Exporting DB Item 206
     [exec] Done Exporting DB Item 207
     [exec] Done Exporting DB Item 208
     [exec] Done Exporting DB Item 209
     [exec] Done Exporting DB Item 210
     [exec] Done Exporting DB Item 211
     [exec] Done Exporting DB Item 212
     [exec] Done Exporting DB Item 213
     [exec] Done Exporting DB Item 214
     [exec] Done Exporting DB Item 215
     [exec] Done Exporting DB Item 216
     [exec] Done Exporting DB Item 217
     [exec] Done Exporting DB Item 218

BUILD SUCCESSFUL
Total time: 15 minutes 46 seconds

C:\IBM\WebSphere\PortalServer\config>_
```

Figure 5-33 Current database exported

4. Create a backup copy of *wps_home*/config/wpconfig.properties before changing any values.
5. Create a backup copy of *wps_home*/config/helpers/transfer_db2.properties.
6. Edit *wps_home*/config/helpers/transfer_db2.properties (Table 5-33 shows the values).

Note: If you need explanations of what each property is used for, take a look in the configuration file or look in the InfoCenter, which can be installed from the setup CD.

Be sure to use / (slash) instead of \ (backslash).

If there are two values, the first is generic and the second is one we use in our example environment.

The user we are using is a local user that needs admin access to DB2. It is not an user in the Domino directory!

Table 5-33 Properties

Field	Value
DbSafeMode	false
DbType	db2
DbDriver	COM.ibm.db2.jdbc.app.DB2Driver

Field	Value
DbDriverDS	COM.ibm.db2.jdbc.DB2XADataSource
DbLibrary	*DB2_Home*/java/db2java.zip c:/program files/IBM/SQLLIB/java/db2java.zip
WpsDbName	wps50
DbUrl	jdbc:db2:*WpsDbName* jdbc:db2:wps50
DbUser	weaadmin
DbPassword	lpuwea
WmmDbName	wps50
WmmDbUrl	dbc:db2:*WmmDbName* jdbc:db2:wps50
WmmDbUser	weaadmin
WmmDbPassword	lpuwea
WpcpDbName	wpcp50
WpcpDbUrl	dbc:db2:*WpcpDbName* jdbc:db2:wpcp50
WpcpDbUser	weaadmin
WpcpDbPassword	lpuwea
FeedbackDbName	fdbk50
FeedbackDbUrl	dbc:db2:*FeedbackDbName* jdbc:db2:fdbk50
FeedbackDbUser	weaadmin
FeedbackDbPassword	lpuwea

7. Save the file.
8. Enter the following into the command prompt to import the transfer_db2.properties values into the wpsconfig.properties file (see Figure 5-34 on page 186):

```
WPSconfig -DparentProperties="full_path_to_transfer_db2.properties"
-DSaveParentProperties=true
```

In our example, it is:

```
WPSconfig -DparentProperties="c:\program
files\websphere\portalserver\config\helpers\transfer_db2.properties"
-DSaveParentProperties=true
```

```
C:\WINNT\system32\cmd.exe
Storing DbUrl=jdbc:db2:wps50
Storing DbUser=db2admin
Storing DbPassword=db2admin
Storing DbLibrary=c:/IBM/sqllib/java/db2java.zip
Storing WpsXDbName=wps5TCP
Storing WpsDbNode=wpsNode
Storing WpcpDbNode=wpcpNode
Storing WpcpXDbName=wpcp5TCP
Storing FeedbackXDbName=fdbk5TCP
Storing WpcpDbName=wpcp50
Storing WpcpDbUser=db2admin
Storing WpcpDbPassword=db2admin
Storing WpcpDbUrl=jdbc:db2:wpcp50
Storing FeedbackDbName=fdbk50
Storing FeedbackDbUser=db2admin
Storing FeedbackDbPassword=db2admin
Storing FeedbackDbUrl=jdbc:db2:fdbk50
Storing WmmDbName=wps50
Storing WmmDbUser=db2admin
Storing WmmDbPassword=db2admin
Storing WmmDbUrl=jdbc:db2:wps50
Successfully copied properties to C:\IBM\WebSphere\PortalServer\config\wpconfig.
properties

C:\IBM\WebSphere\PortalServer\config>_
```

Figure 5-34 Importing properties

9. From *wps_home*/config, enter the following command:

   ```
   WPSconfig.bat create-local-database-db2
   ```

   You should see a `BUILD SUCCESSFUL` message (see Figure 5-35).

```
C:\WINNT\system32\cmd.exe
sfully.

     [exec] UPDATE DATABASE CONFIGURATION FOR wps50 USING LOGSECOND 10
     [exec] DB20000I  The UPDATE DATABASE CONFIGURATION command completed succes
sfully.

   [logmsg] 2004.12.03 01:11:29.891 action-create-wps-db-mp
   [logmsg]   EJPC3003I Database "wps50" created


action-create-wps-db-iseries:

action-switch-database:

action-check-wps-wmm-dbname:
[checkwpswmmdbname] The WMM database will not be created because 'WpsDbName' and
 'WmmDbName' are identical.
[checkwpswmmdbname] Property isWpsDbNameDifferentWmmDbName was set to 'false'.

create-wmm-db:

BUILD SUCCESSFUL
Total time: 4 minutes 19 seconds

C:\IBM\WebSphere\PortalServer\config>_
```

Figure 5-35 Importing properties

10. Enter the following commands to validate configuration properties:

```
WPSconfig.bat validate-database-connection-wps -DDbPassword=lpuwea
WPSconfig.bat validate-database-connection-wmm -DWmmDbPassword=lpuwea
WPSconfig.bat validate-database-connection-wpcp -DWpcpDbPassword=lpuwea
-DFeedbackDbPassword=lpuwea
WPSconfig.bat validate-database-driver
```

11. Enter the following commands to run the configuration task:

```
WPSconfig.bat database-transfer-import
```

12. You should see a `BUILD SUCCESSFUL` message. If the configuration fails, verify the values in the wpconfig.properties file and then repeat this step.

13. Open the DB2 Command Line Processor by selecting **Start** → **Programs** → **IBM DB2** → **Command Line Tools** → **Command Line Processor**.

14. For the databases created by the script (in our example, wps50, wpcp50, and fdbk50), run the following commands:

```
connect to wps50 user weaadmin using lpuwea
reorgchk update statistics on table all
terminate
db2rbind wps50 -l db2rbind.out -u weaadmin -p lpuwea

db2
connect to wpcp50 user weaadmin using lpuwea
reorgchk update statistics on table all
terminate
db2rbind wpcp50 -l db2rbind.out -u weaadmin -p lpuwea

db2
connect to fdbk50 user weaadmin using lpuwea
reorgchk update statistics on table all
terminate
db2rbind fdbk50 -l db2rbind.out -u weaadmin -p lpuwea
```

Note: If you used other user names or passwords for the databases during the creation of the databases in step 6, you must modify these commands to match your user names and passwords.

15. Add db2java.zip to the class path information in WebSphere Application Server. Perform the following steps to add the required DB2 JDBC provider files to the WebSphere Application Server class path:

    a. Assuming the WebSphere Application Server is still running, open the Administrative Console by accessing the following URL in a browser:

    ```
    http://hostname.yourco.com:9090/admin
    ```

In our example, it is:

```
http://wea5d.itso.ral.ibm.com:9090/admin
```

b. Because we did not enable security yet, you can use any user name to log on to the Administrative Console.

c. After logging in, select **Servers** → **Application Servers** and then click **WebSphere_Portal** from the list of application servers.

d. Select **Process Definition** from the list of additional properties, and then select **Java Virtual Machine** from the list of additional properties.

e. In the Classpath field, add the directory path where the db2java.zip file is located, for our example, C:/PROGRA~1/IBM/SQLLIB/java/db2java.zip.

f. Click **OK**.

g. Click the **Save** link to go to the Save page.

h. Click **Save**.

16. Change to the directory *was_home*/bin. Start the WebSphere Portal Server:

```
cd \program files\websphere\appserver\bin
startserver WebSphere_Portal
```

17. To verify this configuration, point your browser to the portal, for example:

```
http://wea5d.itso.ral.ibm.com:9081/wps/portal
```

18. Log on and go to **Content Publishing**.

Tune DB2 for the portal

Open a DB2 Command window by selecting **Start** → **Programs** → **IBM DB2** → **Command Line Tools** → **Command Window** and run the following commands:

```
db2set DB2_EVALUNCOMMITTED=YES
db2set DB2_INLIST_TO_NLJN=YES

db2
connect to wpcp50 user weaadmin using lpuwea
update db cfg for wpcp50 using locklist 1024
connect reset

connect to wps50 user weaadmin using lpuwea
CREATE INDEX weaadmin.IX2110D ON weaadmin.PROT_RES (PARENT_OID,OID)
CREATE INDEX weaadmin.IX2140B ON weaadmin.LNK_USER_ROLE (ROLE_INST_OID)
commit
connect reset
quit
```

Note: If you used other user names or passwords for the databases during the creation of the databases, you must modify these commands to match your user names and passwords! If you choose other names for the WebSphere Portal Server database or the WebSphere Portal Content Publishing database, use your names instead!

Configure Portal for Lotus Domino Directory

1. Create a backup copy of *wps_home*/config/wpconfig.properties before changing any values.
2. Create a backup copy of *wps_home*/config/helpers/security_domino.properties.
3. Edit *wps_home*/config/helpers/security_domino.properties (use the values in Table 5-34).

Note: If you need explanations of what each property is used for, take a look in the configuration file or look in the InfoCenter, which can be installed from the setup CD.

Users who are used in this configuration file are users in the Domino directory.

Table 5-34 Properties

Field	Value
WasUserid	cn=wpsbind,o=ITSORaleigh
WasPassword	wpsbind
WpsHostName	wea5d.itso.ral.ibm.com
PortalAdminId	cn=weaadmin,o=ITSORaleigh
PortalAdminIdShort	weaadmin
PortalAdminPwd	weaadmin
PortalAdminGroupId	cn=wpsadmins
PortalAdminGroupIdShort	wpsadmin
LTPAPassword	passw0rd
LTPATimeout	120
SSODomainName	itso.ral.ibm.com
LookAside	false

Field	Value
LDAPHostName	wea5e.itso.ral.ibm.com
LDAPPort	389
LDAPAdminUId	cn=admin,o=ITSORaleigh
LDAPAdminPwd	dbnadm
LDAPServerType	DOMINO502
LDAPBindID	cn=wpsbind,o=ITSORaleigh
LDAPBindPassword	wpsbind
LDAPSuffix	
LdapUserPrefix	cn
LdapUserSuffix	o=ITSORaleigh
LdapGroupPrefix	cn
LdapGroupSuffix	
LDAPUserObjectClass	dominoPerson
LDAPGroupObjectClass	dominoGroup
LDAPGroupMember	member
LDAPUserFilter	(&(|(cn=%v)(uid=%v))(objectclass=dominoPerson))
LDAPGroupFilter	(&(cn=%v)(|(objectclass=dominoGroup)(objectclass=groupOfUniqueNames)))
LDAPsslEnabled	false

4. Save the file.
5. Assuming the command prompt is still open, point it to *was_home*/bin and check that the WebSphere Application Server is started and the WebSphere Portal Server is stopped:

   ```
   cd \program files\websphere\appserver\bin
   serverstatus -all
   ```

6. If the WebSphere Portal Server is started, stop it:

   ```
   stopserver WebSphere_Portal
   ```

7. If the WebSphere Application Server is stopped, start it:

   ```
   startserver server1
   ```

8. Change to the directory *wps_home*/config.
9. Enter the following command to Import the contents of security_domino.properties into WPSconfig.properties (see Figure 5-36):

   ```
   WPSconfig -DparentProperties="full_path_to_security_domino.properties"
   -DSaveParentProperties=true
   ```

   For our example, it is:

   ```
   WPSconfig -DparentProperties="c:\program
   files\websphere\portalserver\config\helpers\security_domino.properties"
   -DSaveParentProperties=true
   ```

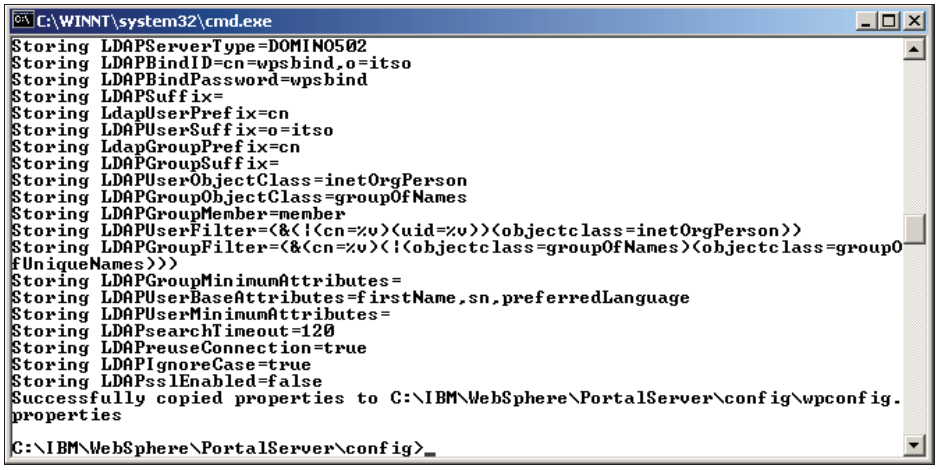

Figure 5-36 Importing properties

10. Enter the following command to validate the settings to access LDAP:

    ```
    WPSconfig.bat validate-ldap
    ```

    If this task fails, check the values in the wpconfig.properties file (see Figure 5-37 on page 192). Check also that the LDAP directory is up and running.

```
C:\WINNT\system32\cmd.exe
[ldapcheck] ##################################################################

action-validate-ldap-portal-admin-group:
[ldapcheck] ##################################################################
[ldapcheck] ldapURL         : domino.itso.ral.ibm.com:389
[ldapcheck] ldapUser        : cn=wpsadmin,o=itso
[ldapcheck] ldapPassword    : *
[ldapcheck] ldapSslEnabled  : false
[ldapcheck] objectDn        : cn=wpsadmins
[ldapcheck] ##################################################################
[ldapcheck] Checking for 'cn=wpsadmins'
[ldapcheck] ##################################################################

action-validate-ldap-bind-user:
[ldapcheck] ##################################################################
[ldapcheck] ldapURL         : domino.itso.ral.ibm.com:389
[ldapcheck] ldapUser        : cn=wpsbind,o=itso
[ldapcheck] ldapPassword    : *
[ldapcheck] ldapSslEnabled  : false
[ldapcheck] ##################################################################

BUILD SUCCESSFUL
Total time: 11 seconds

C:\IBM\WebSphere\PortalServer\config>_
```

Figure 5-37 Validating settings to access LDAP

11. Enter the appropriate command to run the configuration task:

    `WPSconfig.bat enable-security-ldap`

    If the configuration task fails, verify the values in the wpconfig.properties file. Before running the task again, be sure to stop the WebSphere Portal application server by entering the following command from the *was_home*/bin directory and specify the WebSphere Application Server user ID and password (as defined by the WasUserid and WasPassword properties):

    `stopserver WebSphere_Portal -user wpsbind -password wpsbind`

12. Change to directory *was_home*/bin, and enter the following command:

    `stopServer.bat server1 -user wpsbind -password wpsbind`

13. To allow users or portal administrators to create and modify directory attributes through self-registration and self-care screens or the Manage Users and Groups portlet, perform the following steps:

    a. Open the PumaService.properties file. You can find this file in the *wps_home*/shared/app/config/services directory.

    b. Add `user.sync.remove.attributes=cn,CN`.

    c. Save the file.

Note: If you do not perform these steps, WebSphere Portal will not be able to create or update a user by using portal functions because it is misconfigured.

14. Start the Application Server and the portal server:

```
startServer.bat server1
startServer.bat WebSphere_Portal
```

15. Log in to the WebSphere Application Server Administrative Console with the administrative user ID you created in the Domino, in our example, wpsbind. Select **Start** → **Programs** → **IBM WebSphere** → **Application Server v5.0** → **Administrative console**.
16. Select **Security** → **User Registry** → **LDAP** and select **Advanced LDAP Settings**.
17. Change User ID Map to `person:shortname;*:cn`.
18. Click **OK**.
19. Select **Save** and save the configuration changes.
20. Restart server1 and WebSphere_Portal.
21. To verify the configuration, open a browser and access WebSphere Portal (http:// hostname.yourco.com: port_number/wps/portal). Verify that you can log in. In our scenario, the URL is http://wea5d.itso.ral.ibm.com:9081/wps/portal.

Update WebSphere Member Manager for Domino Directory

1. Make a copy of *wps_home*\shared\app\wmm\wmm.xml.
2. Edit *wps_home*\shared\app\wmm\wmm.xml.
3. Find the wmmGenerateExtID property in the file and verify it is set to `true`. For example:

```
wmmGenerateExtID="true"
```

4. Look for the tag `<supportedLdapEntryTypes>` and modify each "objectClassesForWrite" adding, at the end, `ibm-appUUIDAux` (four times).

```
objectClassesForWrite="dominoPerson;ibm-appUUIDAux"
searchBases="o=ITSORaleigh"/>

objectClassesForWrite="dominoGroup;ibm-appUUIDAux" searchBases=""/>

objectClassesForWrite="organization;ibm-appUUIDAux" />

objectClassesForWrite="organizationalUnit;ibm-appUUIDAux" />
```

5. Make a copy of *wps_home*\config\templates\wmm\wmmLDAPAttributes_DOMINO502.xml.
6. Edit *wps_home*\config\templates\wmm\wmmLDAPAttributes_DOMINO502.xml.

Inside that file, look for wmmAttributeName=”extId”. There is a parameter that reads “`pluginAttributeName="distinguishedName"`, which should be changed to:

```
pluginAttributeName="ibm-appUUID"
```

7. Make a copy of *wps_home*\wmm\wmmLDAPServerAttributes.xml.
8. Edit *wps_home*\wmm\wmmLDAPServerAttributes.xml. Map `extId` to `ibm-appUUID`. To do that, change the line

   ```
   pluginAttributeName="distinguishedName"
   ```

   to

   ```
   pluginAttributeName="ibm-appUUID"
   ```

9. Restart the Domino Server.

Note: If you do not restart the Domino Server, you might not be able to log in to the portal.

Configure WebSphere Portal Server for IBM HTTP Server

1. Create a backup copy of *wps_home*/config/wpconfig.properties before changing any values.
2. Create a backup copy of *wps_home*/config/helpers/config_http.properties.
3. Check that *wps_home*/config/helpers/config_http.properties contains your machine host name and fully qualified domain name, as well as port 80 as your HTTP port (see Table 5-35).

Table 5-35 WebSphere Portal

Field	Value
WpsHostName	wea5d.itso.ral.ibm.com
WpsHostPort	80

4. Save the file.
5. Open a command prompt and change the directory to the *wps_root*/config directory.
6. Enter the following into the command prompt to import the config_http.properties content into wpsconfig.properties:

   ```
   WPSconfig -DparentProperties="full_path_to_helper_file"
   -DSaveParentProperties=true
   ```

In our example, it is:

```
WPSconfig -DparentProperties="c:\program
files\websphere\portalserver\config\helpers\config_http.properties"
-DSaveParentProperties=true
```

7. Enter the following command to configure WebSphere Portal for the Web server:

```
WPSconfig.bat httpserver-config
```

8. Restart both Web servers by selecting **Start** → **Settings** → **Control Panel** → **Administrative Tools** → **Services** and stop (if they are running) and start IBM HTTP Administration V1.3.26 and IBM HTTP Server V1.3.26.
9. Restart WebSphere Portal by entering the following commands from the *was_root*/bin directory:

```
stopServer WebSphere_Portal -user wpsbind -password wpsbind
startServer WebSphere_Portal
```

10. Verify that the portal can be accessed from the local Web server. For example, open a browser to:

```
http://wea5d.itso.ral.ibm.com/wps/portal
```

Install Everyplace Access Services

1. Assuming the WebSphere Everyplace Access install program is still open, choose **Everyplace Access Services V5.0** and click **Next** (see Figure 5-38 on page 196).

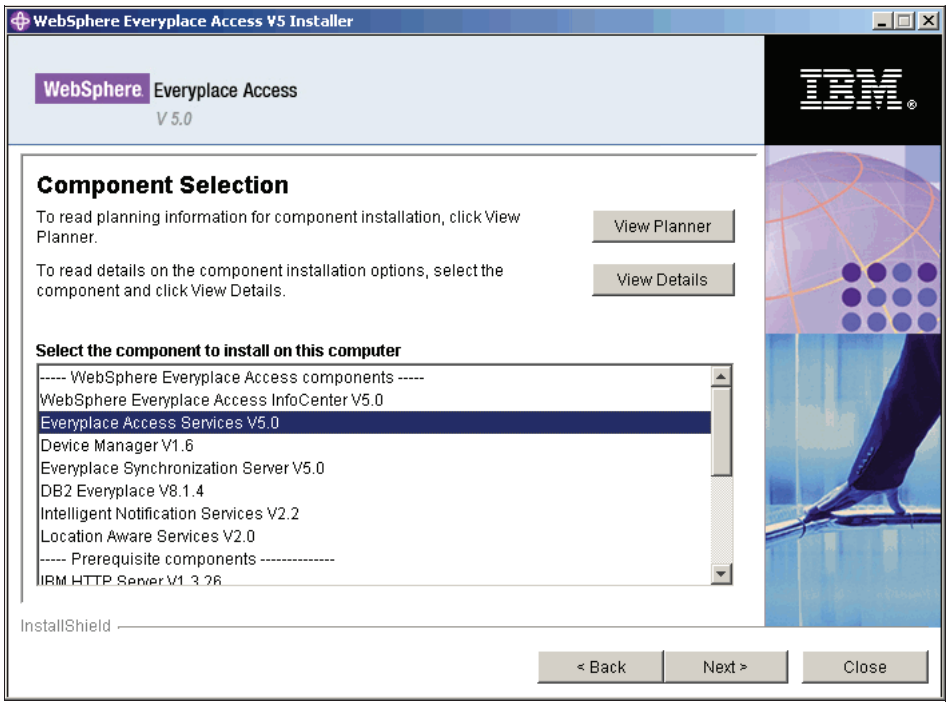

Figure 5-38 Component selection: Everyplace Access Services

2. Insert the CD when prompted and click **Next**.
3. Select **English** as the language and click **OK**.
4. Click **Next** on the welcome panel.
5. Specify the installation directory for Everyplace Access Services and click **Next** (see Table 5-36).

Table 5-36 Everyplace Access Services directory

Field	Value
Directory	C:\Program Files\WebSphere\EAS

6. Review the summary information to validate the install directory and click **Next** to start copying files.
7. After the install finishes, a panel displays information about the success of the install. Click **Finish**.

Configure Everyplace Access Services

1. Check that all WebSphere Application Server servers are running:

   ```
   serverstatus -all -username wpsbind -password wpsbind
   ```

2. If they are stopped, start them with the **startserver** command from the same directory:

   ```
   startserver server1
   startserver WebSphere_Portal
   ```

3. Make sure the database server and the directory server is running.
4. Verify that security is enabled for the portal and application server. To verify that security is enabled, attempt to log in to the WebSphere Application Server Administrative Console. If you are challenged to provide a user ID and password, security is enabled. If you are only prompted for a user name, security is not enabled.
5. Make a copy of *eas_home*\config\EASinstallconfig.properties.
6. Edit *eas_home*\config\EASinstallconfig.properties, where eas_home is the directory you specified during the installation (see Table 5-37). In our example it is C:\Program Files\WebSphere\EAS.

Note: If you need explanations of what each property is used for, take a look in the configuration file or look in the InfoCenter, which can be installed from the setup CD.

Be sure to use / (slash) instead of \ (backslash).

The user weaadmin for the database is a user of the local system. All other users are users in the Domino directory.

Table 5-37 Properties

Field	Value
instServerInstall	true
instDatabaseInstall	true
instPortalIntegration	true
instNotesPortlets	true
instExchangePortlets	false
instDMS	true
instBlackberry	false

Field	Value
instWPSInstallLocation	C:/Program Files/WebSphere/PortalServer
instWPSHostname	wea5d.itso.ral.ibm.com
instWPSHome	/portal
instWPSCustomPage	/myportal
instWPSBaseURL	/wps
instWPSAdminName	weaadmin
instWPSAdminPassword	weaadmin
instWPSPort	80
instWASInstallationLocation	C:/Program Files/WebSphere/AppServer
instWASAdminNode	wea5d
instWASAdminCell	wea5d
instWASUsername	wpsbind
instWASPassword	wpsbind
instWASHostName	wea5d.itso.ral.ibm.com
instDBDatasourceHelper	com.ibm.websphere.rsadapter.DB2DataStoreHelper
instDBType	db2
instDBPath	C:/Program Files/IBM/SQLLIB
instDBAdminName	weaadmin
instDAdminPassword	lpuwea
instJDBCDriverName	com.ibm.db2.jdbc.app.DB2Driver
instJDBCImplementationClass name	COM.ibm.db2.jdbc.DB2ConnectionPoolDataSource
InstJDBCDriverPath	C:/Program Files/IBM/SQLLIB/java/db2java
instDBServerHostname	wea5d.itso.ral.ibm.com
instDBLocalInstance	DB2
instWEASDB	WEASDB
instDMS_DMSServerName	wea5d.itso.ral.ibm.com

Field	Value
instDMS_DMSAdminGroup	dmadmins

7. Save the EASinstallconfig.properties file.
8. Run the following command to configure all components:

   ```
   cd C:\Program Files\WebSphere\EAS\config\EASWASconfig.bat eas-basic-config
   ```

9. If the configuration fails, correct the problem and run the configuration task again.
10. Log in to the WebSphere Everyplace Access portal as an administrator and verify that the new WebSphere Everyplace Access theme and “look and feel” has been applied.

Install Device Manager

1. Assuming that the WebSphere Everyplace Access install program is still open, choose **Device Manager V1.6** and click **Next** (see Figure 5-39).

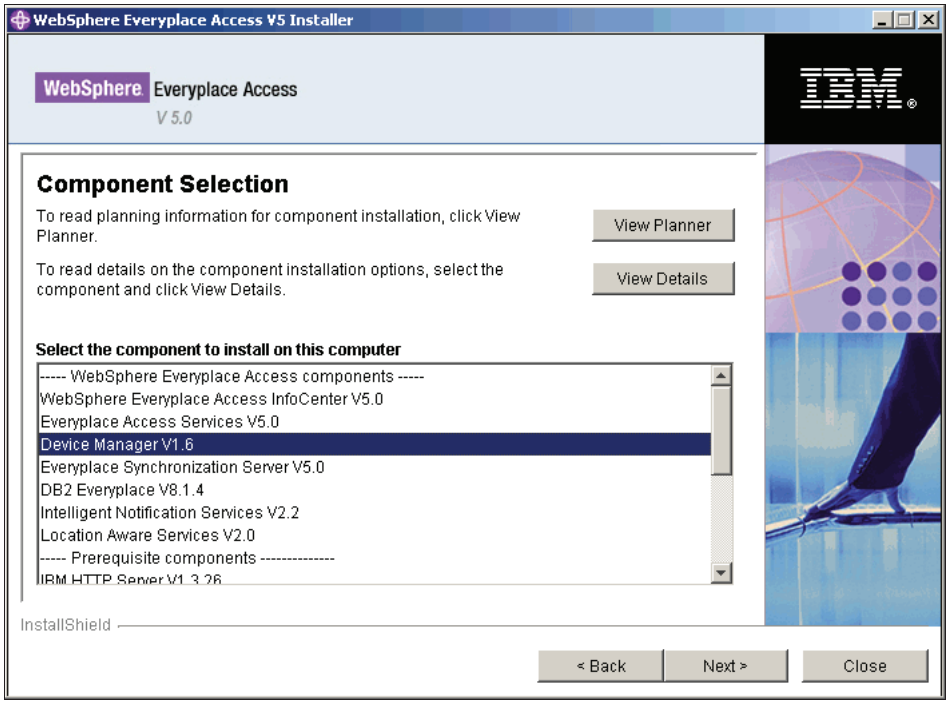

Figure 5-39 Component selection: Device Manager

2. Insert the CD when prompted and click **Next**.

3. Select **English** as the language and click **OK**.
4. Click **Next** on the welcome panel.
5. Specify the installation directory for Device Manager and click **Next** (see Table 5-38).

Table 5-38 Device Manager installation directory

Field	Value
Directory	C:\Program Files\WebSphere\DMS16

6. Select **Device Manager Server** and **Device Manager database**. Click **Next**.
7. Review the summary information and click **Next** to start copying files.
8. After the install finishes, a panel displays information about the success of the install. Click **Finish** to exit the Device Manager install program.

If an error occurs when the files are installed, the installation stops. For example, if the prerequisite check for the operating system recognizes that a prerequisite is not supported, an error message is displayed and the installation stops.

When the installation stops, the rollback feature of the installation removes the partially installed set of files and returns the computer to its original state.

Configure Device Manager

1. Check that all WebSphere Application Server servers are running:

```
serverstatus -all -user wpsbind -password wpsbind
```

2. If they are stopped, start them with the **`startserver`** command from the same directory:

```
startserver server1
startserver WebSphere_Portal
```

3. Make a copy of *dms_home*\config\DMSinstallconfig.properties, where dms_home is the directory you specified during the installation. In our example, it is C:\Program Files\WebSphere\DMS16.
4. Edit *dms_home*\config\DMSinstallconfig.properties (see Table 5-39 on page 201).

Note: If you need explanations of what each property is used for, take a look at the configuration file or look in the InfoCenter, which can be installed from the setup CD.

Be sure to use / (slash) instead of \ (backslash).

The user weaadmin for the database is an user of the local system. All other users are users in the Domino directory.

Table 5-39 Properties

Field	Value
instDBType	db2
instDBPath	C:/Program Files/IBM/SQLLIB
instDBUserId	weaadmin
instDBPassword	lpuwea
instDBName	dms
instDBInstance	db2
instDBDropFlag	false
instDBAdmin	db2admin
instDBAdminPassword	lpudbase
instDBHome	C
instDBFiles	C:/Program Files/WebSphere/DMS16/dmsdb
instJavapath	C:/Program Files/WebSphere/DMS16/Java/win/jre
instWASPath	C:/Program Files/WebSphere/AppServer
instNode	wea5d
instHostName	wea5d.itso.ral.ibm.com
instWASUsername	wpsbind
instWASPassword	wpsbind
instRemoteWebServer	false
instWebServerHome	C:/Program Files/IBMHttpServer

Field	Value
instWPSHttpRouter	http://wea5d.itso.ral.ibm.com/UserGroupInfoWebService/servlet/rpcrouter
instWPSHttpAltRouter	http://wea5d.itso.ral.ibm.com/UserGroupInfoWebServiceAlt/servlet/rpcrouter
instWPSUserName	weaadmin
instWPSUserPw	weaadmin
instDMAdminGroup	dmadmins
instRemoteDB	false

5. Save the DMSinstallconfig.properties file.
6. Run the command to configure all components:

```
cd c:\Program Files\WebSphere\DMS16\config\DMSconfig.bat
```

If an error occurs when the properties file is run with the command, the configuration stops. Messages are written to the dms_config.log file. For example, if a value for a property is not valid, an error message is displayed and the configuration stops. Fix the error and run the configuration command again.

When the configuration command to implement the values in the properties file is run, the previous configuration values are preserved. If an error occurs, the new values are ignored and the values are rolled back to the preserved values.

7. To test your database connection, select **Start** → **Programs** → **IBM DB2** → **Command Line tools** → **Command Line Processor** and try to connect to the new database:

   ```
   connect to dms user weaadmin using lpuwea
   ```

   If the connection goes well, type `quit`.

Install Everyplace Synchronization Server

1. Assuming the WebSphere Everyplace Access install program is still open, choose **Everyplace Synchronization Server** and click **Next** (see Figure 5-40 on page 203).

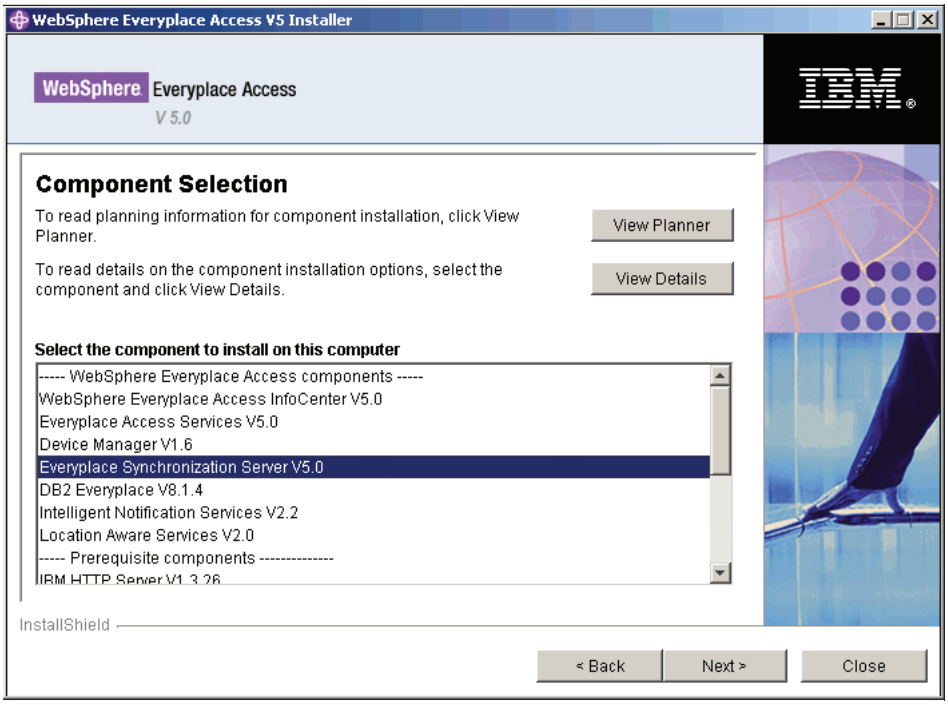

Figure 5-40 Component selection: Everyplace Synchronization Server

2. Insert the CD when prompted and click **Next**.
3. Select **English** as the language and click **OK**.
4. Click **Next** on the welcome panel.
5. Specify the installation directory for Everyplace Synchronization Server and click **Next** (see Table 5-40).

Table 5-40 Everyplace Synchronization Server install directory

Field	Value
Directory	C:\Program Files\WebSphere\IBMSyncServer

6. Review the summary information to validate the install directory and click **Next** to start copying files.
7. After the install finishes, a panel displays information about the success of the install. Click **Finish**.

Configure Everyplace Synchronization Server

1. Check that all WebSphere Application Server servers are running:

   ```
   serverstatus -all -user wpsbind -password wpsbind
   ```

2. If they are stopped, start them with the **startserver** command from the same directory:

   ```
   startserver server1
   startserver WebSphere_Portal
   ```

3. Make sure the database server and the directory server is running.
4. Make a copy of *ess_home*\config\ESSinstallconfig.properties, where ess_home is the directory you specified during the installation. In our example, it is C:\Program Files\WebSphere\IBMSyncServer.
5. Edit *ess_home*\config\ESSinstallconfig.properties (see Table 5-41).

Note: If you need explanations of what each property is used for, take a look at the configuration file or look in the InfoCenter, which can be installed from the setup CD.

Be sure to use / (slash) instead of \ (backslash).

The user weaadmin for the database is an user of the local system. The user essadmin will be created on the local system. wpsbind is a user in the Domino directory.

Table 5-41 Properties

Field	Value
instPath	C:/Program Files/WebSphere/IBMSyncServer
instDatabaseInstall	true
instServerInstall	true
instPortletsInstall	true
instDBType	db2
instDBUserid	essadmin Note: The configuration script will create this user ID. It must be eight characters and must not begin with ibm, sys, or sql.
instDBPassword	lpuess
instDBPath	C:/Program Files/IBM/SQLLIB

Field	Value
instDBURL	jdbc:db2:
instDBDriver	com.ibm.db2.jcc.DB2Driver
instDBLibPath	C:/Program Files/IBM/SQLLIB/java/db2java.zip;C:/Program Files/IBM/SQLLIB/java/db2jcc.jar;C:/Program Files/IBM/SQLLIB/java/db2jcc_license_cu.jar
instDBHostName	wea5d.itso.ral.ibm.com
instDBDropFlag	true
instDBPort	50000
instCell	wea5d
instNode	wea5d
instWASUserName	wpsbind
instWASPassword	wpsbind
instWPSHost	wea5d.itso.ral.ibm.com
instWPSHome	/portal
instWPSPath	C:/Program Files/WebSphere/PortalServer
instWPSUrlPrefix	/wps
instWPSUsername	weaadmin
instWPSPassword	weaadmin
instWPSPort	80
instWPSAdminGroup	wpsadmins
instUserGroup1	essusers
instNonLockUserGroup	essuers_nonlock
instAdminGroup1	essadmins
instESSAdmin1	weaadmin
instESSAdminPwd1	weaadmin
instESSAdmin2	
instESSAdminPwd2	

Field	Value
instJavaPath	C:/Program Files/WebSphere/IBMSyncServer/java/jre
instWASPath	C:/Program Files/WebSphere/AppServer
instHttpServerPath	C:/Program Files/IBMHttpServer
instInfoLocale	en
instBackendDomino	true
instBackendExch2000	false
instBackendExch55	false
instDominoDataRoot	C:/Program Files/WebSphere/IBMSyncServer/NotesData
instNotesDataPath	C:/Program Files/WebSphere/IBMSyncServer/NotesData
instNotesPath	C:/Program Files/Lotus/Notes
instDominoHost	wea5e.itso.ral.ibm.com
instDominoUserID	essadmin
instDominoPassword	dpessadm
instDominoAbbreviatedServername	wea5e/ITSORaleigh
instContextRoot	/ess
instESSAdminRMIPort	20000
instDBDefaultDB2	weaadmin
instUseExistingDBInstance	false

6. Save the ESSinstallconfig.properties file.
7. In a command window, go to *ess_home*/config and begin the configuration:

```
cd \Program Files\WebSphere\IBMSyncServer\config
ESSWASconfig.bat basic-config
```

8. After finishing the configuration, you should see a `BUILD SUCCESSFUL` message.

After installing and configuring the Everyplace Synchronization Server, you should set the DB2 service to start automatically. By default, it is set to manual. To set the DB2 service to start automatically, perform the following steps:

1. Select **Start** → **Settings** → **Control Panel** → **Administrative Tools** → **Services**.
2. Look for a service called DB2-*essname*, where essname is the name you choose during the configuration in the instDBUserid field. In our example, the name is essadmin, so the service is called DB2-essadmin.
3. Right-click the selected service and choose **Properties**.
4. Change the Startup type to **Automatic** and click **OK**.
5. Start DB2-*essname*.

Install Intelligent Notification Services

1. Assuming the WebSphere Everyplace Access install program is still open, choose **Intelligent Notification Services** and click **Next** (see Figure 5-41).

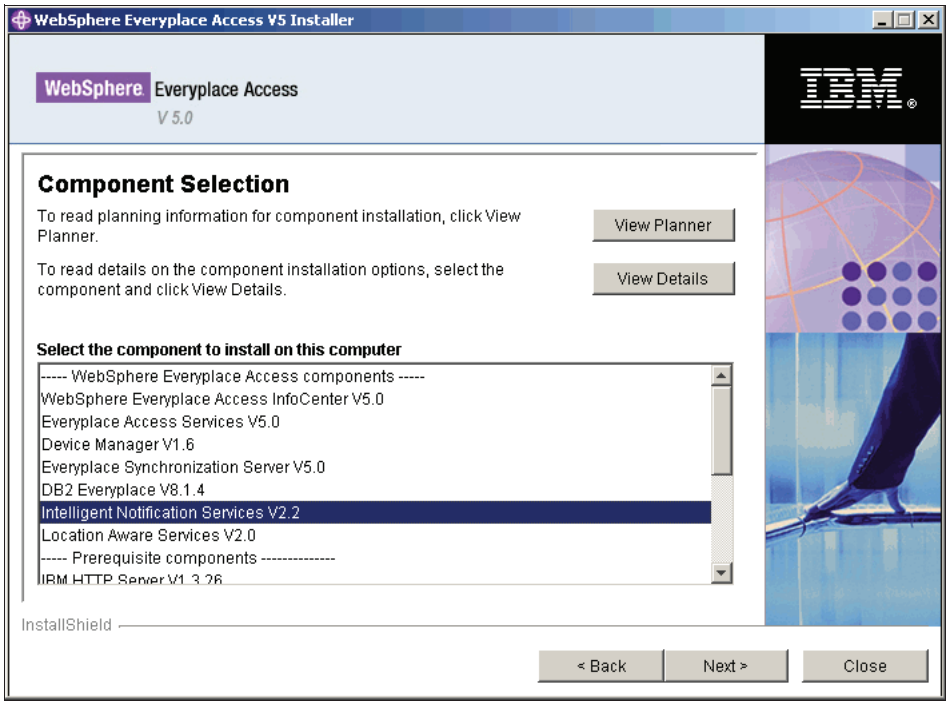

Figure 5-41 Component selection: Intelligent Notification Services

2. Insert the CD when prompted and click **Next**.

3. Select **English** as the language and click **OK**.
4. Click **Next** on the welcome panel.
5. Specify the installation directory for Intelligent Notification Services and click **Next** (see Table 5-42).

Table 5-42 Intelligent Notification Services install directory

Field	Value
Directory	C:\Program Files\WebSphere\INS

6. Review the summary information to validate the install directory and click **Next** to start copying files.
7. After the install finishes, a panel displays information about the success of the install. Click **Finish**.

Configure Intelligent Notification Services

1. Check that all WebSphere Application Server servers are running:

   ```
   serverstatus -all
   ```

2. If they are stopped, start them with the **`startserver`** command from the same directory:

   ```
   startserver server1
   startserver WebSphere_Portal
   ```

3. Make sure the database server and the directory server is running.
4. Make a copy of *ins_home*\config\INSinstallconfig.properties, where ins_home is the directory you specified during the installation. In our example, it is C:\Program Files\WebSphere\INS.
5. Edit *ins_home*\config\INSinstallconfig.properties (see Table 5-43 on page 209 for the values).

Note: If you need explanations of what each property is used for, take a look at the configuration file or look in the InfoCenter, which can be installed from the setup CD.

Be sure to use / (slash) instead of \ (backslash).

The user weaadmin for the database is an user of the local system. All other users are users in the Domino directory.

Table 5-43 Properties

Field	Value
instNMConfig	true
instSMConfig	true
instMCSConfig	true
instMCSDomino	true
instDatabaseConfig	true
instPortletsConfig	true
instNode	wea5d
instWASPath	C:/Progra~1/WebSphere/AppServer
instWASUserName	wpsbind
instWASPassword	wpsbind
instDBUserid	weaadmin
instDBPassword	lpuwea
instDBHostName	wea5d.itso.ral.ibm.com
instDBPort	6789
instDBPath	C:/Progra~1/IBM/SQLLIB
instDBLibPath	C:/Progra~1/IBM/SQLLIB/java/db2java.zip
instNotesPath	C:/Progra~1/Lotus/Notes
instNotesDataPath	C:/Program Files/WebSphere/INS/NotesData
instDominoUserid	user.id
instDominoPassword	dpinsadm
instWPSHost	wea5d.itso.ral.ibm.com
instWPSPath	C:/Progra~1/WebSphere/PortalServer
instPWSUrlPrefix	/wps
instWPSURLConfigPrefix	/config
instWPSAdminUser	weaadmin
instWPSPassword	weaadmin

Field	Value
instWPSPort	80
instWPSAdminGroup	wpsadmins
instINSAdminuser	insadmin
instINSAdminPassword	dpinsadm
removeINSAdminUserOnUninstall	true
instINSAdminGroup	insadmins
removeINSAdminGroupOnUninstall	true
instINSUserGroup	insusers
removeINSUserGroupOnUninstall	true
installLocation	C:/Program Files/WebSphere/INS

6. Save the INSinstallconfig.properties file.
7. In a command window, go to *ins_home*/config and begin the configuration:

   ```
   cd \Program Files\WebSphere\INS\config\INSWASconfig.bat basic-config
   ```

8. After finishing the configuration, you should see a `BUILD SUCCESSFUL` message.
9. For Intelligent Notification Services, you need to run **db2jstrt**. The variable *port_number* is the port that the feature is listening on. This was specified during in the INSInstall. The default port is 6789. Use the following command:

   ```
   db2jstrt port_number
   ```

   In our example, it is:

   ```
   db2jstrt 6789
   ```

After configuring the Intelligent Notification Services server, we recommend running the setSmQueues script. Otherwise, Intelligent Notification Services will stop after reaching the default subscriptions limit.

1. Make sure the Intelligent Notification Services server (INSServer) is stopped. Open a command prompt and run:

   ```
   cd \program files\websphere\appserver\bin
   serverstatus -all -user wpsbind -password wpsbind
   ```

2. If it is started, stop it with:

```
stopserver INSServer -user wpsbind -password wpsbind
```

3. In the command prompt, go to *ins_home*\config\templates\mq and run the **setSmQueue** command. The values for *brokerQMgrHost* and *brokerQMgrServer* can be checked in *ins_home*\config\xml\subscriptionManagerConfig.xml. Use the following command:

```
setSmQueues WAS_brokerQMgrHost_brokerQMgrServer
```

For our example, it is:

```
setSmQueues WAS_wea5d_INSServer
```

Install DB2 Everyplace

1. Assuming the WebSphere Everyplace Access install program is still open, choose **DB2 Everyplace** and click **Next** (see Figure 5-42).

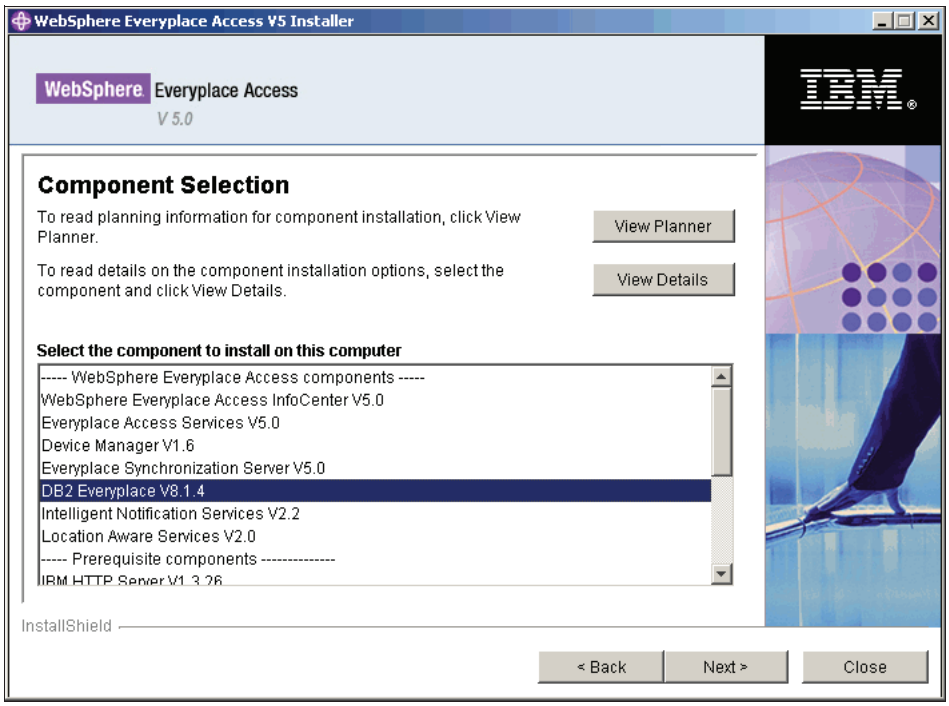

Figure 5-42 Component selection: DB2 Everyplace

2. Insert the CD when prompted and click **Next**.
3. Click **Next** on the welcome panel.

4. Specify the installation directory for DB2 Everyplace and click **Next** (see Table 5-44).

Table 5-44 DB2 Everyplace install directory

Field	Value
Directory	C:\Program Files\WebSphere\DB2Everyplace

5. Review the summary information to validate the install directory and click **Next** to start copying the files.
6. After the install finishes, a panel displays information about the success of the install. Click **Finish**.

Configure DB2 Everyplace

1. Check that all WebSphere Application Server servers are running:

```
serverstatus -all -user -wpsbind -password wpsbind
```

2. If they are stopped, start them with the **`startserver`** command from the same directory:

```
startserver server1
startserver WebSphere_Portal
```

3. Make sure the database server and the directory server are running.
4. Make a copy of *db2e_home*\config\dsyconfig.properties, where db2e_home is the directory you specified during the installation. In our example, it is C:\Program Files\WebSphere\DB2Everyplace.
5. Edit *db2e_home*\config\dsyconfig.properties (see Table 5-45 for the values).

Note: If you need explanations of what each property is used for, take a look at the configuration file or look in the InfoCenter, which can be installed from the setup CD.

Be sure to use / (slash) instead of \ (backslash).

The user weaadmin for the database is an user of the local system. All other users are users in the Domino directory.

Table 5-45 Properties

Field	Value
createControldb	true
isDB2MessageStore	false

Field	Value
dsyctldbuser	weaadmin
dsyctldbPassword	lpuwea
wpsHost	wea5d.itso.ral.ibm.com
portalUser	weaadmin
portalPassword	weaadmin
syncgroup	SyncGroup
groupPrefix	DB2e
Virtual Host	default_host
wasAdminServer	server1
wasHome	C:/Progra~1/WebSphere/AppServer
wasUserName	wpsbind
wasPassword	wpsbind
wasNode	wea5d
ip	wea5d.itso.ral.ibm.com
serverName	IBMDB2eServer
jdbcDriverClasspath	
wasCell	wea5d

6. Save the dsyconfig.properties file.
7. In a command window, go to *db2e_home*/config and begin the configuration:

```
cd \Program Files\WebSphere\DB2Everyplace\config
DSYconfig.bat basic-config
```

8. After finishing the configuration, you should see a `BUILD SUCCESSFUL` message.

Install Location Aware Services

1. Assuming the WebSphere Everyplace Access install program is still open, choose **Location Aware Services** and click **Next** (see Figure 5-43 on page 214).

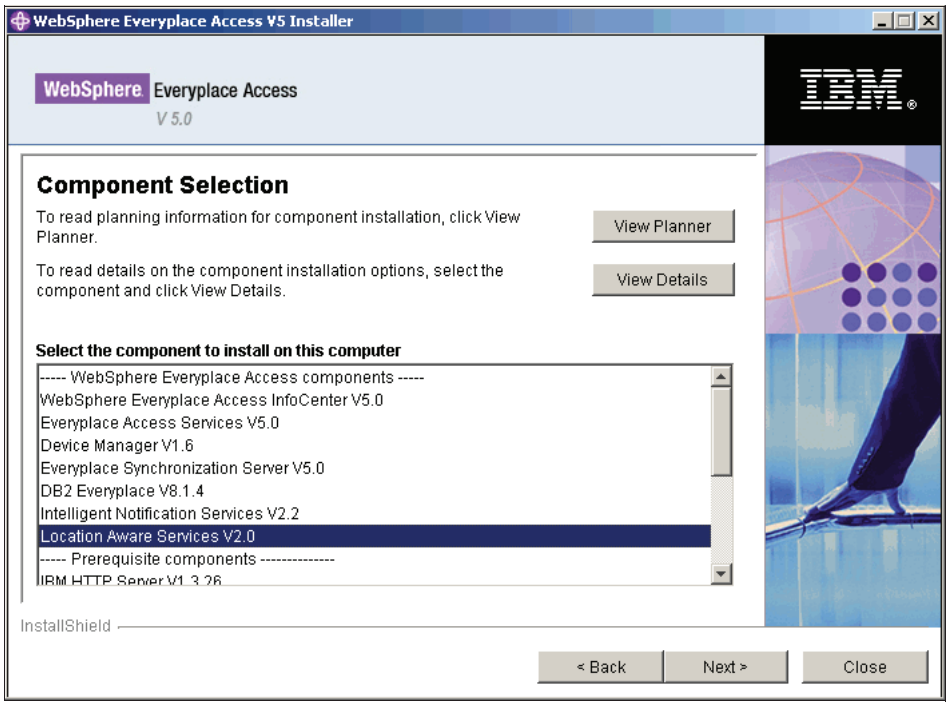

Figure 5-43 Component selection: Location Aware Services

2. Insert the CD when prompted and click **Next**.
3. Select **English** as the language and click **OK**.
4. Click **Next** on the welcome panel.
5. Specify the installation directory for Location Aware Services and click **Next** (see Table 5-46).

Table 5-46 Location Aware Services install directory

Field	Value
Directory	C:\Program Files\WebSphere\LAS

6. Review the summary information to validate the install directory and click **Next** to start copying the files.
7. After the install finishes, a panel displays information about the success of the install. Click **Finish**.

Configure Location Aware Services

1. Check that all the WebSphere Application Server servers are running:

   ```
   serverstatus -all -user wpsbind -password wpsbind
   ```

2. If they are stopped, start them with the **startserver** command from the same directory:

   ```
   startserver server1
   startserver WebSphere_Portal
   ```

3. Make sure the database server and the directory server are running.
4. Make a copy of *las_home*\config\LASinstallconfig.properties, where las_home is the directory you specified during the installation. In our example, it is C:\Program Files\WebSphere\LAS.
5. Edit *las_home*\config\LASinstallconfig.properties (see Table 5-47for the values).

Note: If you need explanations of what each property is used for, take a look at the configuration file or look in the InfoCenter, which can be installed from the setup CD.

Be sure to use / (slash) instead of \ (backslash).

The user weaadmin for the database is an user of the local system. All other users are users in the Domino directory.

Table 5-47 Properties

Field	Value
instProduct	WEA
LasHost	wea5d.itso.ral.ibm.com
LasInstallLocation	C:/Program Files/WebSphere/LAS
WasHome	C:/Program Files/WebSphere/AppServer
CellName	wea5d
NodeName	wea5d
WasAdminServer	server1
WasUserid	wpsbind
WasPassword	wpsbind
DefaultVirtualHostName	default_host

Field	Value
LasDbType	db2
LasDbInstPath	C:/Program Files/IBM/SQLLIB
LasDbLocalInstance	db2
LasDbServerHost	wea5d.itso.ral.ibm.com
LasDbUser	weaadmin
LasDbPassword	lpuwea
LasDbName	lasdb
LasDbJdbcPort	6789
LasDbLibrary	C:/Program Files/IBM/SQLLIB/java/db2java.zip
LasDbDriver	COM.ibm.db2.jdbc.net.DB2Driver
LasDbUrl	jdbc:db2:
LasJdbcProvider	las50JDBC
LasDbDriverDs	COM.ibm.db2.jdbc.DB2ConnectionPoolDataSource
LasDbLibraryDS	C:/Program Files/IBM/SQLLIB/java/db2java.zip;C:/Program Files/IBM/SQLLIB/java/db2jcc.jar
LasDbName	las50ds
WpsHome	C:/Program Files/WebSphere/PortalServer
PortalServerName	WebSphere_Portal
WpsHostName	wea5d.itso.ral.ibm.com
WpsHostPort	80
WpsContextRoot	wps
PortalAdminidShort	weaadmin
PortalAdminPassword	weaadmin
LasAdminGroupIdShort	lasadmins
LasServerName	LasAppServer

6. Save the LASinstallconfig.properties file.

7. In a command window, go to *ins_home*/config and begin the configuration:

```
cd \Program Files\WebSphere\LAS\config
LASWASconfig.bat las-basic-config
```

8. After finishing the configuration, you should see a `BUILD SUCCESSFUL` message.

Additional installations

To improve the performance of Intelligent Notification Services, we recommend installing additional WebSphere Application Server fixes. For a component installation on a single computer, you should apply the fixes located in the directory WAS_INS on CD3-3.

Make sure that WebSphere Application Server, WebSphere Portal Server, IBM HTTP Server and IBM HTTP Administration Server are stopped.

1. To see if the WebSphere Application Server servers are stopped, open a command prompt and run the **`serverstatus -all`** command in the *was_home*\bin directory:

   ```
   cd \program files\websphere\appserver\bin
   serverstatus -all
   ```

2. If they are started, stop them with the **`stopserver`** command from the same directory:

   ```
   stopserver server_name
   ```

   where server_name is the name of the server, for example, server1, INSServer, or WebSphere_Portal.

3. To stop both IBM HTTP Servers, select **Start** → **Settings** → **Control Panel** → **Administrative Tools** → **Services**. Right-click **IBM HTTP Server** and select **Stop**. Right-click **IBM HTTP Administration Server** and select **Stop**.
4. Go to *MQ_Home*\java\lib, where MQ_Home is the installation directory where WebSphere MQ embedded messaging is installed. In our example, it is C:\Program Files\IBM\WebSphere MQ.
5. Make a backup copy of com.ibm.mqjms.jar and com.ibm.mq.jar.
6. Unzip IC38409.windows.zip into *MQ_Home*\java\lib. It will overwrite the two files we just backed up. The IC38409.windows.zip is located in the directory WAS_INS on CD3-3
7. Go to *MQ_Home*\WEMPS\bin and make a backup copy of imbdfmqm.lil.
8. From the WAS_INS directory on CD 3-3, copy the imbdfmqm.lil file to *MQ_Home*\WEMPS\bin. That will overwrite the file we just backed up.

9. Assuming the WebSphere Everyplace Access install program is still open, choose **WebSphere Application Server fix pack and interim fix** and click **Next**.
10. Insert the CD when prompted and click **Next**.
11. Select **English** as the language and click **OK**.
12. Click **Next** on the welcome panel.
13. Review the license agreement, select **I accept the terms in the license agreement**, and click **Next**.
14. The next panel should display the currently installed version of WebSphere Application Server. If it does not, click the empty text box and the information should appear.
15. Select **IBM WebSphere Application Server v5.0.2.3 + Enterprise v5.0.2.2**, accept the default install location of the Application Server, and click **Next**.
16. Select **Install fixes** and click **Next**.
17. Click **Browse** to specify the Fix Pack location. Go to the CD 3-3, select **WAS_INS**, and click **Open**. Click **Next**.
18. Select the two available fixes (Messaging eFix and PQ78200) and click **Next**.
19. Review the summary information and click **Next**.
20. The final install panel should display the following message when it is complete:

    ```
    The following fixes were successfully installed:
    ```

    The fixes will appear in the field below the message.
21. Click **Finish**.
22. Go to *WAS_Home*\tranlog\INSServer\ and delete all files in this directory.

Another fix has to be applied to DB2 for DB2e improvements:

1. Select **Start** → **Settings** → **Control Panel** → **Administrative Tools** → **Services** and stop all services related to DB2.
2. Copy hotfixpkg_11633.exe to a local temporary directory. This file can be found in the hotfix directory of CD 1-1.
3. Open a command window and, from the temporary directory, run the following command:

    ```
    hotfixpkg_11633 -a -f
    ```
4. Go to the DB2 install directory and run **`hotfix -l`** and **`db2level`** to verify that 11633 was applied:

    ```
    cd \Program Files\IBM\SQLLIB
    ```

```
hotfix -l
db2level
```

5. You should see Hotfix 11633 in the output of the commands.
6. Restart DB2 either by starting all the services you stopped in step 1 or by rebooting the machine.

Note: If your INSServer will not start correctly after applying the patches, be sure to delete all the files in *WAS_Home*\tranlog\INSServer\.

6

AIX component installation

This chapter describes how to install all the components of WebSphere Everyplace Access on AIX and configure it to use a Domino Directory. It provides step-by-step instructions to install and configure the Domino LDAP as well as WebSphere Everyplace Access and its requirements.

© Copyright IBM Corp. 2005. All rights reserved.

6.1 Overview

Websphere Everyplace Access V5 only supports a component install on AIX, which provides a flexible install path for distributing and scaling components. It gives the choice to install only the components that are required to implement WebSphere Everyplace Access in a given environment, including the prerequisite software.

In our sample environment, we will install all the components of WebSphere Everyplace Access on a single AIX computer. Lotus Domino, which acts as mail server and LDAP Directory, is installed on a separate Windows OS machine.

It is important that each machine has a host and domain name, which is registered in the DNS Server, so that both machines can be accessed by its name. In our example, the server with WebSphere Everyplace Access is called m10695bf.itso.ral.ibm.com and the server containing Lotus Domino is domldap.pvclab.com.

On domldap, we will install Lotus Domino and Lotus Notes. The Notes client is needed to configure Lotus Domino. This server is only an example for a mail and LDAP server, because in a given environment, for example, at a client, you would generally use existing installations.

On m10695bf, we will install all components of WebSphere Everyplace Access and its requirements. First, we will install the prerequisite software:

- DB2
- WebSphere Application Server
- WebSphere Portal Server

After the prerequisite software is in place, we will install all WebSphere Everyplace Access features

- Everyplace Access Services
- Device Management Services
- Everyplace Synchronization Server
- Intelligent Notification Services
- DB2e
- Location Aware Services

6.2 Server 1 - Lotus Domino

This section describes the installation of the Domino machine. It includes the preparation of the machine, the installation of the Notes Client to administer and configure Domino, as well as the Domino installation and configuration for WebSphere Everyplace Access.

In our example, we will install Lotus Domino V6.5.1 and Lotus Notes V6.5.1 on the machine. As described above, the machine name is domldap.pvclab.com. This name is registered in DNS so that the machine is accessible with this name.

6.2.1 Preparation

Before installing Lotus Domino, check that the computer is prepared.

Check the Service Pack version

WebSphere Everyplace Access requires Service Pack 4 for Windows 2000 Server and Advanced Server. Service Pack 4 must be installed before the WebSphere Everyplace Access installation. To verify that the correct service pack version is installed:

1. Select **Start** → **Run**.
2. Type `winver` and press **Enter** to display information about Windows.
3. Verify that Service Pack 4 is installed.
4. If Service Pack 4 is not installed, refer to the Microsoft support site or Windows Update for Windows 2000 to download and install the service pack.

Check for a static IP address

WebSphere Everyplace Access requires that the computer have a static IP address.

1. Select **Start** → **Settings** → **Network and Dial-up Connections**.
2. Right-click the LAN connection for your network adapter and click **Properties**.
3. In the Network Adapter Properties window, select **Internet Protocol (TCP/IP)** from the list of components used by the connection and click **Properties**. The Internet Protocol (TCP/IP) will display.
4. Verify that **Use the following IP address** is selected. If **Obtain an IP address automatically** is selected, the computer has a dynamic IP address. If this is the case, contact your network administrator to obtain and configure a static IP address.

Check for fully-qualified host name

WebSphere Portal also requires the use of a fully qualified host name, which is typically the host name of the server, along with its fully-qualified domain name (FQDN). The Domino and the WebSphere Everyplace Access Server should have access to each other. To check that your computer has a host name and a FQDN:

1. Select **Start** → **Settings** → **Control Panel** → **System** and click **Network Identification**.
2. Click **Properties**. In our example, the computer name should be domldap and the full computer name domldap.pvclab.com.
3. If there is only a host name, contact your system administrator or change the host name and FQDN. To do that, enter a host name in the field **Computer Name**.
4. To specify a FQDN, click **More** and enter it in the field **Primary DNS suffix of this**. Click **OK**.
5. Click **OK**. If you changed any settings, reboot your computer.
6. Try to ping yourself. For example:

   ```
   ping domldap.pvclab.com
   ```

7. You should see a reply.

Check port bindings

Specific ports are required to install Lotus Domino. If two applications attempt to use the same port, a port conflict results. To ensure that the required port bindings are available, the netstat utility can be used.

1. Select **Start** → **Programs** → **Accessories** → **Command Prompt** to launch a command prompt.
2. Type `netstat -an` at the command prompt.
3. Look at the numbers listed in the Local Address column. The fifth number is the port number. For example, in the IP address 1.2.3.4:80, 80 is the port number.
4. Verify that port 80, required by Lotus Domino, is not in use. If it is in use, you may experience port conflicts.

If port 80 is in use, it is possible that IIS is installed. If the Microsoft Internet Information Services (IIS) Web server is running, you will have a port conflict with IBM HTTP Server. Both of these Web servers listen on port 80, unless otherwise configured. To prevent this conflict, disable the Microsoft IIS Web server.

To see if IIS is enabled:

1. Select **Start** → **Settings** → **Control Panel** → **Add/Remove Programs**.
2. Select **Add/Remove Windows Components**.
3. If IIS is listed, it has been installed on the computer.

To disable IIS:

1. Select **Start** → **Programs** → **Administrative Tools**.
2. Open **Services**.
3. Locate and highlight **IIS Admin Service**.
4. Select the **Action** menu and click **Properties**. A window opens.
5. Change the **Startup type** to **Disabled** and click **Stop** to stop the server.
6. Click **Yes** to stop any services that are stopped as a result.
7. Locate the **World Wide Web Publishing Service**. Disable it at startup using the steps listed above.

6.2.2 Install Lotus Notes

The Notes Client is required to configure Lotus Domino. Therefore, the Domino Administrator has to be installed along with the Lotus Notes Client.

1. Start the installation either by using an installation CD or a file that contains the installation files. For CD Installation, go to step 3.
2. Specify where the installation files should be extracted and click **Next** (see Table 6-1).

Table 6-1 Installation file path

Field	Value
Directory	C:\Program Files\Lotus Notes 6

3. The Lotus Notes Installation window will appear. Click **Next**.
4. Select **I accept the terms in the license agreement** and click **Next**.
5. Enter a name and company and click **Next**.
6. Accept the default folders and click **Next** (see Table 6-2).

Table 6-2 Default folder

Field	Value
Directory	C:\Program Files\Lotus\Notes

7. Be sure to select **Domino Administrator** and click **Next**.
8. Accept the default and click **Install**.
9. Click **Finish**.

Note: After finishing the Lotus Notes installation, the Directory created in step 2 can be deleted, including all the files.

6.2.3 Installing Domino

This section describes how to install Lotus Domino so that it can be configured later for WebSphere Everyplace Access.

1. Start the installation either by using an installation CD or a file that contains the installation files. For CD installation, go to step 3.
2. Specify where the installation files should be extracted and click **Next** (see Table 6-3).

Table 6-3 Installation files path

Field	Value
Directory	C:\Program Files\Lotus Domino 6

3. The Lotus Domino Installation window will appear. Click **Next**.
4. Accept the license by clicking **Yes**.
5. Enter a name and company. Leave Partitioned Installation unchecked and click **Next**.
6. Except the default folders and click **Next**.
7. Choose **Domino Enterprise Server** and click **Next**.
8. Accept the default and click **Next**.
9. Click **Finish**.
10. Start the configuration wizard by selecting **Start** → **Programs** → **Lotus Applications** → **Lotus Domino Server**.
11. Select **Start Domino as a Windows service** and **Don't ask me again** and click **OK**.
12. Select a different font if you want and click **Next**.
13. Choose **Set up the first server or a stand-alone server** and click **Next**.
14. The Server name should be already set (see Table 6-4 on page 227). A server description/title is optional. Leave the check box unchecked and click **Next**.

Table 6-4 Server name

Field	Value
Server name	domldap

15. Choose a Organization name and a password and click **Next** (see Table 6-5).

Table 6-5 Organization name and password

Field	Value
Organization name	pvclab
Certifier password	pvc1class

16. Choose a Domino Domain Name and click **Next** (see Table 6-6).

Table 6-6 Domino Domain Name

Field	Value
Domino Domain Name	pvclab

17. Specify an administrator name and password (see Table 6-7). Select **Also save a local copy of the ID File** and click **Next**.

Table 6-7 Administrator user ID and password

Field	Value
First name	
initlas	
Last name	admin
Password	pvc1class

18. Select **Web Browsers (HTTP services)**, **Directory services (LDAP services)**, and click **Next**.
19. Click **Next**.
20. Select both check boxes and click **Next**.
21. Review the summary and click **Setup**.
22. When the configuration is finished, click **Finish**.

6.2.4 Lotus Domino configuration

After installing Lotus Domino, it needs to be configured so that WebSphere Everyplace can use it as its LDAP Directory. First, Lotus Notes is set up to connect to Lotus Domino. Then the Domino LDAP is configured to match the needs of WebSphere Everyplace. Finally, the required users in Domino LDAP are created.

Initial setup of Lotus Notes

1. Start the Lotus Domino Server if it is not already started by selecting **Start** → **Programs** → **Lotus Applications** → **Lotus Domino Server**.
2. Start the Lotus Domino Administrator by selecting **Start** → **Programs** → **Lotus Applications** → **Lotus Domino Administrator**.
3. If this is the first start of Lotus Domino Administrator or Lotus Notes on this computer, it has to be configured. Click **Next**.
4. Type the Lotus Domino Administrator name and the appropriate server (see Table 6-8). Click **Next**. If the server cannot be found, a screen will appear to specify the server, for example, by its host name, including the fully-qualified domain name.

Table 6-8 Lotus Domino Administrator

Field	Value
User name	admin
Domino Server	domldap

5. Provide the password (for our example, dpnadm) and click **OK**.
6. Do not select Setup Instant Messaging. Click **Next**.
7. Leave all check boxes unchecked and click **Next**.
8. The Notes setup should be complete. Click **OK**.

LDAP configuration

The features of the portal require that LDAP users access specific attribute types in Domino. For example, within the edit mode of some collaborative portlets, a pick list of available servers displays if the user has access to the attributes shown in the steps below. The following instructions provide steps that enable anonymous LDAP users to access these attributes.

For complete information, refer to the Domino documentation on the Lotus Web site at: `http://www.lotus.com/ldd/doc`. The guide, *Lotus Domino 6*

Administering the Domino System, Volume 1, provides details about setting up the LDAP service and methods for extending the schema.

To allow anonymous users to query LDAP, follow these steps:

1. Open the Schema database (schema.nsf).
2. Select the **All Schema Documents** view, and then click **New Document - Add Attribute Type**.
3. Complete these fields on the **Basic** tab (see Table 6-9).

Table 6-9 Basic tab values

Field	Action
LDAP Name	Enter `HTTP-HostName`.
OID	2.16.840.1.113678.2.2.2.2.461.
Syntax Name	Select **Directory String**.
Description	(Optional) Enter a description for the attribute.
Equality match	Leave as is.
Ordering match	Leave as is.
Substrings match	Leave as is.
Single valued Choose one	Leave as is.
Collective	Leave as is.
No user modification	Leave as is.

4. Click **Save & Close**. The document is saved as a draft and needs to be approved.
5. From the Domino LDAP schema view, select the **Draft Documents** → **Draft Attribute Types** view. Select the HTTP-HostName draft document, and select **Approve** → **Approve Selected Drafts**.
6. Open the names.nsf file (named <your domain> Directories, for example, IBM's Directories).
7. Select the **Configuration** → **Servers** view and highlight **Configurations**.
8. If there is already a configuration document, open it. Otherwise, click **Add Configuration** to create a new Configuration Settings document.
9. On the Basic tab, for the option **Use these settings as the default settings for all servers**, click **Yes**. This is required for the LDAP tab to appear for use in the next step.

10. On the LDAP tab, click **Select Attribute Types**.
11. The LDAP Attribute Type Selection dialog box will appear. Select ***** in the Object Classes drop-down list and click **Display Attributes**.
12. From Selectable Attribute Type box, select the following fields, and then click **Add** to add them to the Queriable Attribute Types box:
    - AltFullName
    - dominoCertificate
    - givenName
    - HTTP-Hostname
    - Location
    - mail
    - mailaddress
    - MailDomain
    - MailFile
    - MailServer
    - member
    - NetAddresses
    - PublicKey
    - Sametime
    - sn
    - uid
    - userCertificate
13. Click **OK** to close the LDAP Attribute Selection dialog box, and return to the Configuration Settings document.
14. Check that all the attributes selected in the previous steps are included in the **Anonymous users can query field**.
15. For the option **Allow LDAP users write access**, click **Yes**.
16. Keep all the other default LDAP settings and click **Save & Close**.
17. Open the Schema database (schema.nsf). This can be done by either selecting **File** → **Database** → **Open** and then selecting the appropriate Domino Server and opening **Domino LDAP Schema** or by selecting the **Files** tab and opening **schema.nsf**.
18. In the left navigation, expand **All Schema Documents**, select **LDAP Attribute Types**, and click **Add Attribute Type**.

19. Complete these fields on the **Basic** tab (see Table 6-10).

Table 6-10 Basic tab values

Field	Action
LDAP Name	Enter `ibm-appUUID`.
OID	1.3.18.0.2.4.2323.
Notes mapping	Should be filled with ibm-appUUID.
Syntax name	Select **Directory String**.
Schema	Should be filled with **IBM SecureWay Directory**.
Syntax type	Should be filled with 1.3.6.1.4.1.1466.115.121.1.15.
Description	(Optional) Enter a description.
Usage	Should be filled with User Applications.
Equality match	Select **Case Exact IA5 Match**.
Ordering match	Select **Case Ignore Ordering Match**.
Substrings match	Select **Case Ignore Substring Match**.
Single valued	Choose **Yes**.
Collective	Choose **Yes**.
No user modification	Choose **No**.

20. Click **Save & Close**. The document is saved as a draft and needs to be approved.
21. Select the **Draft Documents** → **Draft Attribute Types** view. Select the ibm-appUUID draft document, and select **Approve** → **Approve Selected Drafts**.
22. Click **LDAP Object Class** and click **Add Object Class**.
23. Enter the following information in the **Basic** tab (see Table 6-11).

Table 6-11 Basic tab values

Field	Action
LDAP Name	Enter `ibm-appUUIDAux`.
OID	1.3.18.0.2.6.475.
Notes mapping	Should be filled with ibm-appUUID.

Field	Action
Object Class Type	Select **Auxillary Object Class**.
Schema	Should be filled with **IBM SecureWay Directory**.
Superior Object Class	top.
Description	(Optional) Enter a description.
Mandatory Attribute Types	
Optional Attribute Types	Select **ibm-appUUID**.

24. Click **Save & Close**. The document is saved as a draft and needs to be approved.
25. Select the **Draft Documents** → **Draft Object Classes** view. Select the ibm-appUUIDAux draft document and select **Approve** → **Approve Selected Drafts**.

Adding portal administrators to the Domino Directory

If you do not have a user to administer your portal or you do not have an existing LDAP, you should create a new user to act as the portal administrator. The following steps should be followed if the portal administrative user does not exist in the directory.

1. In the Domino Administrator, navigate to the **People & Groups** tab and select the **People** view. From the action bar, click **Add Person**.
2. Enter the following values in the fields (see Table 6-12).

Table 6-12 Portal administrator

Field	Value
Last Name	wpsbind
User Name	wpsbind/<Organization name> wpsbind
Short name/UserID	wpsbind
Internet password	wpsbind

In our scenario the Organization name is pvclab, so the user name is:

```
wpsbind/pvclab
wpsbind
```

3. Click **Save & Close**.

4. Click **Add Person** again.
5. Enter the following values in the fields (see Table 6-13).

Table 6-13 Everyplace Access administrator

Field	Value
Last Name	wpsadmin
User Name	wpsadmin/<Organization name> wpsadmin
Short name/UserID	wpsadmin
Internet password	wpsadmin

In our scenario, the Organization name is pvclab, so the user name is:

```
wpsadmin/pvclab
wpsadmin
```

6. Click **Save & Close**.
7. Click **Save & Close**.
8. Click **Add Person** again
9. Enter the following values in the fields (see Table 6-14).

Table 6-14 Everyplace Synchronization Server administrator

Field	Value
Last Name	essadmin
User Name	essadmin/<Organization name> essadmin
Short name/UserID	essadmin
Internet password	essadmin

In our scenario, the Organization name is pvclab, so the user name is:

```
essadmin/pvclab
essadmin
```

10. Click **Save & Close**.
11. Click **Save & Close**.
12. Click **Add Person** again
13. Enter the following values in the fields (see Table 6-15 on page 234).

Table 6-15 Intelligent Notification Services administrator

Field	Value
Last Name	insadmin
User Name	insadmin/<Organization name> weaadmin
Short name/UserID	insadmin
Internet password	insadmin

In our scenario, the Organization name is pvclab, so the user name is

```
insadmin/pvclab
insadmin
```

14. Click **Save & Close**.

Creating required groups

1. In the Domino Administrator, navigate to the **People & Groups** tab and select the **Groups** view and, from the action bar, click **Add Group**.
2. Enter the following values in the fields (see Table 6-16).

Table 6-16 Group

Field	Value
Group name	wpsadmins
Group type	Multi-purpose
Members	wpsbind/<Organization name> wpsadmin/<Organization name> insadmin/<Organization name>

In our scenario, the Organization name is pvclab, so the members are:

```
wpsbind/pvclab
wpsadmin/pvclab
insadmin/pvclab
```

3. Click **Save & Close**.
4. Click **Add Group**.
5. Enter the following values in the fields (see Table 6-17 on page 235).

Table 6-17 Group

Field	Value
Group name	essadmins
Group type	Multi-purpose

6. Click **Save & Close**. Repeat steps 4 - 6 for the following groups:
   - essusers
   - essusers_nonlock
   - dmadmin -members admin, essadmin
   - insadmin- members admin, insadmin
   - insusers
   - lasadmins -members admin, lasadmins
   - SyncGroup

Updating the Access Control List to the Domino Directory

You must be sure that the wpsadmins group we created has the right permissions and roles in the Domino directory.

1. Open the names.nsf file by selecting **File** → **Database** → **Open** and then selecting the appropriate Domino Server and opening **names.nsf** or by selecting the **Files** tab and opening **names.nsf**.
2. From main menu, select **File** → **Database** → **Access Control**.
3. Select **Access Control List** → **Basic**, click **Add**, and choose the just created wpsadmins group.
4. The wpsadmins group requires either Author or Editor access. Select the following Role Types for the wpsadmin group:
   - GroupCreator
   - GroupModifier
   - UserCreator
   - UserModifier
5. Ensure that the User Type is set to **Person Group**.
6. Check **Delete Documents**.
7. Click **OK** to save these settings and close the Domino Administrator.

6.2.5 Summary

After you finish the installation of the Domino Server, you should have a setup that is similar to the following. Remember your user IDs and passwords.

- The computer has a host and domain name, such as m10695bf.itso.ral.ibm.com.
- Lotus Notes Administrator Client and Lotus Domino are installed.
- The organization name is pvclab, and the Domino Domain is pvclab.
- The certifier password is pvc1class. This password is used for creating users.
- The Lotus Domino administrative user is admin with pvc1class as the password.
- LDAP is configured as described in “LDAP configuration” on page 228.
- WebSphere Portal users and their passwords wpsadmin and wpsbind are created in the Domino directory.
- The wpsadmins group is created in the Domino directory. The members of this group are weaadmin, insadmin, and wpsbind.
- The users insadmin, using insadmin as a password, and essadmin, using insadmin as a password, are created in the Domino directory.
- The groups essadmins, essusers, essusers_nonlock, dmadmins, insadmin, insusers, lasadmins, and SyncGroup are created.
- The wpsadmins group has the right permissions on the names.nsf.

6.3 Server 2 - WebSphere Everyplace Access

This section describes the installation of the WebSphere Everyplace Access machine. It includes the preparation of the machine, the installation of the Domino Server code required for Everyplace Synchronization and Intelligent Notification Services, as well as the WebSphere Everyplace Installation.

The Component Install of WebSphere Everyplace Access does not include a configuration tool. After you install a component, you must run configuration tasks to configure the feature.

As described above, the machine name is m10695bf.itso.ral.ibm.com. This name is registered in DNS so that the machine is accessible with this name.

6.3.1 Requirements

Before installing WebSphere Everyplace Access on AIX, ensure that it meets both the hardware and software requirements.

Software requirements

- AIX 5L V5.2 with maintenance level 2 or higher
- Domino Server V6.0.1 CF3: Required for Everyplace Synchronization Server and Intelligent Notification Services

Hardware requirements

- IBM @server pSeries with a 1 GHz or higher CPU.
- Memory of 2 GB (minimum); however, 4 GB is recommended.
- Paging Space set to 1 or 1.5 times the physical memory (2 GB physical memory = 2 GB to 3 GB paging space).
- Disk space of 15 GB for the installation, not including paging space and log files.
- CD-ROM drive.
- SVGA or higher display resolution.
- Mouse or pointing device and keyboard.

6.3.2 Preparation

Before installing WebSphere Everyplace Access, check that the computer is prepared. That means the network is configured, including the host and domain name, and all the necessary users are created on the system.

Install additional AIX file sets (optional)

The following file sets can be installed using SMIT and are used to support versions of DB2 installed in non-English languages. They do not need to be installed if DB2 only supports English.

- X11.fnt.ucs.ttf (AIX Windows Unicode True Type Fonts)
- XlC.rte 5.0.2.x

Asian languages also require the following file sets:

- X11.fnt.ucs.ttf_CN (for zh_CN or Zh_CN)
- X11.fnt.ucs.ttf_KR (for ko_KR)
- X11.fnt.ucs.ttf_TW (for zh_TW or Zh_TW)

These file sets can be downloaded from:

http://techsupport.services.ibm.com/server/fixes

Disable the WebSM service on AIX

WebSM is used by administrators to manage AIX computers, but it requires port 9090, which conflicts with WebSphere Application Server Administrative Console.

From an AIX command prompt, issue the following commands:

```
usr/websm/bin/wsmserver -disable
netstat -na |grep 9090 (if the command prompt is returned, WebSM has been
successfully disabled)
```

Check for a fully-qualified host name and static IP address

WebSphere Portal requires the use of a fully qualified host name, which is typically the host name of the server, along with its fully-qualified domain name (FQDN). The Domino and the WebSphere Everyplace Access Server should have access to each other. To check that your computer has a fully-qualified domain host name and static IP address, do the following:

1. Type **smitty** from an AIX command prompt.
2. Select **Communications Applications and Services**.
3. Select **TCPIP**.
4. Select **Minimum Configuration & Startup**.
5. Select the **Network Interface** used to connect the server to the network from the list.
6. Verify that the HOSTNAME, DOMAIN Name, and all the IP address information is correct.
7. Make any necessary changes to the network interface configuration and press Enter to commit the changes or press F10 if no changes are necessary.
8. Attempt to ping the WebSphere Everyplace Access Server:

   ```
   ping m10695bf.itso.ral.ibm.com
   ```

9. You should see a reply.
10. Try to ping the Domino Server:

    ```
    ping domldap.pvclab.com
    ```

11. You should see a reply.

Set the size of the AIX file systems

In order to install all the necessary prerequisites and WebSphere Everyplace Access Components, it is necessary to modify the size of several AIX file systems:

1. Open an AIX command window.
2. Increase the /usr file system to 5 GB:

   ```
   chfs -a size=8G /usr
   ```

3. Increase the /tmp file system to 2 GB:

   ```
   chfs -a size=2G /tmp
   ```

4. Increase the /home file system to 2 GB:

   ```
   chfs -a size=2G /home
   ```

5. Increase the /opt file system to 1 GB:

   ```
   chfs -a size=1G /opt
   ```

6. Increase the / file system to 1 GB:

   ```
   chrs -a size=1G /
   ```

7. Verify the size of all file systems modified in the previous steps:

   ```
   df -g
   ```

WebSphere Application Services Embedded Messaging Setup

Embedded Messaging is an optional feature installed with WebSphere Application Server and is required only if you plan to install Intelligent Notification Services.

1. Using smitty, create and mount a journalized file system called /var/mqm.
2. Ensure that the file system is allocated at least 60 MB of disk space.
3. Create the groups mqm and mqbrkrs.
4. Create a new user for Embedded Messaging
   - Name: mqm
   - Primary Group: mqm
   - Group Set: mqm, system
5. Add the root user to the groups mqbrkrs and mqm.
6. Log off and back on as the root user.

6.3.3 Install the Lotus Domino Server on AIX

The WebSphere Everyplace Access components Everyplace_Synchronization Server and Intelligent Notification Server require that Lotus Domino Server be installed in order to communicate with back-end Domino Mail servers.

Verify that the prerequisite files are installed and configured

Intelligent Notification Services requires that I/O Completion Ports be installed and available.

1. Verify that I/O Completion Ports is installed (V5.1.0.35 or higher) by issuing the following commands from an AIX command prompt:

   ```
   lslpp -l bos.iocp.rte
   ```

   Example 6-1 shows the output of the command.

Example 6-1 lslpp -l bos.iocp.rte output

```
Path:  /etc/objrepos
bos.iocp.rte 5.2.0.10 COMMITTED I/O Completion Ports API
```

2. If the fileset is not installed, it can be downloaded from `http://techsupport.services.ibm.com/server/fixes` or installed via the AIX OS CDs.
3. Set the I/O Completion Ports to defined.
4. Type **`cfgmgr`** at an AIX command prompt to set the I/O Completion Ports to defined.
5. Ensure that the I/O Completion Ports are available:
   - Launch SMIT.
   - Select `Devices`.
   - Select `I/O Completion Ports`.
   - Select `Change/Show Characteristics of I/O Completion Ports`.
   - If the state is not set to available, press F4 and select **Available** and press Enter.
6. Reboot the system to complete the change.

Create the AIX Lotus Domino user and group

1. Use SMITTY to create a new group called notes.
2. Add the root user to the new group.
3. Use SMITTY to create a new user
   - Name: notes

- Primary Group: notes
- Group Set: system, bin, sys, and notes

Install the Lotus Domino Server

1. Mount the WebSphere Everyplace Access CD 9-3.
2. Launch the Lotus Domino Installer:

   ```
   cd cdrom/server/aix ( cdrom = cdrom file system name)
   ./install
   ```

3. Press Tab on the first three Domino Server Installation Screens.
4. Review the license agreement and then press Tab.
5. Press Tab again to agree to the license agreement.
6. After you agree to the license agreement, you are prompted with a series of install questions. Answer the questions as shown below:
   - Do you want to install data directories only? `No`
   - Select Setup type: `Domino Enterprise Server`
   - Do you want to install all template files for this Domino Server? `Yes`
   - Do you want to configure this server with ASP functionality? `No`
   - Current program directory setting: `/opt/lotus`
   - Do you want to run more than one server based on this installation? `No`
   - Current data directory setting: `/local/notesdata`
   - Current UNIX user setting: `notes`
   - Current UNIX group setting: `notes`
7. Press Tab on the remaining screens in order to begin the install.

Install the Domino Server hot fix

1. Copy hot fix 601CF3HF25-aix.tar to a temporary directory:

   ```
   cd /cdrom/fixes (cdrom = cdrom file system name)
   cp 601CF3HF25-aix.tar /tmp
   ```

2. Extract the hot fix files:

   ```
   cd /tmp
   tar --xvf 601CF3HF25-aix.tar
   ```

3. Launch the hot fix install program:

   ```
   cd aix
   ./instal
   ```

4. Accept all of the defaults by pressing the Tab key.

5. Verify that the user ID and group are both set to notes.
6. Unmount Mount WebSphere Everyplace Access CD 9-3.

6.3.4 Installation of WebSphere Everyplace Access

This section describes all the steps that are necessary to install WebSphere Everyplace Access. At first, all the required software packages, such as DB2, WebSphere Application Server, WebSphere Portal Server, and all the needed fix packs are installed. After that, the components of WebSphere Everyplace Access are installed. Each component installation is split into two parts. First, the component is copied to the computer and the system registry information is configured. Then the component has to be configured by running the configuration tasks to set up the needed features. The configuration tasks include editing configuration files and invoking commands from the command line to set up the component.

DB2 Universal Database Workgroup Installation

1. Mount the WebSphere Everyplace Access Setup CD and start the WebSphere Everyplace Access V5 Installer:

   ```
   ./cdrom/install.sh ( cdrom = cdrom file system name)
   ```

2. Select **English** and click **OK**.
3. Click **Next** or launch the InfoCenter.
4. View the license agreement and select **I accept the terms in the license agreement** and click **Next**.
5. Select **DB2 Universal Database Workgroup V8.1.6** and click **Next**.
6. Insert the CD (labeled as CD 1-2) when prompted and click **Next**.
7. Click **Installation Prerequisites** if you want to review the requirements for DB2. Close the browser when you are finished.
8. Click **Install Products**.
9. Ensure that DB2 UDB Workgroup Server Edition is selected and click **Next**.
10. Click **Next** on the welcome panel.
11. Review the license agreement and select **I accept the terms in the license agreement** and click **Next**.
12. Select **Typical** as the installation type and click **Next**.
13. Set user information for the DB2 Administrative Server (see Table 6-18 on page 243).

Table 6-18 User information

Field	Value
User Name	dasusr1
Password	dasusr1
Home directory	/home/dasusr1
Group	dasadm1

14. On the Set up a DB2 instance panel, select **Create a DB2 instance** and click **Next**.
15. On the Set user information panel, select **New user**.
16. Enter the User name for this instance of DB2 and click **Next** (see Table 6-19). The DB2 install program will create this user on the local computer. If this is the first time you are installing DB2, the default user name is db2inst1.

Table 6-19 User information

Field	Value
User Name	db2inst1
Password	db2inst1
Home directory	/home/db2inst1
Group	db2inst1

17. Enter the User name for this db2fence user and click **Next** (see Table 6-20). The DB2 install program will create this user on the local computer. If this is the first time you are installing DB2, the default user name is db2fenc1.

Table 6-20 User information

Field	Value
User Name	db2fenc1
Password	db2fenc1
Home directory	/home/db2fenc1
Group	db2fgrp

18. Select **Do not prepare the DB2 tools catalog on this computer** and click **Next**.

19. Set up the administration contact list and click **Next**. If you deselect SMTP, you will see a pop-up message. Click **OK**.
20. Set up an administrator contact for the DB2 health monitor to send the notification to. You can select **Defer this task until after the installation is complete**.
21. Review the summary and click **Finish** to begin the install.
22. After the installation finishes, a setup complete screen appears. Verify that everything installed correct and click **Finish**.
23. The DB2 Universal Database First Steps interface will open. Click **Exit First Steps**.
24. Leave the WebSphere Everyplace Access install program open.

Edit DB2 Universal Database Workgroup settings

1. Launch the DB2 Control Center. For example:

```
xhost + localhost
su - db2inst1
export DISPLAY=localhost:0.0
db2cc
```

2. Expand the current node.
3. Expand **Instances**.
4. Right-click **db2instance** and select **Configure Parameters**.
5. Scroll down to the Diagnostic section.
6. Change **NOTIFYLEVEL** to 1 (errors only).
7. Scroll down to the Environment section.
8. Change **NUMDB** to 25.
9. Click **OK**.
10. Close the DB2 Control Center.
11. Change to the DB2 instance owner and modify DB2 Environment Settings in order to correct a shared memory problem between DB2 and WebSphere Application Server:

```
su - db2inst1
```

12. Edit the .profile in /home/db2inst1 and add `export EXTSHM=0`.
13. Save the .profile.
14. Running the following commands from an AIX command line.

```
db2set DB2ENVLIST=EXTSHM
db2stop
```

```
db2start
```

15. Leave the WebSphere Everyplace Access install program open.

Edit DB2 Universal Database Workgroup settings

1. Launch the DB2 Control Center. For example:

```
xhost + localhost
su - db2inst1
export DISPLAY=localhost:0.0
db2cc
```

2. Expand the current node.
3. Expand **Instances**.
4. Right-click **db2instance** and select **Configure Parameters**.
5. Scroll down to the Diagnostic section.
6. Change **NOTIFYLEVEL** to 1 (errors only).
7. Scroll down to the Environment section.
8. Change **NUMDB** to 25.
9. Click **OK**.
10. Close the DB2 Control Center.
11. Change to the DB2 instance owner and modify DB2 Environment Settings in order to correct a shared memory problem between DB2 and WebSphere Application Server:

```
su - db2inst1
```

12. Edit the .profile in /home/db2inst1 and add `export EXTSHM=0`.
13. Save the .profile.
14. Running the following commands from an AIX command line.

```
db2set DB2ENVLIST=EXTSHM
db2stop
db2start
```

15. Leave the WebSphere Everyplace Access installer open.

WebSphere Application Server installation

1. Assuming the WebSphere Everyplace Access installer program is still open, choose **WebSphere Application Server 5.0** (includes IBM HTTP Server) and click **Next**.
2. Insert CD 3-2 when prompted and click **Next**.
3. Select **English** and click **OK**.

4. Click **Next** on the Installation Wizard.
5. Accept the license agreement and click **Next.**
6. Click **Next**.

> **Note:** You might see a message that indicates that a supported operating system was not detected. If you are running AIX 5L V5.2 ML 2 or higher, you can ignore this message.

7. Select **Full** and click **Next**.
8. Verify the IBM WebSphere Application Server and IBM HTTP Server installation directories and click **Next** (see Table 6-21).

Table 6-21 Install directories

Field	Value
IBM WebSphere Application Server V5	/usr/WebSphere/AppServer
IBM HTTP Server V1.3.26	/usr/IBMHttpServer

9. Verify that the install program detects the correct Node Name and the Host Name or IP address and click **Next**.
10. Review the install summary and click **Next**.
11. Once the installation completes, the registration screen appears. Uncheck **Register This Product Now** and click **Next**.
12. Click **Finish**.
13. The WebSphere Application Server First Steps will open.
14. Click **Verify Installation**. If the installation was successful, you will see messages similar to the following:

```
IVTL0070I: IVT Verification Succeeded
IVTL0089I: Installation Verification is complete
```

15. Click **Stop the Server**.
16. Click **Exit** to close WebSphere Application Server First Steps.
17. Click **Finish** on the WebSphere Application Server install program.

WebSphere Application Server Enterprise installation

1. Assuming the WebSphere Everyplace Access install program is still open choose **WebSphere Application Server Enterprise V5.0** and click **Next**.
2. Insert CD 3-2 when prompted and click **Next**.

3. Select **English** as the language and click **OK**.
4. Click **Next** on the welcome panel.
5. Review the license agreement, select **I accept the terms in the license agreement**, and click **Next**.
6. Select **Add to existing copy of WebSphere Application Server, v5.0** and click **Next**.
7. Select **Typical** install type and click **Next**.
8. Review the summary panel and click **Install** to start the install.
9. After finishing the installation, click **Next** on the registration panel and click **Finish** to exit the WebSphere Application Server install program.

WebSphere Application Server Fix Pack installation

1. Ensure that WebSphere Application Server is stopped:

   ```
   cd /usr/WebSphere/AppServer/bin
   ./stopServer.sh server1
   ```

2. Ensure that IBM HTTP Server and IBM HTTP Administration Server are stopped:

   ```
   cd /usr/HTTPServer/bin
   ./apachectl stop
   ./adminctl stop
   ```

3. Assuming the WebSphere Everyplace Access install program is still open, choose **WebSphere Application Server fix pack and interim fix** and click **Next**.
4. Insert CD 3-4 when prompted and click **Next**.
5. Select **English** as the language and click **OK**.
6. Click **Next** on the Update Installation Wizard on the welcome panel.
7. Select **IBM WebSphere Application Server v5.0.0 + Enterprise v5.0.0**, accept the default install location of the Application Server, and click **Next**.
8. Select **Install fix packs** and click **Next**.
9. Click **Browse** to specify the Fix Pack location. Go to CD 3-4, select **WAS502BASE**, and click **Open**. Click **Next**.
10. Select **was50_fp2_aix** and click **Next**.
11. Select the external components to update, IBM HTTP Server and Embedded Messaging, accept the default values for the install directories, and click **Next**.
12. Review the summary information and click **Next**.

13. The final install panel should display the following message when it is complete:

    ```
    The following fix pack was successfully installed: was50_fp2_aix
    ```

14. Click **Run wizard again** and repeat steps 9 on page 247 - 13 for was50_pme_fp2_aix, which is located in the WAS502PME directory on CD 3-4.

Note: If the Update installer fails to find the fixes in one of the directories you specify, it may be necessary to reboot and start the install program again.

15. Click **Run wizard again** to install the first set of WebSphere Everyplace Access Enterprise Fix Pack 2 eFixes.
16. Select **Install fixes** and click **Next**.
17. Click **Browse** to specify the Fix Pack location. Go to CD 3-4, select **WAS502EFIX**, and click **OK**. Click **Next**.
18. Select all the available fixes and click **Next**. If you get a message that indicates a specific fix is not supported, click **OK**, click **Back**, and deselect the specified fix. Click **Next**. (There might be multiple unsupported fixes, so repeat this deselect step as needed.)
19. Review the summary information and click **Next**.
20. The final install panel should display the following message when it is complete:

    ```
    The following fixes were successfully installed:
    ```

    The fixes will appear in the field below the message.

21. Click **Run wizard again** and repeat steps 17 - 22 to install the additional WebSphere Everyplace Access Enterprise Fix Pack 2 eFixes, which are located in the WAS502EFIX2 directory on CD 3-4.
22. Click **Finish**.
23. Verify the installation by running the First Steps GUI from an AIX command prompt:

    ```
    cd /usr/WebSphere/AppServer/bin
    ./firststeps.sh.
    ```

24. Click **Verify Installation**. You should see a message similar to following:

    ```
    IVTL0070I: IVT Verification Succeeded
    IVTL0080I: Installation Verification is complete
    ```

25. Click **Stop the Server**. After the server stops click **Exit** to close First Steps.

WebSphere Portal Server installation

Ensure the WebSphere Application Server is running by running the following commands:

1. To verify that the WebSphere Application Server is started, open an AIX command prompt and run ./**`serverStatus.sh -all`**.
2. Change to the /usr/WebSphere/AppServer/bin directory.
3. Type **`./serverStatus.sh -all`**.
4. If the server status is stopped, start server1 by typing the **`./startServer.sh server1`** command.
5. Assuming the WebSphere Everyplace Access install program is still open, choose **WebSphere Portal Server V5.0** and click **Next**.
6. Insert CD 2-1 when prompted and click **Next**.
7. Select **English** as the language and click **OK**.
8. Click **Next** on the welcome panel.
9. Review the license agreement, select **I accept the terms in the license agreement**, and click **Next**.
10. Verify the WebSphere Application Server install location. Correct the install location if needed and click **Next**.
11. Specify where you want to install WebSphere Portal and click **Next** (see Table 6-22).

Table 6-22 WebSphere Portal installation directory

Field	Value
Directory	/usr/WebSphere/PortalServer

12. Enter your Portal administrative user name and password (see Table 6-23). This password is used to log on to the Portal and configure the Portal. It is temporary, because later we will move to the Domino Directory, where we created the admin in the Lotus Domino Preparation. Click **Next**.

Table 6-23 Portal administrator

Field	Value
User name	wpsadmin
Password	wpsadmin

13. Review the summary information and click **Next**.
14. After the install completes, click **Finish**.

15. To verify that the WebSphere Application Server is started, open an AIX command prompt and run **./serverStatus.sh -all**:

```
cd /usr/WebSphere/AppServer/bin
./serverStatus.sh -all
```

16. If the server for WebSphere_Portal status is stopped, start server1:

```
./startServer.sh WebSphere_Portal
```

17. Open a browser and use the following URL to access the portal, http://hostname:9081/wps/portal, where host name is the machine where we installed the Portal Server (in our example, m10695bf.itso.ral.ibm.com). The portal will open in your browser.

18. Log on to the portal with the administrator ID that you created.

WebSphere Portal Server Fix Pack installation

1. Open a command prompt, go to *was_home*/bin, and set up the JAVA environment for the update installer:

```
cd /usr/WebSphere/AppServer/bin
./setupCmdLine.sh
```

2. Verify that all WebSphere Application Server servers are stopped:

```
./serverstatus.sh -all
```

3. If they are started, stop them with the **stopserver** command from the same directory:

```
./stopserver.sh server1
./stopserver.sh WebSphere_Portal
```

4. Create an update directory in *wps_home*:

```
mkdir /usr/WebSphere/PortalServer/update
```

5. Create a fixpacks directory in the update directory

```
mkdir /usr/WebSphere/PortalServer/update/fixpacks
```

6. If the previous CD is still mounted, manually unmount it and mount the new CD 2-2.

7. Copy the contents of CD 2-2 to *wps_home*/update.

8. Move WP_PTF_502.jar and WPCP_PTF_502.jar, which you previously copied from CD 2-2 to *wps_home*/update, to the *wps_home*/update/fixpacks directory.

9. Run the WebSphere Portal update installer to apply the Fix Pack by running the following commands:

```
cd /usr/WebSphere/PortalServer/update
```

```
./updatePortal.sh -fixpack -installDir "/usr/WebSphere/PortalServer"
-fixpackDir "/usr/WebSphere/PortalServer/update/fixpacks" -install
-fixpackID WP_PTF_502
```

Note: If you receive a message that indicates the *WAS_HOME* is not set, the Java environment may not be properly set. Repeat step 1.

10. Run the following configuration task:

```
cd /usr/WebSphere/PortalServer/config
./WPSconfig.sh WP-PTF-502 -DPortalAdminPwd=wpsadmin
```

Note: If the WP-PTF-502 task fails for some reason, correct the cause of the failure and run the following configuration tasks from the *wps_home*/config directory:

```
./WPSconfig.sh UNINSTALL-WP-PTF-502 -DPortalAdminPwd=wpstemp
```

If the WP-PTF-502 task failed at task 44 of 50 with the following error: `XMLC0009E: Invalid password for user wpsadmin`, verify the Portal Administrator password and run the WP-PTF-502 command again with a valid password. You do not need to run the UNINSTALL-WP-PTF-502 configuration task.

11. Verify that all the WebSphere Application Server servers are started:

```
cd /usr/WebSphere/AppServer/bin
./serverstatus.sh -all
```

12. If they are not started, then issue the **startserver** command from the same directory:

```
./startserver.sh server1
./startserver.sh WebSphere_Portal
```

13. Open a browser and use the following URL to access the portal, http://*hostname*:9081/wps/portal, where hostname is the machine where installed the Portal Server (in our example, wea5d.itso.ral.ibm.com). The portal will open in your browser.
14. Log on to the portal with the administrator ID. In our example, it is wpsadmin with wpsadmin as the password.
15. The fix installation is complete. The contents of the *wps_home*/update directory are no longer needed and can be deleted.

WebSphere Application Server Enterprise Fix Pack installation

1. Verify that all WebSphere Application Server servers are started:

```
cd /usr/WebSphere/AppServer/bin
```

```
./serverStatus.sh -all
```

2. If they are started, stop them with the **stopserver** command from the same directory:

```
./stopServer.sh server1
./stopServer.sh WebSphere_Portal
```

3. Assuming the WebSphere Everyplace Access install program is still open, choose **WebSphere Application Server fix pack and interim fix** and click **Next**.
4. Insert CD 3-4 when prompted and click **Next**.
5. Select **English** as the language and click **OK**.
6. Click **Next** on the welcome panel.
7. Review the license agreement, select **I accept the terms in the license agreement**, and click **Next**.
8. Click **Next** on the Update Installation Wizard.
9. Ensure that IBM WebSphere Application Server v5.0.0 + Enterprise v5.0.0 is highlighted and click **Next**.
10. Select **Install Fixpacks** and click **Next**.
11. Click **Browse** to specify a Fix Pack location. Select the **WAS5022BASE** directory from the CD-ROM device and click **Open**. Click **Next**.
12. Select **was502_cf2_aix** and click **Next**.
13. Review the summary information and click **Next**.
14. The final install panel should display the following message when it is complete:

```
The following fix pack was successfully installed: was502_cf2_aix
```

15. Click **Run wizard again** and repeat steps 11 - 13 for was502_pme_cf2_aix, which is located in the WAS5022PME directory on CD 3-4.
16. Click **Run wizard again** and repeat steps 11 - 13 for was502_cf3_aix, which is located in the WAS5023BASE directory on CD 3-4.
17. Click **Run wizard again** to install interim fixes for WebSphere Application Server V5.0.2.3.
18. Select **Install fixes** and click **Next**.
19. Click **Browse** to specify the Fix Pack location. Go to CD 3-4, select **WAS5023EFIX**, and click **Open**. Click **Next**.
20. Select all available fixes and click **Next**.
21. Review the summary information and click **Next**.

22. The final install panel should display the following message when it is complete:

    ```
    The following fixes were successfully installed:
    ```

    The fixes will appear in the field below the message.

23. Click **Finish**.

24. Verify the installation by running the First Steps GUI from an AIX command prompt:

    ```
    cd /usr/WebSphere/AppServer/bin
    ./firststeps.sh.
    ```

25. Click **Verify Installation**. You should see a message similar to following:

    ```
    IVTL0070I: IVT Verification Succeeded
    IVTL0080I: Installation Verification is complete
    ```

26. Click **Stop the Server**. After the server stops, click **Exit** to close the First Steps WebSphere Portal Server Fix Pack installation.

WebSphere Portal Server cumulative fix installation

1. Open a command prompt, go to *was_home*/bin, and set up the Java environment for the update installer:

   ```
   cd /usr/WebSphere/AppServer/bin
   . ./setupCmdLine.sh
   ```

2. Verify that all WebSphere Application Server servers are stopped:

   ```
   ./serverstatus.sh -all
   ```

3. If they are started, stop them with the **stopserver** command from the same directory:

   ```
   ./stopserver.sh server1
   ./stopserver.sh WebSphere_Portal
   ```

4. Copy the contents of CD 2-3 to *wps_home*/update.

5. Create a fixpacks directory in the update directory:

   ```
   mkdir /usr/WebSphere/PortalServer/update/fixpacks
   ```

6. Move the WP_PTF_5021.jar and the WPCP_PTF_5021.jar, which you previously copied from CD 2-2 to *wps_home*/update, to the *wps_home*/update/fixpacks directory.

7. Edit the soap.client.props file, which is located in *was_home*\properties.

   ```
   cd /usr/WebSphere/AppServer/properties
   ```

8. Change the time out request for the Simple Object Access Protocol (SOAP) client. The default, in seconds, is 180. Change the line to:

   ```
   com.ibm.SOAP.requestTimeout=6000
   ```

9. Run the WebSphere Portal update installer to apply the Fix Pack by running the following commands:

```
cd /usr/WebSphere/PortalServer/update
./updatePortal.sh -fixpack -installDir "/usr/WebSphere/PortalServer"
-fixpackDir "/usr/WebSphere/PortalServer/update/fixpacks" -install
-fixpackID WP_PTF_5021
```

Note: If you receive a message that indicates that *WAS_HOME* is not set, the Java environment might not be properly set up. Repeat step 1.

10. Run the following configuration task:

```
cd /usr/WebSphere/PortalServer/config
./WPSconfig.sh WP-PTF-5021 -DPortalAdminPwd=wpsadmin
```

Note: If the WP-PTF-5021 task fails for some reason, correct the cause of the failure and run the following configuration tasks from the *wps_home*/config directory:

```
./WPSconfig.sh UNINSTALL-WP-PTF-5021 -DPortalAdminPwd=wpsadmin
```

If the WP-PTF-5021 task failed at task 30 of 33 with the following error, `XMLC0009E: Invalid password for user wpsadmin`, verify the Portal Administrator password and run the WP-PTF-5021 command again with a valid password. You do not need to run the UNINSTALL-WP-PTF-5021 configuration task.

11. Verify that all the WebSphere Application Server servers are started:

```
cd /usr/WebSphere/AppServer/bin
./serverStatus.sh -all
```

12. If they are not started, then issue the **`startServer`** command from the same directory:

```
./startServer.sh server1
./startServer.sh WebSphere_Portal
```

13. Open a browser and use the following URL to access the portal: http://hostname:9081/wps/portal, where hostname is the machine where we installed the Portal Server (in our example, m10695bf.itso.ral.ibm.com). The portal will open in your browser.
14. Log on to the portal with the administrator ID. In our example, it is wpsadmin with wpsadmin as the password.
15. The fix installation is complete. The contents of the *wps_home*/update directory are no longer needed and can be deleted.

Configure WebSphere Portal to use DB2

By default, WebSphere Portal installs Cloudscape and sets it up as its database, while WebSphere Everyplace Access requires DB2. The following steps will show how to configure WebSphere Portal with DB2.

1. Export the db2instance environment in your profile by adding the following line to your .profile:

   ```
   if [ -f /home/db2inst1/sqllib/db2profile ]; then .
   /home/db2inst1/sqllib/db2profile; fi
   ```

2. Restart DB2:

   ```
   su - db2inst1
   db2stop
   db2start
   ```

3. Validate that the environment has set the DB2 profile environment variables, such as `DB2INSTANCE=`*`db2inst1`*, where db2inst1represents your database instance by running the **`env`** command.

4. Assuming WebSphere Application Server and WebSphere Portal Server are still running and the command prompt is open, go to *wps_home*/config:

   ```
   cd /usr/WebSphere/PortalServer/config
   ```

5. Export the current database:

   ```
   ./WPSconfig.sh database-transfer-export
   ```

6. After successfully exporting the database, you should see a `BUILD SUCCESSFUL` message.

7. Create a backup copy of *wps_home*/config/wpconfig.properties before changing any values.

8. Create a backup copy of *wps_home*/config/helpers/transfer_db2.properties.

9. Edit *wps_home*/config/helpers/transfer_db2.properties (use the names in Table 6-24 on page 256).

Note: If you need explanations of what each property is used for, look in the configuration file or look in the InfoCenter, which can be installed from the setup CD.

Be sure to use / (slash) instead of \ (backslash).

If there are two values, the first is generic and the second is the one we use in our example environment.

The user we are using is a local user that needs admin access to DB2. It is not an user in the Domino directory!

Table 6-24 Properties

Field	Value
DbSafeMode	false
DbType	db2
DbDriver	COM.ibm.db2.jdbc.app.DB2Driver
DbDriverDS	COM.ibm.db2.jdbc.DB2XADataSource
DbLibrary	*DB2_Home*/java/db2java.zip /home/db2inst1/sqllib/java/db2java.zip
WpsDbName	wps50
DbUrl	jdbc:db2:*WpsDbName* jdbc:db2:wps50
DbUser	db2inst1
DbPassword	db2inst1
WmmDbName	wps50
WmmDbUrl	dbc:db2:*WmmDbName* jdbc:db2:wps50
WmmDbUser	db2inst1
WmmDbPassword	db2inst1
WpcpDbName	wpcp50
WpcpDbUrl	dbc:db2:*WpcpDbName* jdbc:db2:wpcp50
WpcpDbUser	db2inst1
WpcpDbPassword	db2inst1
FeedbackDbName	fdbk50
FeedbackDbUrl	dbc:db2:*FeedbackDbName* jdbc:db2:fdbk50
FeedbackDbUser	db2inst1
FeedbackDbPassword	db2inst1

10. Save the file.

11. Enter the following into the command prompt to import the transfer_db2.properties values into the wpconfig.properties file:

```
cd /usr/WebSphere/PortalServer/config
./WPSconfig.sh
-DparentProperties="/usr/WebSphere/PortalServer/config/helpers/transfer_db2
.properties" -DSaveParentProperties=true
```

12. From *wps_home*/config, enter the following command:

```
./WPSconfig.bat create-local-database-db2
```

13. The message `BUILD SUCCESSFUL` should appear after the setup is complete.
14. Enter the following commands to validate the configuration properties:

```
./WPSconfig.sh validate-database-connection-wps -DDbPassword=db2inst1
./WPSconfig.sh validate-database-connection-wmm -DWmmDbPassword=db2inst1
./WPSconfig.sh validate-database-connection-wpcp -DWpcpDbPassword=db2inst1
-DFeedbackDbPassword=db2inst1
./WPSconfig.sh validate-database-driver
```

Note: If the validate-database commands fail with the message `java]` `java.sql.SQLException: No suitable driver`, ensure that you export the db2instance from step 1 above.

15. Enter the following commands to run the configuration task:

```
./WPSconfig.sh database-transfer-import
```

16. The message `BUILD SUCCESSFUL` should appear after the setup is complete. If the configuration fails, verify the values in the wpconfig.properties file and then repeat this step.
17. Open the DB2 Command Line Processor:

```
su - db2inst1
db2
```

18. For the databases created by the script (in our example, wps50, wpcp50, and fdbk50), run the following commands:

```
connect to wps50 user db2inst1 using db2inst1
reorgchk update statistics on table all
terminate
db2rbind wps50 -l db2rbind.out -u db2inst1-p db2inst1

db2
connect to wpcp50 user db2inst1 using db2inst1
reorgchk update statistics on table all
terminate
db2rbind wpcp50 -l db2rbind.out -u db2inst1 -p db2inst1
db2
```

```
connect to fdbk50 user db2inst1 using db2inst1
reorgchk update statistics on table all
terminate
db2rbind fdbk50 -l db2rbind.out -u db2inst1 -p db2inst1
```

Note: If you used other user names or passwords for the databases during the creation of the databases in step 6, you must modify these commands to match your user names and passwords.

19. Add db2java.zip to the class path information on WebSphere Application Server. Perform the following steps to add the required DB2 JDBC provider files to the WebSphere Application Server class path:
    a. Assuming the WebSphere Application Server is still running, open the Administrative Console by accessing the following URL in a browser:

       ```
       http://m10695bf.itso.ral.ibm.com:9090/admin
       ```

    b. Because we did not enabled security yet, you can use any user name to log on to the Administrative Console.
    c. After logging in, select **Servers** → **Application Servers**, and then click **WebSphere_Portal** from the list of application servers.
    d. Click **Process Definition** from the list of additional properties, and then click **Java Virtual Machine** from the list of additional properties.
    e. In the Classpath field, add the directory path where the db2java.zip file is located, for our example, /home/db2inst1/sqllib/java/db2java.zip.
    f. Click **OK**.
    g. Click the **Save** link to go to the Save page.
    h. Click **Save**.
20. Verify that the WebSphere Portal Server is started:

    ```
    cd /usr/WebSphere/AppServer/bin
    ./serverStatus.sh -all
    ```

21. If it is not started, then issue the **`startServer`** command from the same directory:

    ```
    ./startServer.sh WebSphere_Portal
    ```

22. To verify this configuration, point your browser to the portal, for example:

    ```
    http://m10695bf.itso.ral.ibm.com:9081/wps/portal
    ```

23. Log in with the portal administrator ID wpsadmin and password wpsadmin and go to **Content Publishing**.

Tune DB2 for the portal

Run the following DB2 commands to tune DB2 for WebSphere Portal:

```
su - db2inst1
db2
db2set DB2_EVALUNCOMMITTED=YES
db2set DB2_INLIST_TO_NLJN=YES

db2
connect to wpcp50 user db2inst1 using db2inst1
update db cfg for wpcp50 using locklist 1024
connect reset

connect to wps50 user db2inst1 using db2inst1
CREATE INDEX db2inst1.IX2110D ON db2inst1.PROT_RES (PARENT_OID,OID)
CREATE INDEX db2inst1.IX2140B ON db2inst1.LNK_USER_ROLE (ROLE_INST_OID)
commit
connect reset
quit
```

Note: If you used other user names or passwords for the databases during the creation of the databases, you must modify these commands to match your user names and passwords! If you choose other names for the WebSphere Portal Server database or the WebSphere Portal Content Publishing database, use your names instead!

Configure Portal for Lotus Domino Directory

1. Create a backup copy of *wps_home*/config/wpconfig.properties before changing any values.
2. Create a backup copy of *wps_home*/config/helpers/security_domino.properties.
3. Edit *wps_home*/config/helpers/security_domino.properties (use the values in Table 6-25 on page 260).

Note: If you need explanations of what each property is used for, take a look in the configuration file or look in the InfoCenter, which can be installed from the setup CD.

Users that are used in this configuration file are users in the Domino directory!

Table 6-25 Properties

Field	Value
WasUserid	cn=wpsbind,o=pvclab
WasPassword	wpsbind
WpsHostName	m10695bf.itso.ral.ibm.com
PortalAdminId	cn=wpsadmin,o=pvclab
PortalAdminIdShort	wpsadmin
PortalAdminPwd	wpsadmin
PortalAdminGroupId	cn=wpsadmins
PortalAdminGroupIdShort	wpsadmin
LTPAPassword	passw0rd
LTPATimeout	120
SSODomainName	itso.ral.ibm.com
LookAside	false
LDAPHostName	domldap.pvclab.com
LDAPPort	389
LDAPAdminUId	cn=admin,o=pvclab
LDAPAdminPwd	pvc1class
LDAPServerType	DOMINO502
LDAPBindID	cn=wpsbind,o=pvclab
LDAPBindPassword	wpsbind
LDAPSuffix	
LdapUserPrefix	cn
LdapUserSuffix	o=pvclab
LdapGroupPrefix	cn
LdapGroupSuffix	
LDAPUserObjectClass	dominoPerson
LDAPGroupObjectClass	dominoGroup

Field	Value
LDAPGroupMember	member
LDAPUserFilter	(&(|(cn=%v)(uid=%v))(objectclass=dominoPerson))
LDAPGroupFilter	(&(cn=%v)(|(objectclass=dominoGroup)(objectclass=groupOfUniqueNames)))
LDAPsslEnabled	false

4. Save the file.
5. Stop all WebSphere Application Server servers:

```
cd /usr/WebSphere/AppServer/bin
./stopServer.sh WebSphere_Portal
./stopServer.sh server1
```

6. Change to the directory *wps_home*/config:

```
cd /usr/WebSphere/PortalServer/config
```

7. Enter the following command to import the contents of security_domino.properties into WPSconfig.properties:

```
./WPSconfig.sh
-DparentProperties="/usr/WebSphere/PortalServer/config/helpers/security_dom
ino.propterites" -DSaveParentProperties=true
```

8. Enter the following command to validate the settings to access LDAP:

```
./WPSconfig.sh validate-ldap
```

Note: If this task fails, check the values in the wpconfig.properties file. Also ensure that the LDAP directory is up and running.

9. Run the configuration task to enable security:

```
./WPSconfig.sh enable-security-ldap
```

Note: If the configuration task fails, verify the values in the wpconfig.properties file. Before running the task again, be sure to stop the WebSphere Portal application server by entering the **./stopServer.sh** command from the *was_home*/bin directory and specify the WebSphere Application Server user ID and password (as defined by the WasUserid and WasPassword properties).

Modify PumaService.properties in order to allow users or portal administrators to create and modify directory attributes through self-registration and self-care screens or the Manage Users and Groups portlet. Perform the following steps:

a. Open PumaService.properties file. You can find this file in the *wps_home*/shared/app/config/services directory.

b. Add `user.sync.remove.attributes=cn,CN`.

c. Save the file.

Note: If you do not perform these steps, WebSphere Portal will not be able to create or update a user by using portal functions because of a misconfiguration.

10. Verify that all the WebSphere Application Server servers are started:

```
cd /usr/WebSphere/AppServer/bin
./serverStatus.sh -all
```

11. If they are not started, then issue the **`startServer`** command from the same directory:

```
./startServer.sh server1
./startServer.sh WebSphere_Portal
```

12. Open the Administrative Console by accessing the following URL in a browser:

```
http://m10695bf.itso.ral.ibm.com:9090/admin
```

13. You can use any user name to log on to the Administrative Console

14. Select **Security** → **User Registry** → **LDAP** and select **Advanced LDAP Settings**.

15. Change User ID Map to `person:shortname;*:cn`.

16. Click **Apply**.

17. Select **Save** and save the configuration changes.

18. Restart server1 and WebSphere_Portal:

```
cd /usr/WebSphere/AppServer/bin
./stopServer.sh server1 -username wpsbind -password -wpsbind
./stopServer.sh WebSphere_Portal -username wpsbind -password wpsbind
./startServer.sh server1
./startServer.sh WebSphere_Portal
```

19. To verify the configuration, open a browser and access WebSphere Portal (http:// hostname.yourco.com: port_number/wps/portal). Verify that you can log in. In our scenario, it is http://m10695bf.itso.ral.ibm.com:9081/wps/portal.

Update WebSphere Member Manager for Domino Directory

1. Make a copy of *wps_home*\shared\app\wmm\wmm.xml.
2. Edit *wps_home*\shared\app\wmm\wmm.xml.
3. Find the wmmGenerateExtID property in the file and verify that it is set to true. For example:

   ```
   wmmGenerateExtID="true"
   ```

4. Look for the tag `<supportedLdapEntryTypes>` and modify each "objectClassesForWrite" by adding, at the end, `ibm-appUUIDAux` (four times).

   ```
   objectClassesForWrite="dominoPerson;ibm-appUUIDAux"
   searchBases="o=ITSORaleigh"/>
   objectClassesForWrite="dominoGroup;ibm-appUUIDAux" searchBases=""/>
   objectClassesForWrite="organization;ibm-appUUIDAux" />
   objectClassesForWrite="organizationalUnit;ibm-appUUIDAux" />
   ```

5. Save wmm.xml.
6. Edit *wps_home*\config\templates\wmm\wmmLDAPAttributes_DOMINO502.xml. Inside that file, look for wmmAttributeName="extId". There is a parameter which reads "`pluginAttributeName="distinguishedName"`, which is changed to:

   ```
   pluginAttributeName="ibm-appUUID"
   ```

7. Edit *wps_home*\wmm\wmmLDAPServerAttributes.xml. Map `extId` to `ibm-appUUID`:

   ```
   pluginAttributeName="ibm-appUUID"
   ```

8. Restart the Domino Server.

Note: If you do not restart the Domino server, you might not be able to log in to the portal.

Configure WebSphere Portal Server for IBM HTTP Server

1. Create a backup copy of *wps_home*/config/wpconfig.properties before changing any values.
2. Create a backup copy of *wps_home*/config/helpers/config_http.properties.
3. Check that *wps_home*/config/helpers/config_http.properties contains your machine's host name and fully qualified domain name as well as a port 80 as your HTTP port (see Table 6-26 on page 264).

Table 6-26 WebSphere Portal

Field	Value
WpsHostName	m10695bf.itso.ral.ibm.com
WpsHostPort	80

4. Save the file.
5. Open a command prompt and change the directory to the *wps_root*/config directory.
6. Enter the following into the command prompt to import the config_http.properties content into wpsconfig.properties:

```
./WPSconfig.sh
-DparentProperties="/usr/Websphere/PortalServer/config/helpers/config_http.
properties" -DSaveParentProperties=true
```

7. Enter the following command to configure WebSphere Portal for the Web server:

```
./WPSconfig.sh httpserver-config
```

8. Restart HTTP Server and IBM HTTP Administration Server:

```
cd /usr/IBMHttpServer/bin
./apachectl stop
./adminclt stop
./apcahectl start
./adminclt start
```

9. Restart WebSphere Portal:

```
cd /usr/WebSphere/AppServer/bin
./stopServer.sh WebSphere_Portal -username wpsbind -password wpsbind
./startServer.sh WebSphere_Portal
```

10. Verify that the portal can be accessed from the local Web server, for example, open a browser to:

```
http://m10695bf.itso.ral.ibm.com/wps/portal
```

Additional configuration for IBM HTTP Server

1. Edit the httpd.conf file located in /usr/IBM HTTPServer/conf and change it to the following setting:

```
TIMEOUT 900
```

2. Restart IBM HTTP server:

```
cd /usr/IBMHTTPServer/bin
./apachectl stop
./apachectl start
```

Install Everyplace Access Services

1. Assuming the WebSphere Everyplace Access install program is still open, choose **Everyplace Access Services V5.0** and click **Next**.
2. Insert CD 4 when prompted and click **Next**.
3. Select **English** as the language and click **OK**.
4. Click **Next** on the welcome panel.
5. Specify the installation directory for Everyplace Access Services and click **Next** (see Table 6-27).

Table 6-27 Everyplace Access Services directory

Field	Value
Directory	/usr/WebSphere/EAS

6. Review the summary information to validate the install directory and click **Next** to start copying files.
7. After the install finishes, a panel displays information about the success of the install. Click **Finish**.

Configure Everyplace Access Services

1. Verify that all the WebSphere Application Server servers are started:

```
cd /usr/WebSphere/AppServer/bin
./serverStatus.sh -all
```

2. If they are not started, then issue the **`startServer`** command from the same directory:

```
./startServer.sh server1
./startServer.sh WebSphere_Portal
```

3. Verify that security is enabled for the portal and application server. To verify that security is enabled, attempt to log in to the WebSphere Application Server Administrative Console. If you are challenged to provide a user ID and password, security is enabled. If you are only prompted for a user name, security is not enabled.
4. Make a copy of *eas_home*\config\EASinstallconfig.properties.
5. Edit *eas_home*\config\EASinstallconfig.properties, where eas_home is the directory you specified during the installation (see Table 6-28 on page 266). In our example, the file is located in /usr/WebSphere/EAS.

Note: If you need explanations of what each property is used for, take a look in the configuration file or look in the InfoCenter, which can be installed from the setup CD.

Be sure to use / (slash) instead of \ (backslash).

The user weaadmin for the database is an user of the local system. All other users are users in the Domino directory.

Table 6-28 Properties

Field	Value
instServerInstall	true
instDatabaseInstall	true
instPortalIntegration	true
instNotesPortlets	true
instExchangePortlets	false
instDMS	true
instBlackberry	false
instWPSInstallLocation	/usr/WebSphere/PortalServer
instWPSHostname	m10695bf.itso.ral.ibm.com
instWPSHome	/portal
instWPSCustomPage	/myportal
instWPSBaseURL	/wps
instWPSAdminName	wpsadmin
instWPSAdminPassword	wpsadmin
instWPSPort	80
instWASInstallationLocation	/usr/WebSphere/AppServer
instWASAdminNode	m10695bf
instWASAdminCell	m10695bf
instWASUsername	wpsbind
instWASPassword	wpsbind

Field	Value
instWASHostName	m10695bf.itso.ral.ibm.com
instDBDatasourceHelper	com.ibm.websphere.rsadapter.DB2DataStoreHelper
instDBType	db2
instDBPath	/home/db2inst1/sqllib
instDBUName	db2inst1
instDBAdminName	db2inst1
instDAdminPassword	db2inst1
instJDBCDriverName	com.ibm.db2.jdbc.app.DB2Driver
instJDBCImplementationClass name	COM.ibm.db2.jdbc.DB2ConnectionPoolDataSource
InstJDBCDriverPath	/home/db2inst1/sqllib/java12/db2java.zip
instDBServerHostname	m10695bf.itso.ral.ibm.com
instDBLocalInstance	db2inst1
instWEASDB	WEASDB
instDMS_DMSServerName	m10695bf.itso.ral.ibm.com
instDMS_DMSAdminGroup	dmadmins

6. Save the EASinstallconfig.properties file.
7. Run the command to configure all components:

```
cd /usr/WebSphere/EAS/config
./EASWASconfig.sh eas-basic-config
```

8. If the configuration fails, correct the problem and run the configuration task again.
9. Log in to the WebSphere Everyplace Access portal as an administrator and verify that the new WebSphere Everyplace Access theme and look and feel has been applied.

Install Device Manager

1. Assuming the WebSphere Everyplace Access install program is still open, choose **Device Manager V1.6** and click **Next**.
2. Insert CD 4 when prompted and click **Next**.
3. Select **English** as the language and click **OK**.

4. Click **Next** on the welcome panel.
5. Specify the installation directory for Device Manager and click **Next**.

Table 6-29 Device Manager installation directory

Field	Value
Directory	/usr/WebSphere/DMS16

6. Select **Device Manager Server** and **Device Manager database**. Click **Next**.
7. Review the summary information and click **Next** to start copying files.
8. After the install finished, a panel displays information about the success of the install. Click **Finish** to exit the Device Manager install program.

Configure Device Manager

1. Verify that all the WebSphere Application Server servers are started:

```
cd /usr/WebSphere/AppServer/bin
./serverStatus.sh -all
```

2. If they are not started, then issue the **`startServer`** command from the same directory:

```
./startServer.sh server1
./startServer.sh WebSphere_Portal
```

3. Make a copy of *dms_home*\config\DMSinstallconfig.properties, where dms_home is the directory you specified during the installation. In our example, it is located in /usr/WebSphere/DMS16.
4. Edit *dms_home*\config\DMSinstallconfig.properties (use the values in Table 6-30 on page 269).

Note: If you need explanations of what each property is used for, take a look in the configuration file or look in the InfoCenter, which can be installed from the setup CD.

Be sure to use / (slash) instead of \ (backslash).

The user weaadmin for the database is an user of the local system. All other users are users in the Domino directory.

Table 6-30 Properties

Field	Value
instDBType	db2
instDBPath	/home/db2inst1/sqllib
instDBUserId	db2inst1
instDBPassword	db2inst1
instDBName	dms
instDBInstance	db2inst1
instDBDropFlag	false
instDBAdmin	db2inst1
instDBAdminPassword	db2inst1
instDBHome	/db/db2
instDBFiles	/dmsdb
instJavapath	/usr/WebSphere/DMS16/Java/win/jre
instDBAdminGroup	db2grp1
instWASPath	/usr/WebSphere/AppServer
instNode	m10695bf
instHostName	m10695bf.itso.ral.ibm.com
instWASUsername	wpsbind
instWASPassword	wpsbind
instRemoteWebServer	false
instWebServerHome	/usr/IBMHttpServer
instWPSHttpRouter	http://m10695bf.itso.ral.ibm.com/UserGroupInfoWebService/servlet/rpcrouter
instWPSHttpAltRouter	http://m10695bf.itso.ral.ibm.com/UserGroupInfoWebServiceAlt/servlet/rpcrouter
instWPSUserName	wpsadmin
instWPSUserPw	wpsadmins
instDMAdminGroup	dmadmins

Field	Value
instRemoteDB	false

5. Save the DMSinstallconfig.properties file.
6. Run the command to configure all components:

```
cd /usr/WebSphere/DMS16/config
./DMSconfig.sh
```

7. Open the DB2 Command Line Processor and connect to the Device Manager database:

```
su - db2inst1
db2
connect to dms user db2inst1 using db2inst1
quit
```

Install Everyplace Synchronization Server

1. Assuming the WebSphere Everyplace Access install program is still open, choose **Everyplace Synchronization Server** and click **Next**.
2. Insert the CD when prompted and click **Next**.
3. Select **English** as the language and click **OK**.
4. Click **Next** on the welcome panel.
5. Specify the installation directory for Everyplace Synchronization Server and click **Next** (see Table 6-31).

Table 6-31 Everyplace Synchronization Server install directory

Field	Value
Directory	/usr/WebSphere/IBMSyncServer

6. Review the summary information to validate the install directory and click **Next** to start copying files.
7. After the install finishes, a panel displays information about the success of the install. Click **Finish**.

Configure Everyplace Synchronization Server

1. Verify that all the WebSphere Application Server servers are started:

```
cd /usr/WebSphere/AppServer/bin
./serverStatus.sh -all
```

2. If they are not started, then issue the **startServer** command from the same directory:

```
./startServer.sh server1
./startServer.sh WebSphere_Portal
```

3. Make a copy of *ess_home*\config\ESSinstallconfig.properties, where ess_home is the directory you specified during the installation. In our example, it is C:\Program Files\WebSphere\IBMSyncServer.
4. Edit *ess_home*\config\ESSinstallconfig.properties (use the values in Table 6-32).

Note: If you need explanations of what each property is used for, take a look in the configuration file or look in the InfoCenter, which can be installed from the setup CD.

Be sure to use / (slash) instead of \ (backslash).

The user weaadmin for the database is an user of the local system. The user essadmin will be created on the local system. wpsbind is a user in the Domino directory.

Table 6-32 Properties

Field	Value
instPath	/usr/WebSphere/IBMSyncServer
instDatabaseInstall	true
instServerInstall	true
instPortletsInstall	true
instDBType	db2
instDBUserid	essisnt1 Note: The configuration script will create this user ID. It must be eight characters and must no begin with ibm, sys, or sql.
instDBPassword	essinst1
instDBPath	/usr/opt/db2_08_01
instDBURL	jdbc:db2:
instDBDriver	com.ibm.db2.jcc.DB2Driver

Field	Value
instDBLibPath	/usr/opt/db2_08_01/java/db2java.zip:/usr/opt/db2_08_01/java/db2jcc.jar:/usr/opt/db2_08_01/java/db2jcc_license_cu.jar
instDBHostName	m10695bf.itso.ral.ibm.com
instDBDropFlag	true
instDBPort	52000
instCell	m10695bf
instNode	m10695bf
instWASUserName	wpsbind
instWASPassword	wpsbind
instWPSHost	m10695bf.itso.ral.ibm.com
instWPSHome	/portal
instWPSPath	/usr/WebSphere/PortalServer
instWPSUrlPrefix	/wps
instWPSUsername	wpsadmin
instWPSPassword	wpsadmin
instWPSPort	80
instWPSAdminGroup	wpsadmins
instUserGroup1	essusers
instNonLockUserGroup	essuers_nonlock
instAdminGroup1	essadmins
instAdminGroup2	essadmins
instESSAdmin1	wpsadmin
instESSAdmin2	wpsadmins
instESSAdminPwd1	wpsadmin
instESSAdminPwd2	wpsadmin
instJavaPath	/usr/WebSphere/IBMSyncServer/java/jre

Field	Value
instWASPath	/usr/WebSphere/AppServer
instHttpServer	/usr/IBMHttpServer
instInfoLocale	en
instBackendDomino	true
instBackendExch2000	false
instBackendExch55	false
instDominoDataRoot	/local/notesdata
instNotesDataPath	/local/notesdata
instNotesPath	/opt/lotus/notes/latest/ibmpow
instDominoHost	domldap.pvclab.com
instDominoUserID	admin
instDominoPassword	pvc1class
instDominoAbbreviatedServername	
instContextRoot	/ess
instESSAdminRMIPort	20000
instDBDefaultDB2	db2inst1
instUseExistingDBInstance	false

5. Save the EASinstallconfig.properties file.
6. In a command window, go to *ess_home*/config and begin the configuration:

   ```
   cd /usr/WebSphere/IBMSyncServer/config
   ./ESSWASconfig.sh basic-config
   ```

7. After finishing the configuration, you should see a `BUILD SUCCESSFUL` message.
8. Open the Administrative Console by accessing the following URL in a browser:

   ```
   http://m10695bf.itso.ral.ibm.com:9090/admin
   ```

9. Select **Environment** → **Update Web Server Plugin** in the console navigation tree to go to the Update Web Server Plug-in page.

10. Click **OK** to regenerate the plug-in. You might need to stop the server and then start the server again before the changes to the plug-in configuration go into effect.
11. Verify that the Web server plug-in configuration has been updated and that the SyncML servlet is running by entering the following URL into your browser:

    ```
    http://m10695bf.itso.ral.ibm.com/ess/SyncML
    ```

12. When the login prompt appears, enter the WebSphere Portal administrator ID and password, such as wpsadmin and wpsadmin.
13. Copy the Notes user ID file for the Everyplace Synchronization Server /usr/WebSphere/IBMSyncServer/Notes Data directory. This is the Notes super user ID that is added to each user's mail file Access Control List. The ID file is called admin.id and belongs to the user admin/pvclab in our example.
14. Change the ownership of the ID to the AIX Everyplace Synchronization Server administrator ID:

    ```
    cd /usr/WebSphere/IBMSyncServer/NotesData
    chown essinst1 admin.id
    ```

Install Intelligent Notification Services

1. Assuming the WebSphere Everyplace Access install program is still open, choose **Intelligent Notification Services** and click **Next**.
2. Insert CD 5 when prompted and click **Next**.
3. Select **English** as the language and click **OK**.
4. Click **Next** on the welcome panel.
5. Specify the installation directory for Intelligent Notification Services and click **Next** (see Table 6-33).

Table 6-33 Intelligent Notification Services install directory

Field	Value
Directory	/usr/WebSphere/INS

6. Review the summary information to validate the install directory and click **Next** to start copying files.
7. After the install finishes, a panel displays information about the success of the install. Click **Finish**.

Configure Intelligent Notification Services

1. Ensure that the group insgroup exists in AIX; if it does not, create it.
2. If one does not exist, create an Intelligent Notification Services administrator with the following attributes:
   - Name: `insadmin`
   - Primary Group: `insgroup`
   - Group Set: `mqm,system,`
3. Verify that all the WebSphere Application Server servers are started:

   ```
   cd /usr/WebSphere/AppServer/bin
   ./serverStatus.sh -all
   ```

4. If they are not started, then issue the **`startServer`** command from the same directory:

   ```
   ./startServer.sh server1
   ./startServer.sh WebSphere_Portal
   ```

5. Copy the Notes user ID file for the Intelligent Notification Services /usr/WebSphere/INS/NotesData directory. This is the Notes super user ID that is added to each user's mail file Access Control List. The ID file is called admin.id and belongs to the user admin/pvclab in our example.
6. Make a copy of *ins_home*/config/INSinstallconfig.properties, where ins_home is the directory you specified during the installation. In our example, it is /usr/WebSphere/INS.
7. Edit *ins_home*/config/INSinstallconfig.properties (use the values in Table 6-34).

Note: If you need explanations of what each property is used for, take a look in the configuration file or look in the InfoCenter, which can be installed from the setup CD.

Be sure to use / (slash) instead of \ (backslash).

The user weaadmin for the database is a user of the local system. All other users are users in the Domino directory.

Table 6-34 Properties

Field	Value
instNMConfig	true
instSMConfig	true

Field	Value
instMCSConfig	false
instMCSDomino	false
instDatabaseConfig	true
instPortletsConfig	true
instNode	m10695bf
instWASPath	/usr/WebSphere/AppServer
instWASUserName	wpsbind
instWASPassword	wpsbind
instDBUserid	db2inst1
instDBPassword	db2inst1
instDBName	insdb
instDBHostName	m10695bf.itso.ral.ibm.com
instDBPort	6789
instDBPath	/usr/db2inst1/sqllib
instDBLibPath	/home/db2inst1/sqllib/java12/db2java.zip
instNotesPath	
instNotesDataPath	
instDominoUserid	
instDominoPassword	
instDominoHost	
instINSUserid	
instWPSHost	m10695bf.itso.ral.ibm.com
instWPSPath	/usr/WebSphere/PortalServer
instPWSUrlPrefix	/wps
instWPSHome	/portal
instWPSPath	/usr/WebSphere/PortalServer
instWPSUrlPrefix	/wps

Field	Value
instWPSURLConfigPrefix	/config
instWPSAdminUser	wpsadmin
instWPSPassword	wpsamin
instWPSPort	80
instWPSAdminGroup	wpsadmins
instINSAdminuser	insadmin
instINSAdminPassword	insadmin
removeINSAdminUserOnUninstall	true
instINSAdminGroup	insadmins
removeINSAdminGroupOnUninstall	true
instINSUserGroup	insusers
removeINSUserGroupOnUninstall	true
installLocation	/usr/WebSphere/INS

8. Save the EASinstallconfig.properties file.
9. In a command window, go to *ins_home*/config and begin the configuration:

```
cd /usr/WebSphere/INS/config
./INSWASconfig.sh basic-config
```

10. After finishing the configuration, you should see a `BUILD SUCCESSFUL` message.
11. Change the ownership of the ID to the AIX Everyplace Synchronization Server administrator ID:

```
cd /usr/WebSphere/INS/NotesData
chown insadmin admin.id
```

12. For Intelligent Notification Services, you need to run db2jstrt. Run the command for the appropriate operating system. The variable *port_number* is the port that the feature is listening on. This was specified during the INS installation. The default port is 6789:

```
su - db2inst1
db2jstrt 6789
```

13. After configuring Intelligent Notification Services server, we recommend running the setSmQueues script. Otherwise, Intelligent Notification Services will stop after reaching the default subscriptions limit. Ensure the Intelligent Notification Services server, INSServer, is stopped:

```
cd/usr/websphere/appserver/bin
./serverstatus -all -user wpsbind -password wpsbind
```

14. If INSServer is started, stop it:

```
./stopserver.sh INSServer -user wpsbind -password wpsbind
```

15. In the command prompt, go to *ins_home*/config/templates/mq and run the **setSmQueue** command. The values for *brokerQMgrHost* and *brokerQMgrServer* can be checked in *ins_home*/config/xml/subscriptionManagerConfig.xml:

```
setSmQueue WAS_brokerQMgrHost_brokerQMgrServer
```

For our example, it is:

```
setSmQueue WAS__m10695bf_INSServer
```

Install DB2 Everyplace

1. Assuming the WebSphere Everyplace Access install program is still open, choose **DB2 Everyplace** and click **Next**.
2. Insert CD 5 if prompted and click **Next**.
3. Select **English** as the language and click **OK**.
4. Click **Next** on the welcome panel.
5. Specify the installation directory for DB2 Everyplace and click **Next** (see Table 6-35).

Table 6-35 DB2 Everyplace install directory

Field	Value
Directory	/usr/WebSphere/DB2Everyplace81

6. Review the summary information to validate the install directory and click **Next** to start copying files.
7. After the install finished, a panel displays information about the success of the install. Click **Finish**.

Configure DB2 Everyplace

1. Verify that all the WebSphere Application Server servers are started:

```
cd /usr/WebSphere/AppServer/bin
./serverStatus.sh -all
```

2. If they are not started, then issue the **startServer** command from the same directory:

```
./startServer.sh server1
./startServer.sh WebSphere_Portal
```

3. Make a copy of *db2e_home*/config/dsyconfig.properties, where db2e_home is the directory you specified during the installation. In our example, it is /usr/WebSphere/DB2Everyplace81.
4. Edit *db2e_home*/config/dsyconfig.properties (use the values in Table 6-36).

Note: If you need explanations of what each property is used for, take a look in the configuration file or look in the InfoCenter, which can be installed from the setup CD.

Be sure to use / (slash) instead of \ (backslash).

The user weaadmin for the database is a user of the local system. All other users are users in the Domino directory.

Table 6-36 Properties

Field	Value
createControldb	true
isDB2MessageStore	false
dsyctldbuser	db2inst1
dsyctldbPassword	db2inst1
wpsHost	m10695Bf.itso.ral.ibm.com
portalUser	wpsadmin
portalPassword	wpsadmin
syncgroup	SyncGroup
groupPrefix	DB2e
Virtual Host	default_host
wasAdminServer	server1
wasHome	/usr/ebSphere/AppServer
wasUserName	wpsbind
wasPassword	wpsbind

Field	Value
wasNode	m10695bf
ip	9.42.171.16
serverName	IBMDB2eServer
jdbcDriverClasspath	
wasCell	m10695bf
instance	db2inst1

5. Save the dsyconfig.properties file.
6. In a command window, go to *db2e_home*/config and begin the configuration:

```
cd /usrWebSphere/DB2Everyplace/config
./DSYconfig basic-config
```

7. After finishing the configuration, you should see a `BUILD SUCCESSFUL` message.

Install Location Aware Services

1. Assuming the WebSphere Everyplace Access install program is still open, choose **Location Aware Services** and click **Next**.
2. Insert CD 5 if prompted and click **Next**.
3. Select **English** as the language and click **OK**.
4. Click **Next** on the welcome panel.
5. Specify the installation directory for Location Aware Services and click **Next** (see Table 6-37).

Table 6-37 Location Aware Services install directory

Field	Value
Directory	/usrWebSphere/LAS

6. Review the summary information to validate the install directory and click **Next** to start copying files.
7. After the install finishes, a panel displays information about the success of the install. Click **Finish**.

Configure Location Aware Services

1. Verify that all the WebSphere Application Server servers are started:

```
cd /usr/WebSphere/AppServer/bin
```

```
./serverStatus.sh -all
```

2. If they are not started, then issue the **startServer** command from the same directory:

```
./startServer.sh server1
./startServer.sh WebSphere_Portal
```

3. Make a copy of *las_home*\config\LASinstallconfig.properties, where las_home is the directory you specified during the installation. In our example, it is /usr/WebSphere/LAS.
4. Edit *las_home*/config/LASinstallconfig.properties (use the values in Table 6-38).

Note: If you need explanations of what each property is used for, take a look in the configuration file or look in the InfoCenter, which can be installed from the setup CD.

Be sure to use / (slash) instead of \ (backslash).

The user weaadmin for the database is an user of the local system. All other users are users in the Domino directory.

Table 6-38 Properties

Field	Value
instProduct	WEA
LasHost	m10695bf.itso.ral.ibm.com
LasInstallLocation	/usr/WebSphere/LAS
WasHome	/usr/WebSphere/AppServer
CellName	m10695df
NodeName	m10695bf
WasAdminServer	server1
WasUserid	wpsbind
WasPassword	wpsbind
DefaultVirtualHostName	default_host
LasDbType	db2
LasDbInstPath	/usr/opt/db2_08_01
LasDbLocalInstance	db2inst1

Field	Value
LasDbServerHost	m10695bf.itso.ral.ibm.com
LasDbUser	db2inst1
LasDbPassword	db2inst1
LasDbName	lasdb
LasDbJdbcPort	6789
LasDbLibrary	/usr/opt/db2_08_01/java/db2java.zip
LasDbDriver	COM.ibm.db2.jdbc.net.DB2Driver
LasDbUrl	jdbc:db2:
LasJdbcProvider	las50JDBC
LasDbDriverDs	COM.ibm.db2.jdbc.DB2ConnectionPoolDataSource
LasDbLibraryDS	/usr/opt/db2_08_01/java/db2java.zip:/usr/opt/db2_08_01/java/db2jcc.jar
LasDbName	las50ds
WpsHome	/usr/WebSphere/PortalServer
PortalServerName	WebSphere_Portal
WpsHostName	m10695bf.itso.ral.ibm.com
WpsHostPort	80
WpsContextRoot	wps
PortalAdminidShort	wpsadmin
PortalAdminPassword	wpsadmin
LasAdminGroupIdShort	lasadmins
LasServerName	LasAppServer

5. Save the LASinstallconfig.properties file.

6. In a command window, go to *ins_home*/config and begin the configuration:

```
cd /usr/WebSphere/LAS/config
./LASWASconfig.sh las-basic-config
```

7. After finishing the configuration, you should see a `BUILD SUCCESSFUL` message.

Install additional WebSphere Application Server fixes

In order to improve the performance of Intelligent Notification Services, the installation of several additional WebSphere Application Server fixes is recommended.

1. Stop IBM HTTP Server and IBM HTTP Administration Server:

```
cd /usr/IBMHttpServer/bin
./apachectl stop
./adminclt stop
```

2. Stop all of the WebSphere Application Server servers, where servername is the name of the application server, such as INSServer or WebSphere_Portal:

```
cd /usr/WebSphere/AppServer/bin
./serversStatus.sh -all -user wpsbind -password wpsbind
./stopServer.sh servername -username wpsbind -password wpsbind
```

3. Mount the WebSphere Everyplace Access Setup CD and start the WebSphere Everyplace Access V5 Installer:

```
./cdrom/install.sh (cdrom = cdrom file system name)
```

4. Select **English** and click **OK**.
5. Click **Next** or launch the InfoCenter.
6. Go to *MQ_Home*/java/lib, where MQ_Home is the installation directory where WebSphere MQ embedded messaging is installed. In our example, it is C:\Program Files\IBM\WebSphere MQ.
7. Make a backup copy of com.ibm.mqjms.jar and com.ibm.mq.jar.
8. Unzip IC38409.windows.zip into *MQ_Home*\java\lib. It will overwrite the two files we just backed up. The IC38409.windows.zip is located in the directory WAS_INS on CD 3-3.
9. Go to *MQ_Home*\WEMPS\bin and make a backup copy of imbdfmqm.lil.
10. From the WAS_INS directory on CD 3-3, copy the imbdfmqm.lil file to *MQ_Home*\WEMPS\bin. That will overwrite the file we just backed up.
11. Assuming the WebSphere Everyplace Access install program is still open, choose **WebSphere Application Server fix pack and interim fix** and click **Next**.
12. Insert the CD when prompted and click **Next**.

13. Select **English** as the language and click **OK**.
14. Click **Next** on the welcome panel.
15. Review the license agreement, select **I accept the terms in the license agreement**, and click **Next**.
16. The next panel should display the currently installed version of WebSphere Application Server. If it does not, click the empty text box and the information should appear.
17. Select **IBM WebSphere Application Server v5.0.2.3 + Enterprise v5.0.2.2**, accept the default install location of the Application Server, and click **Next**.
18. Select **Install fix packs** and click **Next**.
19. Click **Browse** to specify the Fix Pack location. Go to the CD 3-3, select **WAS_INS**, and click **Open**. Click **Next**.
20. Select the two available fixes (Messaging eFix and PQ78200) and click **Next**.
21. Review the summary information and click **Next**.
22. The final install panel should display the following message when it is complete:

    ```
    The following fixes were successfully installed:
    ```

    The fixes will appear in the field below the message.
23. Click **Finish**.
24. Go to *WAS_Home*\tranlog\INSServer\ and delete all the files in this directory.

Another fix has to be applied to DB2 for DB2e improvements.

1. Go to **Start** → **Settings** → **Control Panel** → **Administrative Tools** → **Services** and stop all services related to DB2.
2. Copy hotfixpkg_11633.exe to a local temporary directory. This file can be found in the hotfix directory of CD 1-1.
3. Open a command window and, from the temporary directory, run the following command:

   ```
   hotfixpkg_11633 -a -f
   ```
4. Go to the to the DB2 install directory and run **`hotfix -l`** and **`db2level`** to verify 11633 was applied:

   ```
   cd \Program Files\IBM\SQLLIB
   hotfix -l
   db2level
   ```
5. You should see the Hotfix 11633 in the output of the commands.

6. Restart DB2 either by starting all the services you stopped in Step 1 or by stopping IBM HTTP Server and IBM HTTP Administration Server:

```
cd /usr/IBMHttpServer/bin
./apachectl stop
./adminclt stop
./apcahectl start
./adminclt start
```

7. Restart WebSphere Portal:

```
cd /usr/WebSphere/AppServer/bin
./stopServer.sh WebSphere_Portal -username wpsbind -password wpsbind
./startServer.sh WebSphere_Portal
```

Note: If your INSServer will not start correctly after applying the patches, be sure to delete all the files in *WAS_Home*\tranlog\INSServer\.

7

WebSphere Everyplace Client installation and configuration

In this chapter, we describe the installation and configuration of the WebSphere Everyplace Client V5.0.1 for Palm OS and Windows CE mobile devices (Pocket PC 2002 and Windows Mobile 2003).

© Copyright IBM Corp. 2005. All rights reserved.

7.1 Overview

The Everyplace Client is an integrated client application for personal digital assistants (PDAs) and cell phones. It provides a framework that supports information refreshment, security, device management, offline Portal pages, offline forms, and database synchronization.

As of this writing, the list of tested and certified devices supported by Everyplace Client 5 are:

- Pocket PC 2002 and Windows Mobile 2003 based devices:
  - Hitachi G1000
  - HP iPAQ 3760
  - HP iPAQ 1935
  - HP iPAQ 4150
  - HP iPAQ 5550
  - HP iPAQ 6315
  - Symbol 8800
  - MMO2 XDA II
  - Toshiba e405
  - Dell Axim X3
  - Siemens LOOX 610
- Palm OS based devices
  - PalmOne Tungsten C
  - PalmOne Tungsten W
  - PalmOne Treo 600
  - PalmOne Treo 300 (Web download only)
  - Kyocera 7135 (Web download only)
- Symbian OS based devices
  - Sony Ericsson P900
  - Nokia 9500 Communicator
- e-Linux OS based devices:
  - Sharp Zaurus SL-6000 (Japanese only)
- KDDI BREW Business Profile (BBP)
- DoCoMo P900i, N900i, and F900i

Note: Everyplace Client for Treo 300, Kyocera 7135, and Sharp Zaurus SL-6000 devices is WEA R4.3 FP5 based code.

Note: To obtain more information about Everyplace Client supported devices, refer to the WEA support page:

http://www.ibm.com/software/pervasive/ws_everyplace_access/support

The following sections will guide you on installing and configuring Everyplace Client for Palm OS and Pocket PC. However, the recommended method for installing Everyplace Client is to use the DMS update job (see Chapter 9, “Device Services” on page 339 for more information).

7.2 Everyplace Client for Palm OS

The Everyplace Client for Palm OS provides different characteristics, depending on the Palm OS device version. Table 7-1 shows a list of the characteristics supported on each version.

Table 7-1 Everyplace Clients feature support per Palm OS

Palm OS device	Tungsten W	Tungsten C	Treo 600
Integrated shell	Yes (in WEA Client 5.0.1)	Yes (in WEA Client 5.0.1)	Yes (in WEA Client 5.0.1)
E-mail and PIM sync	Yes	Yes	Yes
E-mail attachment support	Yes	Yes	Yes
Invitation support	Yes	Yes	Yes
DB2 Everyplace	V8.1.2 (in WEA Client 5.0) V8.1.4 (in WEA Client 5.0.1)	V8.1.2 (in WEA Client 5.0) V8.1.4 (in WEA Client 5.0.1)	V8.1.2 (in WEA Client 5.0) V8.1.4 (in WEA Client 5.0.1)
Offline browsing	No	Yes	No
Offline forms	No	No	No

Palm OS device	Tungsten W	Tungsten C	Treo 600
Device Manager Agent	V1.3 (in WEA Client 5.0). V1.6 (in WEA Client 5.0.1)	V1.3 (in WEA Client 5.0). V1.6 (in WEA Client 5.0.1)	V1.3 (in WEA Client 5.0). V1.6 (in WEA Client 5.0.1)
Lotus Sametime	Yes	Yes	Yes
Server Initiated Action	No	No	No

7.2.1 Everyplace Client V5.0.1 installation

Assuming your Palm device has previously performed a HotSync synchronization with your desktop, follow these steps to install Everyplace Client for Palm OS:

1. Run the setup.exe program to install Everyplace Client V5.0.1 for Palm OS.
2. Select the setup language for this installation. For the purposes of this installation, select **English**. Click **OK**.
3. You will be presented with a welcome window (see Figure 7-1). Click **Next**.

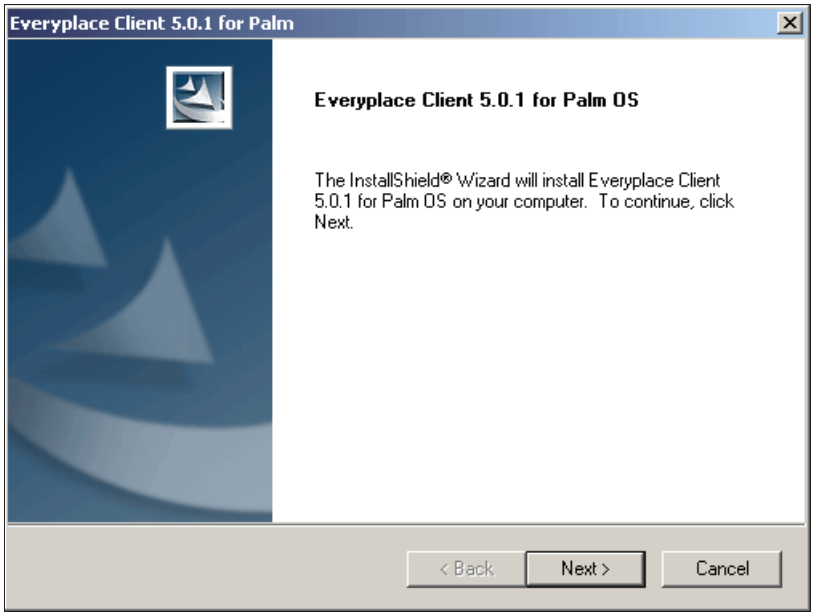

Figure 7-1 InstallShield Welcome window

4. Read through the License Agreement and then click **Yes**. If you are also presented with the License Agreement in Notepad, you may want to close it.

5. Select the type of setup you prefer. Choose between the appropriate Palm OS device or select a custom installation (see Figure 7-2). Click **Next**.

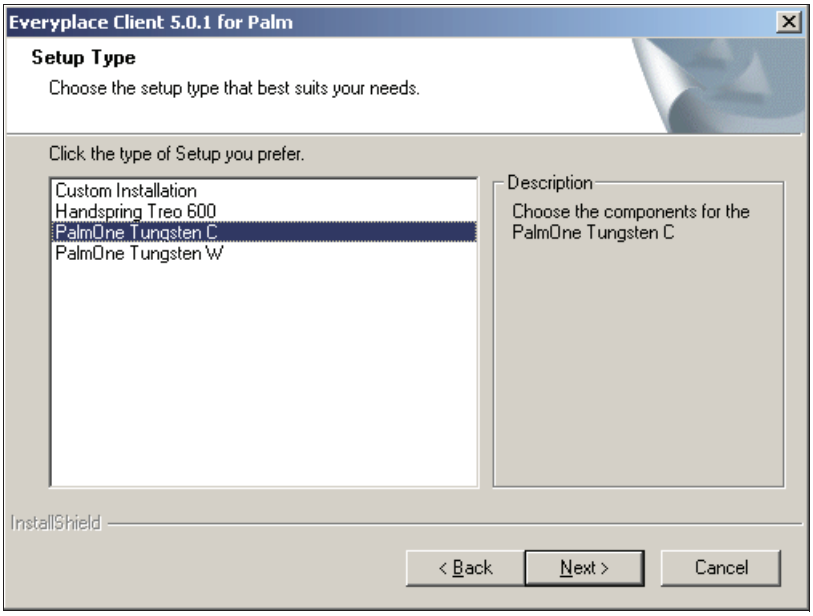

Figure 7-2 Setup type window

6. If you chose a custom installation, select the components you want to install and click **Next** (see Figure 7-3 on page 292).

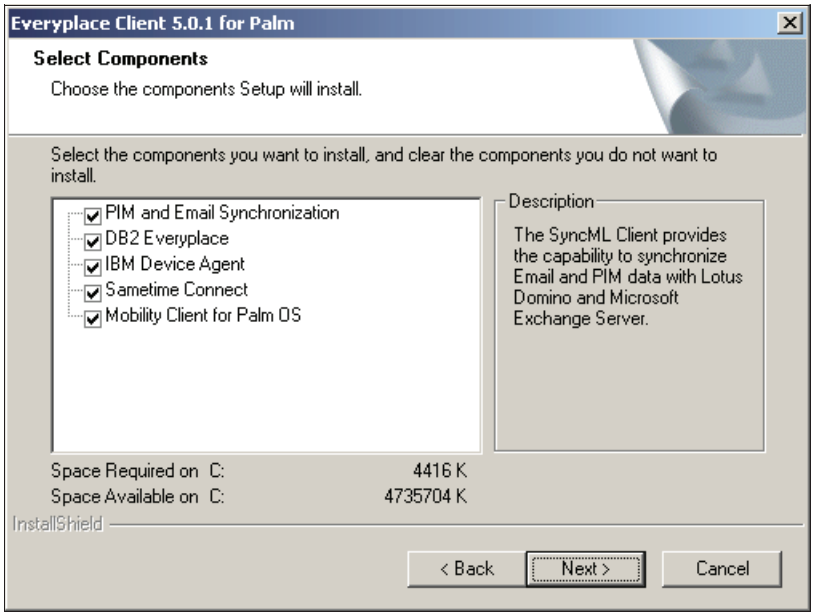

Figure 7-3 Select Components window

7. Specify the destination folder where you want to install the files. For this installation, accept the default destination folder by clicking **Next** (see Figure 7-4 on page 293).

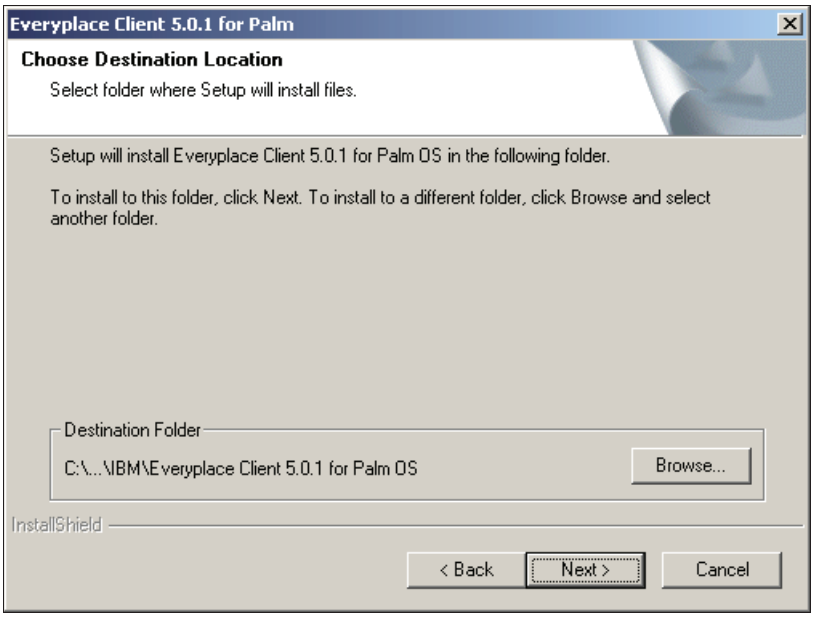

Figure 7-4 Select destination folder for Everyplace Client

8. Review the settings you have selected. If you want to change anything, click **Back**; otherwise, click **Next** (see Figure 7-5 on page 294).

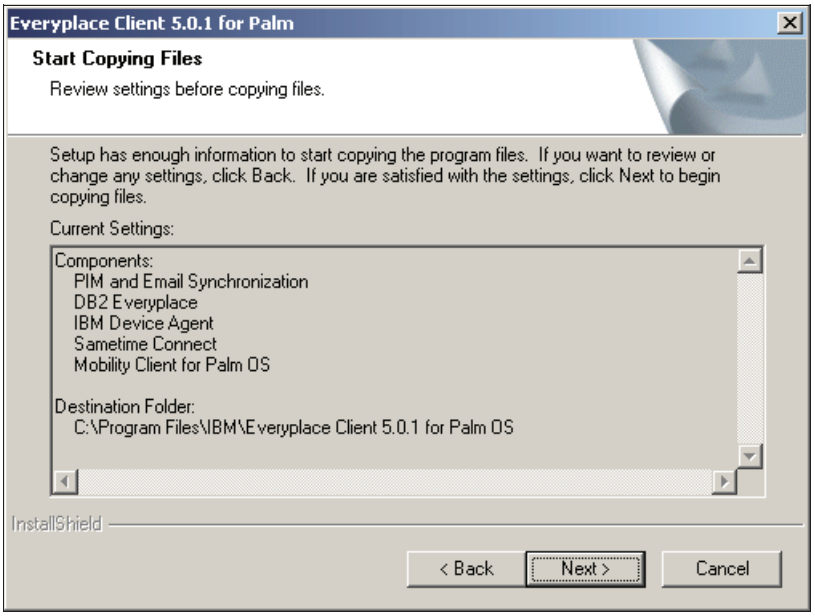

Figure 7-5 Installation selection summary

9. At the end of the installation, the **InstallShield Wizard Complete** window will appear. Click **Finish**. This completes the installation as far as the desktop is concerned.
10. You will get a pop-up window telling you to perform a soft reset and use HotSync to install Everyplace Client on your Palm device (see Figure 7-6). Click **OK**.

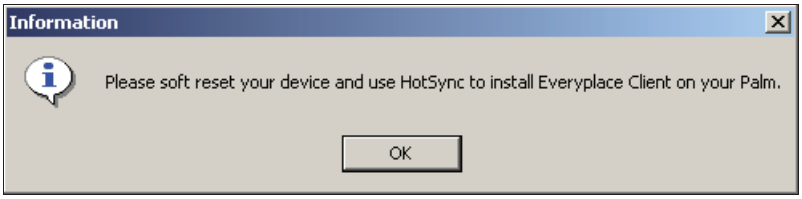

Figure 7-6 Use HotSync pop-up window

Now, if you want to install the client on your device, simply perform a HotSync synchronization. You have to soft reset the Palm device to finish the Everyplace Client installation.

If you wish to install the client on the Palm Simulator for development purposes, you have an alternative method, which is described in the following section.

Installing on Palm Simulator (Palm OS 5.x support)

The following steps illustrates a sample Everyplace Client installation:

1. Start a Simulator session.
2. Right-click in the Simulator window and choose **Install** → **Database**. In the Open window, move to the Everyplace client for Palm OS installation directory (c:\Program Files\IBM\Everyplace Client 5.0.1 for Palm OS\prc in our example) and select all files. Click **Open** (see Figure 7-7).

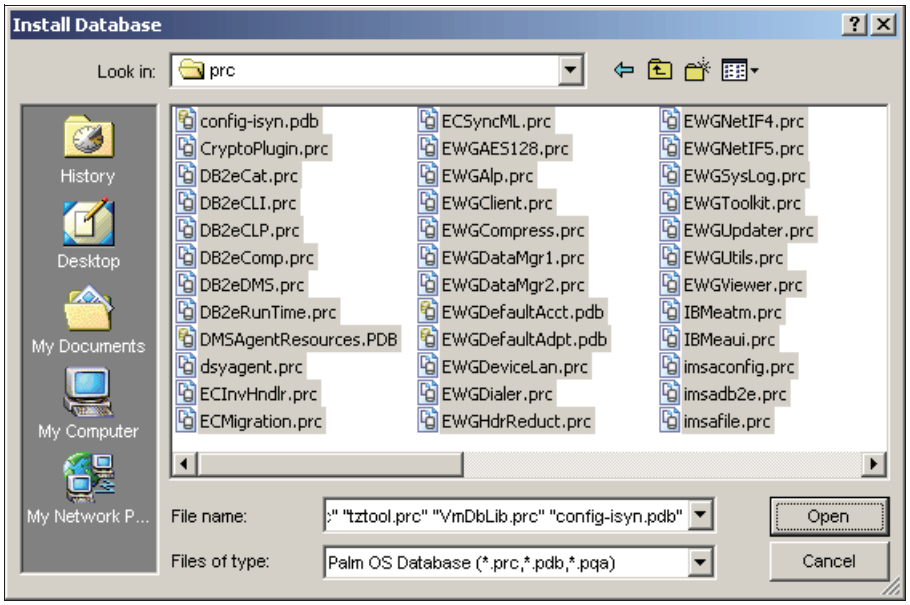

Figure 7-7 Select all Everyplace Client files

3. The installer warns that the Simulator requires a soft reset. Click **OK** (see Figure 7-8).

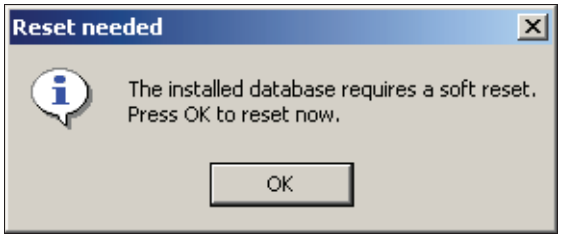

Figure 7-8 Soft reset required

4. The Simulator is now properly configured and ready to use. Now you should save the current session by selecting **Storage** → **Save** from the Simulator menu. When you want to restore the session, simply select **Storage** → **Load** from the Simulator menu.

7.2.2 Everyplace Client configuration

After completing the installation of Everyplace Client for Palm OS, you still need to configure it to tell it where the component servers are. Everyplace Client provides the ability to create multiple network profiles. This will allow you to connect different Everyplace Access servers simply by changing your network profile. For the purposes of this installation, we will stick with the default network profile.

To configure Everyplace Client profile for Palm OS, perform the following steps:

1. Launch Everyplace Client on your Palm by clicking **Everyplace** (see Figure 7-9).

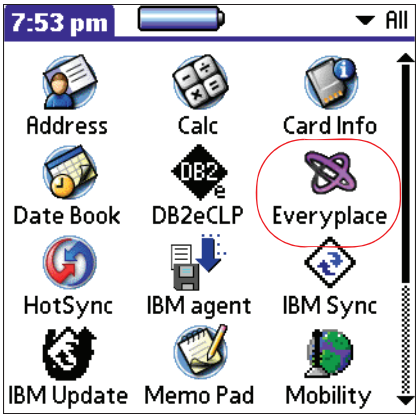

Figure 7-9 Launch Everyplace Client

2. If you have not previously configured Everyplace Client, a message will appear to start the Network Profile wizard to collect the necessary information. Click **OK** (see Figure 7-10 on page 297).

Figure 7-10 Start Network Profile wizard

3. Follow the steps and enter the requested information. Click the right arrow to go to the next screen or the left arrow to go back:
   a. Network profile name: Specify a name for this network profile (see Figure 7-11).

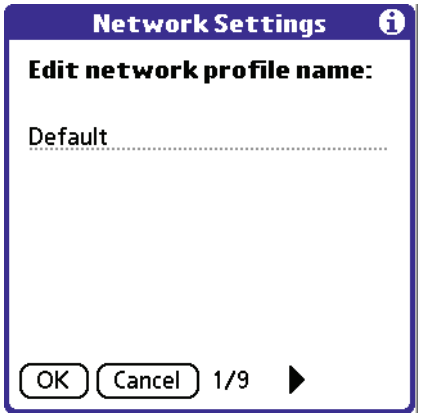

Figure 7-11 Network profile name

   b. User ID and password: Specify the User ID and password to synchronize with the Everyplace Access server (see Figure 7-12 on page 298).

Figure 7-12 User ID and password

c. Everyplace Access Server information: Enter the IP address or host name for the Everyplace Access server and indicate if the Sametime server, DB2 server, and DMS server are the same server. Configure Advanced Settings and Tracing options if necessary (see Figure 7-13).

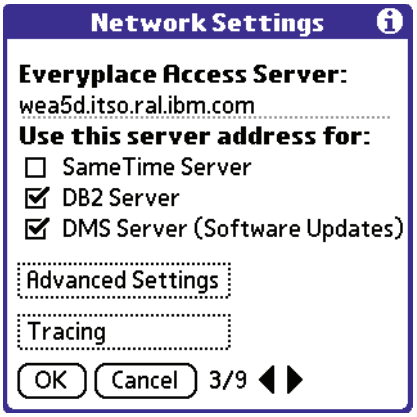

Figure 7-13 Everyplace Access Server information

d. E-mail account: Specify the VersaMail account you want to synchronize with your mail on the server, or select an existing account from the list. Note that the Account Name you specify here must match with the Account Mail set in VersaMail application (see Figure 7-14 on page 299).

Figure 7-14 E-mail account information

e. Calendar: Select the calendar application you want to synchronize (see Figure 7-15).

Figure 7-15 Calendar information

f. Sametime Server: Specify the host name or IP address of the Sametime server, and the user ID and password you want to log on to the Sametime server. Modify Advanced Settings, if necessary (see Figure 7-16 on page 300).

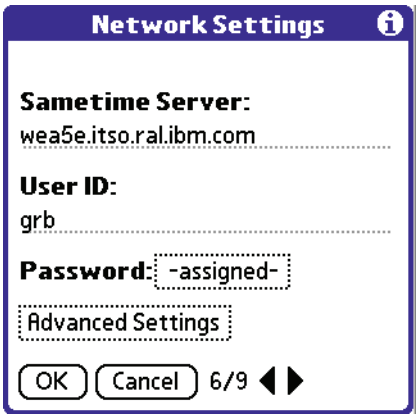

Figure 7-16 Sametime server information

g. DB2 Everyplace server: Enter the host name or IP address of the DB2 Everyplace server. Complete the fields in the Advanced Settings section if necessary (see Figure 7-17).

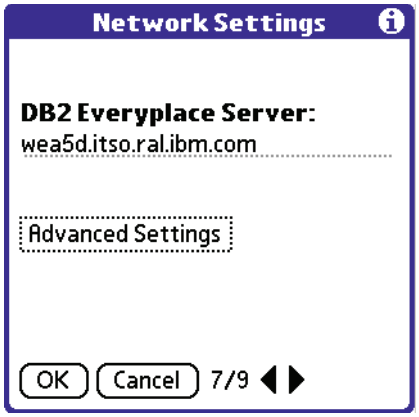

Figure 7-17 DB2 Everyplace server information

h. DMS server: Specify the host name or IP address of the Device Manager server. Complete the fields in the Advanced Settings section if necessary (see Figure 7-18 on page 301).

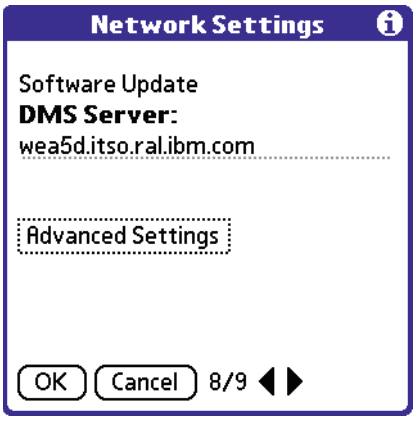

Figure 7-18 DMS server information

i. Mobility Client settings: Select a network profile for the connection to the WebSphere Everyplace Connection Manager (see Figure 7-19).

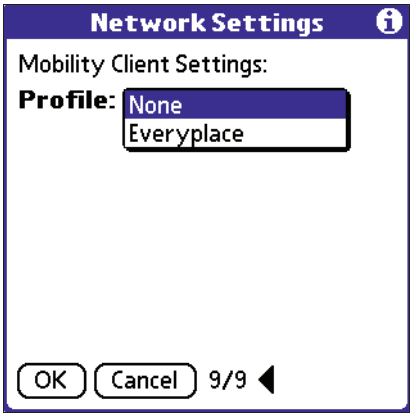

Figure 7-19 Mobility Client settings

j. Click **OK** to create the network profile.

4. You can review and modify the settings you have entered by selecting the appropriate option; otherwise, click **Done** (see Figure 7-20 on page 302).

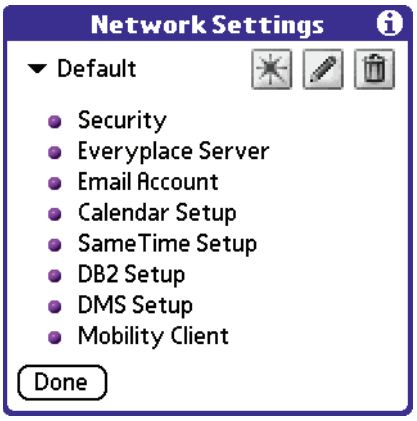

Figure 7-20 Network settings profile

5. Now you are ready to use the WEA Client application for Palm OS.
6. If you want to modify the Network Settings configured before, select **Options** → **Network Settings...** (see Figure 7-21).

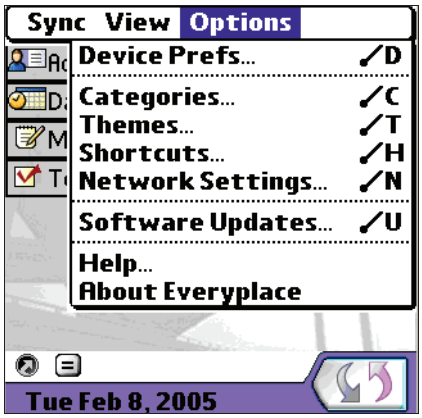

Figure 7-21 Open Network settings profile

Important: To ensure you have the latest code, you should visit the WebSphere Everyplace Access support Web site at `http://www.ibm.com/software/pervasive/ws_everyplace_access/support/` to download the latest Fix Packs and code fixes. Apply these fixes prior to using the samples within this redbook.

7.3 Everyplace Client for Pocket PC

In this section, we explain how to install and configure the Everyplace Client V5.0.1 for a Pocket PC 2002 and Windows Mobile 2003.

7.3.1 Everyplace Client V5.0.1 installation

To install Everyplace Client, perform the following steps:

1. Perform a soft reset on your Pocket PC and verify that your device is placed on the cradle and connected to the desktop using a Microsoft ActiveSync connection.
2. Run the setup.exe program to install Everyplace Client V5.0.1 for Pocket PC 2002 or Windows Mobile 2003. Click **Next**.
3. Select the setup language for this installation. For the purposes of this installation, we will select **English**. Click **OK**.
4. You will now be presented with the welcome window for the installation. Click **Next** (see Figure 7-22).

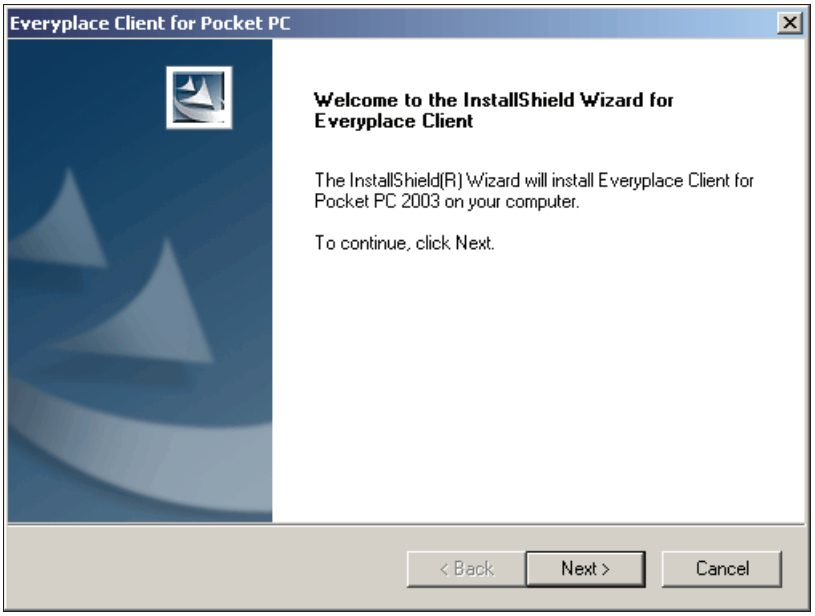

Figure 7-22 InstallShield Welcome window

5. Read through the License Agreement and then click **Yes**. If you are also presented with the License Agreement in Notepad, you may want to close it.
6. Click **OK** in the device soft reset alert pop-up (see Figure 7-23 on page 304).

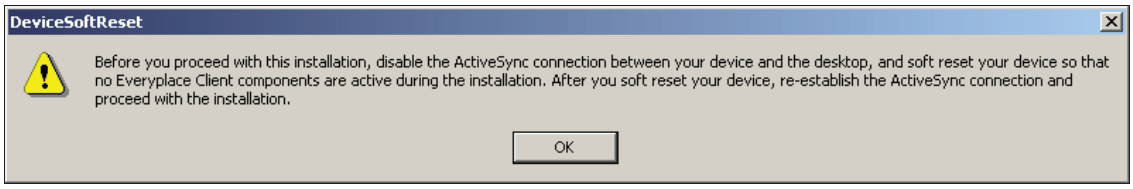

Figure 7-23 Device soft reset alert pop-up window

7. Accept the default destination folder by clicking **Next** (see Figure 7-24).

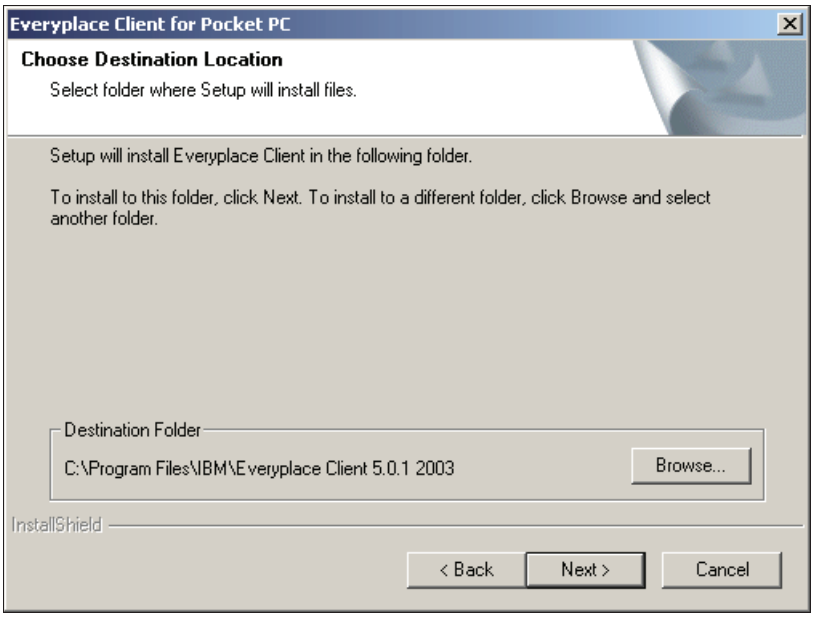

Figure 7-24 Select destination folder for Everyplace Client

8. On the Select Components window, select the components you wish to install and use. Click **Next** (see Figure 7-25 on page 305).

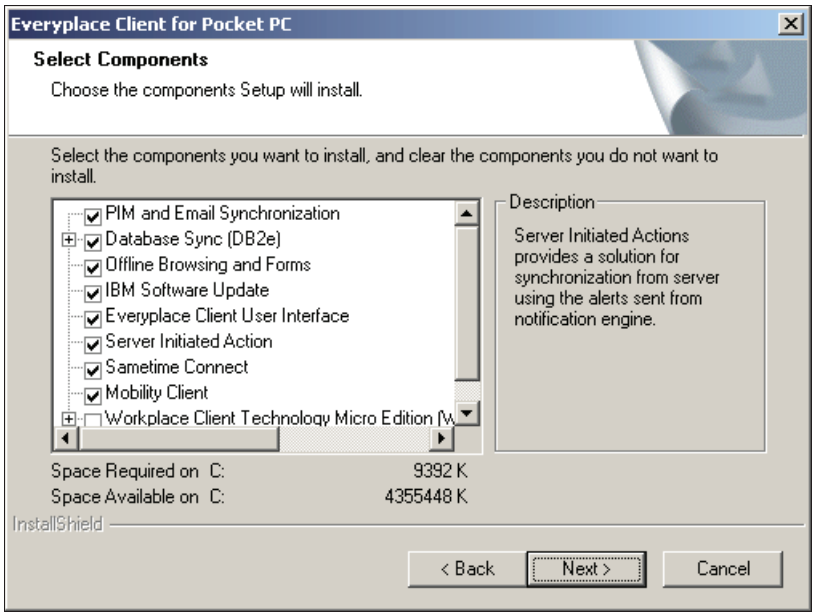

Figure 7-25 Select Everyplace Client components to install

9. Review the settings you have selected. If you want to change anything, click **Back**. Otherwise, click **Next** (see Figure 7-26 on page 306).

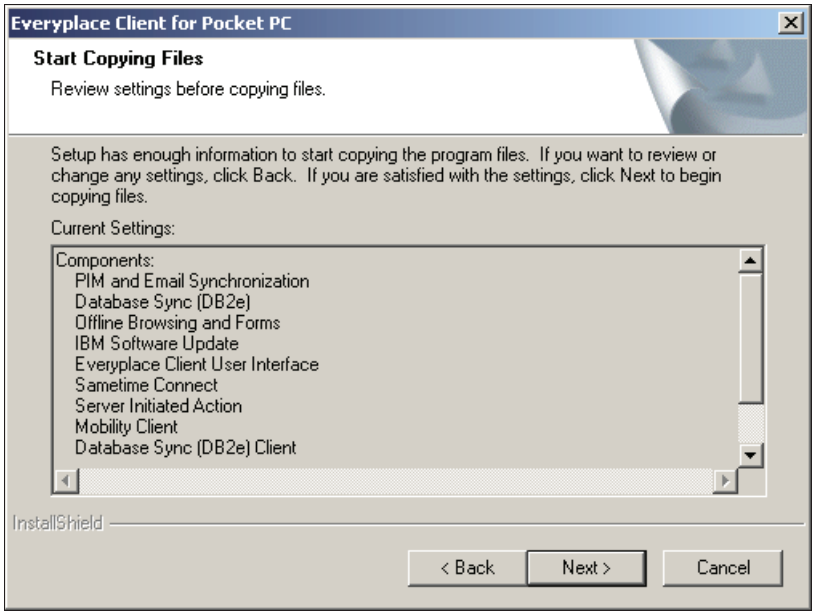

Figure 7-26 Installation selection summary

10. Click **Yes** on the next window (see Figure 7-27).

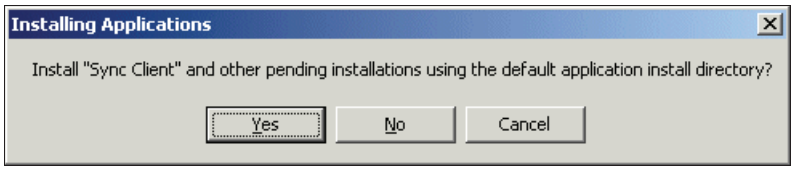

Figure 7-27 Install Sync Client

11. Click **OK** (see Figure 7-28).

Figure 7-28 Check mobile device for additional steps

12. At the end of the installation, the **InstallShield Wizard Complete** window will appear. Click **Finish**. This completes our installation as far as the desktop is concerned (see Figure 7-29 on page 307).

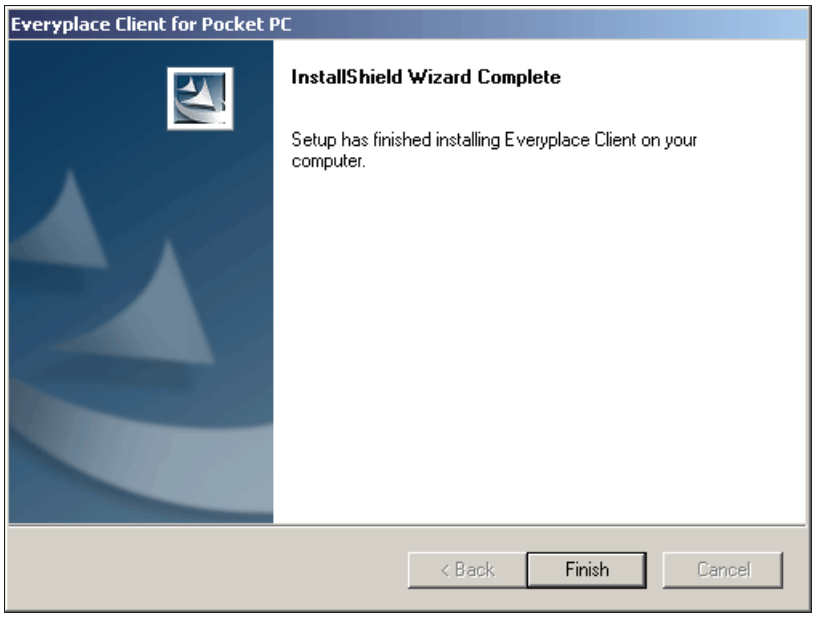

Figure 7-29 Installation complete

13. On your Pocket PC, you will be prompted to enter your user ID and password to log in to your Portal Server. The user ID and password should be for a user who already exists on your WEA Server. Enter the user ID and password and then select the **OK** button in the top-right corner (see Figure 7-30 on page 308).

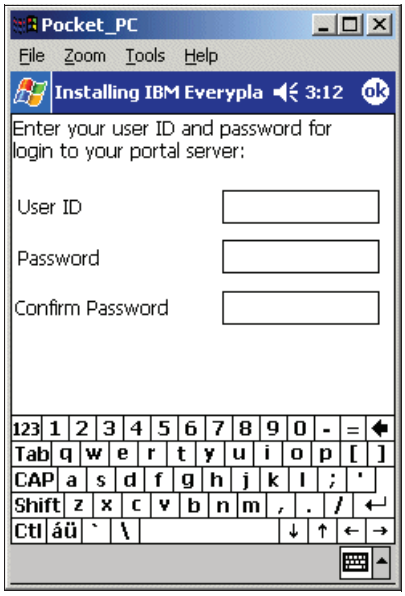

Figure 7-30 Log in user ID and password

14. The Install wizard will copy the appropriate files to the Pocket PC. Depending on the components you have selected, you will next be presented with a series of windows to configure these components. If you have selected the PIM and e-mail synchronization component, you will be prompted to enter your name and e-mail address. Enter your name and e-mail address and select the **OK** button in the top-right corner (Figure 7-31 on page 309).

Figure 7-31 Display name and e-mail address

This completes the installation of Everyplace Client for Pocket PC.

7.3.2 Everyplace Client configuration

After completing the installation of Everyplace Client for Pocket PC, you still need to configure it to tell it where the component servers are. To configure Everyplace Client for Pocket PC, perform the following steps:

1. If you have not previously configured Everyplace Client:
   a. Launch Everyplace Client on your Pocket PC by selecting **Start** → **Everyplace Client**.
   b. You will be prompted for a user name and password. You should enter the user name and password you entered in step 13 on page 307. Click **Log in** (see Figure 7-32 on page 310).

Figure 7-32 Everyplace Client login

If you have previously configured Everyplace Client:

a. Launch Everyplace Client on your Pocket PC by selecting **Start** → **Everyplace Client**.

b. You may be prompted for a user name and password. You should enter the user name and password you entered in step 13 on page 307. Click **Log in** (see Figure 7-33 on page 311).

Figure 7-33 Everyplace Client login

c. The Everyplace Client Home page will appear. Click the wrench button to open the My settings page (see Figure 7-34).

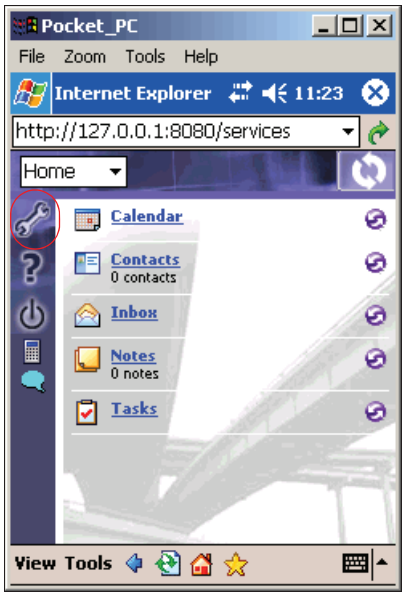

Figure 7-34 Everyplace Client home page

d. On the My settings page, select **Network Profiles** (see Figure 7-35).

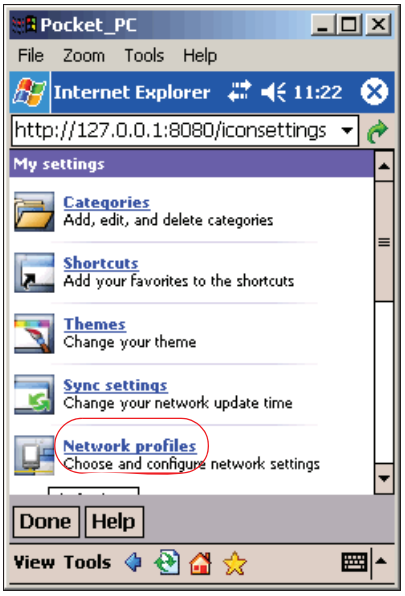

Figure 7-35 Everyplace Client My settings page

2. You will now be presented with the network profiles page. Depending on which components you have selected, you will need to enter the server name and settings for these components. The server name should be fully qualified. If you have installed all your components on the same box, then the server name should be the same for each component. Note the default network profile selection under the words Active network profile.

   Everyplace Client provides the ability to create multiple network profiles. This will allow you to connect different Everyplace Access servers simply by changing your network profile. For the purposes of this installation, we will stick with the default network profile. Enter the server and settings relevant to your component selection and then click **OK** (see Figure 7-36 on page 313).

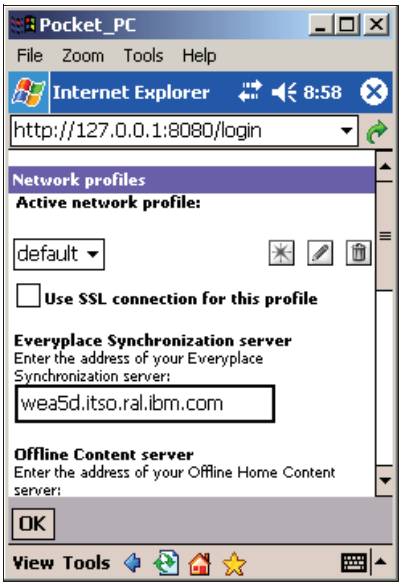

Figure 7-36 Network profile page

This completes the configuration of Everyplace Client for Pocket PC 2002 and Mobile Windows 2003.

8

Everyplace Client secure connections

This chapter describes how to enable Secure Sockets Layer (SSL) to secure communication between WebSphere Everyplace Access server and mobile devices using the Everyplace Client.

© Copyright IBM Corp. 2005. All rights reserved.

8.1 Introduction

To prevent exposing data exchanged between WebSphere Everyplace Access server and the mobile clients, it is necessary to turn on a secure connection using Secure Sockets Layer (SSL). SSL is a protocol that enables secure message communication between a server and a client over the Internet.

The following steps are necessary to enable WebSphere Everyplace Access server security:

- Enable SSL on IBM HTTP Server.
- Enable SSL in WebSphere Everyplace Server.
- Configure WEA files to support SSL.
- Enable SSL in Everyplace Client.

Note: Sametime client does not support a Secure Sockets Layer connection.

8.2 Enabling SSL on IBM HTTP Server

Secure Sockets Layer (SSL) uses key pairs (private and public keys) and certificates for ensuring security. In a production environment, it is necessary to get a certificate from a recognized certificate authority. In our sample scenario, we act as our own certificate authority, so we generate a self-signed certificate using the IBM Key Management (IKEYMAN) utility, which is included in IBM HTTP Server.

8.2.1 Creating a key database

1. Create a directory in the server where the key database will be stored, for example, C:\keys.
2. Start the IBM Key Management utility by selecting **Start** → **Programs** → **IBM HTTP Server 1.3.26** → **Start Key Management Utility**.
3. Select **Key Database File** from the main window and then select **New** (see Figure 8-1 on page 317).

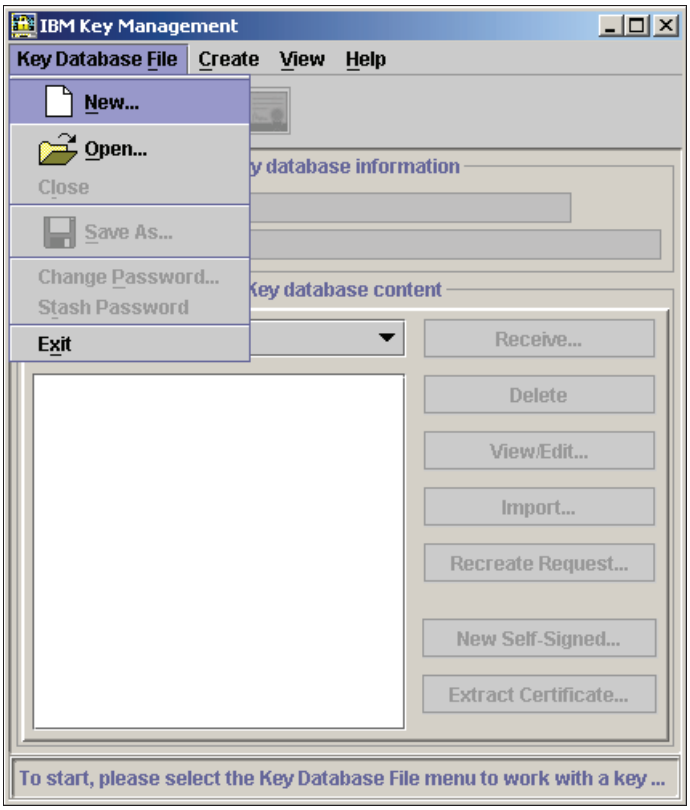

Figure 8-1 IBM HTTP Key Management utility

4. In the New window, choose **CMS key database file**, type the name of the key database, and select the location of the directory you created in step 1 on page 316 to store the key database. Click **OK** (see Figure 8-2).

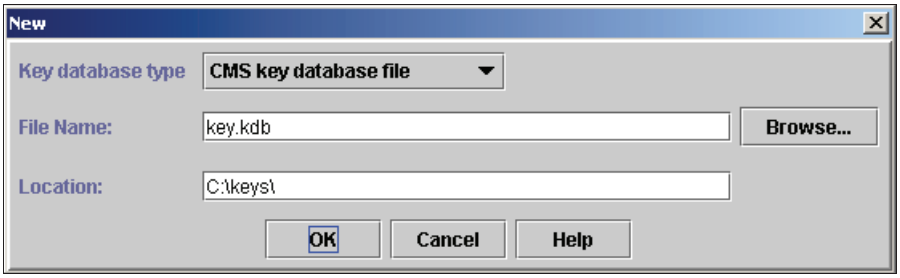

Figure 8-2 Create new key database

5. In the Password Prompt window, enter a password for the key database file. Make sure the **Stash the password to a file** check box is selected. Click **OK** (see Figure 8-3).

Figure 8-3 Set password for the key database file

6. Select the stash password option. The password is encrypted and saved in a file. Click **OK** in the information window (see Figure 8-4).

Figure 8-4 The password is encrypted and saved in a file

8.2.2 Create a self-signed key file

As we mentioned before, you can either create a self-signed certificate or use a certificate from a recognized certificate authority (CA).

Note: The following steps are required only if you want to create a self-signed certificate for development purposes. In a production environment, you need a certificate from a well-known certificate authority (CA).

Follow these steps to create a self-signed certificate:

1. If the Key database file is not open:
   a. In the IBM Key Management utility, select **Key Database File** from the main menu and select **Open**.
   b. Select the key database file just created in 8.2.1, “Creating a key database” on page 316 and click **OK**.
   c. Enter the correct password when prompted.
2. Select **Personal Certificates** in the Key Database content frame and then click the **New Self-Signed** button (see Figure 8-5).

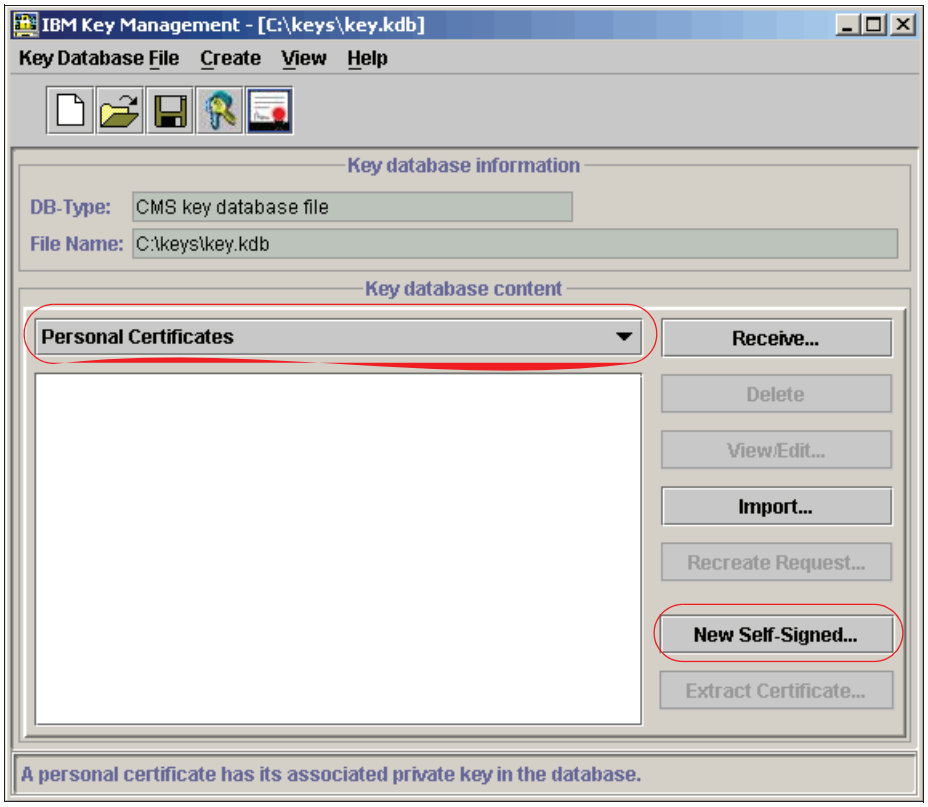

Figure 8-5 Create a self-signed key

3. In the Create New Self-Signed Certificate window, complete the fields and click **OK**. Notice that some fields are optional (see Figure 8-6).

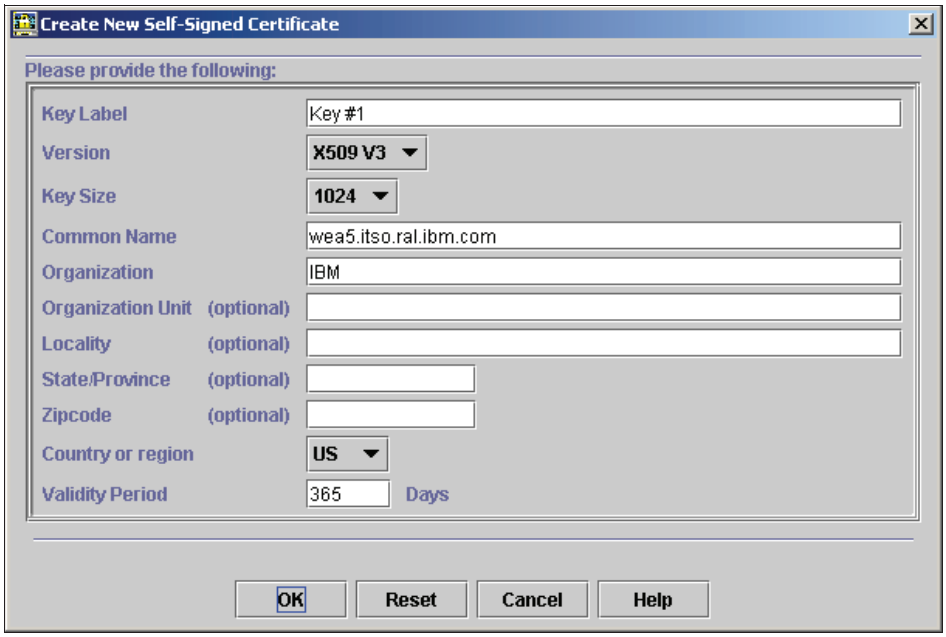

Figure 8-6 Create a new self-signed key

4. Exit the IBM HTTP Key Management utility.

8.2.3 Setting up IBM HTTP Server

The IBM HTTP Server configuration file must be changed in order to enable security. Follow these steps:

1. Open the IBM HTTP Server configuration file located in *HTTPServer_Install_Directory*\conf\httpd.conf.
2. Locate the following line:

   ```
   LoadModule ibm_app_server_http_module
   ```

3. After this line, add the following line to load the IBM SSL module:

   ```
   LoadModule ibm_ssl_module modules/IBMModuleSSL128.dll
   ```

4. At the end of the file, add the following lines. These lines contain directives about the following:
   - Set HTTP server to listen the port number 443.
   - Enable SSL for a virtual host.

– Indicate if a client certificate is required.
– Set the key file to be used.
– Set time out for session IDs for SSL Versions 2 and 3.
– Other directives.

The text shown in *italics* should be edited for your environment:

```
Listen 443
<VirtualHost yourservername.yourco.com:443>
SSLEnable
SSLClientAuth none
ServerName yourservername.yourco.com
DocumentRoot "C:/IBMHTTPServer/htdocs"
<Directory "C:/IBMHTTPServer/htdocs">
Options Indexes
AllowOverride None
order allow,deny
allow from all
</Directory>
</VirtualHost>
Keyfile C:/keys/key.kdb
SSLV2Timeout 100
SSLV3Timeout 1000
```

5. Save and close the httpd.conf configuration file.
6. Restart IBM HTTP Server.

8.2.4 Verifying if security is enabled on IBM HTTP Server

The following procedure may be used to verify if security has been properly enabled:

1. Open a browser.
2. Type `https://yourserver` in the address bar.
3. If using a self-signed certificate, accept the certificate if prompted.

8.3 Enabling SSL in WebSphere Application Server

In this section, we show you how to enable Secure Sockets Layer (SSL) in WebSphere Application Server.

8.3.1 Configuring WebSphere Application Server

Follow this procedure to configure WebSphere Application Server for SSL:

1. Open the WebSphere Application Server Administrative Console by selecting **Start** → **Programs** → **IBM WebSphere** → **Application Server v5.0** → **Administrative Console**.
2. In the console navigation tree, select **Environment** → **Virtual Hosts**. Click **default host** (see Figure 8-7).

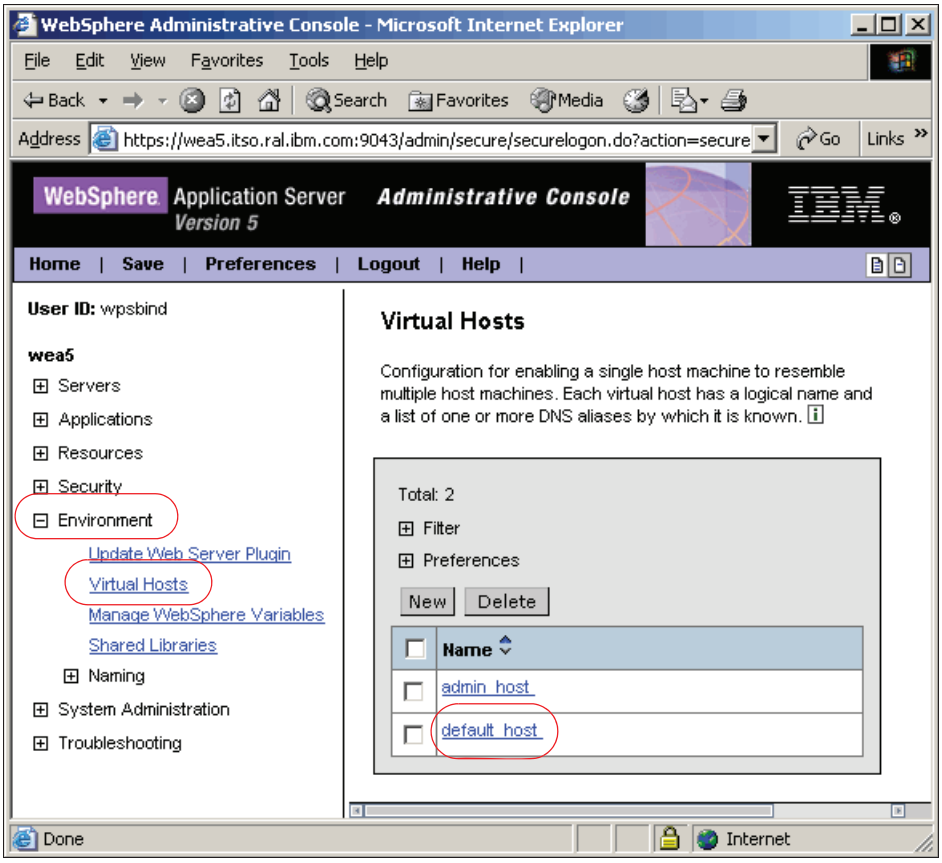

Figure 8-7 Virtual host configuration in WebSphere Application Server

3. In Additional Properties, click **Host Aliases** (see Figure 8-8 on page 323).

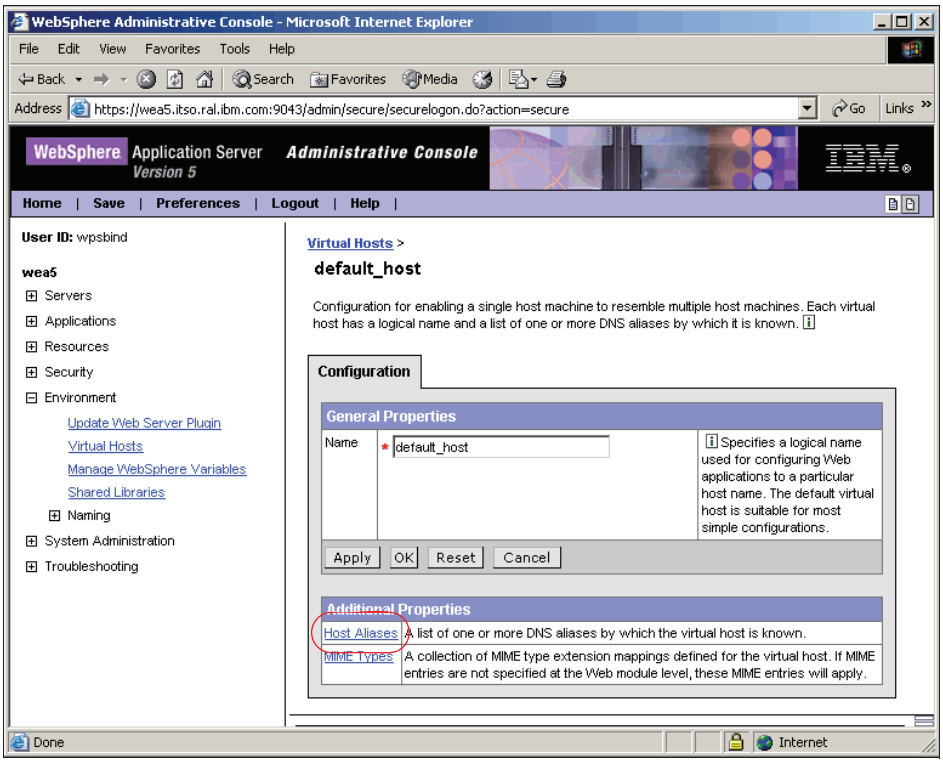

Figure 8-8 Virtual host configuration in WebSphere Application Server

4. In the Host Aliases frame, click **New** (see Figure 8-9 on page 324).

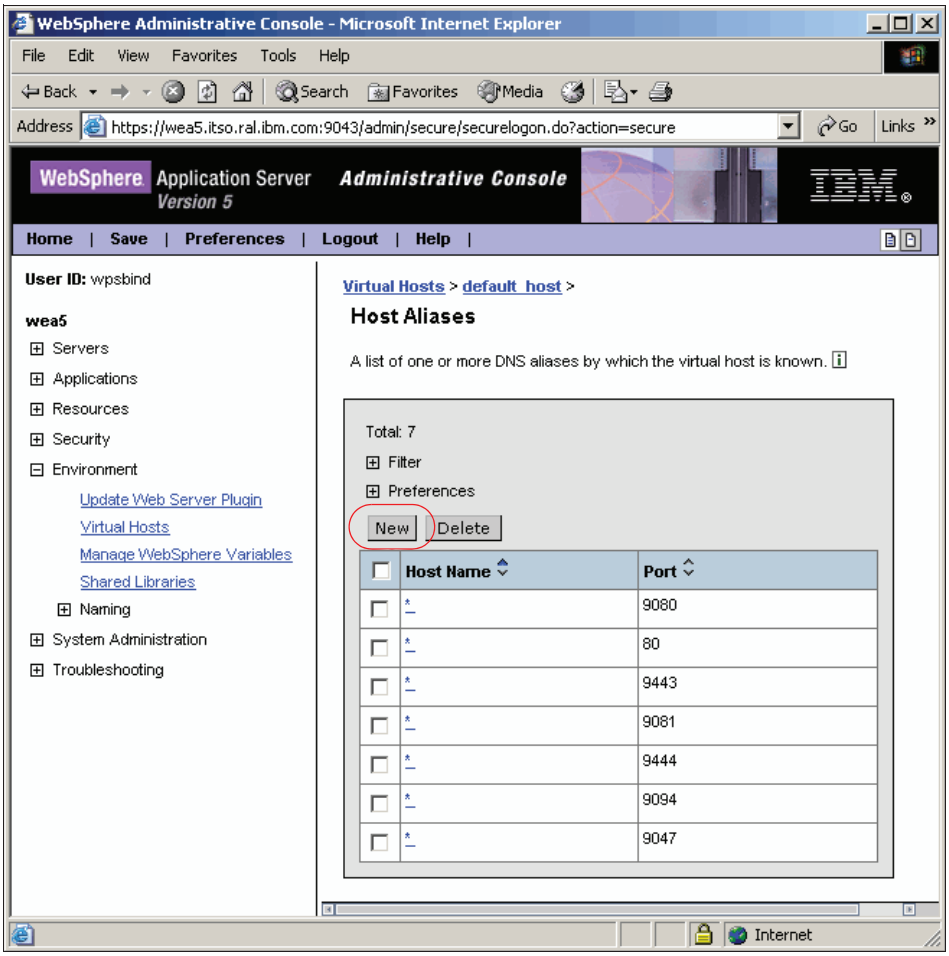

Figure 8-9 Virtual host configuration in WebSphere Application Server

5. Enter the following:
   - Host Name: *
   - Port: 443

   Click **OK** (see Figure 8-10 on page 325).

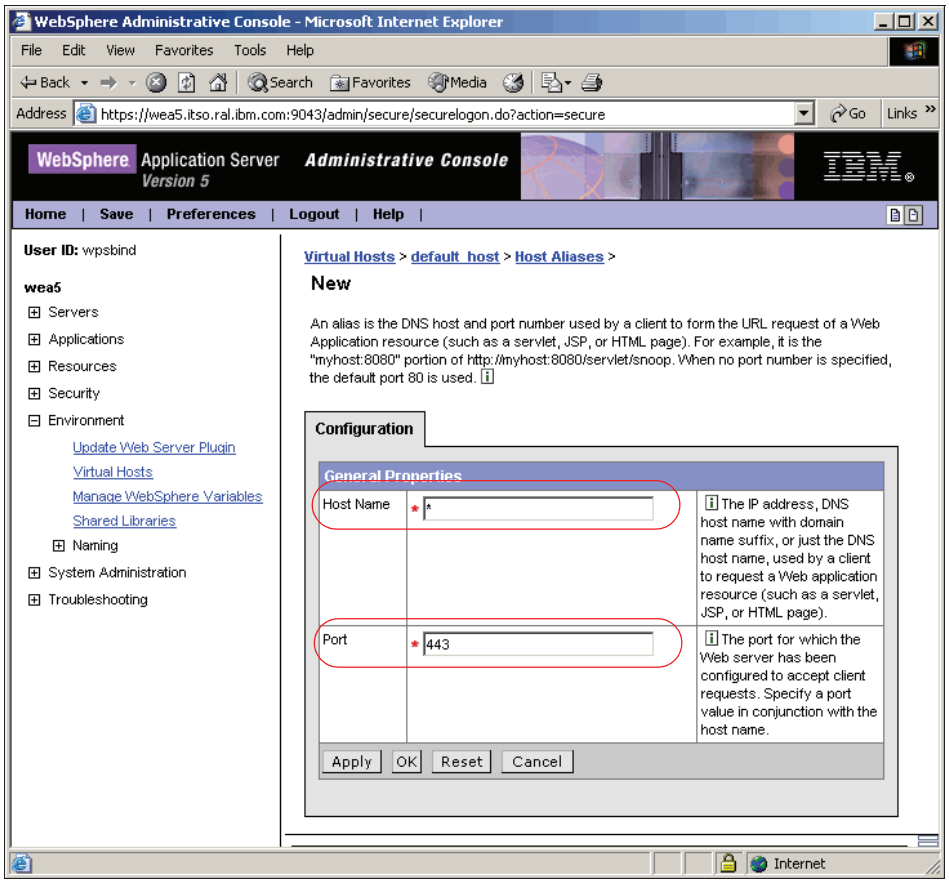

Figure 8-10 Configuring host name and port in WebSphere Everyplace Access

6. Once the new host alias is created, you must save the changes to the master configuration. Click **Save** and accept to update the master repository with the new changes.
7. Update the Web server plug-in configuration. Select **Environment** → **Update Web Server Plugin** and click **OK** to update the plug-in configuration file.
8. Restart IBM HTTP Server.

8.3.2 Verifying if security is enabled in the Application Server

Follow this procedure to verify if SSL has been properly configured in WebSphere Application Server:

1. Open a browser.
2. Access the Portal home page:

   `https://yourserver/wps/portal`

3. Accept the certificate if prompted.

8.4 Configure WEA files to support SSL

In order to enable SSL between WebSphere Everyplace Access server and client, it is necessary to modify the following files.

ConfigService.properties file

The ConfigService.properties file is located in *WebSpherePortal_home*\shared\app\config\services\, where WebSpherePortal_home is in our installation C:\Program Files\WebSphere\PortalServer.

1. Open the ConfigService.properties file.
2. Locate the following line:

   `redirect.login.ssl = false`

3. Set this parameter to true:

   `redirect.login.ssl = true`

4. Locate the following line, `host.port.https`, and set this parameter with the port number used for the virtual host aliases specified in step 5 on page 324 in 8.3.1, “Configuring WebSphere Application Server” on page 322. In our scenario, `host.port.https = 443`.

web.xml file

The web.xml file is located in *WAS_home*\installedApps*hostname*\wps.ear\wps.war\WEB-INF, where WAS_home is, in our installation, C:\Program Files\WebSphere\AppServer, and hostname is, in our scenario, wea5d.

1. Open the web.xml file.
2. Locate the tag `<transport-guarantee>` located into the `<security-constraint>` tag of the protected portal URL.

3. Change the `<transport-guarantee>` value from `NONE` to `CONFIDENTIAL` This value prevents data transmitted between a client and server from being observed by a third party. It requires using SSL.

JSP files that provide a login link

These JSP files are located in *WAS_home*\installedApps*hostname*\wps.ear\wps.war\themes, where WAS_home is, in our installation, C:\Program Files\WebSphere\AppServer and hostname is, in our scenario, wea5d. Search in this directory for all the JSP files that contain the string `screen=”Login”`, which should appear in an anchor similar to this:

```
<a href='<wps:url... screen="Login".../>'>.
```

You should add the `ssl=”true”` attribute into the `<wps:url>` tag of each anchor you find that contains the `screen=”Login”` string. For example:

```
<a href='<wps:url home="public" ssl="true" screen="Login"/>'>
```

Delete compiled JSP files from the application server cache

Delete the files located in *WAS_home*\temp*node_name*\WebSphere_Portal\wps\wps.war where WAS_home is, in our installation, C:\Program Files\WebSphere\AppServer and node_name is, in our scenario, wea5d.

After you have configured WEA files, you must restart the Web server and the WebSphere Portal server.

8.4.1 Verifying if security is enabled on IBM HTTP Server

The following procedure may be used to verify if security has been properly enabled:

1. Open a browser.
2. Type `https://yourserver/wps/portal` in the address bar.
3. If you are using a self-signed certificate, accept the certificate if prompted.
4. Click the login link and enter a user and password to log in to the WEA server. The session will be directed to a secure connection.

8.5 Enabling security for Offline Portal Content

If you are using a self-signed certificate or a certificate from a not well-known certificate authority, it is necessary to perform additional steps to configure Offline Portal Content. Basically, you need to place this certificate in a trusted store where the WebCache servlet can have access. If you do not want to put the certificate in the system keystore, you might create your own custom keystore.

> **Note:** The following steps are required only if you use a self-signed certificate for development purposes. They are not necessary if you use a certificate from a well-known certificate authority (CA).

To place the certificate into a trusted keystore, follow these steps:

1. Extract the self-signed certificate generated in 8.2.2, “Create a self-signed key file” on page 318.
   a. Start the IBM Key Management utility by selecting **Start** → **Programs** → **IBM HTTP Server 1.3.26** → **Start Key Management Utility**.
   b. Open the Key database file.
   c. Select **Personal Certificates** in the drop-down, select your server certificate, and click **Extract Certificate**.
   d. In the Extract Certificate to a File window, select **Base64-encoded ASCII data** as the data type. Enter a certificate file name and an existing directory name in the Location field and click **OK**.
2. Start the IBM Key Management utility included with the WebSphere Application Server (not the utility included with IBM HTTP Server). Open a command window and run the script *WAS_home*\bin\IKeyMan.bat, where WAS_home is, in our installation, C:\Program Files\WebSphere\AppServer.
3. Select **Key Database File** from the main menu and select **Open**.
4. Select **JKS** as the Key database type, browse to *WAS_home*\etc\ directory, and select the DummyServerTrustFile.jks file. Click **OK** (see Figure 8-11 on page 329).

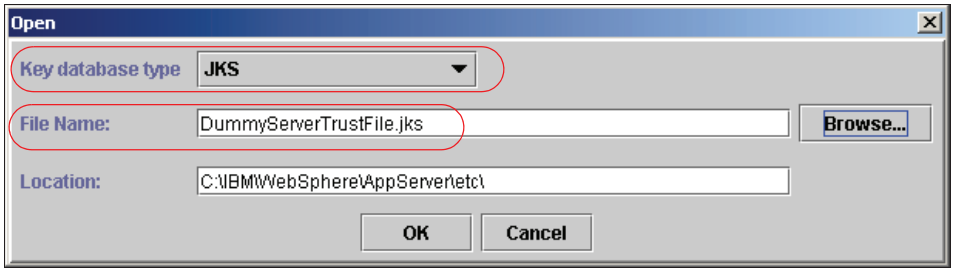

Figure 8-11 Open DummyServerTrustFile.jsk file

5. Type WebAS as the password.
6. Select **Signer Certificates** in the Key Database content frame and then click the **Add...** button (see Figure 8-12 on page 330).

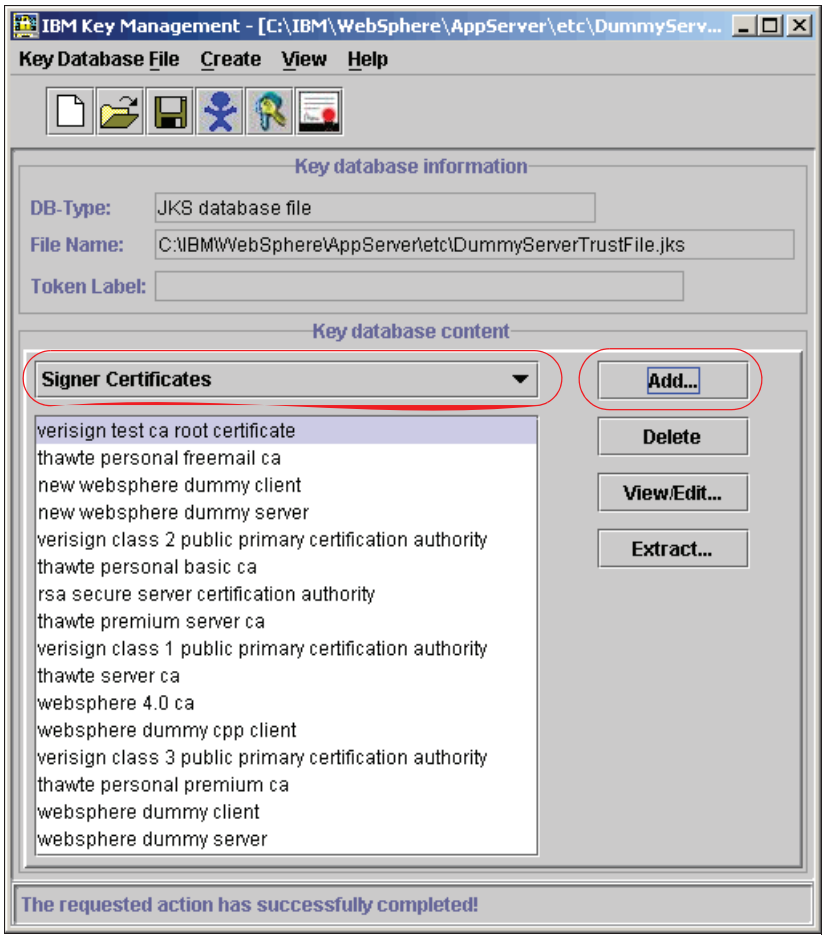

Figure 8-12 Adding the self-signed certificate

7. Browse for the certificate you extracted in step 1 on page 328 and click **OK**.
8. Type a label for the certificate and click **OK**.
9. Exit the IBM HTTP Key Management utility.
10. Restart the WebSphere Application Server.

Now it is necessary to configure offline browsing for the HTTPS protocol:

1. Log in to the WEA server as an administrator user.
2. Select **Administration** on the top-left menu and select **WebSphere Everyplace Access** → **Offline Browsing**.

3. Click the **Configure** icon on the toolbar and update the Portal URL and Port values using HTTPS and :443. For example:

   `https://wea5d.itso.ral.ibm.com:443/wps/myportal`

4. Click **Save**.

8.6 Enabling SSL in Everyplace Client

In this section, we show how to enable SSL in the Everyplace Client on Pocket PC and Palm Devices.

8.6.1 Enabling SSL in Pocket PC devices

1. Open the WebSphere Everyplace Client on the Pocket PC and log in.
2. Click the wrench button to open the **My Tools** page (see Figure 8-13).

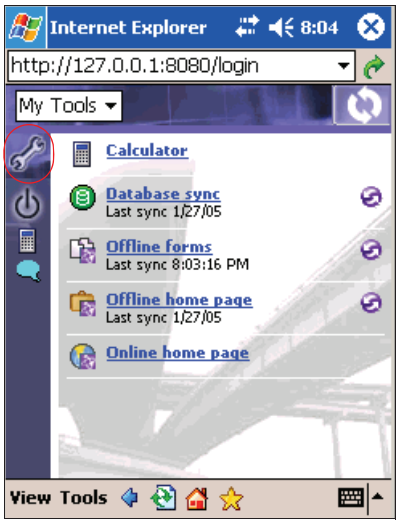

Figure 8-13 My Tools

3. Select the network profile being used to connect to the WebSphere Everyplace Access server and click **Network profiles** (see Figure 8-14 on page 332).

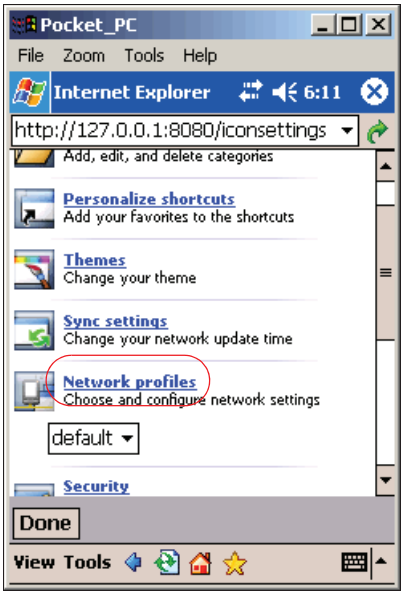

Figure 8-14 Network profiles

4. Enable **Use SSL connection for this profile** option (see Figure 8-15).

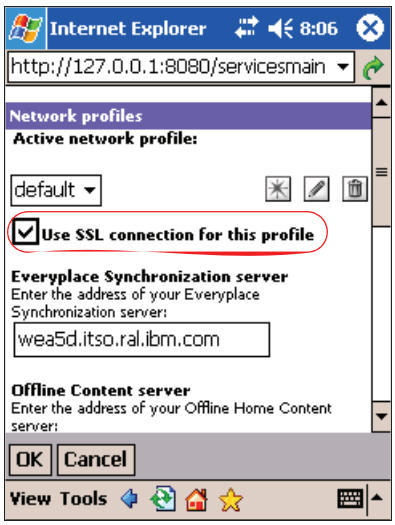

Figure 8-15 Use SSL Connection for this profile

The client will now use SSL when communicating with the server.

8.6.2 Enabling SSL in Palm devices

To enable SSL support on any Everyplace Client component, you first have to install your HTTP server certificate on your Palm device(s). Usually, the certificate is given to you by a recognized certificate authority (CA). Also, you can use a self-signed certificate created with the IKEYMAN tool for development purposes, as explained in 8.2, “Enabling SSL on IBM HTTP Server” on page 316.

To install the server certificate on your Palm device, follow these steps:

1. Export the existing server certificate to a file named cacerts.bin using the DER format. For example, if you are using a self-signed certificate generated with the IBM Key Manager, follow these steps:
   a. Start the IBM Key Manager utility by clicking **Start** → **Programs** → **IBM HTTP Server 1.3.26** → **Start Key Management Utility**.
   b. Open the generated key database for your server by selecting **Key Database File** → **Open**. In the password window, enter the password for the database and click **OK**.
   c. Select **Personal Certificates** in the drop-down to see the certificates contained in the key database, as shown in Figure 8-16 on page 334. Select your server certificate and click **Extract Certificate**.

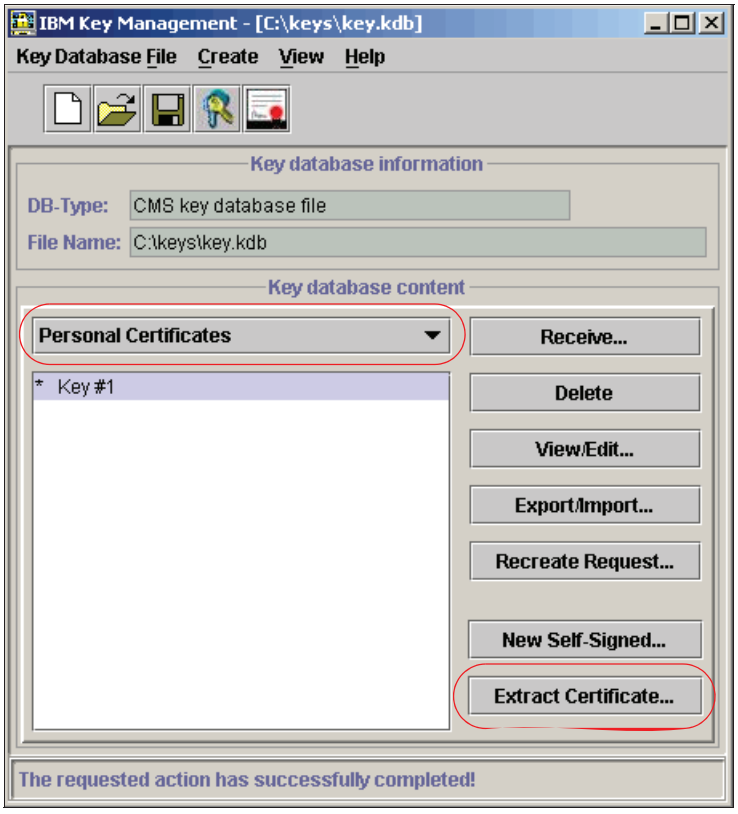

Figure 8-16 Self-signed certificates

d. In the Extract Certificate to a File window, select **Binary DER Data** as the data type, enter cacerts.bin as the certificate file name, and enter an existing directory name in the Location field, as shown in Figure 8-17. Click **OK**.

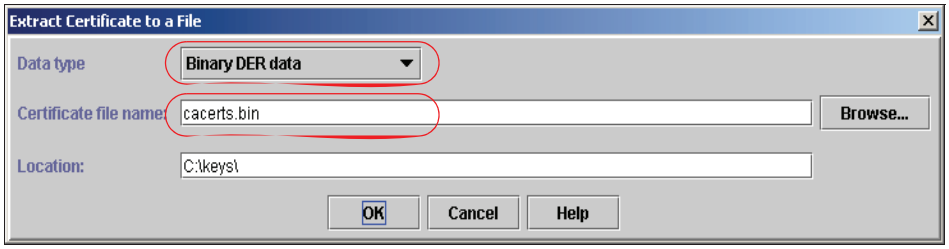

Figure 8-17 Extracting a certificate

e. Close the IBM Key Manager utility.

2. Download the certificate conversion utility for Palm OS (palmdb.exe) from the WebSphere Everyplace Access Support page. Put the file in the same directory where you put the cacerts.bin file.
3. Run the palmdb.exe utility. You will see that the utility creates a new file named SSLCaCerts.pdb. It contains the server certificate in the Palm Database format.
4. Install the SSLCaCerts.pdb file in your Palm device by using HotSync synchronization, for a real device, or using the Install Database option from the emulator or simulator software.

To enable SSL in the supported clients, follow the instructions in the next sections.

For IBM WEA client

1. Open the IBM WEA client by selecting the corresponding icon.
2. Select **Preferences** → **Server Preferences** from the menu bar.
3. Check **Enable SSL** and enter 443 in the Port field. Click **OK** (see Figure 8-18).

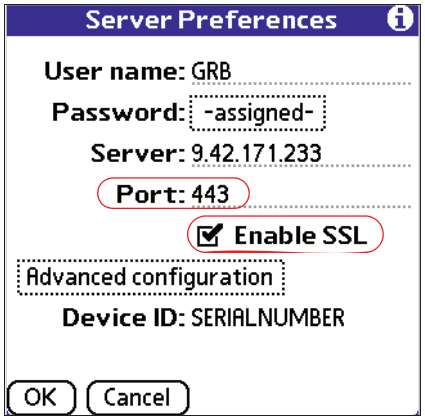

Figure 8-18 Enabling SSL on SyncML client

For DB2 Everyplace Client

1. Open the IBM Sync client by selecting the corresponding icon.
2. Select **Options** → **Settings** from the menu bar to open the Settings window.
3. On the Settings window, select **Advanced** (see Figure 8-19 on page 336).

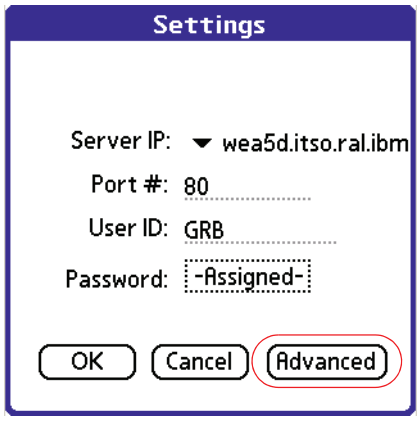

Figure 8-19 Settings window for DB2e client

4. Check **SSL (Secure Socket Layer)** and click **OK** (see Figure 8-20).

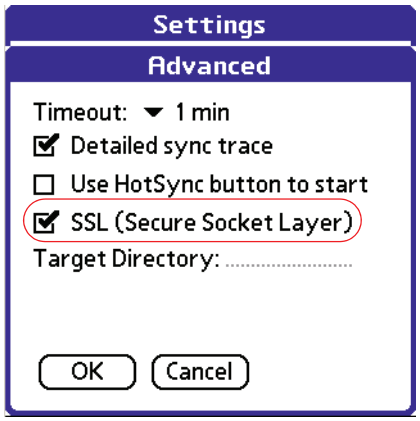

Figure 8-20 Selecting SSL on DB2e client

5. On the Settings window, make sure that the Port is set as 443. Click **OK** (see Figure 8-21 on page 337).

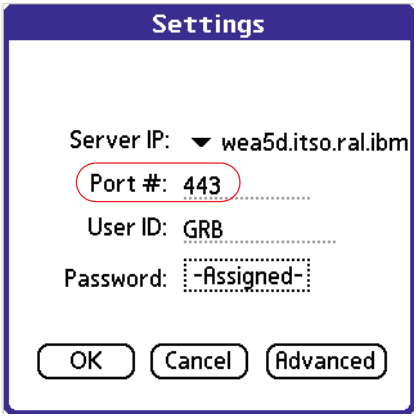

Figure 8-21 Checking the SSL server port

For Web Cache Client (WCC)

1. Open WCC by selecting the corresponding icon.
2. Select **Options** → **Settings** from the menu bar to open the Settings window.
3. Check **SSL** and select **OK** (see Figure 8-22).

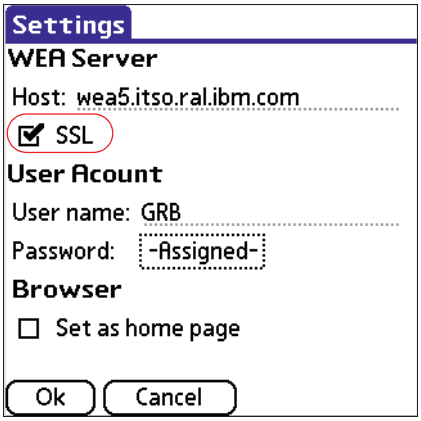

Figure 8-22 Enabling SSL on Web Cache Client

9

Device Services

This chapter describes the Device Services offered in WebSphere Everyplace Access.

In this chapter, we explain how Device Services are integrated in WebSphere Everyplace Access and how to use Device Management portlets. We help you to understand Device Services through scenarios that are common in device management, such as bootstrapping new devices with a WebSphere Everyplace Access Client, configuring devices, taking inventory, and software distribution.

© Copyright IBM Corp. 2005. All rights reserved.

9.1 Device Services overview

Device management is critical because of the increase in the number of mobile devices on the market and the growing complexity of the software in these devices.

Device Services, offered in WebSphere Everyplace Access, facilitates the management of software on mobile devices. WebSphere Everyplace Access integrates with the Tivoli Device Manager to provide device management services.

9.1.1 Architecture

Figure 9-1 shows the different components of the device management services in WebSphere Everyplace Access. In this section, each component is briefly explained.

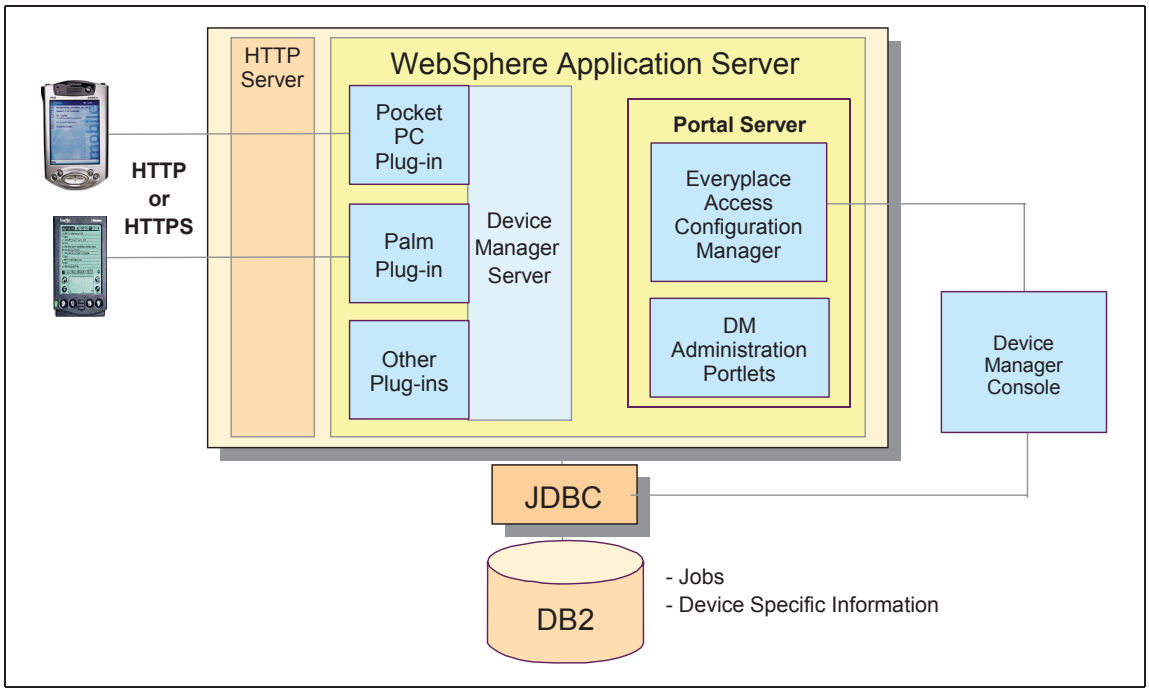

Figure 9-1 WebSphere Everyplace Access Device Services

9.1.2 Device Services

The Device Services is a set of servlets that execute in the application server. Device Services executes the management tasks (jobs) on the connected devices.

Device Management Server includes a DM servlet that ensures that the device is enrolled with the server. For enrolled devices, the DM servlet checks if there are any pending jobs for the device and processes them after prioritizing the jobs. The DM servlet processes the jobs using the device plug-ins that interact with the device.

Device plug-ins are responsible for device identification, communication with the device, processing jobs on the device, and high-level management of tasks. A plug-in is provided for different classes of devices and is extensible to support new devices types. The following plug-ins are provided in the Device Services:

- Nokia OMA DM plug-in
- OSGi plug-in
- Palm OS plug-in
- Sharp Linux Zaurus plug-in
- Sony Ericsson P900 plug-in
- SyncML DM plug-in
- Windows CE plug-in
- WinCEOSGi plug-in
- Windows 32-bit plug-in

9.1.3 Device Services Agent

The Device Services Agent resides on the device. The Device Agent is responsible for executing the commands sent by the Device Management Server. The Client connects and interacts with the Device Management Server using a proprietary protocol. The Device Services Agent is installed along with the WebSphere Everyplace Access Client. The Device Agent can be configured and controlled by the Everyplace Client UI. The Device Agent need not be connected to the server all the time. When the Client Agent connects, the server identifies the client and executes the jobs pending for this device.

9.1.4 Device Services database

The Device Services database is a relational database that stores all the device management information. This database stores device-specific information, including the jobs for the devices. The Device Services database is created with all the necessary tables, views, and queries.

9.1.5 Device Management portlets

Device Management portlets have been completely redesigned in WebSphere Everyplace Access V5. Device Management portlets are installed with the WebSphere Everyplace Access core services.

9.1.6 Device Services console

The Device Services console is a Java utility that the administrator can use to administer and monitor the Device Management Server. The console provides functionality to register and view devices, create jobs for viewing or modifying device or software properties, view the status of the jobs, and so on.

The Device Services console can be downloaded from the Device Management Server and installed on any system. This allows administrators of the devices to control devices from various terminals and not necessarily on the server. The Device Services console requires a DB2 database client for connecting to the Device Management database.

The first time the Device Services console is started, it must be able to connect to the Device Management Server to log in and retrieve the properties file. The Device Services console creates a backup of the properties file, and a subsequent start up will not need to connect to the Device Management Server for login and will connect directly to the Device Services database for administration.

Note: The Device Services console connects to the WebSphere Everyplace Access Subscription Manager to authenticate the user.

With the Device Services console, the following types of jobs can be created:

- Software Distribution job: With this job we can distribute software packages to clients.
- Inventory Collection job: With this job we can query the device and check all the installed software on the device.
- Configuration job: With this job, we can configure the browser settings, PPP connection settings, TCP/IP settings, mail server settings, and Device Management Client settings on the device.

9.2 Setting the stage

Before we begin with the different scenarios of device management, a certain configuration has to be done.

9.2.1 Creating a device management user group

For details about adding and viewing groups and users, see Chapter 3, “Administration” on page 41. For example:

1. Check to see if the user group dmadmins exists. This should have been automatically been created during the installation of WebSphere Everyplace Access.
2. If not, create a user group with the name dmadmins. The name should be exactly the same. Otherwise, Device Management Services will not work.
3. Add the Portal administrator (usually wpsadmin) as a member of the group.

Note: When using Device Management Services, you must log in as the administrator who is a member of the dmadmins group.

9.2.2 Starting the Device Services console

A Device Services console can be downloaded from the Device Management Server and launched on any system. To download the Device Services console, enter the following path:

```
http://dmserver.yourco.com/dmserver/DMconsole
```

Follow the instructions indicated in that page.

On the server machine, the Device Services console can be launched from the WebSphere installed path. Go to WebSphere\DMS16\console and click **DMconsole.bat**.

Enter the administration user ID and password in the login prompt. The user must be a part of the dmadmins user group that was created in the previous section.

If the login was successful, the window in Figure 9-2 on page 344 will be displayed.

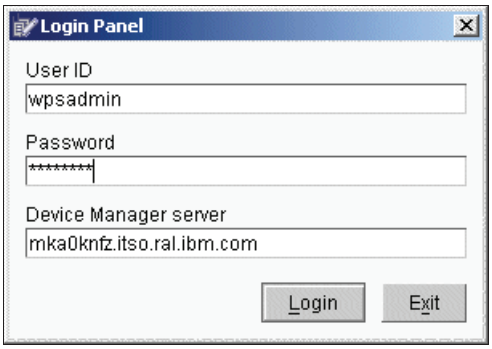

Figure 9-2 Login prompt

If the console is connected to the Device Management Server, and if the user was authenticated and part of dmadmins group, the window shown in Figure 9-3 will be displayed.

Figure 9-3 Device Services console

9.3 Scenarios

In this section, we provide two sample scenarios using Device Services.

9.3.1 Using Device Manager portlets to install the WebSphere Everyplace Access Client

WebSphere Everyplace Access Device Manager portlets can be used to install and configure WebSphere Everyplace Access Client on the device. This scenario will show how to use the Device Management portlets provided in WebSphere Everyplace Access.

Note: This scenario is suitable only for Pocket PC-based devices.

Creating a software package distribution

The Software Package portlets allow us to create software packages to be installed in supported devices. It will create several device manager jobs according to the software package XML descriptor. Later, these jobs will be delivered to the devices through the Device Agent installed as part of the Everyplace Client.

For this scenario, you will need to upload the Everyplace Client package. You can find a package for Pocket PC 2002 and 2003 in the WEA installation media, specifically on CD 4 under the dmsclients directory.

Note: There is a package to update the Everyplace Client on Palm devices, but it requires the previous Everyplace Client version already installed and the Device Agent configured to arm the WEA V5 server.

Follow these steps to create a software package for Everyplace Client for Pocket PC 2002 distribution:

1. Log into the Portal server using the user ID and password of the administrator who is a part of the dmadmins group.
2. Select the **Administration** label. Navigate to **WebSphere Everyplace** → **Device Management** → **Software Packages**.
3. Click **Add**. In the Add Package window, click **Browse** and locate the appropriate client (WEA5_ppc2002_BASE.zip, for this example), as shown in Figure 9-4 on page 346. Click **OK**.

Figure 9-4 Adding a software package

4. You will see the software package created and still unassigned, as shown in Figure 9-5.

Figure 9-5 Software package created

5. Click the membership icon and select **Assign to all users,** as shown in Figure 9-6 on page 347. Click **OK**.

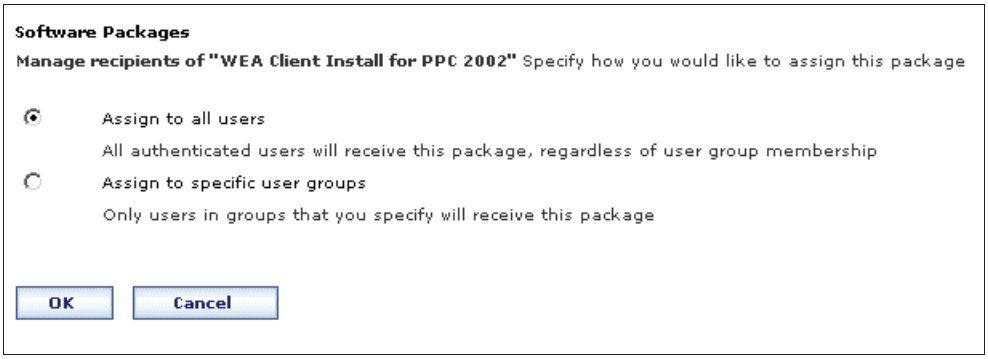

Figure 9-6 Assigning package to all users

6. Finally, the software package is created and is ready for download.

Creating a new device configuration

A device configuration allows us to group several Everyplace Client's device profiles for a particular device type. A device profile defines network configurations to be used by the Everyplace Client, configurations like server addresses, server ports, and so on, in order to protect a user from performing complex configuration tasks on his device. Currently, only Pocket PC and Nokia 9500 devices are supported.

Follow these steps in order to create a device configuration with a device profile inside:

1. Log into the Portal server using the user ID and password of the administrator who is a part of the dmadmins group.
2. Select the **Administration** label. Select **WebSphere Everyplace** → **Device Management** → **Device Configuration**.
3. Click **New.** Enter a name for the configuration and choose Pocket PC as the platform, as shown in Figure 9-7 on page 348. Click **Next**.

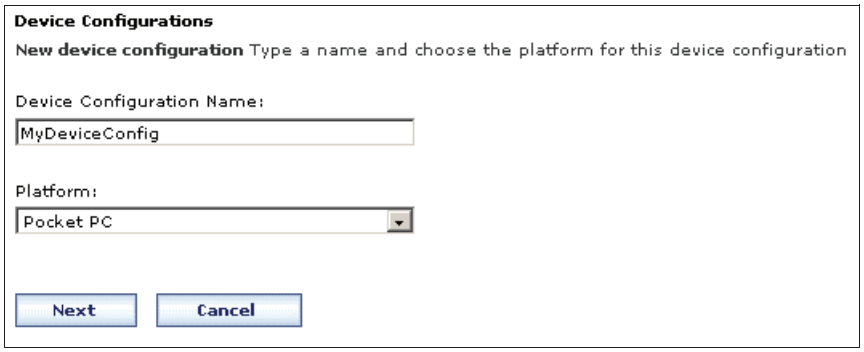

Figure 9-7 Creating a device configuration

4. Name the profile to be created on the device configuration. Here you can enter information about the servers host, ports, and so on, as shown in Figure 9-8. This information will be used by the Everyplace Client in the device. Click **OK.**

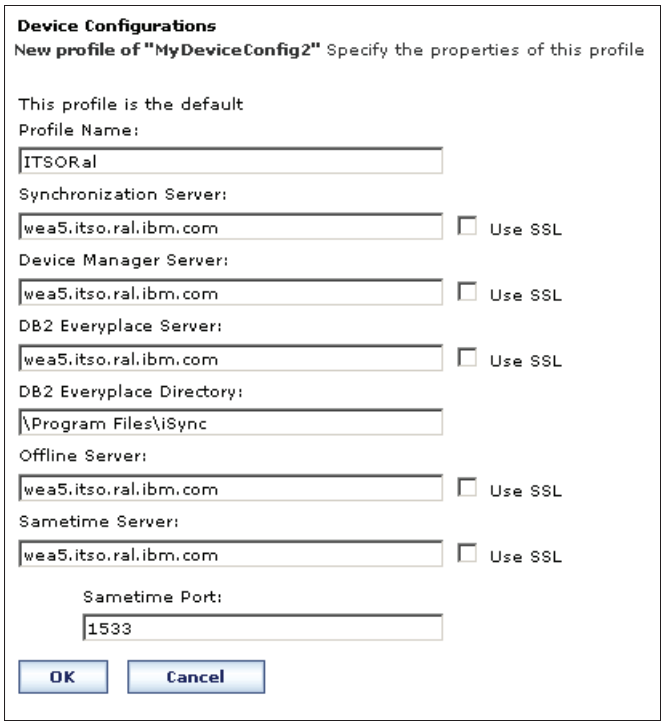

Figure 9-8 Creating a network profile

5. As you can see, this profile will be the default for device synchronization. You can allow the users to specify their own network settings and configure several other options, such as Connection Manager integration. Please refer to the InfoCenter for help. For this scenario, make sure that you have your settings set as shown in Figure 9-9 and click **OK**.

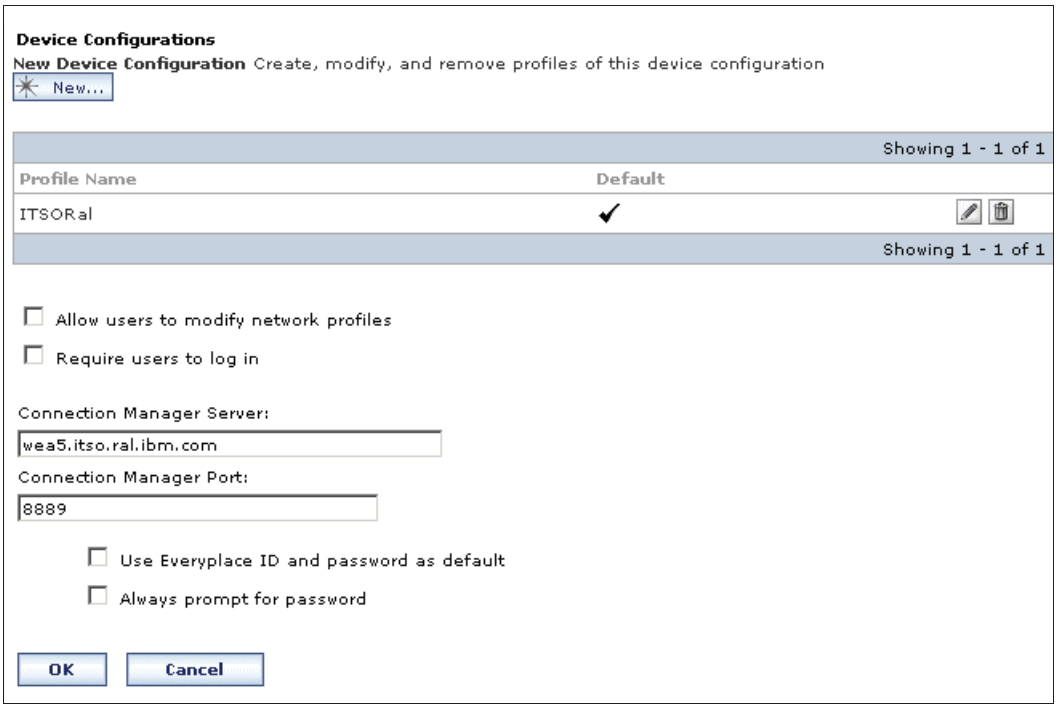

Figure 9-9 Device configuration additional settings

6. Now you will see your newly created device configuration, as shown in Figure 9-10 on page 350. Finally, we will need to assign this configuration to users. Click the membership icon.

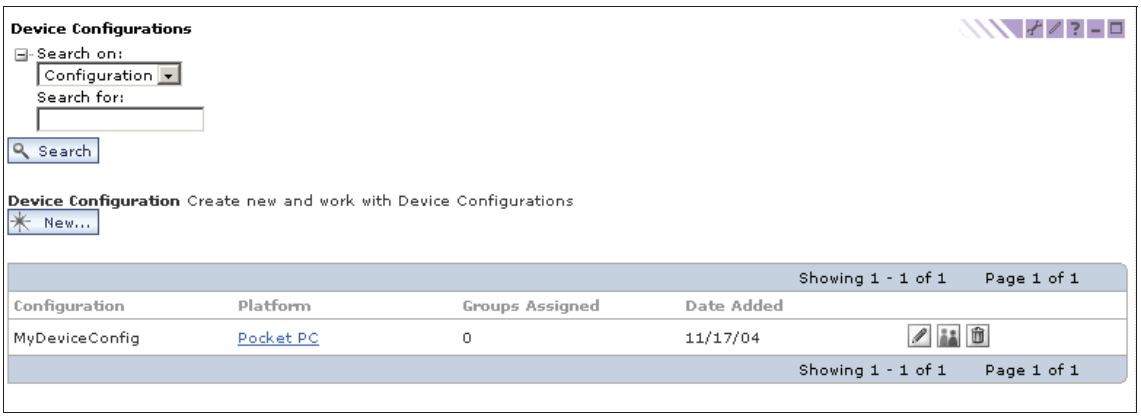

Figure 9-10 Device configuration created

7. You can configure your assignment by group or simply add all the authenticated users to the configuration. We will use the last option. Select **Assign to all users**, as shown in Figure 9-11. Click **OK**.

Figure 9-11 Assigning device configuration to all users

Installing Everyplace Client on the Pocket PC

In this section, we will use the configured software package and device configuration in order to install Everyplace Client on the Pocket PC.

Note: The steps described here are specific to the Everyplace Client package. To install other software packages, the Everyplace Client Device Agent should be used.

Follow these steps:

1. Open the browser on the Pocket PC device and enter the Portal server URL. For example:

   `http://yourserver.com/wps/myportal`

2. Enter the user name and password. The user should be a part of the user group for whom the software package and device configuration has been assigned; in our case, we can use any user available, because we specified All Users in the previous steps. Click **Log in**.

3. You will see the WebSphere Everyplace Access Home page. Select **Mobile Setup** from the first drop-down list and then select **Everyplace Client Installer** from the second one, as shown in Figure 9-12. Click **Everyplace Client Installer**.

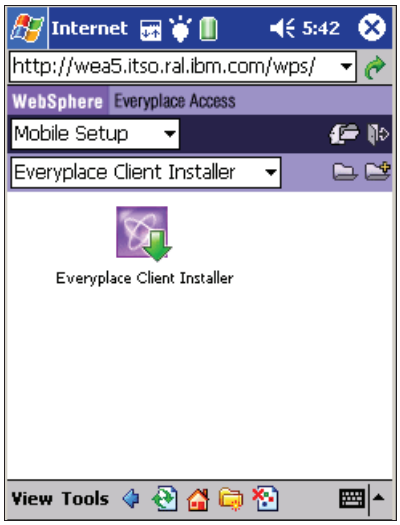

Figure 9-12 Everyplace Client Installer

4. Click **Install** on the window shown in Figure 9-13 on page 352.

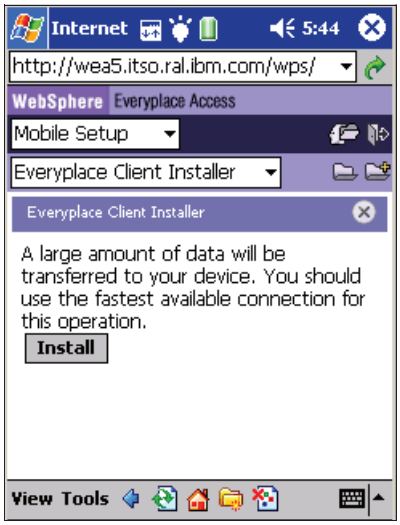

Figure 9-13 Installing Everyplace Client

5. The Device Agent will be downloaded, as shown in Figure 9-14. Click **Yes**. Wait while the agent is downloaded.

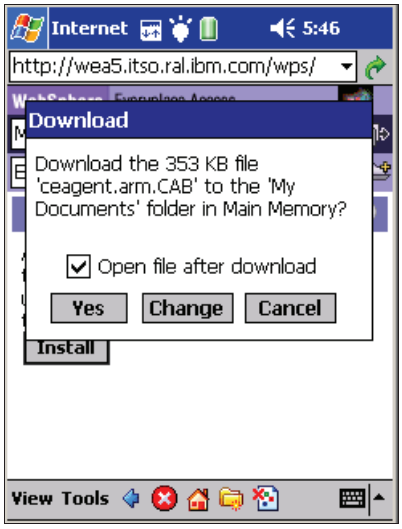

Figure 9-14 Downloading Device Agent cab file

6. You will be asked to enter the WEA user information, as shown in Figure 9-15 on page 353. Enter the password and click **OK**.

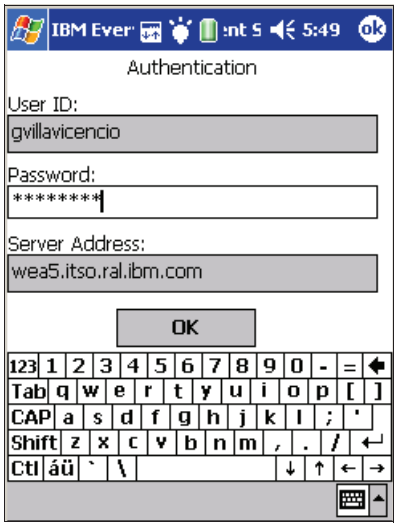

Figure 9-15 Authenticating with Device Agent

7. The installation will take some time. The installation will download the necessary installation files and launch it automatically. The display will show the status of each job being performed. The screen shown in Figure 9-16 should appear on the Pocket PC.

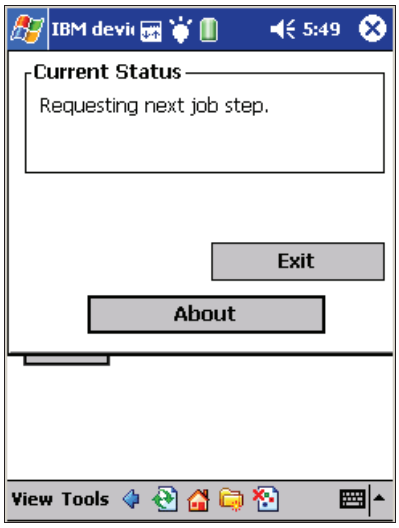

Figure 9-16 Device Agent performing the installation

8. The first time the device connects to the Device Services, the Device Services servlet routes the call to the enrollment server, which enrolls the device with the user. The user is the user ID with which you logged into the Portal server. The first job that is performed is an inventory job. Subsequently, the Device Management Server will check if there were any jobs scheduled for this device class and user group and continue processing them. The Everyplace Client files are downloaded and launched automatically. Once the installation and configuration of the WebSphere Everyplace Access Client is completed successfully, you will see the screen shown in Figure 9-17.

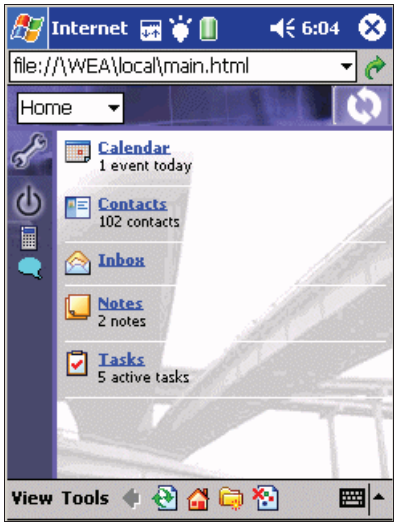

Figure 9-17 Everyplace Client installed

9. Click the wrench icon. Scroll down to network profiles and check the network configuration profile. It should show the profile you had configured for this device with your server addresses, as shown in Figure 9-18 on page 355.

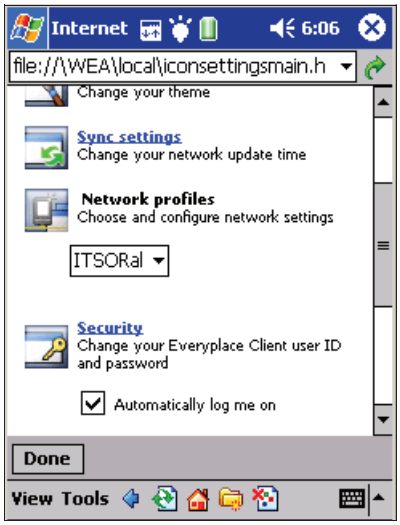

Figure 9-18 Everyplace Client configured

10. The WebSphere Everyplace Access Client is installed and configured. You are all set for the next scenario.

9.3.2 Software distribution using Device Manager Console

Distributing software to devices is the most common application of device management. In this scenario, we will show you how to use the Device Services console and the necessary steps that you will have to perform in order to distribute software to devices.

Distributing software requires you to:

1. Create a software package
2. Register the software with the Device Management Server
3. Create a job for distributing it

As an example, we show you the suggested steps for software distribution when distributing a DB2e application to a Pocket PC device. For details about DB2e application development, see *IBM WebSphere Everyplace Access V5 Handbook for Developers and Administrators Volume II: Application Development*, SG24-6463.

Creating the software package

A software package consists of the application-related files along with two other files: the meta package definition file and the package definition file.

The meta package definition file is the definition file for the entire software package. It lists all the application packages that make up a software package.

For each application package in the software package, the package definition file lists the files that make up the application package, such as graphics files, database files, compiled files, and distribution properties for that application package, such as running a setup file after the files are downloaded and allocating disk space.

For detailed instructions on what constitutes a meta package definition file and package definition file, look into the appropriate plug-in section in the Device Services Library.

Applications to be distributed to Pocket PC devices are packaged as CAB files. Palm device applications (*.PRC) and databases (*.PDB) can be distributed.

Creating a software package

1. The software package has to be accessible by the HTTP Server. Create a folder under the document root of your HTTP Server Program Files/IBM HTTP Server/htdocs. We created a folder called DMSSoftware.
2. Copy your application CAB files to the DMSSoftware directory. Our application has only one CAB file, called WinCEMobileOrderSystem.CAB.
3. Create the package definition files for your applications; an example file is shown in Example 9-1.

Example 9-1 Package definition file: MobileOrderSystemInstall.txt

```
#*DFP-v1.00 DMS Filepack (version v1.00)
after_prog_path=\windows\wceload.exe \temp\WinCEMobileOrderSystem.CAB
%
WinCEMobileOrderSystem.CAB d=\temp
%
%
%
```

4. Create the meta package definition file. There should be only one meta package definition file for the entire software package; an example is shown in Example 9-2.

Example 9-2 Meta package definition file: MobileOrderSystem_install.PKG

```
PackageUserSelection=no
PackageName=MobileOrderSystem
PackageVersion=1.0.0.0
PackageDescription=DB2e Order System Example
[Application1]
ApplicationUrl=MobileOrderSystemInstall.txt
```

```
ApplicationSelectionDisable=yes
ApplicationName=MOBILEORDERSYSTEM
ApplicationVersion=1.0.0.0
ApplicationDescription=Db2e Order System Example
```

5. The package definition files and meta package definition file should be copied to the DMSSoftware directory.

Registering the software with the Device Management Server

1. Open the Device Services console. The software is created for a specific device class. Click **Device Classes.** Right-click the appropriate device class where you are registering the software and select **New Software**.

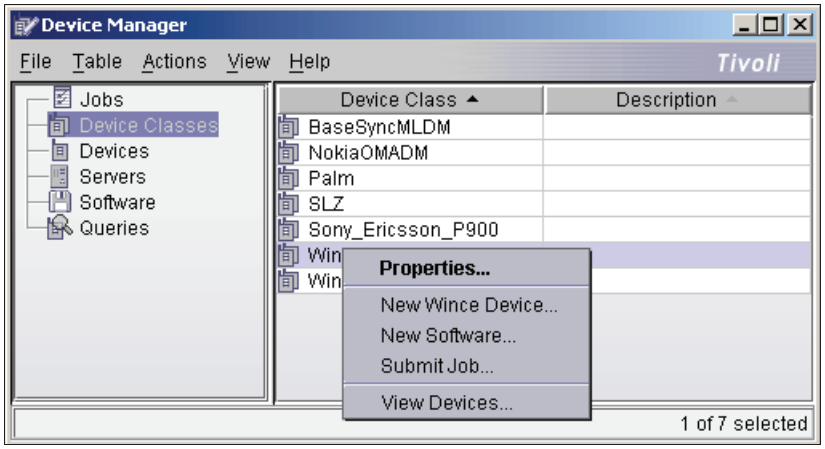

Figure 9-19 Registering new software

2. Select the package type, enter the URL for the package definition file, and click **Fetch**. The software name and version is retrieved from the package definition file, as shown in Figure 9-20 on page 358. Click **Next**.

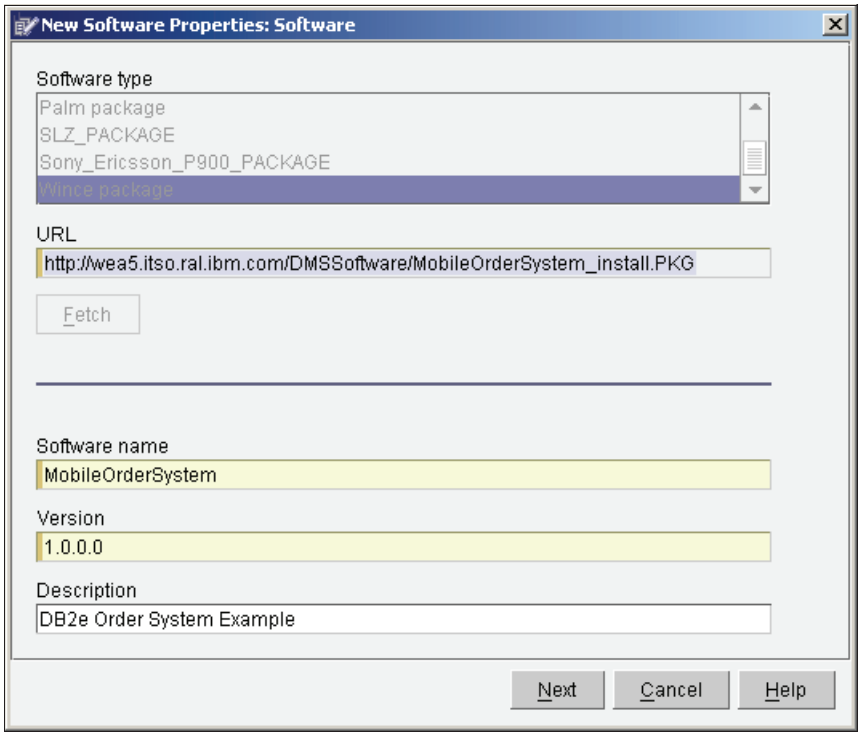

Figure 9-20 New software properties

Note: The URL should be the fully qualified URL for the meta package definition file.

3. Note that the software will be available for two kind of tasks: distribution and removal. Click **OK**.
4. Click **OK** and check if the software is registered by clicking the **Software** tab and select **Return Anything**.

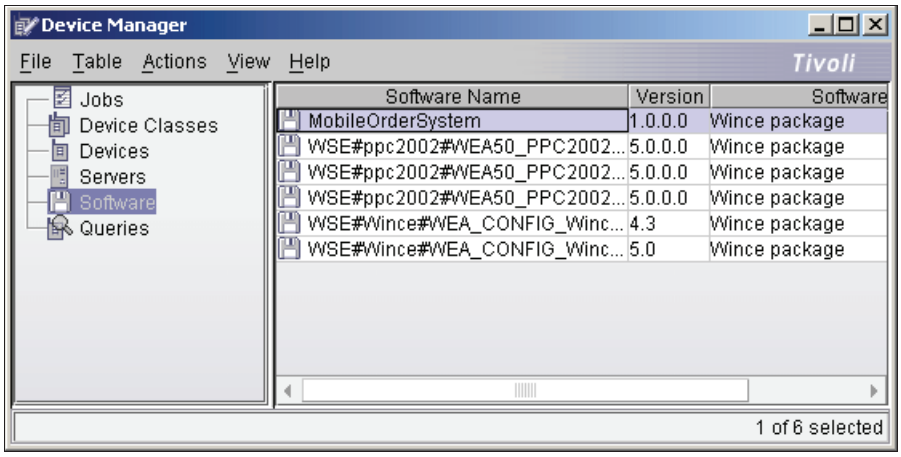

Figure 9-21 Software registered

Creating a software distribution job

With the Device Services console, you can create jobs for specific devices, user groups, device classes, enrolled devices, and so on. You can create the following types of jobs:

- Inventory collection job
- Device configuration job
- Software Distribution job
- Software Removal job

We will create a software distribution job for the user group AllSyncUsers and for Windows CE devices.

To create a software distribution job, do the following:

1. In the Device Services console, right-click **Jobs** and select **Submit Job**.
2. Select the device class and owner group. You can filter by using the query functionality and you can also select if the job is for enrolling or already enrolled users, as shown in Figure 9-22 on page 360. Click **Next**.

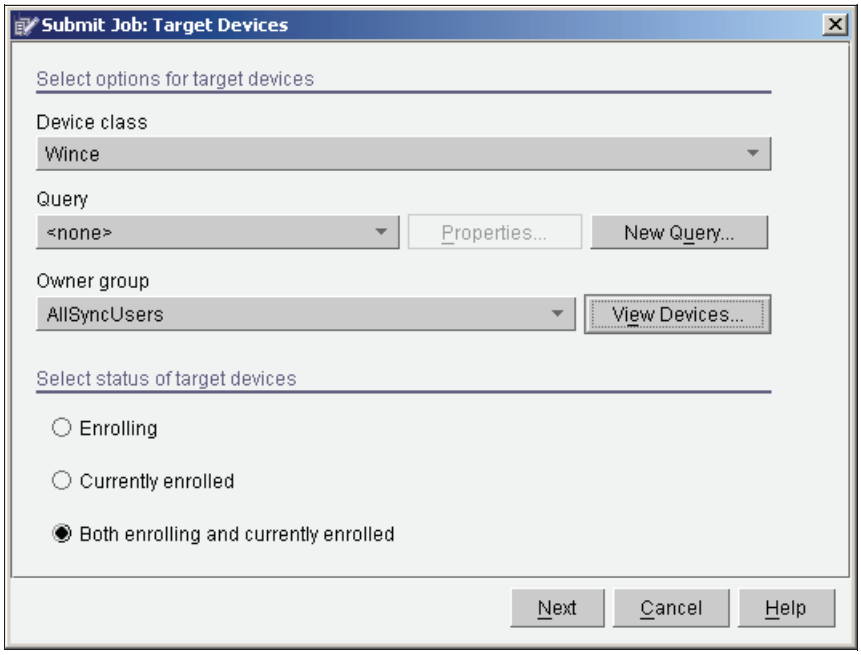

Figure 9-22 Target devices

3. Select **Software Distribution** as the job type. Enter adequate dates for the activation and expiration fields and a description for the package. Click **Next**.

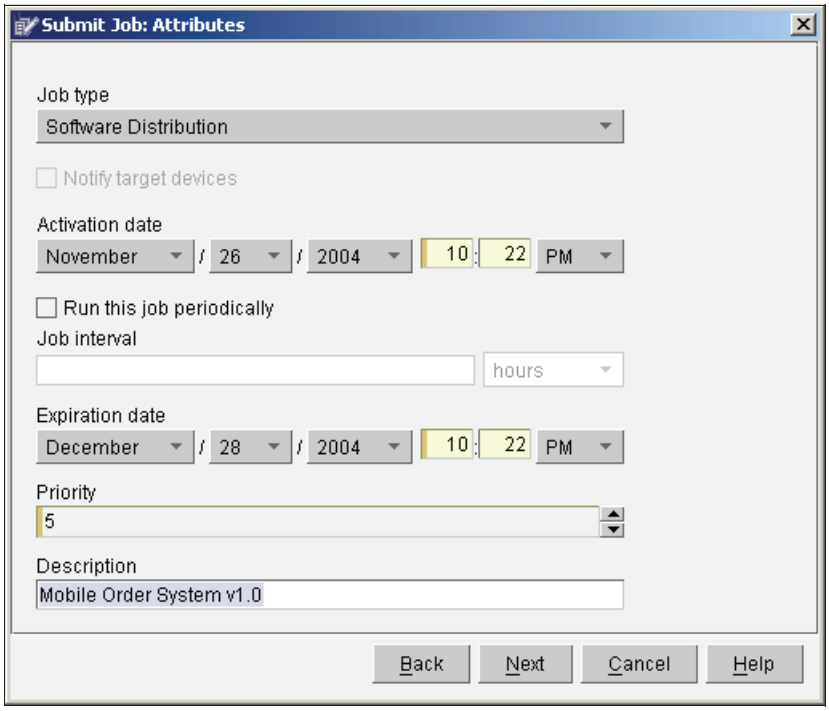

Figure 9-23 Attributes

4. Click **Add Group** and select the software to be distributed, as shown in Figure 9-24. Click **Next**.

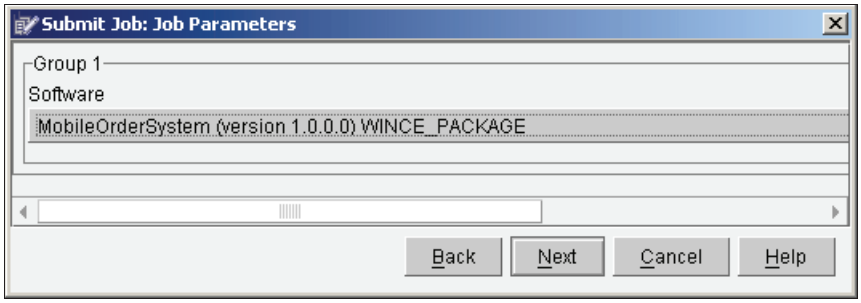

Figure 9-24 Software to be distributed

5. You will be shown the job summary. Click **Next**. You will be shown a job submission status. Click **OK**.
6. The job has been created successfully. Click **Close**.

Job progress

1. To verify the status of your job, click **Jobs**. Click **Target Device Class**. Select **Return anything with a device class that matches**. Select **WinCE** and click **OK**, as shown in Figure 9-25.

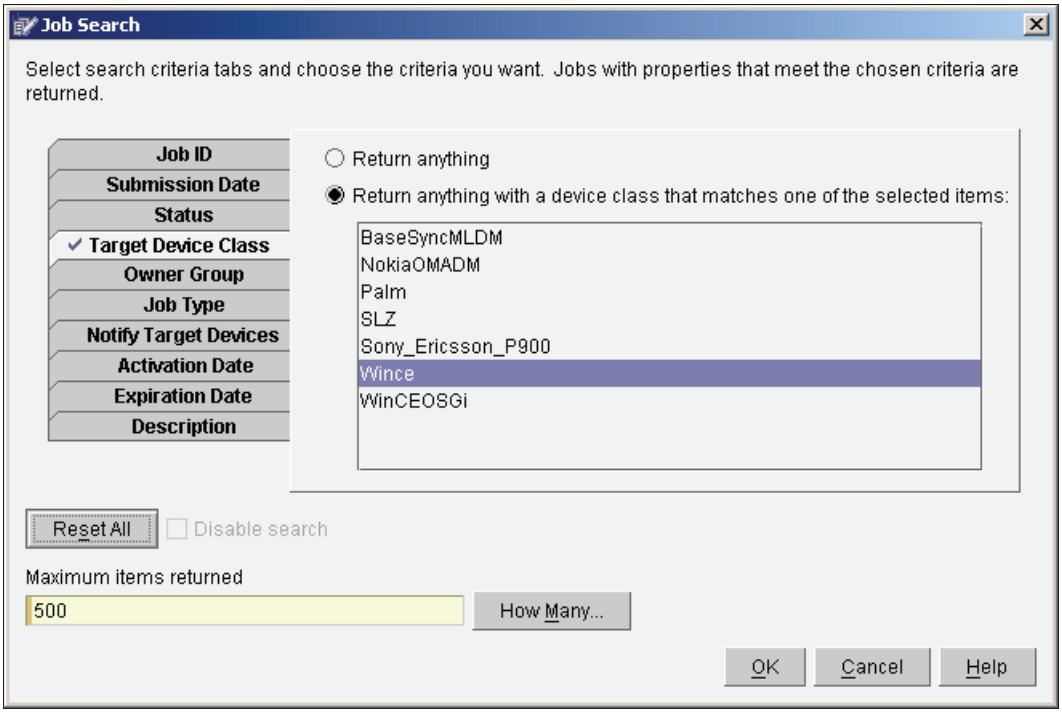

Figure 9-25 Job search

2. You should be able see the job in your list. Right-click the job and select the **View Job Progress Summary** option. This will show the current status of the job, as shown in Figure 9-26 on page 363.

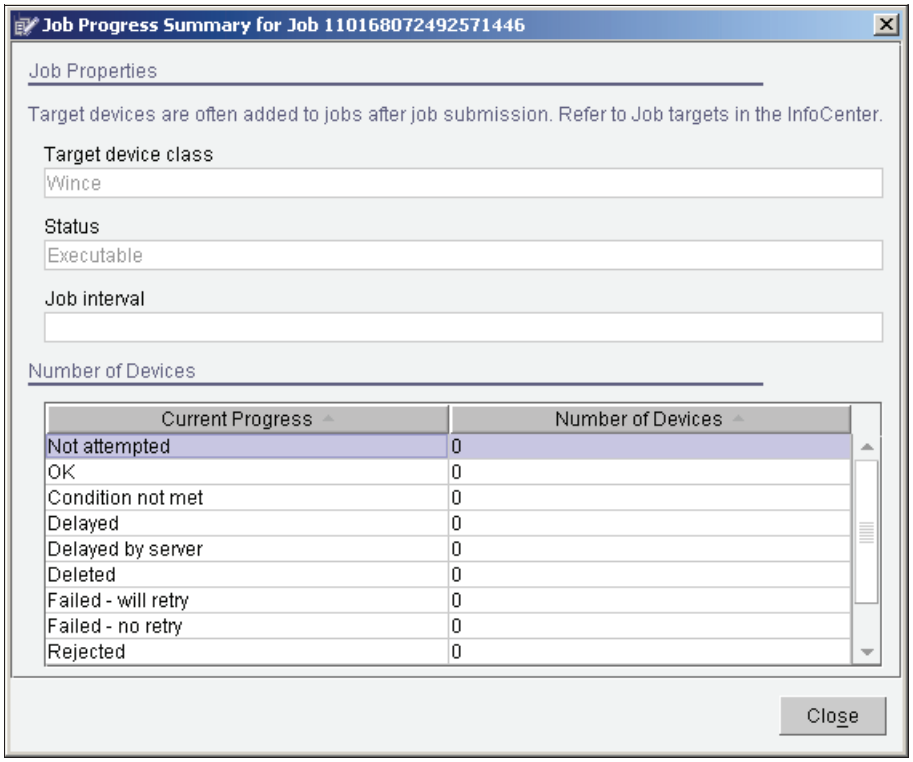

Figure 9-26 Job progress summary

Connect to Device Management Server using a device

1. Start the Everyplace Client in the Pocket PC device.
2. Click the wrench icon. Scroll down and click **Software Update**, as shown in Figure 9-27 on page 364.

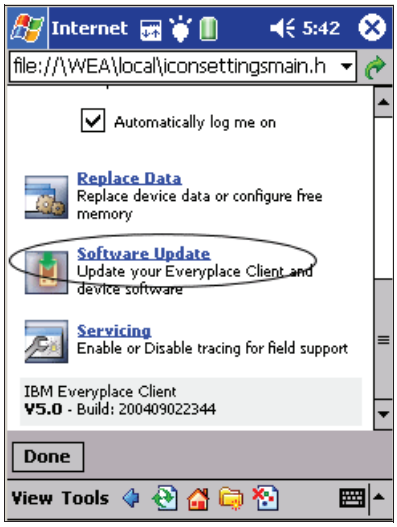

Figure 9-27 Device Agent

3. Click **Get Updates** and wait while the software is downloaded and installed to your device.
4. Device Management Server administrators can check the status of their jobs through the Device Services console. You can see that the last attempt of the job was OK, as shown in Figure 9-28 on page 365.

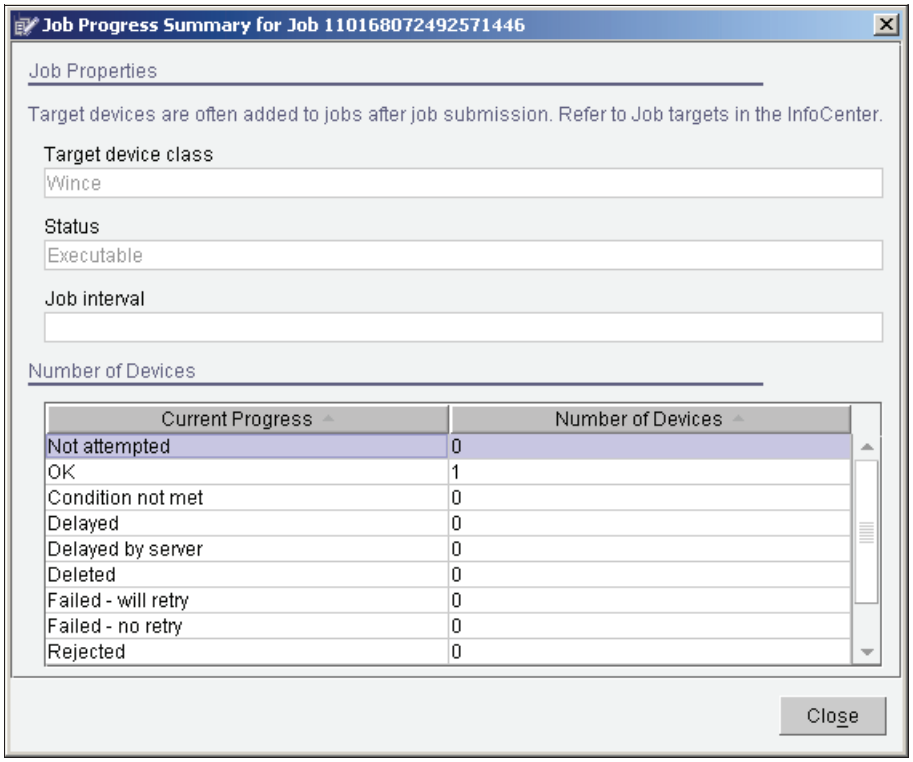

Figure 9-28 Job progress after executing the job on a device

9.3.3 Configuring SSL on a Palm device

With this scenario, we will show how to work with Palm devices to connect to the Device Management Server. Also, we will show you how to create a configuration job. We will be creating a job to enable Palm to connect using SSL.

Steps to connect to the Device Services

For information about how to install and configure Everyplace Access Client components on Palm devices, refer to Chapter 7, “WebSphere Everyplace Client installation and configuration” on page 287.

Note: For the Device Agent to work on Palm devices, it is necessary to have IBM Device Services Conduit for Palm OS installed on the host PC. The program is included in the IBM Everyplace Client CD.

1. Click the applications and click **IBM Agent**, as shown in Figure 9-29 on page 366.

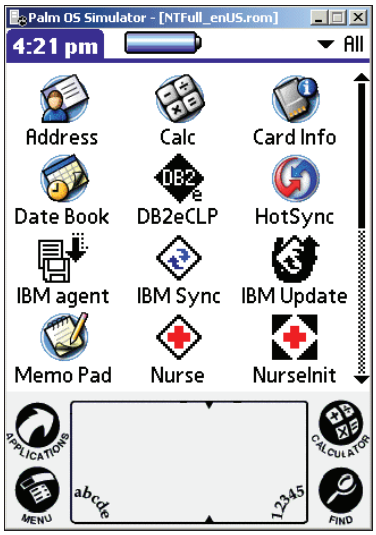

Figure 9-29 IBM Agent for Palm

2. Click the top of the next screen to configure the server and the login settings, as shown in Figure 9-30.

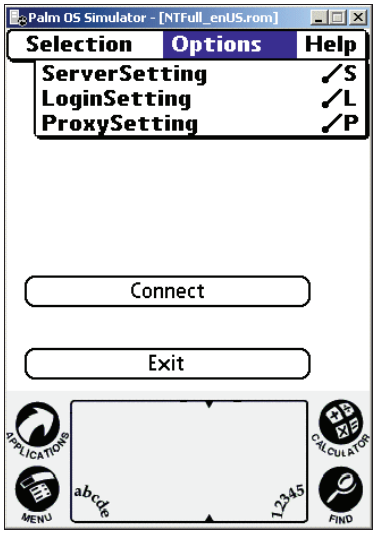

Figure 9-30 Settings

3. Select **Server Setting**, enter the address of your server, and click **OK**, as shown in Figure 9-31 on page 367.

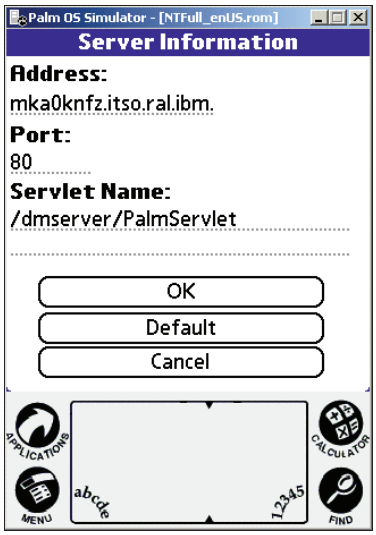

Figure 9-31 Server settings

4. Select **Login Setting** and enter the user name and password of your account on the Everyplace Access server. Enter `HotSync` as the service name, as shown in Figure 9-32.

Figure 9-32 Login configuration

5. Click **OK**. This should bring up the screen shown in Figure 9-33 on page 368. Click **Connect**.

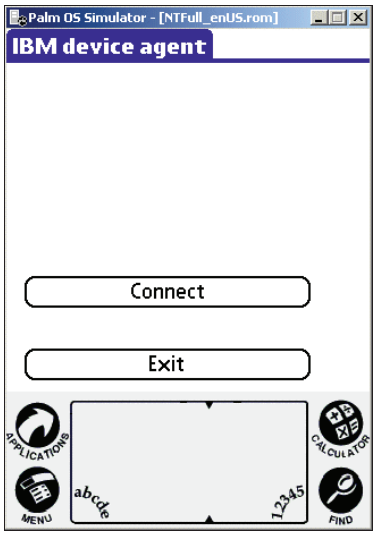

Figure 9-33 IBM Device Agent

6. This will connect to the Device Management Server. Since this is the first time the device is connecting to the server, an inventory scan will be performed, as shown in Figure 9-34.

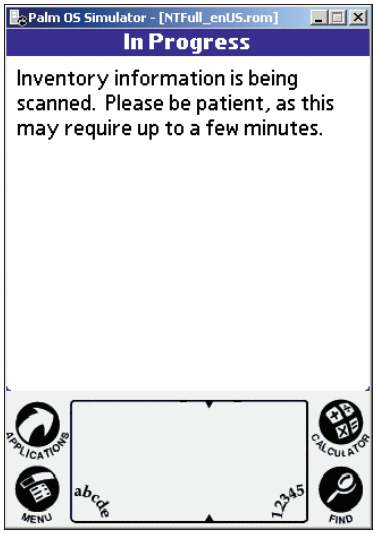

Figure 9-34 Device agent at work

7. You will get a message when the inventory scan is over.

Creating a SSL configuration job

1. Open the Device Services console. Click **Devices** and select **All Palm devices**, as shown in Figure 9-35. Click **OK**.

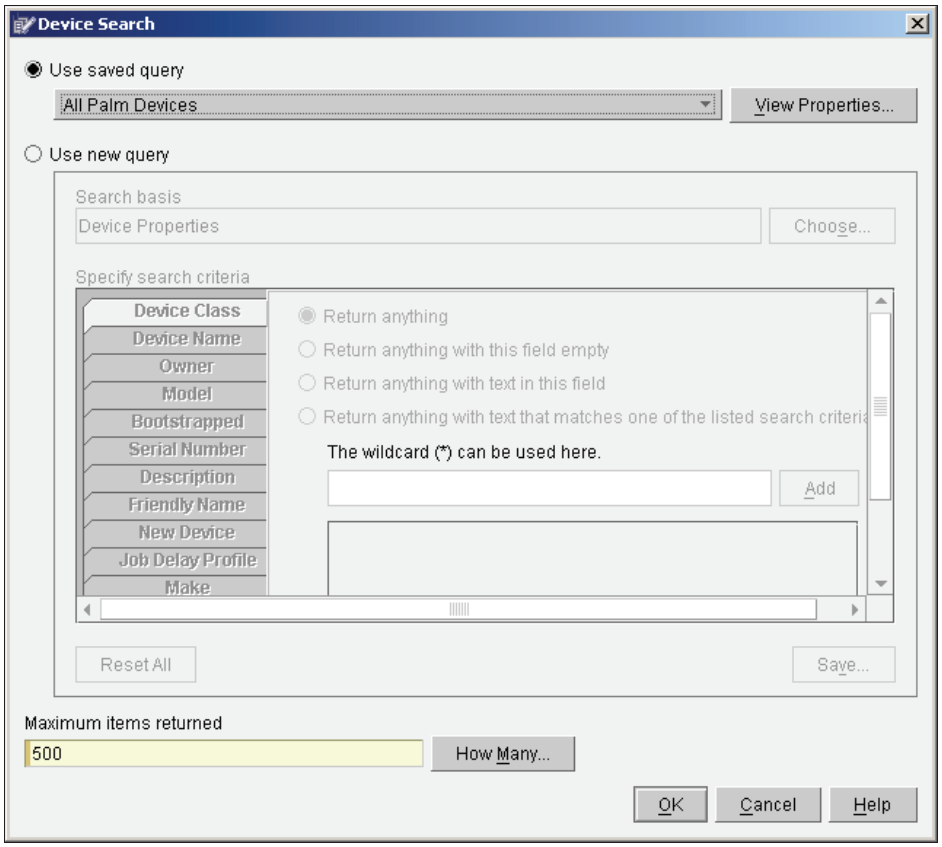

Figure 9-35 Querying Palm devices

2. Right-click the Palm device you want to configure SSL and click **Submit Job**, as shown in Figure 9-36 on page 370.

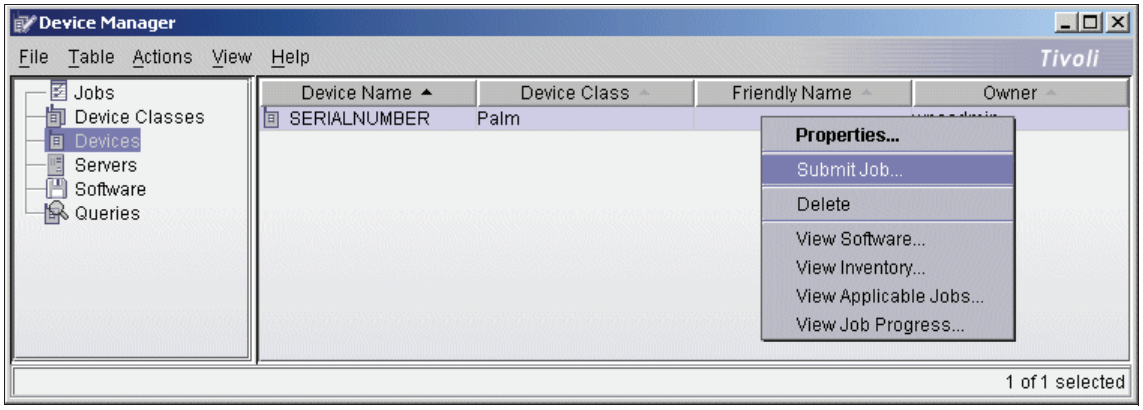

Figure 9-36 Creating a job

Tip: If you want to configure SSL on all the Palm devices that connect, select **Device Classes**, right-click the Palm devices, and select **Submit Job**.

3. Select **Configuration job** as the job type. Enter a suitable description for the job, as shown in Figure 9-37 on page 371. Click **Next**.

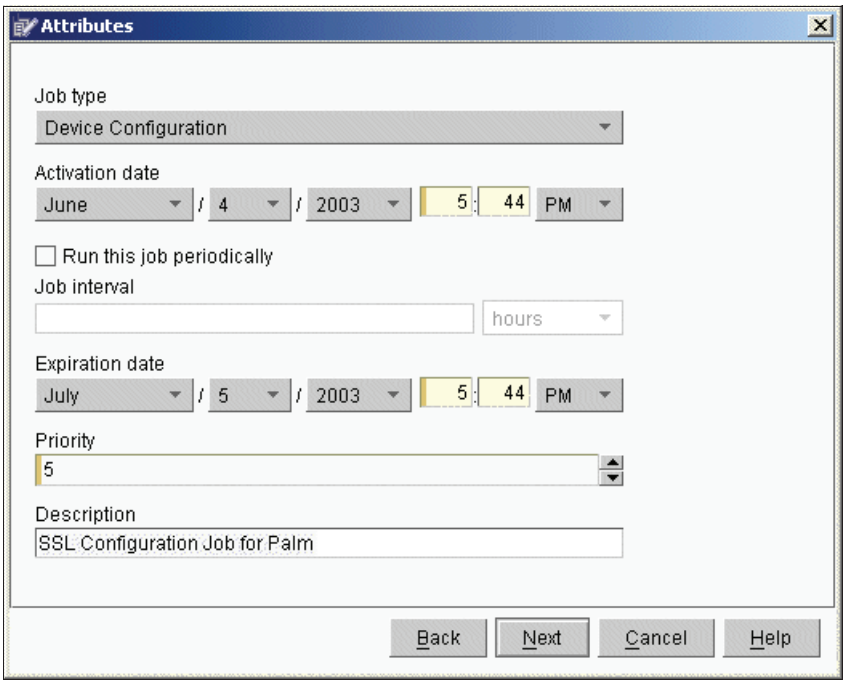

Figure 9-37 Job attributes

4. Select the **Agent** tab. In the SSL On drop-down list, select **On**. Enter 443 as the Management Server port and click **Next**, as shown in Figure 9-38 on page 372.

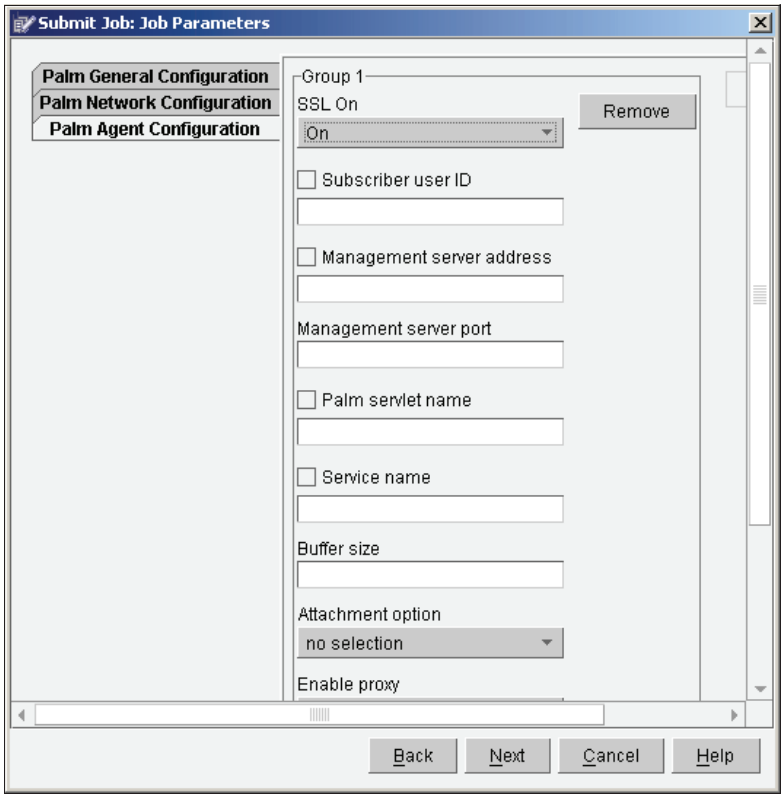

Figure 9-38 Device Agent configuration

5. Click **Next**. This will show you a window for which devices the job is submitted. Click **OK**. A message stating that the job has been successful comes up. Click **OK**.
6. Connect to the Device Services using the IBM Agent on the Palm device.
7. You will get the following messages:

```
Connect to Network Dispatcher
Connect to Management Server
Post Job Result
Complete
Configuration Job Complete
```

8. Exit and start the IBM Agent again. Check the Server Settings. Connect to the server to check if the IBM Agent can communicate using SSL on port 443.

9.4 Troubleshooting

There could be situations where you may need to view the Device Management Server traces to check the status of the server and the jobs submitted. By default, the tracing is disabled. The trace log is primarily a development tool and should be enabled when troubleshooting. Enabling the trace log can affect your system performance. Extended use of trace logging can also consume large amounts of disk space. To manually enable tracing, do the following steps:

1. Go to the directory where WebSphere is installed and navigate to the subdirectory WebSphere\DMS16\dmserver\WEB-INF\classes. Locate traceConfig.properties. You can change the trace level here. Near the bottom of the file are the trace flags for each of the Device Services components. Set the appropriate flags on depending on the problem faced. For example, if there is a problem with plug-ins, you could set the traceEnabled.plugins to true, as shown in Example 9-3.

Example 9-3 Flags for different components of Device Services

```
#trace enabled for components
component.console=false
component.dmserver=false
component.event=false
component.notification=false
component.plugins=false
component.resultscollector=false
component.twgapi=false
component.database=false
component.enrollserver=false
component.datconverter=false
component.mcollect=false
component.notificationhandler=false
component.api=false
component.userservices=false
```

2. Save your changes.
3. Open a command window and navigate to the directory WebSphere\DMS\bin.
4. Run the command **`server -app dmserver -trace set`**. This will prompt the Device Services to re-read the trace settings and act on them.
5. Perform the device management tasks. To view the trace logs, navigate to WebSphere\AppServer\logs and open the file DMS_stdout.log.

10

Instant messaging

This chapter discusses the messaging service offered in Everyplace Access, the components that are needed for enabling the instant messaging service, and how to configure and use the Sametime client.

© Copyright IBM Corp. 2005. All rights reserved.

10.1 Overview

Instant messaging is the most popular means of communication in the connected world. Everyplace Access brings instant messaging to mobile devices. The Everyplace Access Client includes the Lotus Sametime V3.0 client, so that mobile and desktop users can chat with each other seamlessly.

With Sametime, users can set their current status, set alert preferences, manage users and groups, and so on. Figure 10-1 shows the Sametime client architecture.

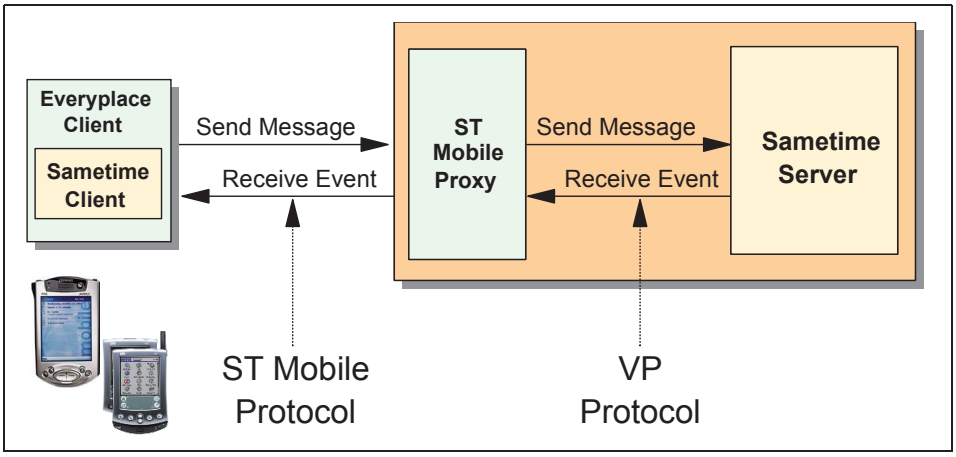

Figure 10-1 Sametime client architecture

The Sametime V3.0 client comes with the Sametime Mobile Protocol Stack, which talks to the Sametime Mobile Server using this protocol. The Sametime Mobile Server is an extension of the Sametime Server. Both the desktop user and the mobile user will connect to the same port on the Sametime Server. The Sametime Mobile (ST Mobile) proxy detects if the incoming request is from a mobile device or a normal desktop and establishes a session using specific protocols.

This chapter shows how a Pocket PC device and a Palm device can use the Sametime client component provided with WebSphere Everyplace Access. In this scenario we used Lotus Domino Server V6.0.4 and Sametime V6.5.1 Server. To enable mobile clients to connect, Lotus Sametime Mobile Extension V3.0 was also installed.

For instructions on how to set up Lotus Domino Server and Lotus Sametime Server, see Appendix A, “A sample Sametime installation” on page 421. The

Sametime Server has to be installed on the same machine as the Lotus Domino Server.

10.1.1 Sametime messaging on Pocket PC

To start and configure Sametime messaging on Pocket PC or Windows Mobile, follow these steps:

1. Select **Start** → **Programs** and then select the **Sametime Connect** icon, as shown in Figure 10-2.

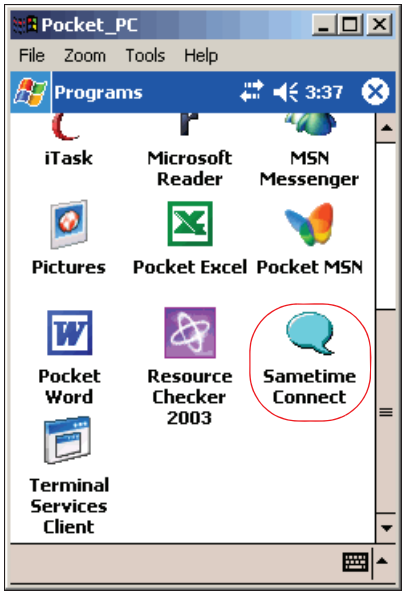

Figure 10-2 Starting Sametime on Pocket PC

2. Also, it is possible to start Sametime Connect from Everyplace Client, as shown in Figure 10-3 on page 378.

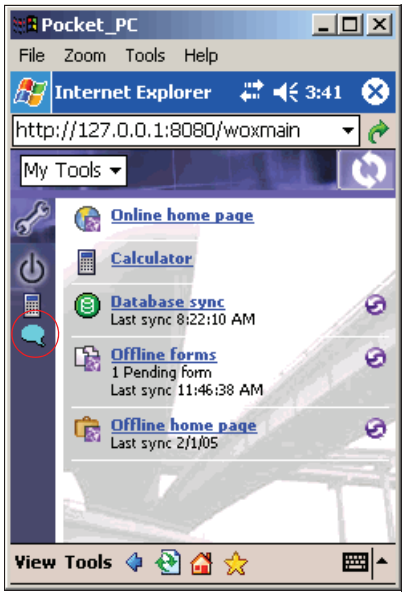

Figure 10-3 Starting Sametime from Everyplace Client on Pocket PC

3. Enter the login information and click the **Connectivity** button, as shown in Figure 10-4.

Figure 10-4 Startup window on Pocket PC

4. Set the host name and port information and click **OK**, as shown in Figure 10-5.

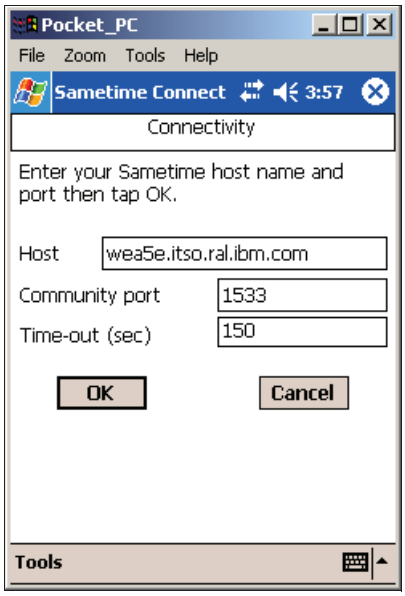

Figure 10-5 Connectivity window on Pocket PC

5. Now you can log in to Sametime.

Adding users and chatting

Once logged in, you need to add Sametime users to your contact list to start a chat session.

1. Click the **Tools** tab and select **Add**, as shown in Figure 10-6 on page 380.

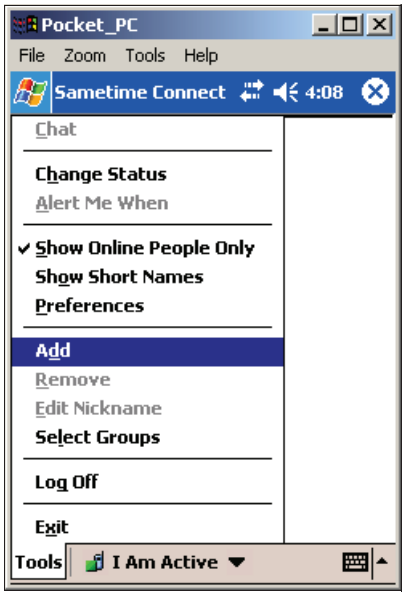

Figure 10-6 Tools

2. Enter the user name, nickname, and group. Click **Add**, as shown in Figure 10-7.

Figure 10-7 Adding a person

3. The user will be added to your Sametime contact list, as shown in Figure 10-8.

Figure 10-8 Sametime contact list

4. To chat with online users, click the user to chat. Then open **Tools** and click **Chat**, as shown in Figure 10-9 on page 382.

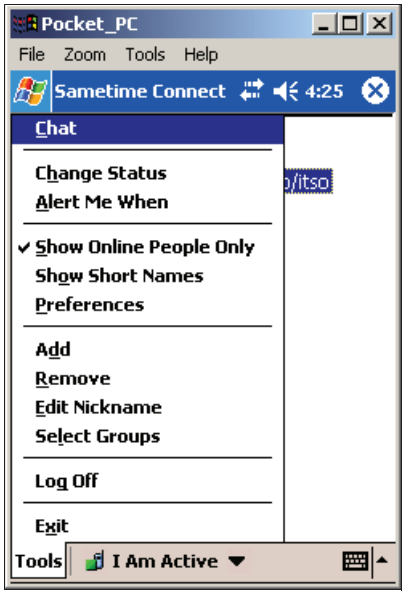

Figure 10-9 Starting a chat session

5. Figure 10-10 shows a sample chat session.

Figure 10-10 Chat session

10.1.2 Sametime messaging on Palm OS

The Sametime messaging configuration on Palm OS is similar to the Pocket PC configuration. This is a brief explanation of the required steps:

1. Open Sametime Connect by clicking its icon.
2. Enter the login and connectivity information. Click the **Log On** button, as shown in Figure 10-11.

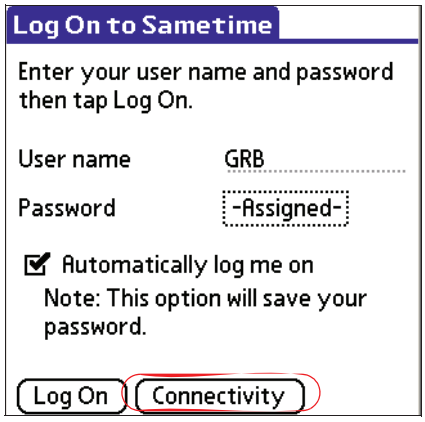

Figure 10-11 Log On to Sametime on Palm OS

3. Click the **Sametime** tab and select **Add** to include a new Sametime contact user. Enter the user name, nickname, and group. Click **Add**, as shown in Figure 10-12.

Figure 10-12 Adding a person

4. To start a chat session with an online user, click the user to chat. Then click **Sametime** → **Tools** → **Chat**. Figure 10-13 shows a sample chat session

Figure 10-13 Chat session

10.1.3 Sample scenario

This sample scenario shows a Pocket PC and Palm OS users interacting with each other using Lotus Sametime. Figure 10-14 on page 385 shows a sample chat session.

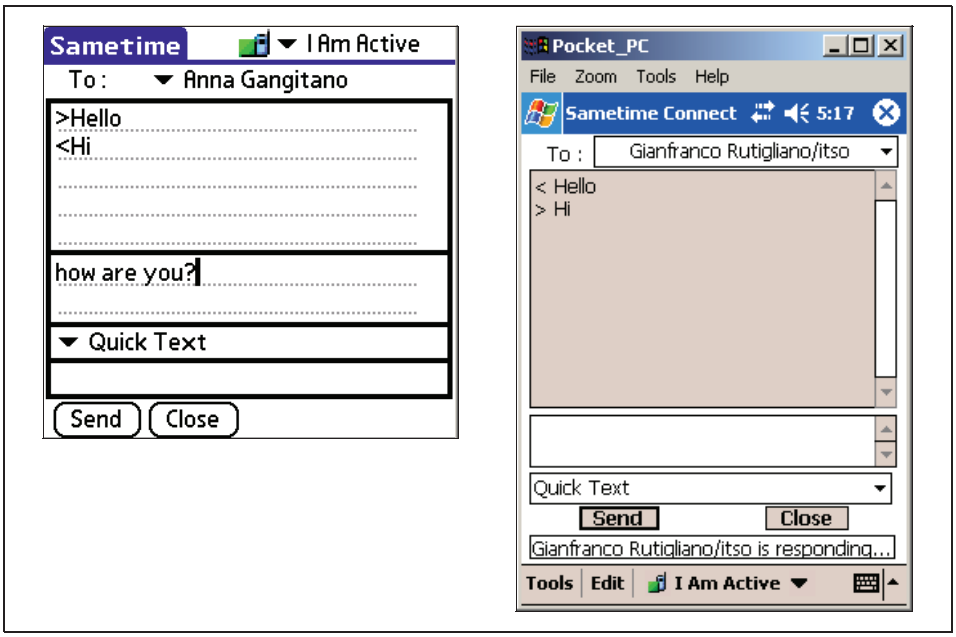

Figure 10-14 Chat session

11

Resource Checker

The Everyplace Resource Checker is a tool to check whether or not Pocket PC 2002 or Windows Mobile 2003 devices are capable of running all the required Everyplace Client components. The Resource Checker is not a comprehensive performance analysis tool; it is intended only to assist the person responsible for installing Everyplace Client to choose a suitable device.

© Copyright IBM Corp. 2005. All rights reserved.

11.1 Introduction

When running the Resource Checker, the user is instructed to run all the applications needed for the use scenario. It then gathers input from the user on the Everyplace Client components and the data profile needed for the particular use case. Next, the Resource Checker analyses the devices system resource profile, including the memory and storage capacity by running processes in real time. Once complete, it displays a summary of the results. The option to view and save a more detailed summary, which could be analyzed by IBM Support Personnel if needed, also exists.

11.2 Installation

For the purpose of this redbook, a Windows Mobile 2003 device and the Windows Mobile 2003 Resource Checker will be used. The following steps will install the Resource Checker on your Windows Mobile 2003 device:

1. Connect your mobile device to the WebSphere Everyplace access server and make sure that ActiveSync is running. (There will be a green circle around the icon.)
2. Locate the file containing the Resource Checker application and double-click Setup.exe to launch the Install Wizard.

> **Note:** The WebSphere Everyplace Access Resource Checker tool can be searched and downloaded from the following Web site:
>
> `http://www.ibm.com/support/us/`

3. The **Welcome to the InstallShield Wizard** panel appears. Click **Next** to continue, as shown in Figure 11-1.

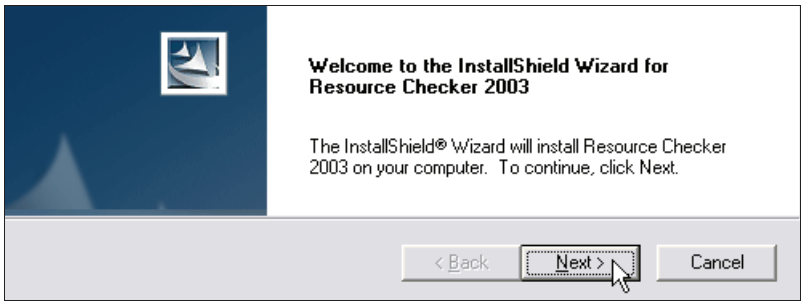

Figure 11-1 Resource Checker installation

4. Click **Yes** to accept the terms of the Software License Agreement.
5. On the **Choose Destination Location** screen, accept the default destination folder and click **Next**.
6. The Install IBM Resource Checker pop-up will appear. Accept the defaults by clicking **Yes**, as shown in Figure 11-2.

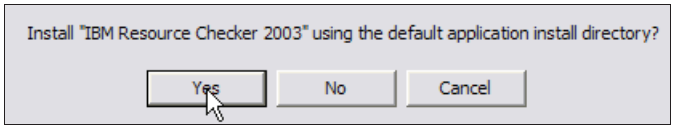

Figure 11-2 Application install directory

7. A pop-up prompting you to check your device for additional steps will appear. Check the device and complete any necessary steps. Click **OK**, as shown in Figure 11-4 on page 390.

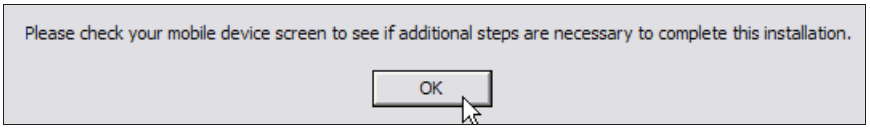

Figure 11-3 Completing the installation

8. Click **Finish**
9. Verify that the Resource Checker icon is listed under **Start** → **Programs** on the device.

11.3 Determining device resources

Before running the application tool, it is important that you have all the following information:

- Device manufacturer and model number
- A list of all the applications (non-Everyplace Client) that would typically be running concurrently on the device, for example, Internet Explorer
- Which of the following Everyplace Client components would be used:
  - PIM and E-Mail Synchronization
  - Database Sync Client
  - Mobility Client
  - Mobile Sametime

  - Software Update
- Approximately how much data will be stored on the device for the following components:
  - PIM and E-Mail data size
  - Database data size

11.4 Running the Resource Checker

WebSphere Everyplace Access Resource Checker uses a graphical user interface that will guide you through the necessary steps.

1. On the Windows 2003 Mobile device, either click the **Resource Checker 2003** icon or select **Start** → **Programs** → **Resource Checker 2003**. The welcome screen will appear, as shown in Figure 11-4. Click **Next**.

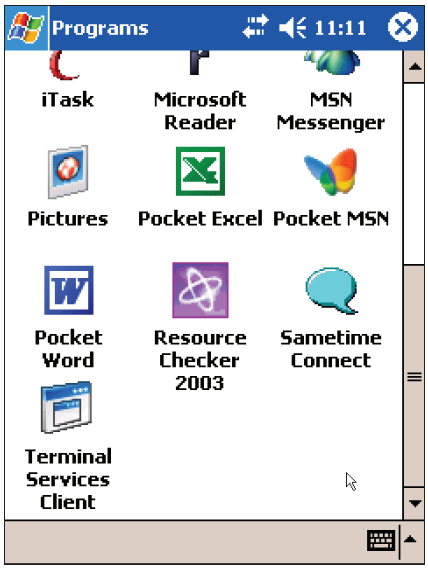

Figure 11-4 Running the tool

Note: The **X** located on the top right hand side of the screen is a smart minimize button, not an Exit button. You may use this button to minimize the application while you launch the required applications in step 2 below. To restore the application, simply follow step 1 above.

2. Follow the instructions on the Setup screen, and launch all the applications that could possibly be running on the device in a typical scenario. It is important to start all the possible applications; failing to do so will produce an un-realistic result. Click **Next** once all the applications are running (see Figure 11-5).

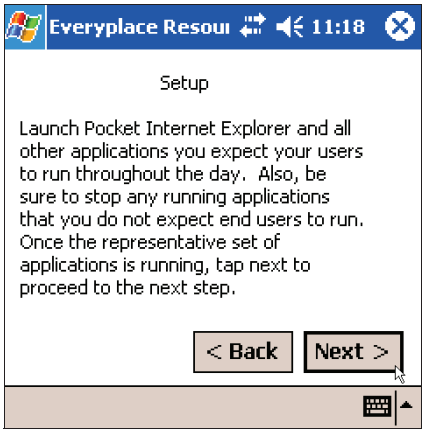

Figure 11-5 Setup

3. The Everyplace Subsystems screen shown in Figure 11-6 on page 392 illustrates the list of all the Everyplace Client components available for use in your scenario. Select the check box for each of the components that you wish to use and click **Next**.

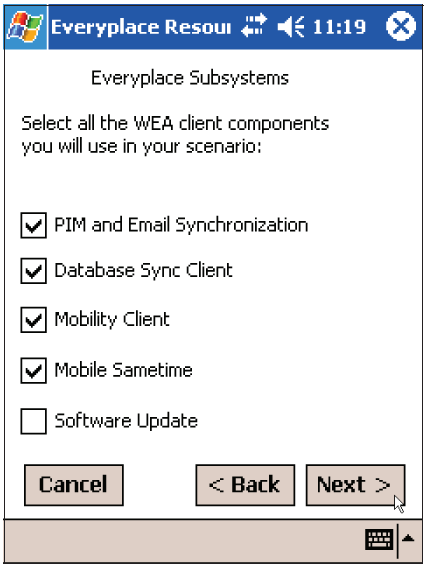

Figure 11-6 Selecting WebSphere Everyplace Access components

4. On the Data Storage Profile page, using the drop-down menus, you can enter the estimated amount of data that will be used by the components and applications in your scenario. Click **Analyze** (see Figure 11-7).

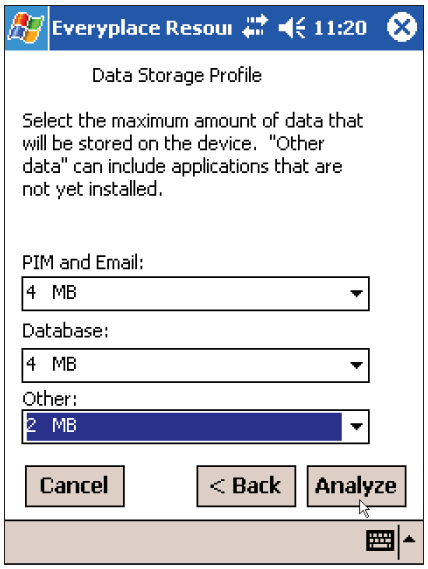

Figure 11-7 Data storage profile

5. The Results page is displayed next and includes a summary of the findings and a stoplight graphic (see Figure 11-8). The stoplight will display either a Green, Yellow, or Red light, which means the following:
   - Green: The device has sufficient memory and process slots to run the scenario, with at least 2 MB of memory and two process slots remaining.
   - Yellow: The device has barely enough memory or process slots to run the scenario.
   - Red: The device does not have sufficient memory or process slots to run the scenario.

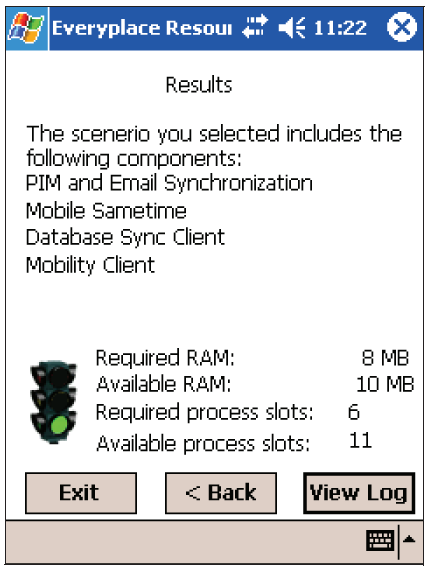

Figure 11-8 Results

Note: For more detailed information, click the **View Log** button (see Figure 11-9). The information in the log file may be saved to another name for comparison purposes if so desired

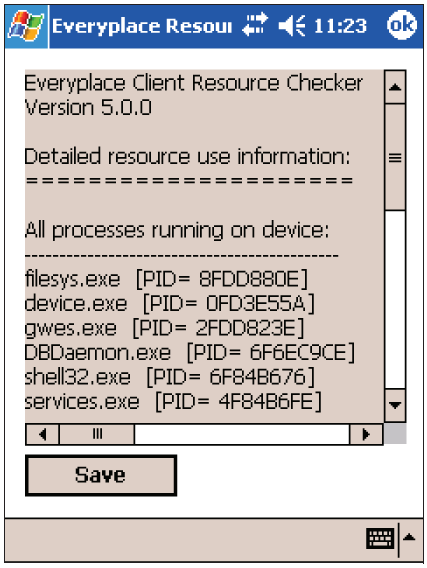

Figure 11-9 Detailed resource information

6. You may now either go back to the Data Storage Profile screen and try entering different values to see the effect on the results or you may click **Exit** to leave the application.

12

Bulk user loading from existing mail environments

This chapter provides information about bulk loading users from existing mail environments. Sample scenarios are included to illustrate this new function.

© Copyright IBM Corp. 2005. All rights reserved.

12.1 Overview

This new feature is comprised of a single portlet that is accessible through the administrative interface for the portal. This portlet lets the Everyplace Synchronization Server administrators import multiple new users from Lotus Domino into WebSphere Portal, create and assign them a default device profile, and then notify each user of their new user name and password by e-mail. Administrators can also create and assign a default device profile to groups of existing users.

> **Note:** The procedure described in this chapter is for a WebSphere Everyplace Access component installation environment only. In a basic installation, the **Choose from a list of portal user portlet** is not available, and therefore the bulk loading could not work properly.

12.1.1 Configure the Bulk Load Portlet

First of all, it is necessary to add the user to the essusers or essadmin group. In this case, we are creating a group named domusers. We will add the user to this group

1. Log in to the portal with the portal administration ID. Click the **Administration** link at the top of the portal.
2. Click the **Access** link on the left.
3. Under the Access label, click **Users and Groups**.
4. Click **all portal user groups** (see Figure 12-1).

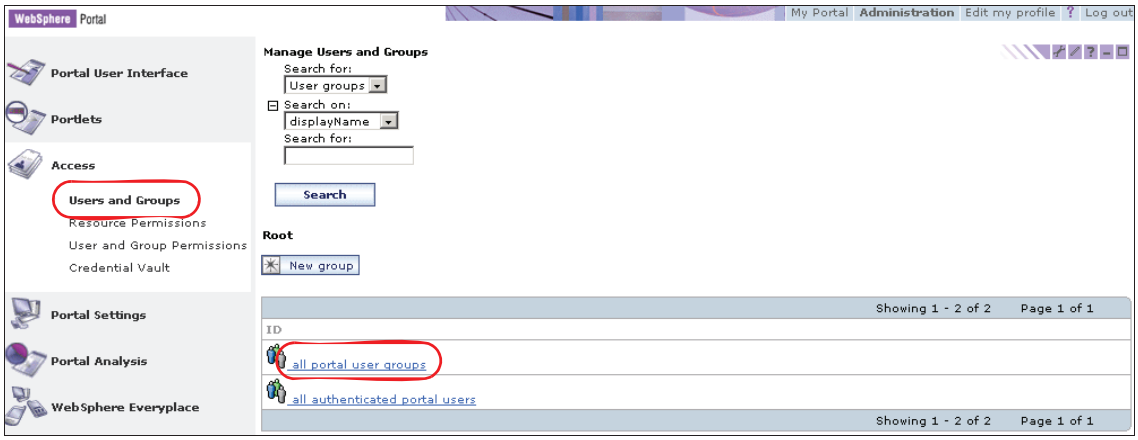

Figure 12-1 Users and Group

5. Click **essusers** (see Figure 12-2).

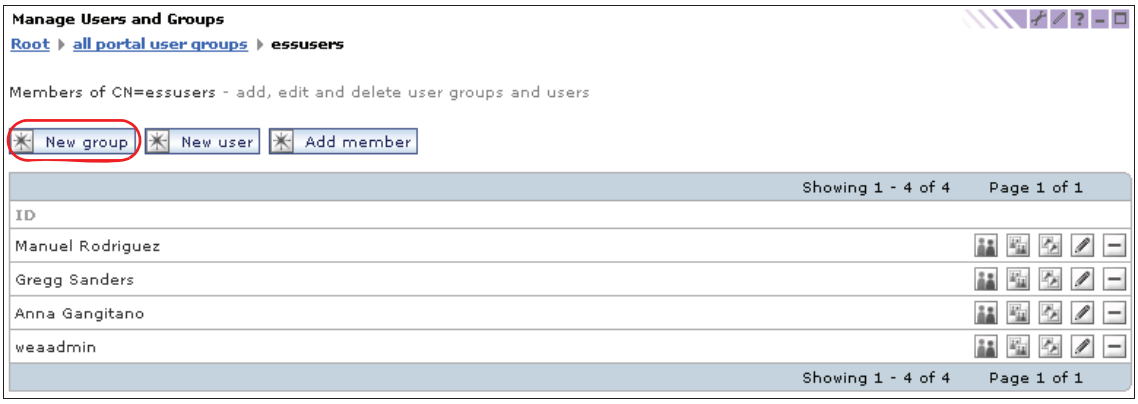

Figure 12-2 Manage Users and Groups

6. Click **New group** to create a group called **domusers** (see Figure 12-3).

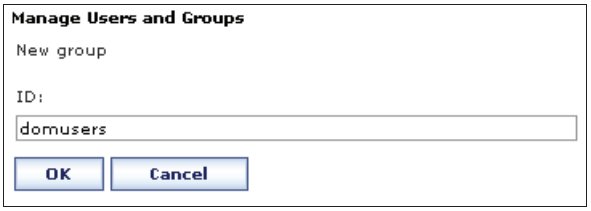

Figure 12-3 Manage Users and Groups - creating a new group

7. Make sure group creation was successful (see Figure 12-4 on page 398).

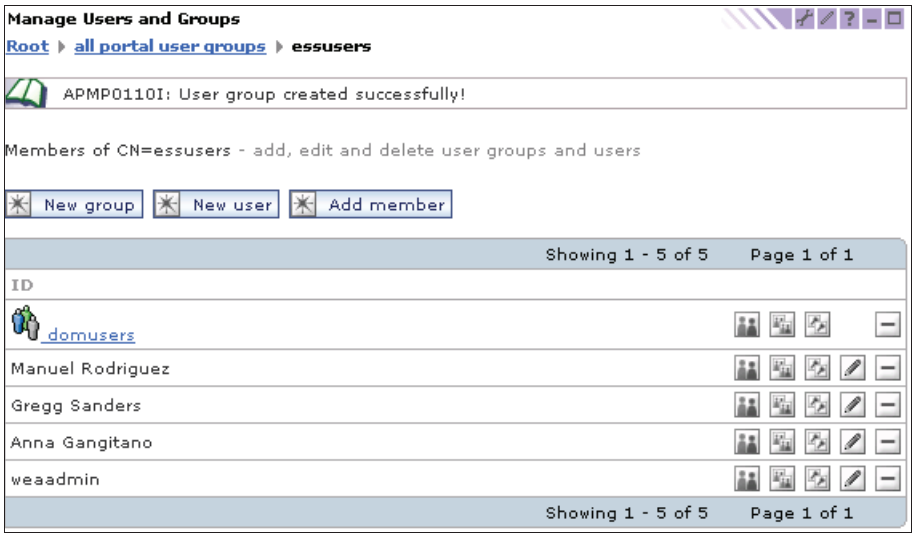

Figure 12-4 Manage Users and Groups

8. After the group is created, click **WebSphere Everyplace** on the left hand side.
9. Under the Everyplace Synchronization Server Administration label, click the **Bulk Load** portlet. You will see a message within the Bulk Load portlet indicating that it needs to be configured. Click the configure icon in the portlet title bar. You will see the following configuration interface:

Figure 12-5 Bulk Load Users portlet

10. Fill in the appropriate values (see Figure 12-6 on page 399).

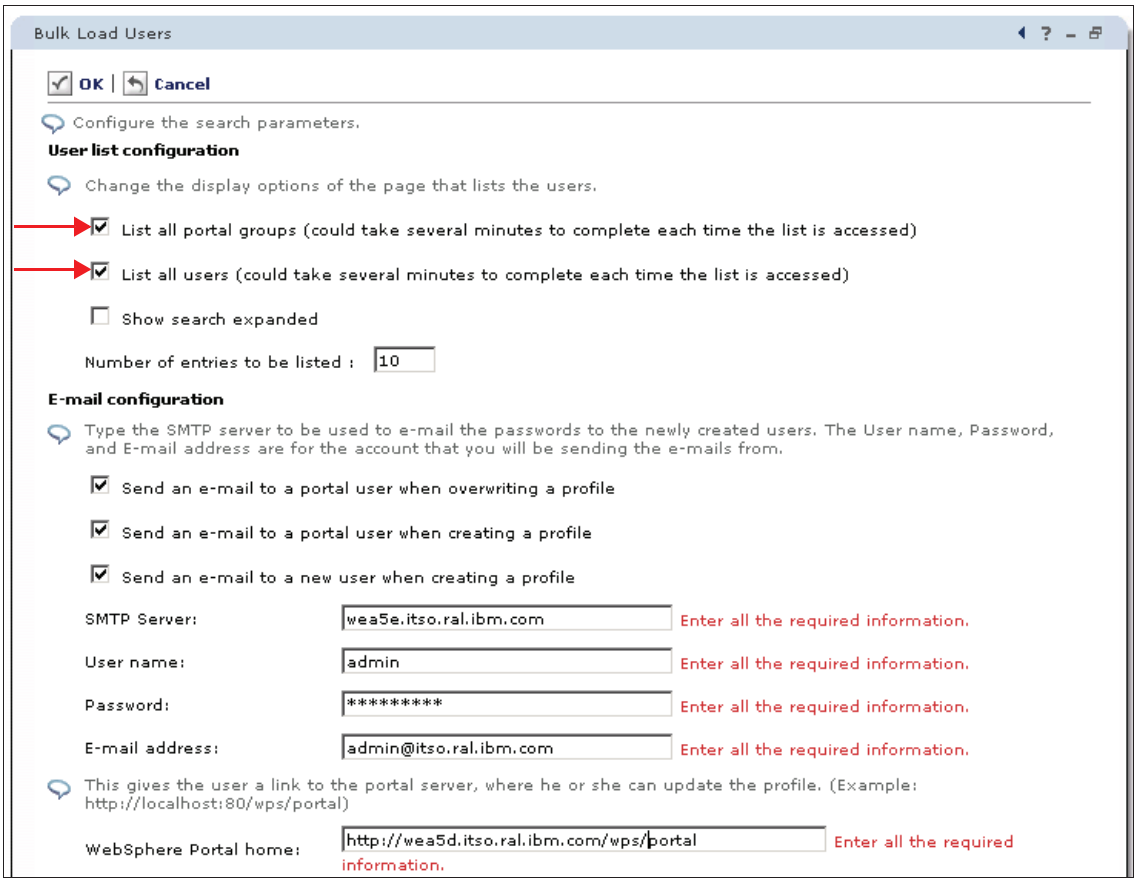

Figure 12-6 Bulk Load Users portlet

11. Make sure to select the **List all portal groups** and **List all users** at the beginning of the page. Also, make sure to enter a valid SMTP e-mail server and the admin account information in order to notify users when changes to their profile take place.

    Note that the SMTP server task is needed. Check on the Domino Server to see if this task is started. If not, check on the basic tab of the server (wea5e.itso.ral.ibm.com, in this example) to see if the SMTP listener task is enabled. Then, under Server Tasks, click **Start** and select SMTP server.

12. Click **OK** to save your Bulk Load configuration.

13. The Bulk Load Users portlet will then display two options (see Figure 12-7):
   - **Create users from file** is used to create new WEA users and associate a sync profile with them.
   - **Choose from a list of portal users** is used to reconfigure the sync profile settings for individual or groups of users.

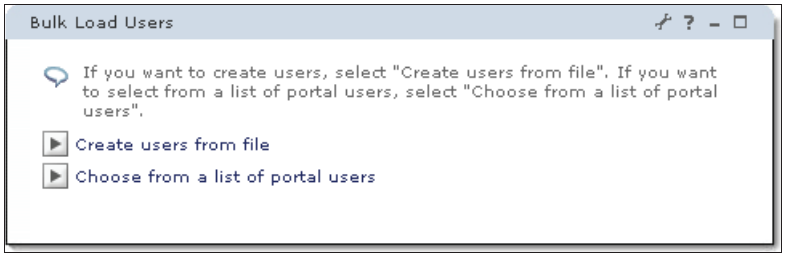

Figure 12-7 Bulk Load Users

14. Leave the browser open while you get a chance to change the e-mail message that gets sent to every user after their profile gets created by the bulk loading process.

12.1.2 Customize e-mail notifications

In this section, we describe the locations and contents of the e-mail notifications that can be customized and sent to WEA portal users.

The txt files that are used by the Bulk Load portlet to compose the e-mail that is sent to the new users are contained within the <portalhome>\installedApps\ESSAdmin_PA_1_0_9D.ear\ESSAdmin.war\WEB-INF\ESSAdmin\email\en directory, where portalhome is the directory to which the Portal component was installed to (the default is c:\program files\WebSphere\PortalServer; see Figure 12-8 on page 401). Alternate languages can be found in the appropriate language directories under <portalhome>\installedApps\ESSAdmin_PA_1_0_9D.ear\ESSAdmin.war\WEB-INF\ESSAdmin\email.

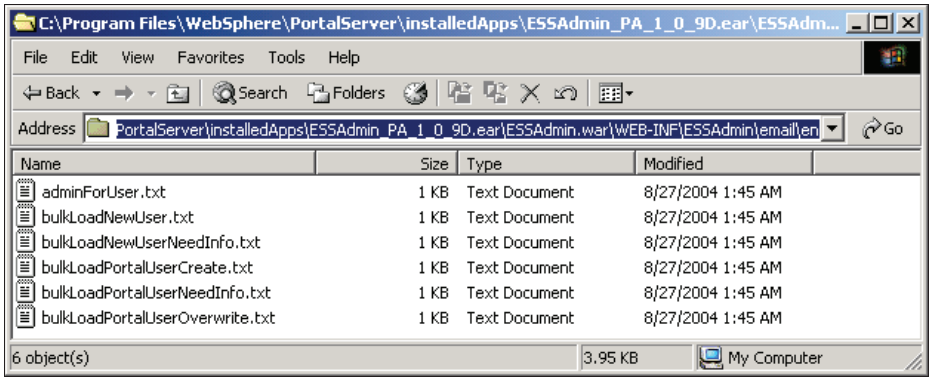

Figure 12-8 Txt files directory

15. The text files that are available include:
    - adminForUser.txt: Informs the existing users that their user-defined device profile has been modified by the administrator (Synchronization Administrator for Users portlet).
    - bulkLoadNewUser.txt: Informs new users that the administrator has created their device profile (Bulk Load portlet).
    - bulkLoadNewUserNeedInfo.txt: Informs new users that the administrator has created their device profile and they need to finish configuring the profile before they synchronize their device (Bulk Load portlet).
    - bulkLoadPortalUserCreate.txt: Informs existing users that the administrator has created their device profile (Bulk Load portlet).
    - bulkLoadPortalUserNeedInfo.txt: Informs existing users that the administrator has created their device profile and they need to finish configuring the profile before they synchronize their device (Bulk Load portlet).
    - bulkLoadPortalUserOverwrite.txt: Informs existing users that the administrator has overwritten their existing device profile with a new device profile (Bulk Load portlet).
16. Open the file bulkLoadPortalUserNeedInfo.txt that has not yet been modified.
17. Change the subject section by adding the word "Important!", as shown in Figure 12-9 on page 402:

```
<subject>Important! Device profile created, need you to update backend
information</subject>
```

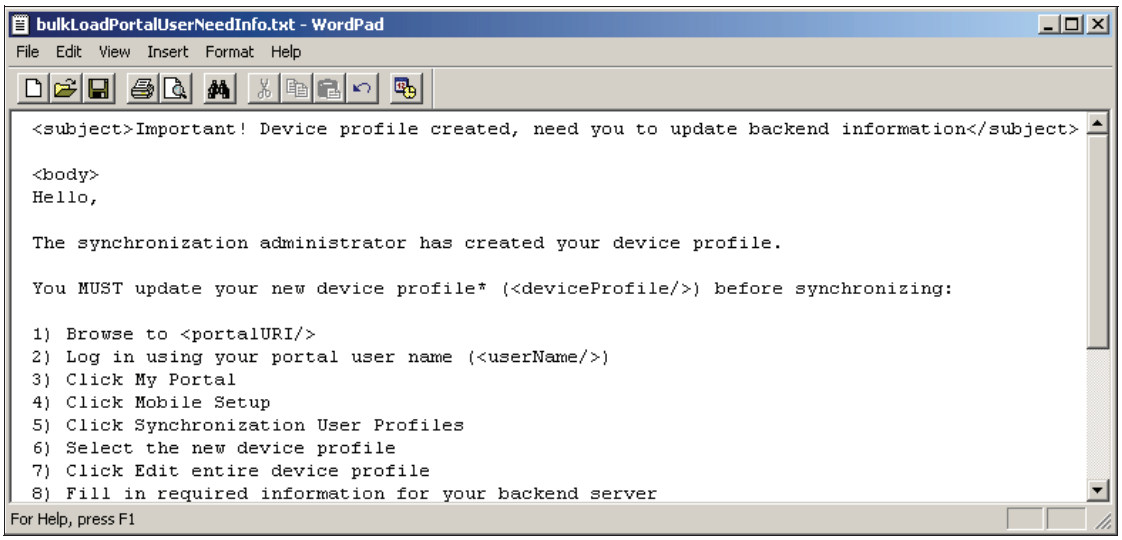

Figure 12-9 bulkloadnewuserneedinfo.txt file

18. Save the file and continue with the bulk loading process. Each user will receive an e-mail when their profile gets created, which will have the updated subject. You can read the e-mail of one of the users at the end of the lab to verify this.

12.1.3 Using the Bulk Load portlet

This final step will process each user, creating a profile that will allow them to synchronize.

1. From the Administration interface in the portal, select **Choose from a list of portal users** (see Figure 12-10).

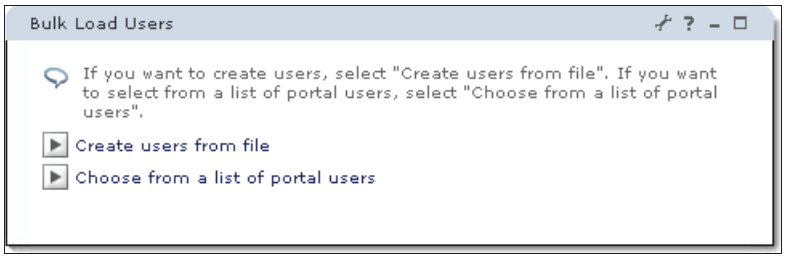

Figure 12-10 Bulk Load Users

2. Select the domusers group and click **Next** (see Figure 12-11 and Figure 12-12).

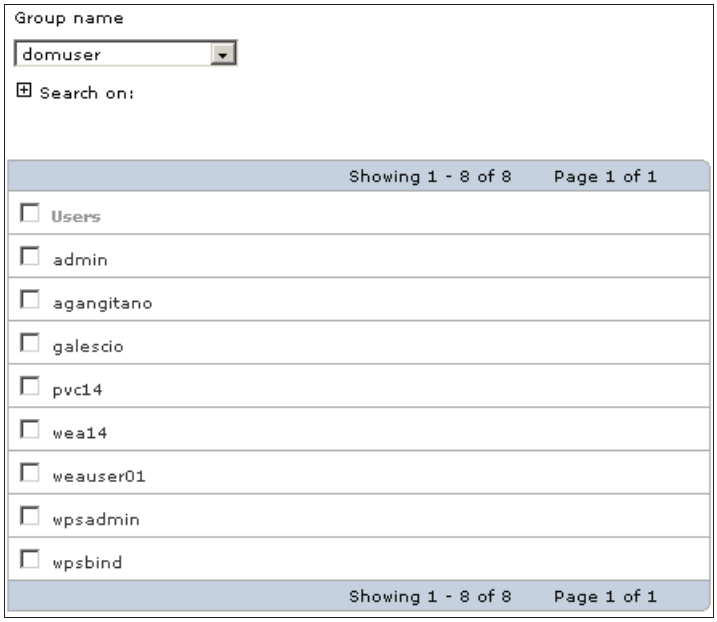

Figure 12-11 Bulk Load Users

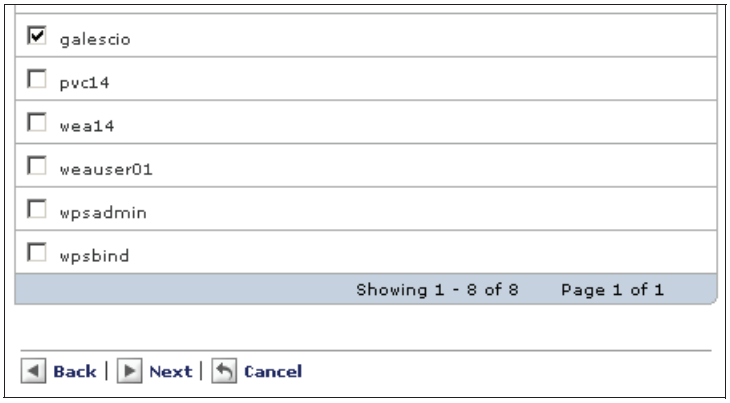

Figure 12-12 Bulk Load Users

3. You will be prompted to select a server to which the user will synchronize data. Select the server and click **Next** (see Figure 12-13 on page 404).

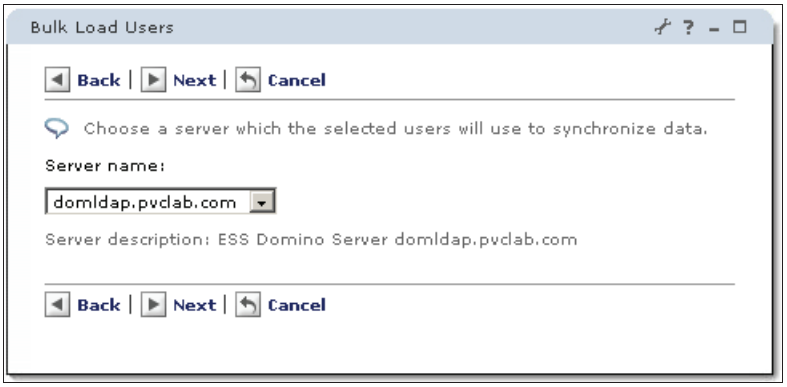

Figure 12-13 Bulk Load Users - choosing server name

4. You will be prompted to select the Sync Profile that you want to associate these new users with. If you do not yet have one, you can create one from here. Click **Create profile** and type in the profile name that you want to be associated with these new users (see Figure 12-14).

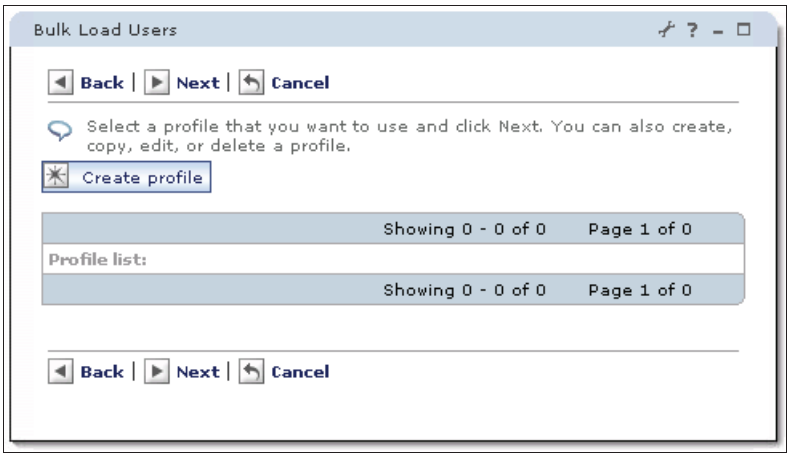

Figure 12-14 Bulk Load Users - create new synchronization profile

5. Type in a name for your new profile and click **Next** (see Figure 12-15 on page 405).

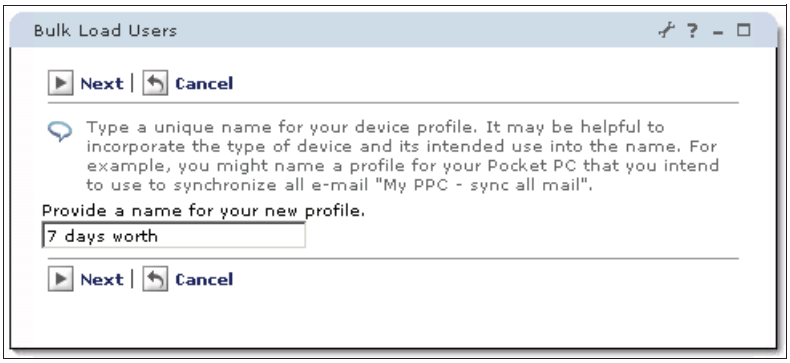

Figure 12-15 Bulk Load Users - providing a name for the new profile

6. Select an existing profile to associate with or select **Create custom settings for 'yourprofilename'**, where yourprofilename is the name you typed in during the previous step. Click **Next** (see Figure 12-16).

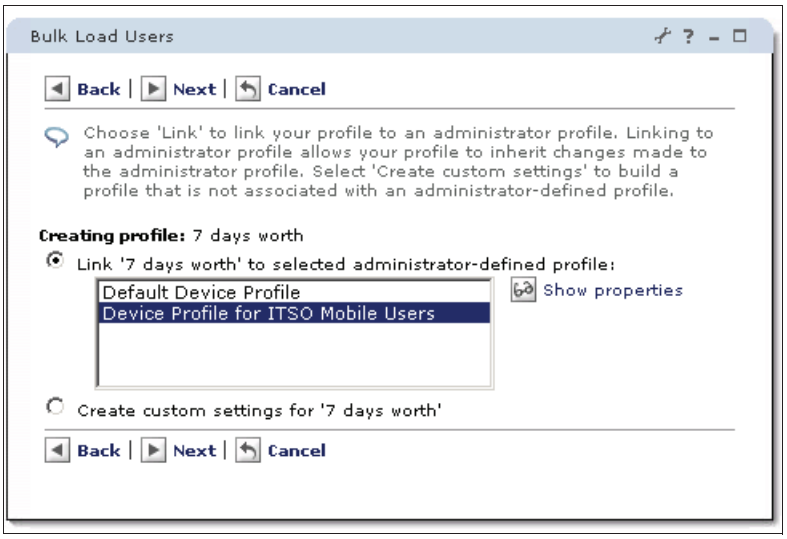

Figure 12-16 Bulk Load Users - creating profiles

7. You will see a confirmation of the synchronization settings that you selected for your profile. Click **Next** (see Figure 12-17 on page 406).

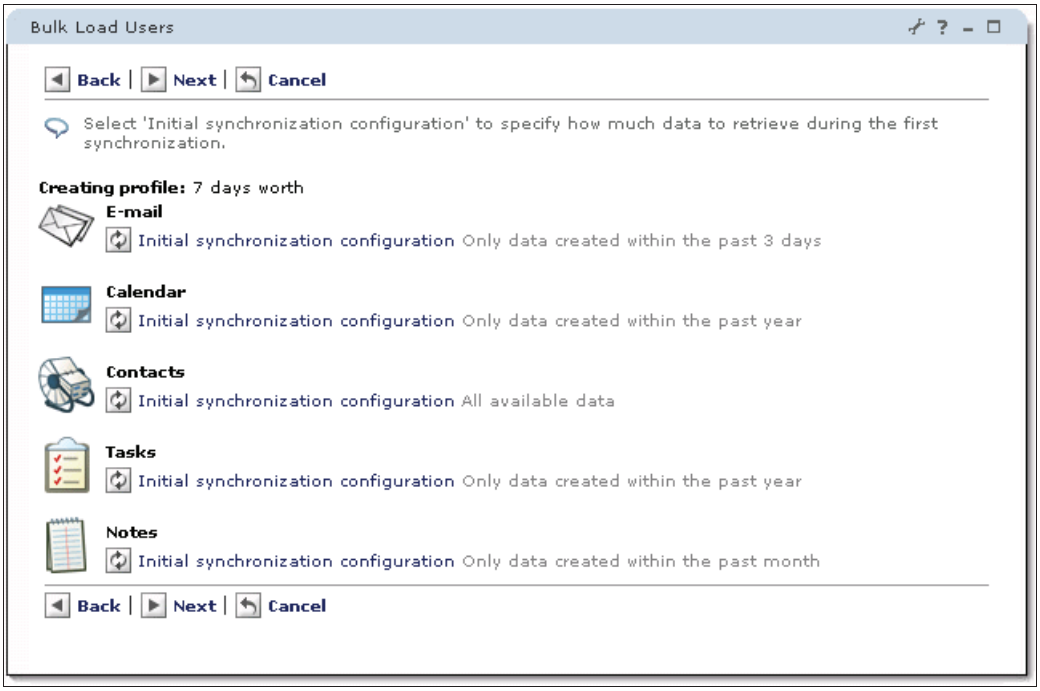

Figure 12-17 Bulk Load Users

8. You will be asked to select the privacy settings for this set of users. Make any changes necessary, then select **Next** (see Figure 12-18 on page 407).

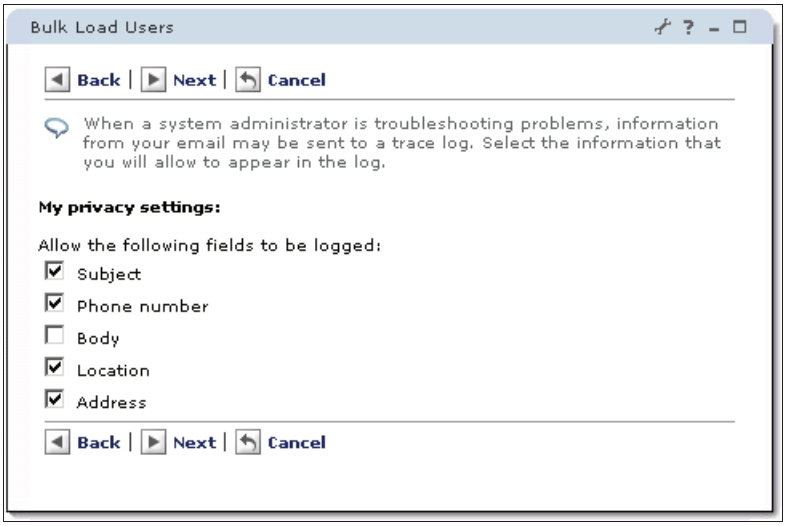

Figure 12-18 Bulk Load Users - privacy settings

9. Select the time zone settings for these users. Initially, you need to select a time zone from the drop-down selection box, and then click **Get locales for this time zone** to populate the second local selection list. Once you have selected the correct time zone and locale for this group of users, click **Next** (see Figure 12-19).

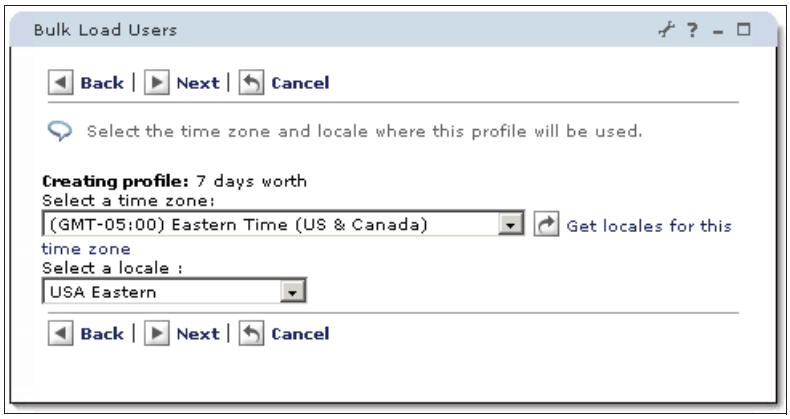

Figure 12-19 Bulk Load Users - selecting a time zone

10. You will, once again, see the profile settings that you selected. Assuming it is correct, click **OK** (see Figure 12-20 on page 408).

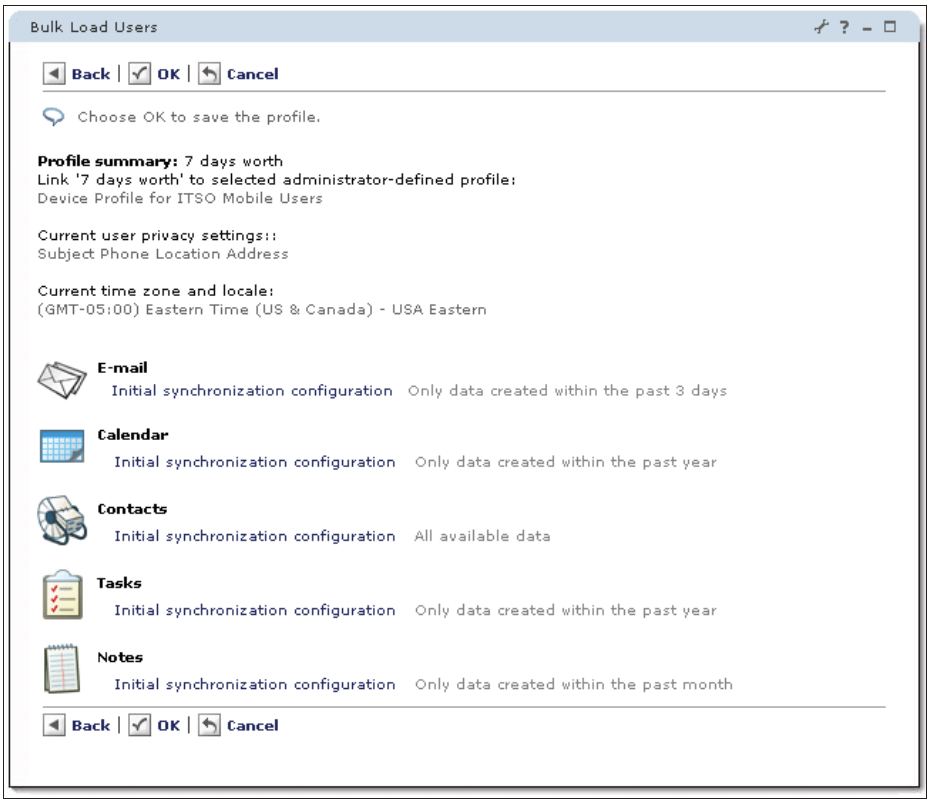

Figure 12-20 Bulk Load Users - profile settings summary

11. You will see your new profile available. Click **Next** (see Figure 12-21 on page 409).

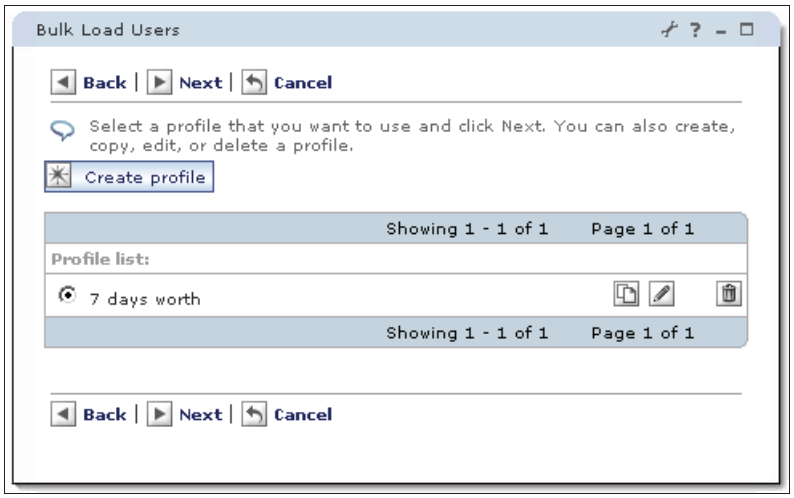

Figure 12-21 Bulk Load Users - profile list

12. With your profile selected, click **Next** on the Select a profile screen. You will see a summary of the users and the profile you are associating with those users next (see Figure 12-22).

Figure 12-22 Bulk Load Users - summary

13. Both the Users and the Profile Summary sections can be expanded to show all of the values within them. To illustrate this, click the **+** symbol next to Users; you will see a result similar to Figure 12-23 on page 410. Clicking the **-** symbol will contract the list.

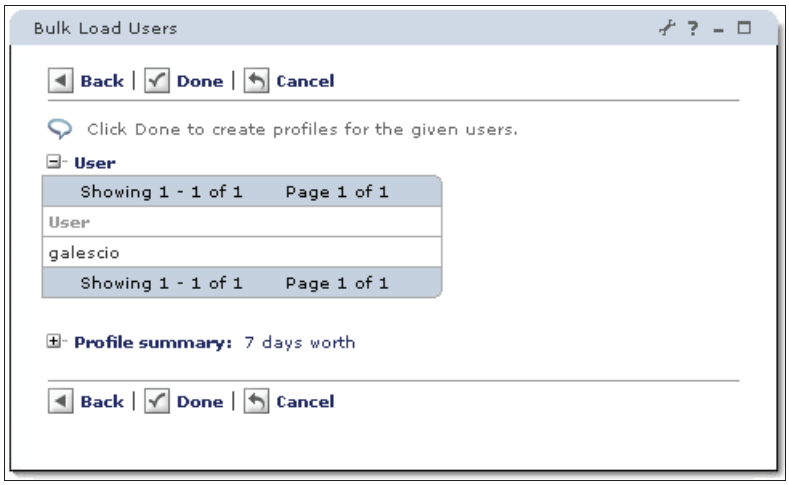

Figure 12-23 Bulk Load Users - summary

14. You can also expand the Profile section and then contract it.
15. If you are satisfied with your users and profile selections, click **Done**. The window shown in Figure 12-24 will appear.

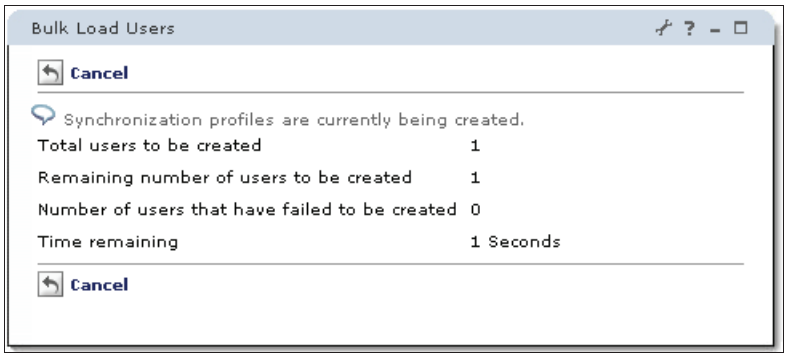

Figure 12-24 Bulk Load Users - profiles creation

16. Wait for the completion of the portlet. You will automatically return to the main Bulk Load Users page.
17. To verify, open the user's mail files; you should see the e-mail that was automatically generated for him (see Figure 12-25 on page 411).

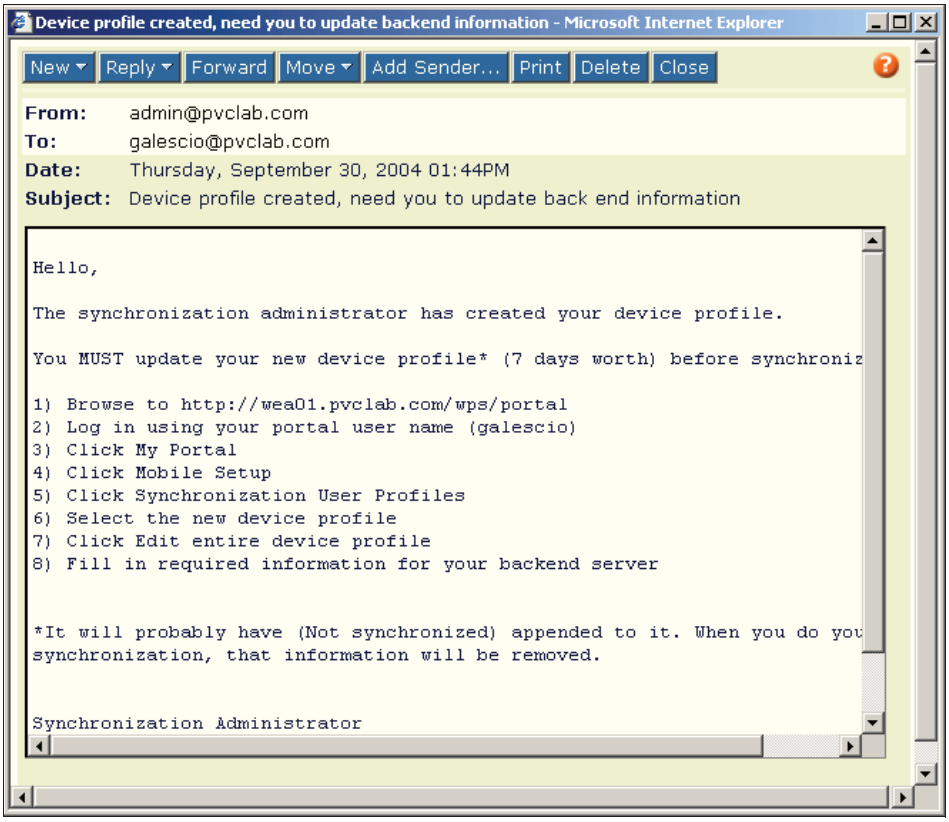

Figure 12-25 E-mail notification of the new device profile created

18. You will also be able to log in to the Portal and see your new profile by selecting **Mobile Setup** → **Synchronization User Profiles** (see Figure 12-26 on page 412).

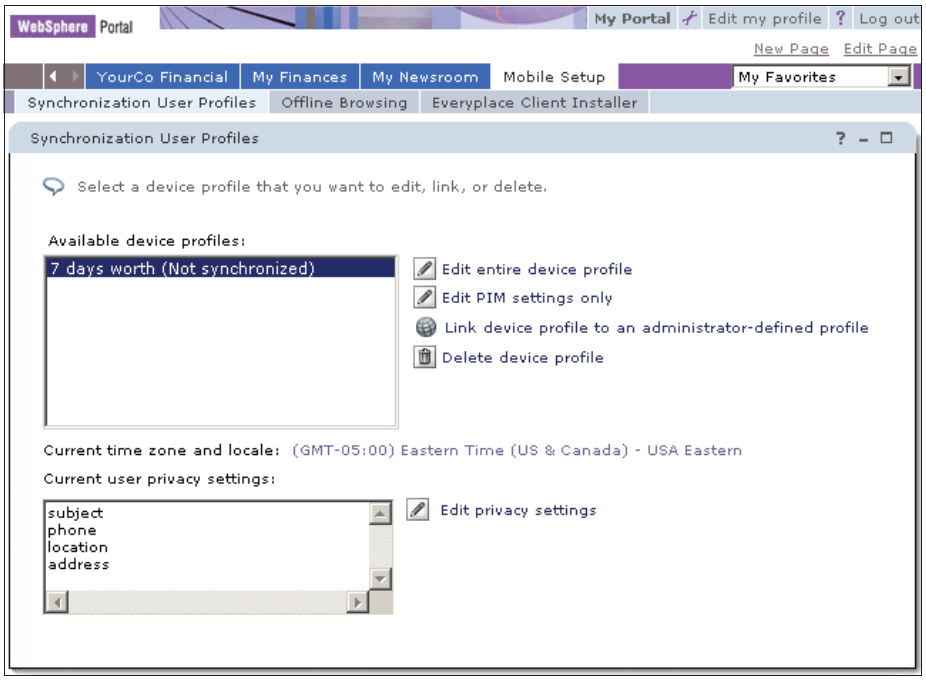

Figure 12-26 User portal - Synchronization User Profiles

19. Note that the synchronization profile has **(Not synchronized)** appended to it. After the first synchronization, this information will be removed. Moreover, before using that profile, you must update the device profile with the back-end information. Select **Edit entire device profile** (see Figure 12-27 on page 413).

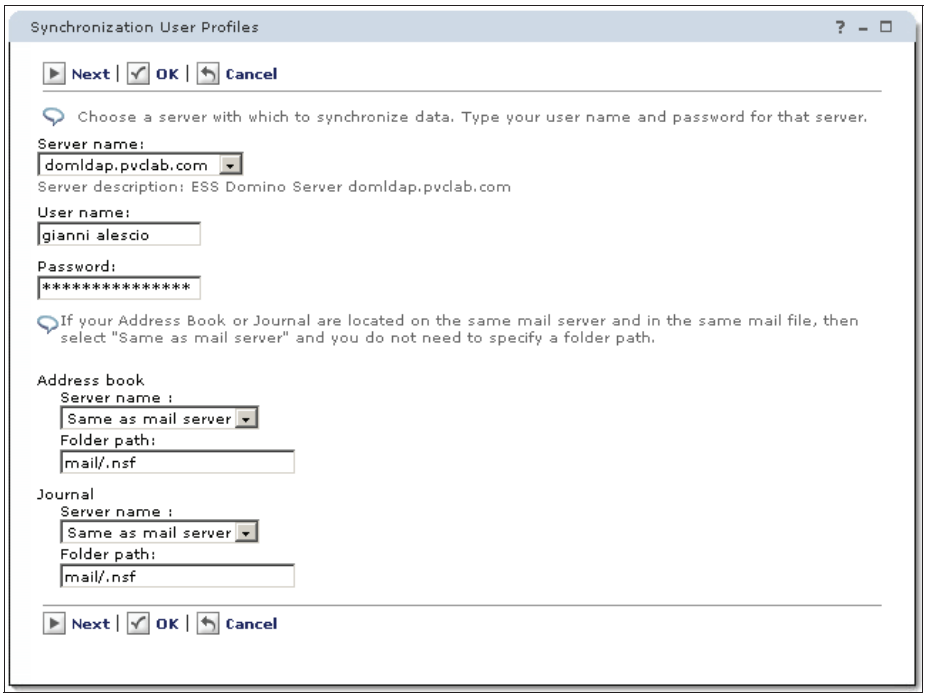

Figure 12-27 Updating a device profile

20. Fill in the User Name and Password fields with the missing information. For the Address book and Journal section, you can choose **Same as mail server**. Select **OK**.

    Note that Figure 12-27 could appear differently for a different environment.

Note that after performing those steps, the user has not yet synchronized the data with a mobile device. For example, the ESSadmin is not automatically added to the ACL of the user's mail box. For more details, see *IBM WebSphere Everyplace Access V5 Handbook for Developers and Administrators Volume III: E-Mail and Database Synchronization*, SG24-6676.

12.1.4 Other functionality

The Bulk Load portlet also allows you to create new users from a file. To perform this scenario, you need:

1. To import data from the Domino server into a file
2. To start using the **Create user from file** portlet

Exporting users from Domino server

Now you will export a user list from Domino in the correct format for the Bulk Load portlet to read.

1. Open the people view in the Domino Administrator (see Figure 12-28):

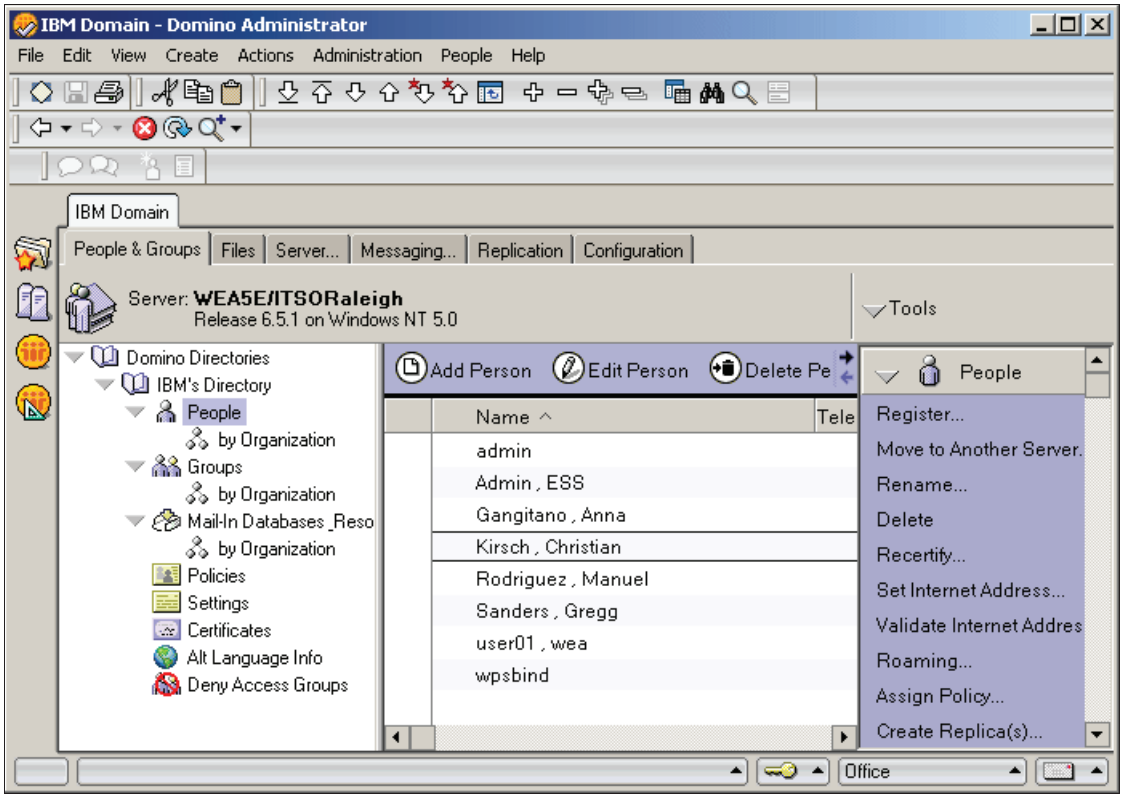

Figure 12-28 IBM Domain - People directory

2. Select the users that you want to export (no need to select any if you plan to export all users) and then select **File** → **Export** from the client menus.
3. You will be prompted for a file name and the location to save the export file to. It is important that the file type is Structured Text (see Figure 12-29 on page 415).

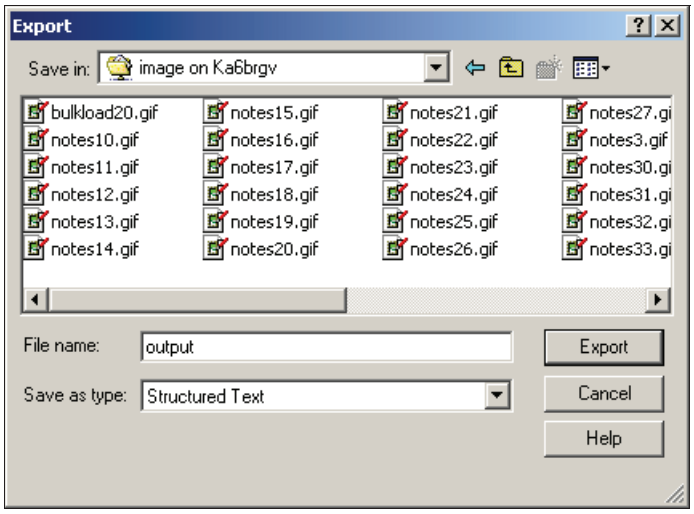

Figure 12-29 Export prompt

4. Next, you will be prompted to specify the characteristics of the export file. Choose **Selected Document** if you only want to export a subset of the directory or **All Documents** if you want to export all of your users. Leave the other settings at their default values (see Figure 12-30).

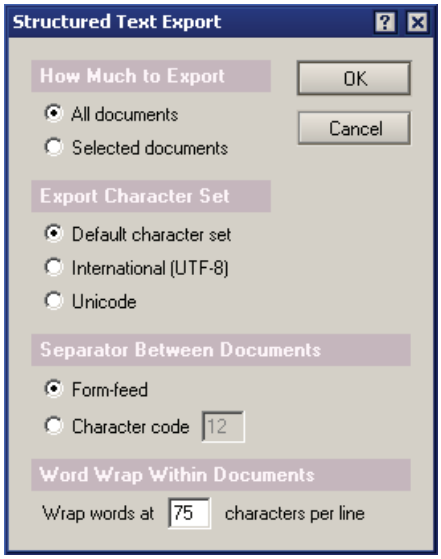

Figure 12-30 Structured Text Export

5. The output file will look similar to Figure 12-31 when viewed from WordPad or Notepad.

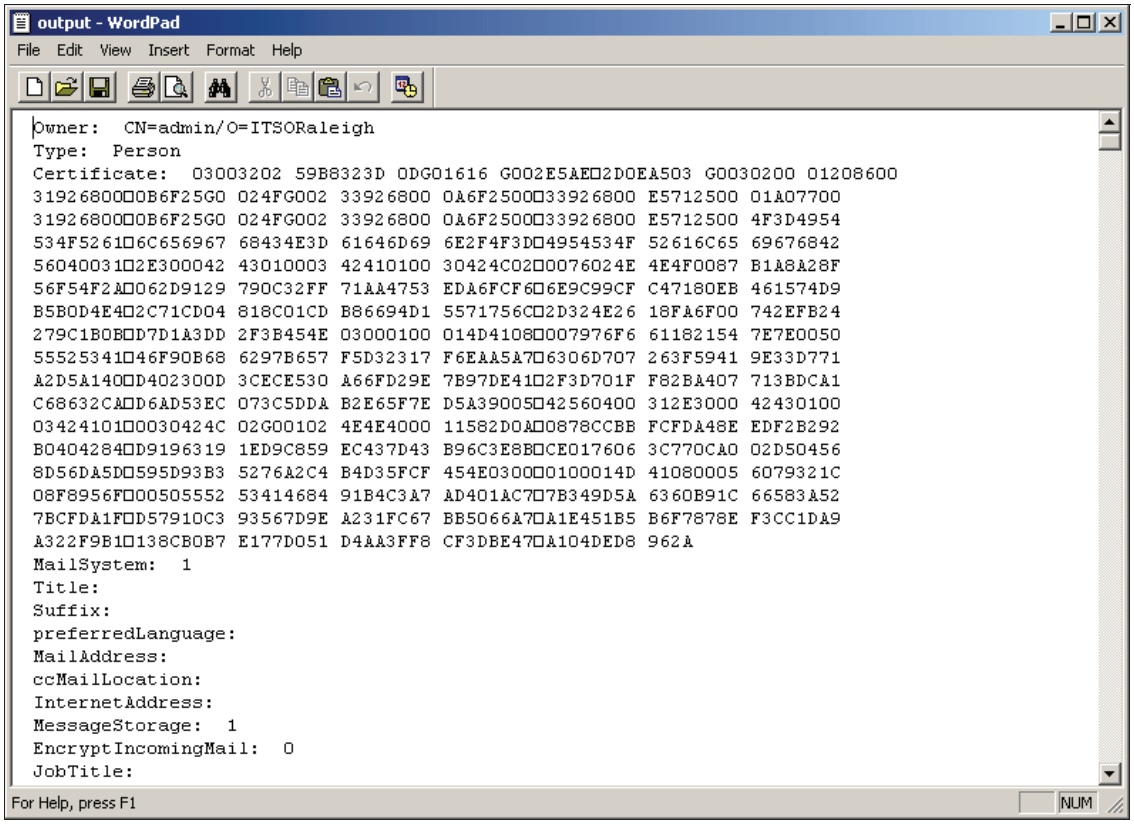

Figure 12-31 Sample output file

Note that the structured text output format includes every field on the person document, which explains why the output is so large for each user.

6. Transfer your exported file to the machine that you can use to administer the WEA server.

Exporting users from Exchange 2000 server

In this section, we are going to export a user list from the Exchange Server in the correct format for the Bulk Load portlet to read.

1. On the Microsoft Exchange 2000 server, open a DOS window and run the following command:

```
csvde -f filename.csv -l "objectClass, mailNickName, mail, givenName, sn"
```

where filename.csv is the name of the file you want to export the list to. The output file will be exported to the directory that the command is run from.

2. You will see the following on the command line (see Figure 12-32):

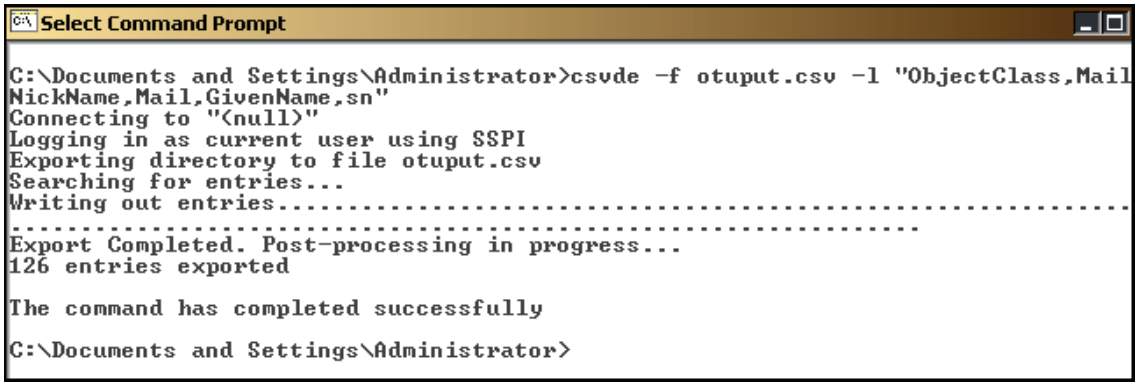

Figure 12-32 Exporting the Exchange 2000 users to a file

3. Running this command creates a log file in the same directory the command was run from. It logs the behavior of the command.

Using the Create users from file option

Follow these steps to create users from a file:

1. Select the **Bulk Load** link (see Figure 12-33).

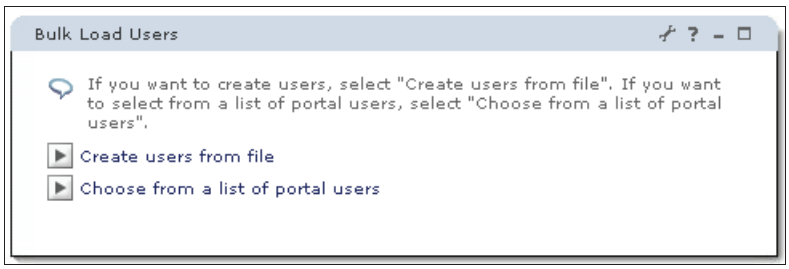

Figure 12-33 Bulk Load main page

2. From the main Bulk Load Users page, click **Create users from file**.
3. Browse to the users output file previously exported from the domino server. Once the Filename field contains your export file, click **Next** (see Figure 12-34 on page 418).

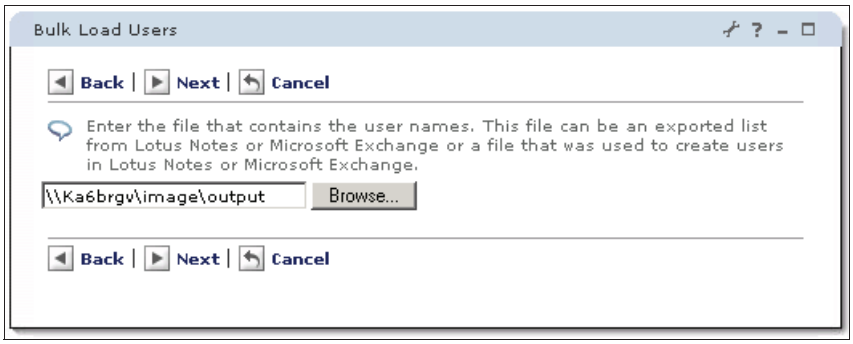

Figure 12-34 Bulk Load Users

4. If the portlet was able to successfully parse the import file, you will be presented with an interface to allow you to select which users should be imported (see Figure 12-35). Note that if any required fields are missing, the portlet will display warnings for each affected user and you will have the opportunity to edit the user profile and provide the missing information.

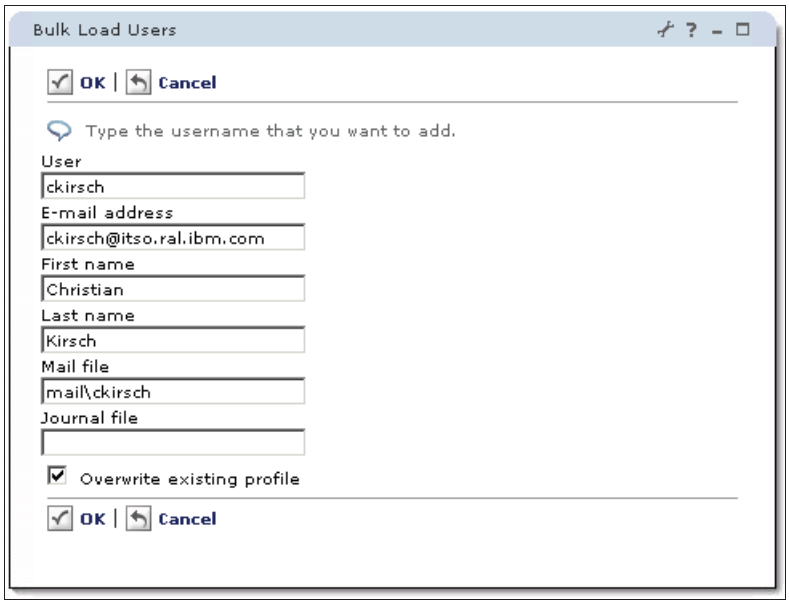

Figure 12-35 Editing user information

5. You should see an OK near the user name (see Figure 12-36 on page 419).

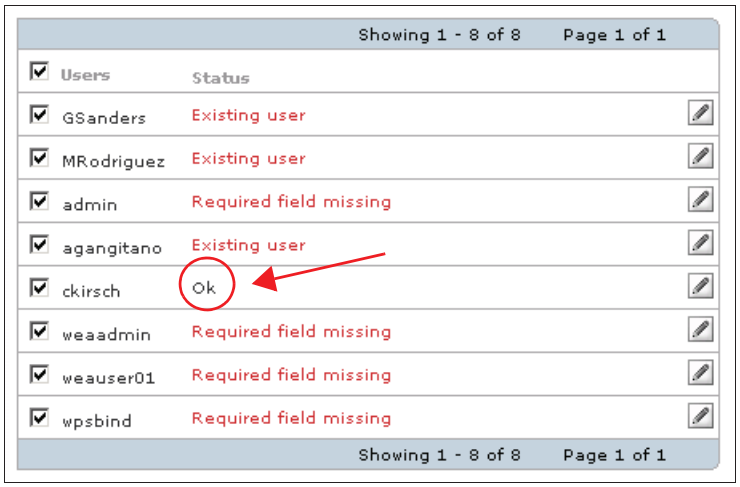

Figure 12-36 Bulk Load Users

6. Follow the same steps as for the **Choose from a list of portal users** portlet to create a profile. At the end, you should see a list of added users.

A

A sample Sametime installation

This appendix provides a sample Sametime server installation and configuration.

© Copyright IBM Corp. 2005. All rights reserved.

Installation and configuration

This appendix covers a sample server installation and configuration of Lotus Sametime Server V6.5.1.

Installation

The Sametime server must be installed on to the Lotus Domino Server. The following steps will take you through the installation process.

1. First, you will need to stop the Domino Server.
   a. From the Domino server, select **Start** → **Programs** → **Administrative Tools** → **Services**.
   b. Check if the Domino Server service is running. If it is, stop it now and also any services related to it (see Figure A-1).

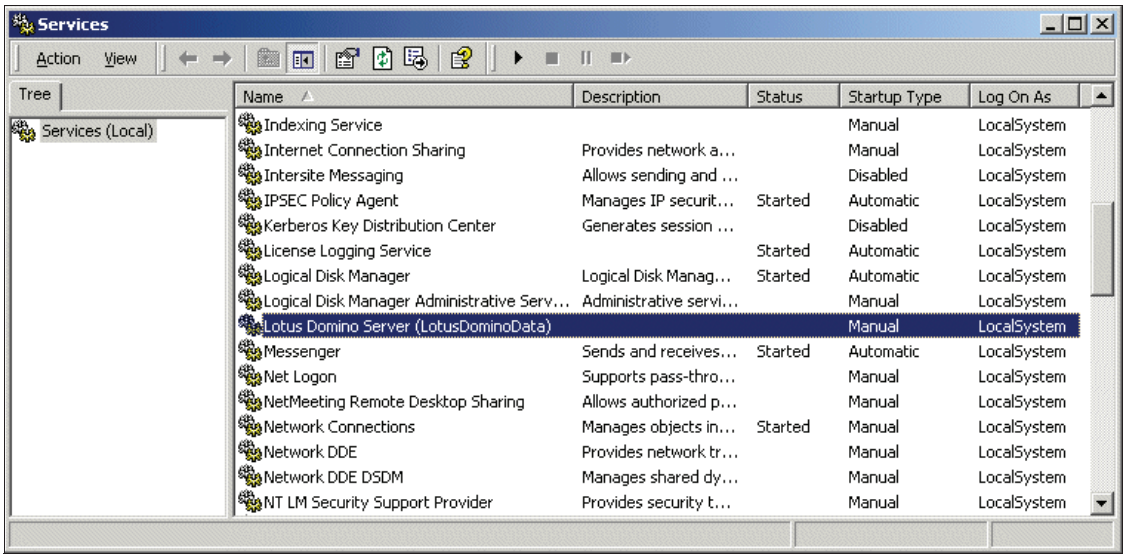

Figure A-1 Lotus Domino Server service

2. Next, you will need to extract the Sametime V6.5.1 installation files. These are provided in the c57lana.exe file.
3. Double-click c57lana.exe to start the extraction process and choose the directory where the extracted files will be placed. In this example, we will be using c:\temp.
4. Once the extraction process is finished, browse to the extract directory (c:\temp, in this example) and execute demo32.exe.

5. Select **English** for the installation language.
6. Next, click **Install the Sametime Server**.
7. Click to **Accept Licence**.
8. Click **Next**. Note that you should have stopped any services related to Domino / LDAP
9. The installation program will search for the Domino server. Click **Yes** to install Sametime as part of Domino (see Figure A-2).

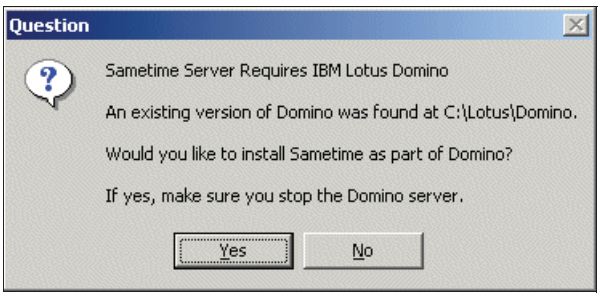

Figure A-2 Sametime server requires Lotus Domino

10. Click **Next** to begin copying the program files (see Figure A-3).

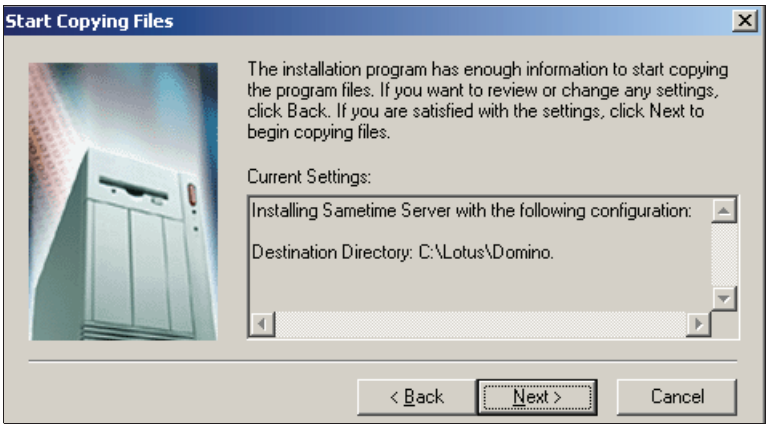

Figure A-3 Copying files

11. Click **Finish** to complete installation (see Figure A-4 on page 424).

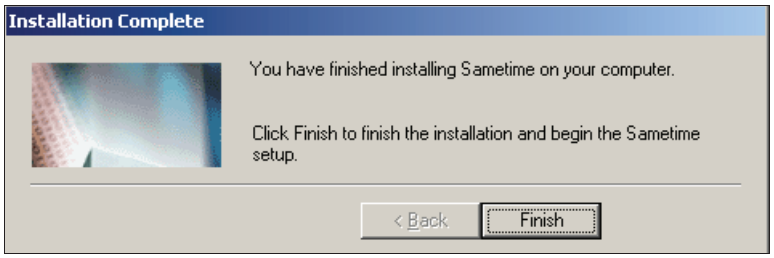

Figure A-4 Finish the installation

Configuration

The following steps will take you through the configuration required for the Sametime server.

1. Enter the name of the Domino Server ID file. In this scenario, it is C:\Lotus\domino\data\server.id (see Figure A-5).

Figure A-5 Domino Server ID file name

2. On the Select the Directory Type page, choose **Domino Directory** from the drop-down list (see Figure A-6).

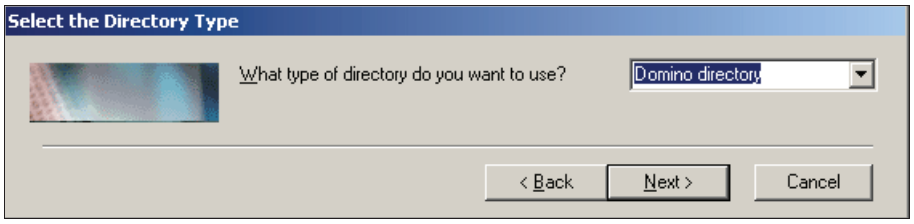

Figure A-6 Directory type

3. Leave the **Allow HTTP tunneling on a Sametime server with a single IP Address** box unchecked (as per the default) (see Figure A-7 on page 425).

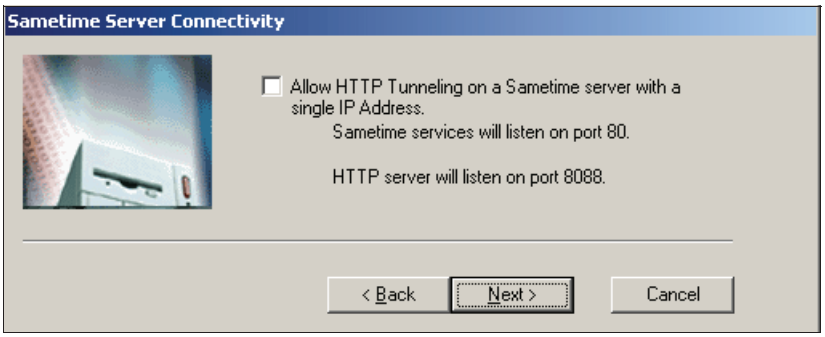

Figure A-7 Sametime Server Connectivity

4. Click **OK** to finish (see Figure A-8).

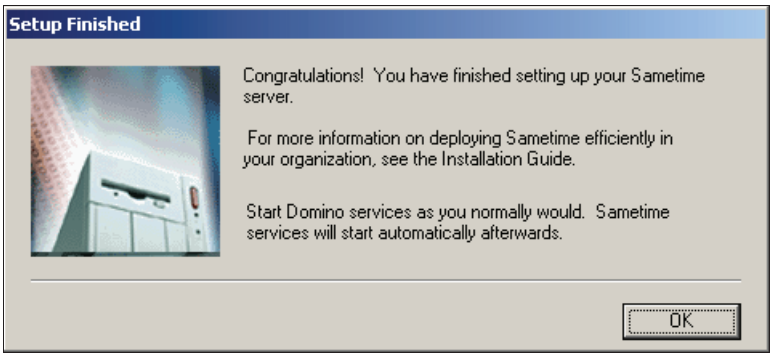

Figure A-8 Finish Sametime setup

5. Start the Domino server. The Sametime server starts automatically when the Domino server starts

At this point, the Sametime server should be up and running. For more detailed information about setting up the Sametime sever, check the installation guide provided with the product.

Setting up Sametime Everyplace (STEP)

This section will take you through the steps required to set up Sametime Everyplace.

Microbrowser

Perform the following steps:

1. To install Sametime Everyplace (STEP), you have to extract the file Sametime31-C50W4NA.exe into a temporary directory (C:/Temp/STEP/ for this sample scenario).
2. Stop the Domino server and any related services.
3. Browse to the directory you chose to extract the files to, then to the STMicroBrowser directory (C:/Temp/STEP/STMicroBrowser/) and run setup.exe.
4. Click **Next** to start the configuration (see Figure A-9).

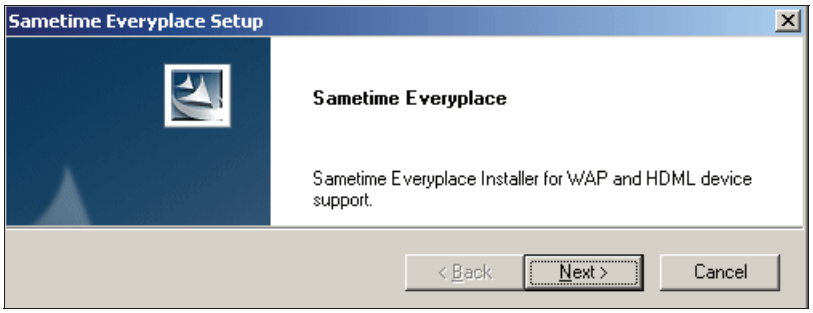

Figure A-9 Start configuration

5. Verify the product requirements and click **Yes** (see Figure A-10).

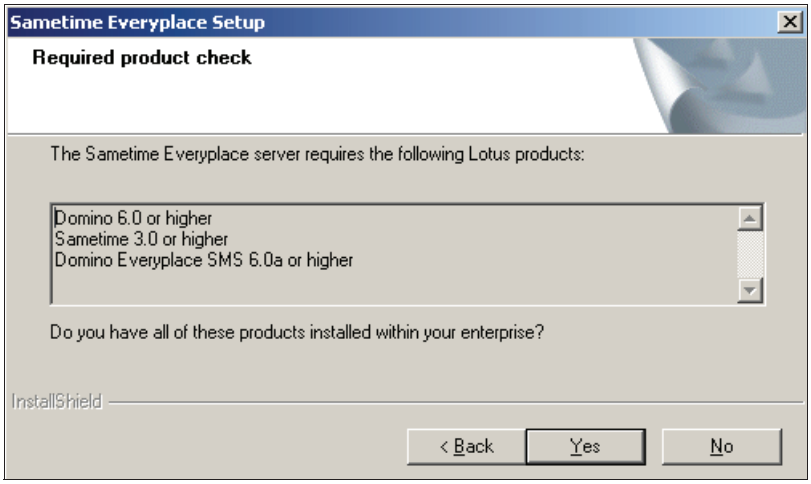

Figure A-10 Required product check

Note: Domino Everyplace SMS is not needed for Sametime Everyplace.

6. Specify the path for the NOTES.INI file (the default path should be correct in most cases) and click **Next** (see Figure A-11).

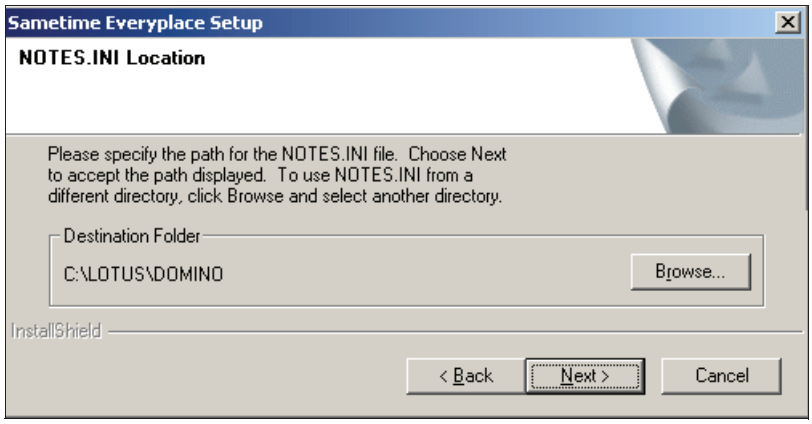

Figure A-11 NOTES.INI location

7. **Accept** the software license agreement.
8. Click **Next** to start the installation.

Mobile extensions

1. After completing the installation of STMicrobrowser, browse to the directory you chose to extract the files to in step 1 of “Microbrowser” on page 426, then to the STMobile directory (C:\Temp\ STEP\STMobile\) and run setup.exe.
2. Click to **Accept** to accept the software license agreement.
3. Click **Next** in the welcome window.
4. Click **Next** to accept the default installation folder (see Figure A-12 on page 428).

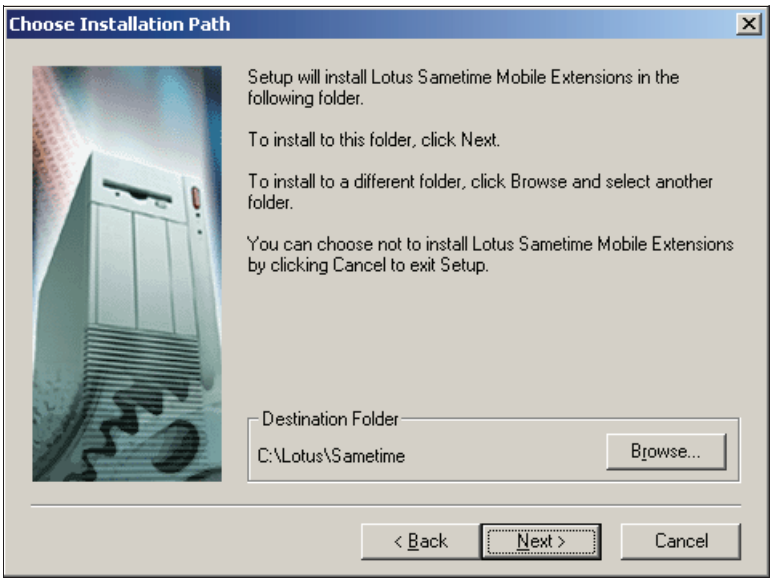

Figure A-12 Installation folder

5. Enter the name of the Sametime Server. In this sample scenario, the fully qualified name is wea5e.itso.ral.ibm.com (see Figure A-13).

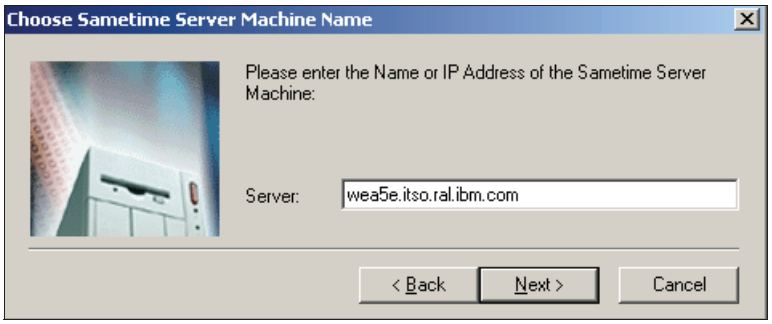

Figure A-13 Sametime Server name or IP address

6. Click **Next** to accept the settings (see Figure A-14 on page 429).

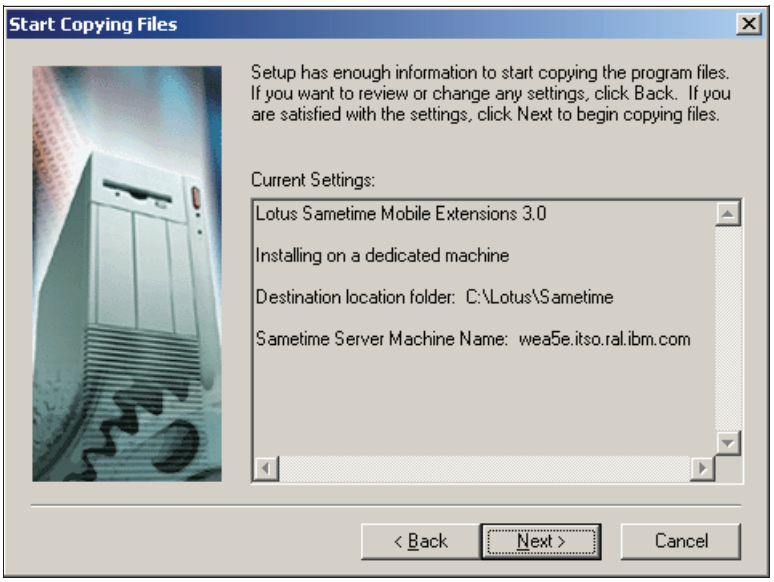

Figure A-14 Current settings

7. Click **Finish** to complete the installation (see Figure A-15).

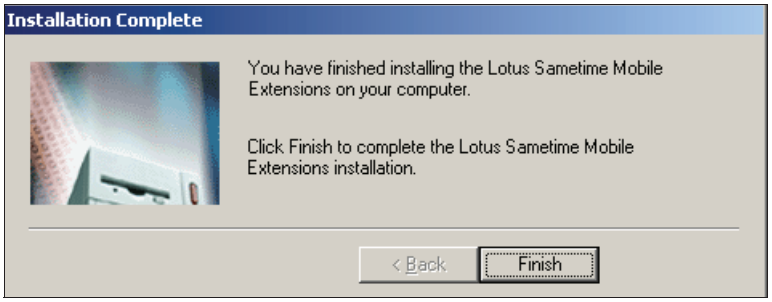

Figure A-15 Installation complete

Checking the installation

These some tips to verify the installation. For example:

1. When you start the Domino Server, check that all the ST* services have been started.
2. If you receive an error while starting, go to **Start** → **Programs** → **Administrative Tools** → **Services** and check if ST Mobile is started; if not, start it manually.

Related publications

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

IBM Redbooks

For information about ordering these publications, see “How to get IBM Redbooks” on page 433. Note that some of the documents referenced here may be available in softcopy only.

- *Getting the Most From Your Domino Directory*, SG24-5986
- *IBM Replication Solutions for Pervasive Computing with DB2 Everyplace and DB2 Satellite Edition*, SG24-6217
- *IBM WebSphere Everyplace Access Version 4.3 Handbook for Developers,* SG24-7015
- *IBM WebSphere Everyplace Access V5 Handbook for Developers and Administrators Volume I: Installation and Administration,* SG24-6462
- *IBM WebSphere Everyplace Access V5 Handbook for Developers and Administrators Volume II: Application Development,* SG24-6463
- *IBM WebSphere Everyplace Access V5 Handbook for Developers and Administrators Volume III: E-Mail and Database Synchronization,* SG24-6676
- *IBM WebSphere Everyplace Access V5 Handbook for Developers and Administrators Volume IV: Advanced Topics,* SG24-6677
- *IBM WebSphere Everyplace Connection Manager Version 5 Handbook,* SG24-7049
- *IBM WebSphere Everyplace Server Service Provider and Enable Offerings: Enterprise Wireless Applications*, SG24-6519
- *IBM WebSphere Portal V5 A Guide for Portlet Application Development*, SG24-6076
- *RDB Synchronization, Transcoding and LDAP Directory Services in IBM WebSphere Everyplace Access Version 4.1.1,* SG24-6856

© Copyright IBM Corp. 2005. All rights reserved.

Other publications

These publications are also relevant as further information sources:

- *DB2 Everyplace Application Development Guide Version 8 Release 1*, SC18-7185
- *IBM DB2 Everyplace Sync Server Administration Guide 7.2*, SC27-0845
- *IBM DB2 Everyplace Sync Server Administration Guide Version 8 Release 1,* SC18-7186

Online resources

These Web sites and URLs are also relevant as further information sources:

- IBM @server Technical Support

  http://techsupport.services.ibm.com/server/fixes
- IBM support and downloads

  http://www.ibm.com/support/us
- Java Community Process, JSR 168:

  http://jcp.org/jsr/detail/168.jsp
- Lightweight Directory Access Protocol standard:

  http://www.ietf.org/rfc/rfc1777.txt
- Lotus Documentation

  http://www.lotus.com/ldd/doc
- Lotus product information:

  http://www.lotus.com/home.nsf/welcome/products
- WebSphere Application Server:

  http://www.ibm.com/software/webservers/appserv
- WebSphere Everyplace Access:

  http://www.ibm.com/software/pervasive/ws_everyplace_access
- WebSphere Portal:

  http://www.ibm.com/software/websphere/portal
- WebSphere Studio:

  http://www.ibm.com/software/websphere/studio/
- WebSphere Transcoding Publisher:

  http://www.ibm.com/software/webservers/transcoding

How to get IBM Redbooks

You can search for, view, or download Redbooks, Redpapers, Hints and Tips, draft publications and Additional materials, as well as order hardcopy Redbooks or CD-ROMs, at this Web site:

ibm.com/redbooks

Help from IBM

IBM Support and downloads

ibm.com/support

IBM Global Services

ibm.com/services

Index

A

Administration 7, 41
- access control 7, 74
- Access menu 47
- Create a new link 55
- Create new label 53
- Create New Pages 50
- Creating groups 78
- Editing pages 59
- Getting started 46
- groups 7
- Manage applications 68
- Manage pages 48, 51, 57
- Manage Portlets 70
- Manage portlets 69
- permissions 81
- Portal analysis 97
- Portal Analysis menu 47
- Portal Settings menu 47
- Portal User Interface menu 47
- Portlet Install 67
- Portlets menu 47
- Resource Permissions 83
- security 7
- Starting DB2 Everyplace server 46
- Starting Device Manager server 46
- Starting Everyplace Access Services 45
- Starting Everyplace Synchronization Server 45
- Starting Intelligent Notification Services 46
- Starting Location Aware Services 46
- Starting services 45
- Starting WebSphere Application Server 45
- Starting WebSphere Portal Server 45
- Supported clients 94
- Supported markup 91
- Themes and skins 64
- User and Group Permissions 88
- users 7
- Web clipping 71
- WebSphere Everyplace menu 47

AIX 20

AIX Component Installation 221
- Additional Installations 283
- DB2 Everyplace configuration 278
- DB2 Everyplace installation 278
- DB2 UDB installation 242
- Device Manager configuration 268
- Device Manager installation 267
- Everyplace Access Services configuration 265
- Everyplace Access Services installation 265
- Everyplace Synchronization Server configuration 270
- Everyplace Synchronization Server installation 270
- Intelligent Notification Services configuration 275
- Intelligent Notification Services installation 274
- LDAP Configuration 228
- Location Aware Services configuration 280
- Location Aware Services installation 280
- Lotus Domino configuration 228
- Lotus Domino installation 226
- Lotus Notes installation 225
- Preparation 237
- Requirements 237
- WAS Fixpack installation 247
- WebSphere Application Server Enterprise installation 246
- WebSphere Application Server installation 245
- WebSphere Portal Fixpack installation 250
- WebSphere Portal Server installation 249

Annotators 14

B

Basic installation
- Domino Server installation 100, 104
- Install Lotus Notes 103
- Installing Domino Server 104
- LDAP configuration 106
- Lotus Domino configuration 106
- Preparation 101
- WEA installation 118

Bulk user loading 395
- Administrators 396
- configuration 396
- create new users 413

© Copyright IBM Corp. 2005. All rights reserved.

default device profile 396
e-mail notifications 400
Everyplace Synchronization Server 396
exporting users from Domino server 414
exporting users from Exchange server 416
Lotus Domino 396
other functionality 413
overview 396
Portlet 396
SMTP server 399
sync profile 404
WebSphere Portal 396
business applications 2
business data 2

C

certificate authority 318
Component Installation 125
Additional Installations 217
DB2 Everyplace configuration 212
DB2 Everyplace installation 211
DB2 UDB Installation 149
Device Manager configuration 200
Device Manager installation 199
Everyplace Access Services configuration 197
Everyplace Access Services installation 195
Everyplace Synchronization Server configuration 204
Everyplace Synchronization Server installation 202
Intelligent Notification Services configuration 208
Intelligent Notification Services installation 207
LDAP Configuration 133
Location Aware Services configuration 215
Location Aware Services installation 213
Lotus Domino Configuration 132
Lotus Notes installation 129
Preparation 141
WAS Fix pack Installation 164
WEA installation 149
WebSphere Application Server Enterprise Installation 161
WebSphere Application Server Installation 158
WebSphere Portal Fixpack Installation 172
WebSphere Portal Server Installation 170
Connection Manager 349
Credential Vault 33, 74

D

Data synchronization 9
DB2 Everyplace 9, 21–22, 25
applications 9
DB2 Everyplace database 9
DB2 Everyplace SDK 9
DB2 Everyplace Sync Server 9
DB2 Universal Database 22
Device Management 20, 339, 343
Device Manager 21, 341
Device Manager console 342
Device Plug-ins 341
Device Services 12, 339
administrators 364
Agent 341
Architecture 340
Client Agent 341
client deployment 12
configuration job 342
database 341
Device configuration 13
Device Management Server 341
Device plug-ins 341
Device Services Library 356
DM Console 342
DM servlet 341
inventory collection job 342
Job progress 362
new device configuration 347
overview 340
Palm device 365
portlets 342
software distribution job 342, 359
software package distribution 345, 355
software registration 357
SSL 365
SSL configuration job 369
Tivoli Device Manager 340
Troubleshooting 373
User Group 343
DHTML 22
DM servlet 341
DoCoMo 17, 288
Domino 100

E

Eclipse 19, 22
e-Linux OS 17, 288

e-mail 2, 5, 7–9, 14
Synchronization 5
Enhanced portlets 27
Bookmarks portlet 38
LDAP Search portlet 39
Lotus Notes Calendar portlet 32
Lotus Notes Contacts portlet 31
Lotus Notes Journal portlet 31
Lotus Notes Mail portlet 30
Lotus Notes ToDo portlet 33
Microsoft Exchange Calendar portlet 35
Microsoft Exchange Contacts portlet 36
Microsoft Exchange Mail portlet 34
Microsoft Exchange Notes portlet 37
Microsoft Exchange Tasks portlet 35
Portlets 28
Productivity portlets 37
World Clock portlet 37
Everyplace Access Services 21
Everyplace Client 8–9, 12, 14–18, 21, 331, 341
Connected browsing 15
DB2 Everyplace database 16
Device Manager 16
eLinux 14
e-mail 16
Launch 310
Offline Form 16
Offline Portal 16
Palm OS 14
PIM 16
Pocket PC 2002 14
Sametime Connect 16
Symbian 14
Windows Mobile 2003 14
Everyplace Synchronization Server 20–21
Everyplace Synchronization Service 8
Attachments 7
Filtering 7
Invitations 7
Lotus Domino 8
Microsoft Exchange 8
Read status 8
Recoverability 8
Everyplace Toolkit 19, 22
Extensible Stylesheet Language 14

F

Fragmentation 14

G

Geocoding 12
geographical coordinates 12
Group Permissions 74
Groups
all portal users group 78
Creating groups 78
dmadmins 79
essadmins 79
essusers 79
essusers_nonlock 79
Include groups 80
Include users 80
wpsadmins 79

H

HTML 14, 22, 28
HTTPServlet 6

I

IBM Directory Services 22
IBM Everyplace Client 8
IBM HTTP Server 22, 316, 320
IBM Java Toolkit 22
IBM Key Management 316, 328
IBM SecureWay Firewall 25
IBM WebSphere Everyplace Access v5.0 1
IBM WebSphere Studio 19
Instant messaging 375
Adding users 379
alert preferences 376
chat session 379
components 375
Everyplace Client 377
Lotus Domino Server 376
Lotus Sametime Mobile Extension 376
overview 376
Palm OS 383
Pocket PC 377
Sametime Client 375–376
Sametime Mobile Protocol Stack 376
Sametime Mobile Server 376
STMobile 376
Windows Mobile 377
Intelligent Notification Services 9, 20–21
delivery channels 10
framework 11
Notification Manager 10

Simple notifications 9
subscriber's preferences 10
subscription 10
Subscription Manager 10
Subscription-based notifications 10
Internet 42
intranet 42
Inventory collection 13

J

J2EE 6, 19, 22, 67
Java 3, 22
Java APIs 11
JavaScript 22
JDBC 5, 9, 21
JSP 22

L

Labels 53
Layout 59
LDAP 39
LDAP server 23
Location Aware Services 11–12, 20–21
Device position 12
Directory 12
Lotus Domino 127
Lotus Domino server 7–8
Adapter 8
Address Book 8
Calendar 8
e-mail 8
Journals 8
To Do 8
Lotus Notes 103
PIM and e-mail portlets 29

M

Managing Users and Groups 48
Mapping 12
Mapping Contexts 81
messaging 375
Messaging Services
Sametime 6
Microsoft Exchange server 7–8
Adapter 8
Calendar 8
Contacts 8
credential slot 33
e-mail 8
Notes 8
PIM and e-mail portlets 33
Tasks 8
Mobile Application Builder 19, 22
Mobile computing 3

O

Offline Portal 13
Offline Portal Content 328

P

Pages 81
Palm device 376
Palm OS 17, 288
Personal Information Management 7
PIM 2, 5, 7–8, 14, 28
Pocket PC 376
Pocket PC 2002 16, 288, 345
Portal 42
Portal Container 6
Portal technology 6, 25
Portlet Applications 81
Portlets 6
portlets 6–7, 19, 67, 81
Activate 71
Add 60
Appearance 61
container 62–63
Copy 71
Deactivate 71
Delete 60
Edit 60
layout 63
Locks 62
Modify parameters 71
Move 60
Search 70
Show info 71
PPP connection 342
Preparation 237

R

Redbooks Web site 433
Contact us xiv
Resource Checker 17, 387

ActiveSync 388
Data Storage Profile 392, 394
Database Sync Client 389
device resources 389
e-mail 389
Everyplace Client 389
installation 388
Mobile Sametime 389
Mobility Client 389
PIM 389
Software Update 390
Windows Mobile 2003 388
Resource Permissions 74
Reverse geocoding 12
Roles 82
Administrator 50, 83
Delegator 83
Editor 50, 83
Manager 50, 83
Privileged user 51, 83
Security Administrator 83
User 83
Routing 12

S

Sametime 421
configuration 422, 424
Installation 422
Lotus Domino Server 422
Sametime Everyplace 425
Domino server 426
Microbrowser 426
Mobile Extensions 427
setting up 425
Secure Sockets Layer 315–316, 321
configure WEA files 326
Everyplace Client 315, 331
IBM HTTP Server 316
key database 316
mobile devices 315
Offline Portal Content 328
Palm devices 333
Pocket PC devices 331
self-signed key file 318
WebSphere Application Server 321
Server Initiated Actions 12
administrative portlet 12
delivery channel 12
Servlet Container 6
servlets 6, 22
Skins 64
skins 5, 43
Add 66
default skin 66
Delete 66
Software distribution 13
SSL 315–316, 326, 331, 365
STEP 425
Subscription Manager 342
Symbian OS 17, 288
SyncML 8–9, 15

T

TCP/IP 342
Themes 5, 42, 64
default theme 66
Delete 66
Edit 66
Tivoli Configuration Manager 13
Tivoli Device Manager 340
Transcoding plug-ins 14
Transcoding Technology 13–14
Fragmentation 14
Web Clipping 14

U

User Groups 81
Users
Creating users 74
Editing user 77

V

Virtual Resources 82

W

WAP 24
WAR 67–68
WEA InfoCenter 21
Web applications 19
Web ARchives 67
Web Clipping 7, 14, 72
Web content 2, 5
Web Modules 81
Web services 19, 22
WebSphere Application Server 2–4, 6, 20, 22, 321,

328
WebSphere Edge Server 2, 25
WebSphere Everyplace Access 1–2, 4, 19–21, 48, 91, 316, 326, 340
Administration 5
Administration navigation 46
Application Development Components 22
authentication 6
Basic Install 100
Basic Portal services 5
Client components 21
Desktop Web browser 23
Device Services 6
Enterprise Resources 2
Everyplace Access 2–3
Everyplace Client 4
Everyplace Toolkit 4
Featured components 21
Handheld device browser 23
Intelligent Notification Services 6
Load Balancing 2
Location Aware Services 6
Lotus Domino 23
Messaging Services 6
Microsoft Exchange 23
Mobile Application Builder 4
Mobile client devices 2
Network 2
Operating systems 23
Page Aggregation 4
Portlet Container & Services 4
Server components 21
Support components 22
synchronization 7
Third-party components 23
Transcoding 5
WebSphere Studio Application Developer 4
WebSphere Studio Device Developer 4
WebSphere Studio Site Developer 4
WebSphere Everyplace Client 287
Configuration on Palm OS 296
Configuration on Pocket PC 309
Installation for Palm OS 290
Installation for Pocket PC 303
Palm Simulator 295
supported devices 288
WebSphere Everyplace Connection Manager 24
WebSphere Micro Environment 19
WebSphere MQ Everyplace 24
WebSphere Portal 3–4, 6, 9, 20, 22, 25, 42, 44, 48, 69, 81, 91, 93
Administration Portal 64
Portal Administration 46, 74
Portal User Interface 64
resources 81
WebSphere Studio 19
WebSphere Studio Device Developer 19, 22
WebSphere Studio Site Developer 22
Windows Mobile 2003 16, 288
WML 28

X

XHTML 20
XML 3, 5, 8, 14, 22, 345
XML applications 19
XSL 14

(0.5" spine)
0.475"<->0.875"
250 <-> 459 pages

IBM WebSphere Everyplace Access V5 Handbook for Developers and Administrators

Volume I: Installation and Administration

Extend your e-business applications to PDAs, phones, and other device types

Install WebSphere Everyplace Access on AIX and Windows

Deploy online portlet applications for PDAs

This IBM Redbook is part of a series of four volumes related to WebSphere® Everyplace® Access V5.0. These Redbooks will help you plan, install, administer, and develop mobile applications to run in a WebSphere® Everyplace® Access V5.0 environment. The information provided in these Redbooks target business-to-employee (B2E) enterprise applications, but most of the scenarios presented will apply to business-to-consumer (B2C) applications as well. In these Redbooks, you will find step-by-step examples and scenarios showing ways to integrate your enterprise applications into a WebSphere Everyplace Access environment using the WebSphere Studio Site Developer and the Everyplace Toolkit, as well as extending your online and offline application capabilities to use other advanced functions.

In this redbook, you will also find step-by-step sample installation and administration procedures to help you get online and access your enterprise applications from PDAs, such as Pocket PCs and Palm devices. The redbook includes topics such as product installation, administration, instant messaging implementation, device management, and how to establish secure connections.

A basic knowledge of Java technologies, such as servlets, JavaBeans, EJBs, JavaServer Pages (JSPs), as well as XML applications and the terminology used in Web publishing, is assumed.

INTERNATIONAL TECHNICAL SUPPORT ORGANIZATION

BUILDING TECHNICAL INFORMATION BASED ON PRACTICAL EXPERIENCE

IBM Redbooks are developed by the IBM International Technical Support Organization. Experts from IBM, Customers and Partners from around the world create timely technical information based on realistic scenarios. Specific recommendations are provided to help you implement IT solutions more effectively in your environment.

For more information:
ibm.com/redbooks

SG24-6462-00 ISBN 0738490733